МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

ТРУДЫ

IX МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

«ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва и Подмосковье

20–22 мая 2015 г.

МОСКВА

2015

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

ТРУДЫ

IX МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

«ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва и Подмосковье

20–22 мая 2015 г.

МАКС ПРЕСС

МОСКВА – 2015

УДК 510.5+519.71
ББК 22.12:22.18
Д48

Отв. ред. *В.Б. Алексеев, Д.С. Романов, Б.Р. Данилов*

Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г.: Труды / Отв. ред. В.Б. Алексеев, Д.С. Романов, Б.Р. Данилов. – М.: МАКС Пресс, 2015. – 284 с.
ISBN 978-5-317-04970-6

В сборнике представлены труды девятой международной конференции «Дискретные модели в теории управляющих систем», проводимой Московским государственным университетом имени М. В. Ломоносова и посвященной 90-летию со дня рождения члена-корреспондента РАН Сергея Всеволодовича Яблонского. Тематика конференции включает следующие направления: дискретные функциональные системы, свойства дискретных функций, синтез и сложность управляющих систем, надежность, контроль и диагностика управляющих систем, автоматы, теория графов, комбинаторика, теория кодирования, математические методы защиты информации, теория распознавания образов, математическая теория интеллектуальных систем, прикладная математическая логика. Конференция организована при поддержке Российского фонда фундаментальных исследований (проект № 15-01-20193-г).

Ключевые слова: дискретные функциональные системы, дискретные функции, синтез и сложность управляющих систем, надежность управляющих систем, контроль и диагностика управляющих систем, автоматы, теория графов, комбинаторика, теория кодирования, математические методы защиты информации, распознавание образов, интеллектуальные системы, прикладная математическая логика.

УДК 510.5+519.71
ББК 22.12:22.18

Discrete Models in Control Systems Theory: IX International Conference, Moscow and Moscow region, 20–22 May, 2015: Proceedings / M.E.: V. B. Alekseev, D. S. Romanov, B. R. Danilov. — M.: MAKS Press, 2015. – 284 p.

The collection represents proceedings of the nineth international conference “Discrete Models in Control Systems Theory” that is held by Lomonosov Moscow State University and is dedicated to the 90th anniversary of Sergey Vsevolodovich Yablonsky’s birth. The conference subject area includes: discrete functional systems; discrete functions properties; control systems synthesis, complexity, reliability, and diagnostics; automata; graph theory; combinatorics; coding theory; mathematical methods of information security; theory of pattern recognition; mathematical theory of intelligence systems; applied mathematical logic. The conference is sponsored by Russian Foundation for Basic Research (project N 15-01-20193-г).

Keywords: discrete functional systems, discrete functions properties, control systems synthesis and complexity, control systems reliability and diagnostics, automata, graph theory, combinatorics, coding theory, mathematical methods of information security, pattern recognition, intelligence systems, applied mathematical logic.

Напечатано с готового оригинал-макета

Подписано в печать 12.05.2015 г.
Формат 60x90 1/16. Усл.печ.л. 17,75. Тираж 140 экз. Заказ 093.
Издательство ООО “МАКС Пресс”. Лицензия ИД N 00510 от 01.12.99 г.
119992, ГСП-2, Москва, Ленинские горы, МГУ им. М.В. Ломоносова,
2-й учебный корпус, 527 к. Тел. 8(495)939-3890/91. Тел./Факс 8(495)939-3891.

ISBN 978-5-317-04970-6

Член-корр. РАН Сергей Всеволодович Яблонский
(06.12.1924 – 26.05.1998)

Сергей Всеволодович Яблонский (06.12.1924 — 26.05.1998)

Цикл конференций «Дискретные модели в теории управляющих систем» был заложен Сергеем Всеволодовичем Яблóнским, выдающимся российским учёным, одним из основателей отечественной школы математической кибернетики и дискретной математики. Данная конференция посвящена 90-летию со дня его рождения.

С. В. Яблонский родился 6 декабря 1924 года в Москве в семье профессора механики. Его математическое дарование проявилось еще в школе, и в 1940 г. он стал победителем 6-й Московской математической олимпиады школьников. Окончив школу, он поступил в Московский университет на механико-математический факультет. Но это был 1941 год, и война надолго оторвала С. В. Яблонского от учёбы. Осенью 1942 года после окончания первого курса он 18-летним юношей ушёл на фронт и в составе 242-го танкового полка прошёл трудный боевой путь по дорогам Великой Отечественной войны. О доблести и самоотверженности Сергея Всеволодовича говорят его боевые награды — два ордена Отечественной войны, два ордена Красной Звезды, орден Славы 3-й степени, боевые медали.

К занятиям любимой наукой Сергей Всеволодович смог вернуться лишь в победном 1945 году. Возвратившись в МГУ, он активно включился в учёбу и в 1950 г. с отличием окончил механико-математический факультет МГУ. Научные исследования в студенческие годы он вел под руководством Нины Карловны Бари, и в 1950 г. опубликовал первую свою научную работу «О сходящихся последовательностях непрерывных функций» в «Вестнике Московского университета».

В 1950 г. Сергей Всеволодович поступил в аспирантуру механико-математического факультета МГУ, где его научным руководителем был Пётр Сергеевич Новиков, оказавший большое влияние на формирование научных интересов Сергея Всеволодовича. Тематикой исследований Сергея Всеволодовича стали вопросы выразимости в математической логике. Его исследования показали, что эти вопросы, порождённые математической логикой, находят более адекватное описание и решение в теории дискретных многозначных функций. Разработка этой теории и решение ряда конкретных задач в ней (в частности, окончательное решение проблемы полноты в 3-значной логике) составили основу кандидатской диссертации С. В. Яблонского «Вопросы функциональной полноты в k-значном исчислении», защищённой им в 1953 г.

С 1953 года Сергей Всеволодович начал работать в Отделении прикладной математики Математического института им. В. А. Стеклова, которое позднее было преобразовано в Институт прикладной математики. Он продолжил исследования в области дискретных многозначных функций и в 1958 г. в «Трудах Математического института им. В. А. Стеклова» (т. 51) опубликовал большую обзорную статью «Функциональные построения в k-значной логике», в которой удачно систематизировал накопленные к тому времени результаты в

этой области. Эта статья сыграла огромную роль в становлении дискретной математики и математической кибернетики, и на протяжении многих лет была основным учебным пособием по теории дискретных функций для многих исследователей.

В это же время Сергей Всеволодович активно включился в исследование проблем, связанных с синтезом логических устройств. Среди работ этого периода важное место занимают его работы (совместно с И. А. Чегис) о тестировании электрических схем. Их работа «Логические способы контроля работы электрических схем», опубликованная в 1958 г. в том же 51-м томе «Трудов МИАН им. В. А. Стеклова», представляла новый взгляд на проблемы построения тестов и дала толчок развитию комбинаторно-логических методов как в теории надёжности схем, так и в распознавании образов.

Изучая логические вопросы в теории схем, Сергей Всеволодович непосредственно сталкивался и с новым математическим термином «кибернетика», вокруг которого шли философские и идеологические споры. Глубоко понимая важность математических проблем, связанных с кибернетикой, Сергей Всеволодович сразу же активно встал на её защиту. Большое влияние в этом оказал на него Алексей Андреевич Ляпунов, вместе с которым они в 50-х и 60-х годах проводили знаменитый семинар по кибернетике. Сергей Всеволодович принял активное участие в организации периодического сборника «Проблемы кибернетики», издание которого началось в 1958 г. А. А. Ляпуновым. Сергей Всеволодович осознавал важность выделения в кибернетике чисто математических вопросов и отделение их от философии и идеологии. Итогом его анализа явилась опубликованная в 1959 г. в сборнике «Проблемы кибернетики» статья «Основные понятия кибернетики», в которой выделено и математически формализовано понятие управляющей системы, указаны проблемы и направления развития теории управляющих систем. Разъяснению и пропаганде идей кибернетики Сергей Всеволодович уделял большое внимание, о чём говорят его доклады, представленные на 3-м (в 1956 г. с соавторами) и 4-м Всесоюзных математических съездах, на Международном конгрессе по обработке информации ИФИП-68, на других конференциях, а также его публикации по теоретическим и прикладным проблемам кибернетики: статья в «Морском сборнике» (1960 г., с А. И. Бергом и А. А. Ляпуновым), ротапринт Института мировой экономики и международных отношений (1961 г., с А. А. Ляпуновым), статья в сборнике «Проблемы кибернетики» (1963 г., с А. А. Ляпуновым).

С 1958 г. Сергей Всеволодович возглавил отдел математической кибернетики в Институте прикладной математики, созданный им совместно с А. А. Ляпуновым. В этот период Сергей Всеволодович проводит исследования, связанные с проблемами сложности алгоритмов для минимизации схем. Полученные им в этом направлении важные результаты, объясняющие трудности в построении минимальных схем, вошли в его докторскую диссертацию «О некоторых математических вопросах теории управляющих систем», которую он успешно защитил в 1962 г. В 1966 г. С. В. Яблонский (совместно с Ю. И. Журавлёвым и О. Б. Лупановым) был удостоен Ленинской премии за цикл работ по теории

управляющих систем. В 1968 г. он был избран членом-корреспондентом АН СССР по отделению математики, в работе которого он принял самое активное участие, ряд лет являясь заместителем академика-секретаря и членом бюро отделения математики. Он был одним из основателей и действительным членом Академии криптографии, в которой он также активно работал.

Сергей Всеволодович всегда понимал важность дискретных методов в теории управляющих систем и необходимость развития различных направлений дискретной математики как основы для построения и анализа дискретных моделей в различных приложениях.

Он внёс огромный вклад в координацию и развитие научных исследований в области математической кибернетики и дискретной математики, глубоко понимая необходимость обмена информацией о новых научных результатах и поддержки исследований в данных направлениях. Большую роль в этом сыграл его «пятничный» семинар по математическим вопросам кибернетики в МГУ, которым он руководил более 30 лет. На этом семинаре обсуждались новые наиболее интересные результаты в области математической кибернетики и дискретной математики, с которыми выступали математики не только Москвы, но и других городов и даже других стран. Сам факт выступления на этом семинаре уже являлся высокой оценкой полученных результатов.

Сергей Всеволодович принимал активное участие в организации и проведении первых Всесоюзных конференций по проблемам теоретической кибернетики, а затем в течение многих лет был бессменным председателем оргкомитета этих конференций. Он активно способствовал становлению и росту научных коллективов в Нижнем Новгороде, Новосибирске, Казани, Саратове, Иркутске, других городах. Большую роль в популяризации теории дискретных функций сыграла изданная С. В. Яблонским в 1966 г. совместно с его учениками Г. П. Гавриловым и В. Б. Кудрявцевым книга «Функции алгебры логики и классы Поста».

С 1974 г. Сергей Всеволодович стал главным редактором сборников «Проблемы кибернетики» (с 1989 г. они выходят под названием «Математические вопросы кибернетики»). Он принял активное участие в работе над «Математической энциклопедией», где разрабатывал и редактировал раздел, посвященный дискретной математике и математической кибернетике. Совместно с О. Б. Лупановым подготовил к изданию широко известный среди специалистов сборник статей «Дискретная математика и математические вопросы кибернетики».

Огромен вклад Сергея Всеволодовича в подготовку кадров в области математической кибернетики и дискретной математики. Параллельно с работой в ИПМ Сергей Всеволодович с 1954 г. вёл преподавание на механико-математическом факультете МГУ. Здесь он разрабатывал и оттачивал спецкурсы «Введение в дискретную математику» и «Основы кибернетики». С 1963 г. он — профессор МГУ. Сергей Всеволодович принял активное участие в организации в МГУ в 1970 году факультета вычислительной математики и кибернетики, где с 1971 года создал и возглавил кафедру теории автоматов и математической логики, которая вскоре была переименована в кафедру математической киберне-

тики. Эта кафедра, которой бессменно руководил С. В. Яблонский, подготовила несколько сотен специалистов в области математической кибернетики и дискретной математики. На факультете ВМК Сергей Всеволодович начал чтение курсов «Введение в дискретную математику» и «Основы кибернетики» уже как обязательных курсов для студентов. Разработанная им программа этих курсов легла позднее в основу составленной им программы курса «Дискретная математика», принятой для университетов всей страны, что оказало огромное влияние на ознакомление с основами дискретной математики студентов-математиков всего Советского Союза. Сергей Всеволодович организовывал Всесоюзные методические совещания по проблемам преподавания дискретной математики. До сих пор основным учебником по дискретной математике в нашей стране и некоторых других странах является изданный в 1979 и переиздававшийся много раз учебник С. В. Яблонского «Введение в дискретную математику».

Активное участие принял Сергей Всеволодович в организации Международного математического центра им. С. Банаха. Он долгое время был членом совета этого центра и организовывал проведение в центре семестров по дискретной математике.

За большие заслуги в области научно-организационной деятельности Сергей Всеволодович был награждён орденом Трудового Красного знамени.

Сергей Всеволодович много работал со студентами и аспирантами, ставя перед ними задачи достаточно широкого спектра. Под его руководством выполнено и защищено более 25 кандидатских диссертаций, среди его учеников доктора наук, члены научных академий. Уже несколько поколений учеников и последователей Сергея Всеволодовича образуют созданную им мощную научную школу, объединяющую исследователей не только нашей страны, но и некоторых других стран.

Алексеев В. Б.

О построении квантовых хеш-функций

Аблаев Марат Фаридович

Казанский федеральный университет, e-mail: mablayev_mf@gmail.com

Данная работа продолжает исследования, результаты которых представлены в [1, 2, 3]. Построение квантовых хеш-функций является новой областью квантовой информатики усиливающей направление, названное “post-quantum cryptography”. Это направление занимается выработкой методов борьбы с возможностями потенциальных квантовых вычислителей, реализующих квантовые алгоритма Шора факторизации.

Следующая система понятий, обозначений и боле формализованные формулировки результатов приводится в работах [1, 2, 3].

- Через $(\mathcal{H}^2)^{\otimes s}$ обозначают 2^s-мерное Гильбертово пространство — пространство состояний квантовой системы, образованной из s кубитов.
- Пусть $\mathbb{X}$ — конечное множество. Функция $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ называется $(K; s)$ классически-квантовой односторонней функцией, если ψ эффективно вычисляется и является необратимой.
- Если $\log K > s$, то $(K; s)$ классически-квантовая функция ψ является односторонней.
- Функция $\psi : w \mapsto |\psi(w)\rangle$ называется δ-устойчивой (resistant), если для каждой пары w, w' различных элементов из $\mathbb{X}$ выполняется

$$|\langle\psi(w)|\psi(w')\rangle| \leq \delta.$$

- Если функция $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ δ-устойчива. то

$$s \geq \log\log|\mathbb{X}| - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

- Пусть $K = |\mathbb{X}|$, $s \geq 1$. Одностороннюю δ-устойчивую функцию $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ называют δ-устойчивой $(K; s)$-квантовой хеш-функцией (δ-R $(K; s)$-квантовой хеш-функцией).

В работах [1, 2, 3] рассматривается конструкция (квантовый хеш генератор), позволяющая строить квантовые хеш-функции. Предложенные конструкции применяются для квантовых систем с вещественными амплитудами (в процессе построения конкретных квантовых хеш-функций происходит модификация вещественных амплитуд квантовой системы).

Основной результат. В данной работе предлагаются конструкции построения квантовых хеш-функций, изменяющие комплексную фазу квантовой системы. Это позволяет

- сэкономить один кубит в ранее рассмотренных конструкциях и
- упростить часть математических выкладок.

Примеры конкретных конструкций в терминах преобразовании фазы. Пусть $\mathbb{Z}_q$ — группа, а $B \subset \mathbb{Z}_q$ — специальное (см. [2]) подмножество. Квантовая хеш-функция $\psi_{q,B} : \{0,1\}^{\log q} \to (\mathcal{H}^2)^{\otimes(\log|B|+1)}$ из [2] теперь экономнее на один кубит: $\psi_{q,B} : \{0,1\}^{\log q} \to (\mathcal{H}^2)^{\otimes \log|B|}$ и имеет вид

$$|\psi_{q,B}(a)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} e^{i\frac{2\pi}{q}ab_j}|j\rangle.$$

Конструкция квантовой хеш-функции на основе техники отпечатков Фрейвалда (Freivalds fingerprinting technique) [3] выглядит в "фазовой терминологии" следующим образом:

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{|F_M|}} \sum_{l=1}^{|F_M|} |l\rangle \otimes \left(\frac{1}{\sqrt{T}} \sum_{j=1}^{T} e^{i\frac{2\pi}{q}h_j(f_l(w))}|j\rangle \right).$$

Значения величин, входящих в формулу, разъясняются в работе [3].

Работа выполнена при поддержке РФФИ.

Список литературы

[1] Аблаев Ф. М., Аблаев Ф. М. Квантовое хеширование на основе классических ϵ-универсальных хеш-семейств // Материалы VII международной конференции «Проблемы теоретической кибернетики». — Казань: Отечество, 2014. — С. 14–15.

[2] Аблаев Ф. М., Аблаев М. Ф., Васильев А. В. Универсальное квантовое хеширование // Ученые записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, кн. 3. — С. 7–18.

[3] Ablayev F., Ablayev M. Quantum Hashing via Classical ϵ-universal Hashing Constructions // arXiv:1404.1503v2 [quant-ph], 2015.

О билинейной сложности умножения матриц размеров $k \times 2$ и 2×2

Алексеев Валерий Борисович

Московский государственный университет имени М. В. Ломоносова, e-mail: vbalekseev@rambler.ru

Одной из трудных задач в теории сложности вычислений оказалась задача о минимальной сложности умножения матриц. Уже более 25 лет не удается существенно понизить асимптотическую оценку $O\left(n^{2.38}\right)$ для числа арифметических операций в алгоритмах умножения двух матриц порядка n, полученную в [1]. Чтобы лучше понять возникающие здесь трудности, исследуются аналогичные вопросы в других алгебрах, а также частные случаи задачи умножения матриц. Одним из направлений является получение точных оценок сложности умножения матриц конкретных размеров. Наиболее часто исследуется билинейная сложность этой задачи. В билинейных алгоритмах можно умножать не

только элементы исходных матриц, но и их линейные комбинации, но только линейные комбинации элементов первой матрицы на линейные комбинации элементов второй матрицы. Такое ограничение позволяет не предполагать коммутативности элементов матриц, что существенно, если эта конструкция используется рекурсивно и элементы матриц сами являются подматрицами (как в [2]). Число умножений линейных комбинаций в билинейном алгоритме называется билинейной сложностью алгоритма (сложения и умножения на константу не учитываются), а минимальную билинейную сложность алгоритмов, решающих данную задачу, называют билинейной сложностью задачи.

Обозначим через $< m, n, p >_F$ задачу умножения матрицы размера $m \times n$ на матрицу размера $n \times p$ над некоторым полем F. Через $rk_F < m, n, p >$ обозначим билинейную сложность этой задачи. Теорема о двойственности [3] утверждает, что $rk_F < m, n, p >$ не изменяется при любой перестановке чисел m, n, p. Обычный алгоритм умножения матриц (строка на столбец) является билинейным и его билинейная сложность равна mnp.

Можно показать, что

$$rk_F < m_1 m_2, n_1 n_2, p_1 p_2 > \quad \leq \quad rk_F < m_1, n_1, p_1 > \cdot \quad rk_F < m_2, n_2, p_2 >$$

(см., например, [4]). Поэтому верхнюю оценку для больших параметров можно понижать, понижая ее для малых параметров. А для малых параметров можно понижать верхнюю оценку, просто находя конкретные билинейные алгоритмы. Именно так показано, что $rk_F < 2, 2, 2 > \quad \leq 7$ [2], $rk_F < 3, 3, 3 > \quad \leq 23$ [5], $rk_F < 5, 5, 5 > \quad \leq 100$ [6], $rk_F < m, 2, p > \quad \leq \lceil \frac{3mp + \max(m,p)}{2} \rceil$ [7]. Таблицу имеющихся верхних оценок для $rk_F < m, n, p >$ при малых значениях параметров можно найти в [8].

Для умножения двух квадратных матриц порядка n только при $n = 2$ известно точное значение $rk_F < 2, 2, 2 >= 7$ над любым полем F [9], но уже для $n = 3$ известно только, что $19 \leq \quad rk_F < 3, 3, 3 > \quad \leq 23$ [10].

В данной работе мы рассматриваем $rk_F < m, 2, 2 >$. Из [7] следует, что $rk_F < m, 2, 2 > \quad \leq \lceil \frac{7}{2} m \rceil$ над любым полем. В [11] получена общая нижняя оценка, из которой, в частности, следует, что $rk_F < m, 2, 2 > \quad \geq 3m + 1$ над любым полем. В работах [12], [13], [14] установлены точные значения $rk_F < 3, 2, 2 >= 11$, $rk_F < 4, 2, 2 >= 14$ и оценки $17 \leq \quad rk_F < 5, 2, 2 > \quad \leq 18$ для любого поля F. Здесь мы получаем общую нижнюю оценку, усиливающую оценку из [11].

Теорема. *Любой билинейный алгоритм для умножения матрицы размера* $m \times 2$ *на матрицу размера* 2×2 *над произвольным полем имеет билинейную сложность не менее* $3m + 2$. *Тот же результат справедлив для умножения матрицы размера* $2 \times m$ *на матрицу размера* $m \times 2$ *и для умножения матрицы размера* 2×2 *на матрицу размера* $2 \times m$.

Нетрудно видеть, что приведенные выше нижние оценки для $m = 3, 4, 5$ являются частными случаями этой теоремы. И действительно, доказательство теоремы является обобщением метода, использованного при получении этих

результатов, на общий случай. С учетом результата из [11], приведенного выше, достаточно доказать, что над любым полем не существует билинейного алгоритма для умножения матрицы размера $m \times 2$ на матрицу размера 2×2 с билинейной сложностью $3m + 1$. Удается показать, что доказательство отсутствия билинейного алгоритма с билинейной сложностью 16 для умножения матрицы размера 5×2 на матрицу размера 2×2, приведенное в [14], обобщается на произвольные m.

Работа выполнена при поддержке РФФИ (проект № 13-01-00183-а).

Список литературы

[1] Coppersmith D., Winograd S. Matrix Multiplication via Arithmetic Progressions // J. Symbolic Computation. — 1990. — V. 9, № 3. — P. 251–280.

[2] Strassen V. Gaussian elimination is not optimal // Numer. Math. — 1969. — V. 13. — P. 354–356. [Имеется перевод: Штрассен В. Алгоритм Гаусса не оптимален // Кибернетический сборник. — Вып. 7. — М.: Мир, 1970. — С. 67–70].

[3] Hopcroft J. E., Musinski J. Duality applied to the complexity of matrix multiplication and other bilinear forms // SIAM J. Comput. — 1973. — V. 2, N 3. — P. 159–173.

[4] Алексеев В. Б. Сложность умножения матриц. Обзор // Кибернетический сборник. Новая серия. — Вып. 25. — М.: Мир, 1988. — С. 189–236.

[5] Laderman J. D. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications // Bull. Amer. Math. Soc. — 1976. — V. 82, N 1. — P. 126–128.

[6] Макаров О. М. Некоммутативный алгоритм умножения квадратных матриц пятого порядка, использующий сто умножений // Журн. выч. матем. и матем. физики. — 1987. — Т. 27, № 2. — С. 311–315.

[7] Hopcroft J. E., Kerr L. R. On minimizing the number of multiplications necessary for matrix multiplication // SIAM J. Appl. Math. — 1971. — V. 20, № 1. — P. 127–148.

[8] Смирнов А. В. О билинейной сложности и практических алгоритмах умножения матриц // Журн. выч. матем. и матем. физики. — 2013. — Т. 53, № 12. — С. 1970–1984.

[9] Winograd S. On multiplication of 2×2 matrices // Linear Algebra and Appl. — 1971. — V. 4. — P. 381–388.

[10] Bläser M. On the complexity of the multiplication of matrices of small formats // J. Complexity. — 2003. — V. 19. — P. 43–60.

[11] Bläser M. Lower bounds for the multiplicative complexity of matrix multiplication // Comput. Complexity. — 1999. — V. 8. — P. 203–226.

[12] Alekseyev V. B. On the complexity of some algorithms of matrix multiplication // Journal of Algorithms. — 1985. — V. 6, № 1. — P. 71–85.

[13] Алексеев В. Б., Смирнов А. В. О точной и приближенной билинейных сложностях умножения матриц размеров 4×2 и 2×2 // Современные проблемы математики. — 2013. — Вып. 17. — С. 135–152.

[14] Алексеев В. Б. О билинейной сложности умножения матриц размеров 5×2 и 2×2 // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. — 2014. — Т. 156, кн. 3. — С. 19–29.

Обобщение одного метода восстановления ключа фильтрующего генератора

Алексеев Евгений Константинович[1], **Кущинская Людмила Александровна**[2]

[1] ООО «КРИПТО-ПРО», e-mail: geni-cmc@mail.ru

[2] Московский государственный университет имени М. В. Ломоносова, e-mail: lyudmila.kuschinskaja@yandex.ru

Одним из способов, часто используемых при криптографическом анализе, является аппроксимация булевых функций(отображений). Яркими примерами служат корреляционный [1] и линейный [2] методы криптоанализа, в которых в качестве аппроксимирующей функции выступают аффинные(линейные) функции. В работе [3] рассмотрен случай аппроксимации функции усложнения фильтрующего генератора с помощью алгебраически вырожденной функции. В работе показано, что данный метод оказывается неприменим в случае, когда длина ключа фильтрующего генератора является простым числом.

Постановка задачи

Рассмотрим потоковый шифр, построенный на основе линейного отображения $A : V_n \to V_n$ и булевой функции $f \in F_n$. Результатом зашифрования открытого текста $x = x_0, \ldots, x_n, \ldots$ на ключе $u^* \in V_n$ является шифртекст $c = c_0, \ldots, c_n, \ldots$, где $c_i = x_i \oplus z_i$, $i \geq 0$ и $z_i = f(A^i u^*)$ — бит, полученный на выходе фильтрующего генератора на i-м такте работы. Рассматривается следующая задача: известно N последовательных бит шифртекста $c_0, c_1, \ldots, c_{N-1}$, полученных при зашифровании известного открытого текста $x_0, x_1, \ldots, x_{N-1}$ на неизвестном ключе $u^* \in V_n$. Требуется найти ключ u^*. Учитывая схему построения рассматриваемого шифра, исходная криптографическая задача сводится к задаче решения системы алгебраических уравнений вида

$$z_i = f(A^i u^*), \quad i = \overline{0, N-1}.$$

В работе [3] был предложен метод решения данной криптографической задачи для случая, когда $n = k \cdot s$ — составное число. Метод основан на возможности построения такого подпространства $L < V_n$ размерности k, что $A^t L = L$, где $t = \frac{2^n-1}{2^k-1}$. В случае, когда n есть простое число, данный метод аналогичен полному перебору всех возможных ключей из V_n.

Пусть нам известны следующие величины: m, $\hat{P} = \{p_i | p_i \in \left(\frac{1}{2}; 1\right]\}$, $\hat{T} = \{t_i | t_i \in \mathbb{Z},\ t_1 = 0\}$, $\hat{L} = \{L_i - \text{плоскость в } V_n\}$, $\hat{C} = \{c_i | c_i \in \{0, 1\}\}$, $i = \overline{1, m}$ такие, что:

- с вероятностью p_1 функция усложнения f совпадает с константой c_1 на плоскости $A^{t_1}(L_1) = L_1$, т. е. $Pr\left[f(v) = c_1 | v \in L_1\right] = p_1 > 1/2$;
- L_1 под действием оператора $A^{t_2 - t_1}$ переходит в плоскость L_2 (которая, возможно, является смежным классом уже по другому подпространству), на которой функция f с вероятностью p_2 совпадает с константой c_2, т. е. $Pr\left[f(v) = c_2 | v \in L_2\right] = p_2 > 1/2$;
- и так далее до некоторого m.

Составим вектор $w = (c_1 \oplus \widetilde{z}_1, \ldots, c_m \oplus \widetilde{z}_m)$, $\widetilde{z}_i = z_{t_i}$, $i = \overline{1, m}$. На основе вектора w будем принимать решение относительно возможного расположения ключа в плоскости L_1. Пусть нам удалось построить несколько, а именно s, рассмотренных ранее конструкций. Таким образом, нам известно s; $\mathbb{M} = \{m_i\}$, где $m_i \in \mathbb{N}$; $\mathbb{P} = \{p_j^{(i)}\}$, где $p_j^{(i)} \in \left(\frac{1}{2}; 1\right]$; $\mathbb{L} = \{L_j^{(i)}\}$, где $L_j^{(i)}$ – плоскость в V_n; $\mathbb{C} = \{c_j^{(i)}\}$, где $c_j^{(i)} \in \{0, 1\}$; $\mathbb{T} = \{t_j^{(i)}\}$, где $t_j^{(i)} \in \mathbb{Z}$; $i = \overline{1, s}; j = \overline{1, m_i}$.

Обозначим множество смежных классов $\{L_1^{(i)} | i = \overline{1, s}\}$ через L_{start}. Пусть имеется некоторое решающее правило вида $F(L_j) \geq 0$, в соответствии с которым принимается или отвергается смежный класс $L_j \in L_{start}$, а $\alpha_j, \beta_j -$ вероятности ошибок первого и второго рода для класса $L_1^{(j)} \in L_{start}$.

Пусть $L^* = L_{start}$, $M = V_n \setminus \bigcup_{L \in L_{start}} L$.

Описание алгоритма

1. Первый этап. $\widetilde{L} := \emptyset$.
   - 1.а) Если $L^* = \emptyset$, то переходим ко второму этапу. Иначе выбираем произвольный элемент L_i из множества L^*; $L^* := L^* \setminus \{L_i\}$.
   - 1.б) Зафиксируем параметры, соответствующие данному смежному классу L_i. Построим вектор $w \in V_{m_i}$ как это было показано выше. Если выполнено неравенство $F(L_i) \geq 0$, то положим $\widetilde{L} = \widetilde{L} \cup \{L_i\}$. Переходим к пункту 1.а).
2. Второй этап.
   - 2.а) Если $\widetilde{L} = \emptyset$, то положим $S := M$ и переходим к пункту 2.г), иначе выбираем Y из множества $\widetilde{L}$; $\widetilde{L} := \widetilde{L} \setminus \{Y\}$.
   - 2.б) Если $Y = \emptyset$, то переходим к пункту 2.а). Иначе выбираем $v \in Y$; $Y := Y \setminus \{v\}$.
   - 2.в) Если $f(A^i v) = z_i$ для любого $i = \overline{0, N-1}$, то выдаем v в качестве ответа и останавливаемся, иначе переходим к пункту 2.б).
   - 2.г) Если $S = \emptyset$, то заканчиваем работу без результата, иначе выбираем $u \in S$; $S := S \setminus \{u\}$.

2.д) Если $f(A^i u) = z_i$ для любого $i = \overline{0, N-1}$, то выдаем u в качетсве ответа и останавливаемся, иначе переходим к пункту 2.г).

Надежность

Будем считать, что ключ распределен равномерно по пространтсву ключей V_n: $Pr\left[u^* = v\right] = \frac{1}{2^n},\ \forall v \in V_n$. Тогда вероятность δ_i того, что ключ окажется в множестве $L_1^{(i)}$: $\delta_i = Pr\left[u^* \in L_1^{(i)}\right] = \frac{|L_1^{(i)}|}{2^n},\ \forall L_1^{(i)} \in L_{start}$.

Надежность метода π может быть оценена следующим образом:

$$\pi \geq \frac{|M|}{2^n} + \sum_{j=1}^{s}(1-\beta_j)\cdot\delta_j \geq 1 - \sum_{j=1}^{s}\beta_j\delta_j.$$

Неравенство объясняется тем, что плоскости из L_{start} могут пересекаться.

Трудоемкость

Приведем верхнюю оценку средней трудоемкости алгоритма. Обозначим за D_1 среднюю трудоемкость в случае, когда $u^* \in M$, и за D_2 - когда $u^* \notin M$. Тогда средняя трудоемкость D может быть вычислена следующим образом:

$$D = s + \frac{|M|}{2^n}D_1 + (1 - \frac{|M|}{2^n})D_2, \text{ где}$$

$$D_1 = \sum_{j=1}^{s}|L_1^{(j)}|\cdot\alpha_j + |M|,$$

$$D_2 \leq \sum_{u\in V_n\setminus M}\frac{1}{2^n - |M|}\left[\sum_{L_1^{(j)}\in L_{start}, u\notin L_1^{(j)}}|L_1^{(j)}|\cdot\alpha_j + \sum_{L_1^{(j)}\in L_{start}, u\in L_1^{(j)}}|L_1^{(j)}|\cdot(1-\beta_j)\right].$$

Список литературы

[1] Meier W., Staffelbach O. Fast correlation attacks on certain stream cipher // Journal of Cryptology. — 1989. — V. 1, Iss. 3. — P. 159–176.

[2] Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology. — EUROCRYPT '93. Lecture Notes in Computer Science. Volume 765. — 1994. — P. 386–397.

[3] Алексеев Е. К. Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной // Сборник статей молодых ученых факультета ВМК МГУ. — 2011. — Т. 8. — С. 20–34.

О надежности одной схемы

Алехина Марина Анатольевна, Барсукова Оксана Юрьевна

Пензенский государственный университет, e-mail: ama@sura.ru, dm@pnzgu.ru

Пусть $n \in \mathbf{N}$, а P_3 — множество всех функций трехзначной логики, т. е. функций $f(x_1, ..., x_n) : \{0,1,2\}^n \to \{0,1,2\}$. Рассмотрим реализацию функций

из множества P_3 схемами из ненадежных функциональных элементов в базисе, состоящем из функции Вебба $\{V_3(x_1, x_2)\}$ ($V_3(x_1, x_2) = \max\{x_1, x_2\} + 1 \pmod 3$). Предполагается, что элементы схемы переходят в неисправные состояния независимо друг от друга.

Будем считать, что схема из ненадежных элементов реализует функцию $f(\tilde{x}^n)$ ($\tilde{x}^n = (x_1, ..., x_n)$), если при поступлении на входы схемы набора $\tilde{a}^n$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a}^n)$.

Пусть схема S реализует функцию $f(\tilde{x}^n)$, $\tilde{a}^n$ — произвольный входной набор схемы S, $f(\tilde{a}^n) = \tau$. Обозначим через $P_i(S, \tilde{a}^n)$ вероятность появления значения i ($i \in \{0, 1, 2\}$) на выходе схемы S при входном наборе $\tilde{a}^n$, а через $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}^n$. Ясно, что $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n) = P_{\tau+1}(S, \tilde{a}^n) + P_{\tau+2}(S, \tilde{a}^n)$. (В выражениях $\tau + 1$ и $\tau + 2$ сложение осуществляется по $\bmod 3$.)

Например, если входной набор $\tilde{a}^n$ схемы S такой, что $f(\tilde{a}^n) = 0$, то вероятность появления ошибки на этом наборе равна $P_{f(\tilde{a}^n)\neq 0}(S, \tilde{a}^n) = P_1(S, \tilde{a}^n) + P_2(S, \tilde{a}^n)$.

Ненадежностью схемы S, реализующей функцию $f(\tilde{x}^n)$, будем называть число $P(S)$, равное наибольшей из вероятностей появления ошибки на выходе схемы S. *Надежность* схемы S равна $1 - P(S)$.

Пусть базисные элементы с вероятностью ε ($\varepsilon \in (0, 1/4)$) подвержены инверсным неисправностям на выходах, т.е. каждый элемент базиса на любом входном наборе $\tilde{a}^2$ таком, что $\varphi(\tilde{a}^2) = \tau$, с вероятностью ε выдает значение $\tau + 1 (\bmod 3)$ и с вероятностью ε выдает значение $\tau + 2 (\bmod 3)$. Очевидно, что ненадежность базисного элемента равна 2ε, а надежность — $1 - 2\varepsilon$.

Пусть $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию f. Схема A из ненадежных элементов, реализующая функцию f, называется *асимптотически оптимальной по надежности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Задача построения надежных схем, а также асимптотически оптимальных по надежности схем, в различных полных конечных базисах решалась О. Ю. Барсуковой [1], причем во всех рассмотренных базисах названные схемы имели ненадежность, асимптотически (при $\varepsilon \to 0$) не больше $2k\varepsilon$ ($k \in \mathbf{N}$, k зависит от базиса). Поэтому возник вопрос, существует ли схема (в каком-либо полном конечном базисе), ненадежность которой асимптотически равна $l\varepsilon$, где число l — нечетное? Ответ на него положителен и получен в этой статье, а именно в базисе, состоящем из функции Вебба, построена схема, ненадежность которой асимптотически равна 7ε при $\varepsilon \to 0$.

Прежде чем предъявить эту схему, приведем известные результаты по надежности схем в рассматриваемом базисе: 1) любую функцию $f \in P_3$ можно реализовать такой схемой D, что $P(D) \leq 8\varepsilon + 268\varepsilon^2$ при всех $\varepsilon \in (0, 1/10^4]$ (и, следовательно, любую функцию из P_3 можно реализовать схемой, ненадежность которой асимптотически (при $\varepsilon \to 0$) не больше 8ε); 2) для произвольной функции $f \in K$ любая схема S, реализующая f, при $\varepsilon \in (0, 1/10^4]$ функционирует с ненадежностью $P(S) \geq 6\varepsilon - 10\varepsilon^2 + 6\varepsilon^3$ (и, следовательно, любая

схема, реализующая функцию $f \in K$, функционирует с ненадежностью, которая асимптотически (при $\varepsilon \to 0$) не меньше 6ε). Здесь $K = \bigcup_{n=3}^{\infty} K(n)$, $K(n)$ — множество функций трехзначной логики, каждая из которых зависит от переменных $x_1, ..., x_n$ $(n \geq 3)$, принимает все три значения $0, 1, 2$ и не представима в виде $\max\{x_k, h(\tilde{x}^n)\} + c$ $(k \in \{1, 2, ..., n\},\ c \in \{0, 1, 2\},\ h(\tilde{x}^n)$ — произвольная функция трехзначной логики.

Теперь рассмотрим пример.

Пример 1. На рис. 1 изображена схема C из четырех элементов, которая реализует функцию $f(x_1, x_2) = \min\{J_0(x_1), J_0(x_2)\}$ (см. табл. 1, в которой $m = \max\{x_1, x_2\}$). Вычислим ненадежность $P(C)$ схемы C.

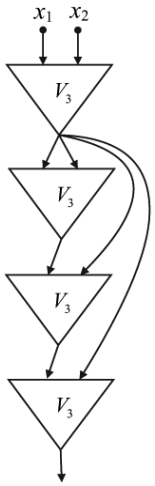

Рис. 1. Схема C.

1) Пусть входной набор $\tilde{a}^2$ схемы C такой, что $\tilde{a}^2 = (00)$. Тогда при отсутствии неисправностей в схеме C на ее выходе появляется значение 2. Вычислим вероятность появления 2 на выходе схемы C по формуле полной вероятности и получим: $P_2(C, \tilde{a}^2) = 1 - 7\varepsilon + 29\varepsilon^2 - 57\varepsilon^3 + 45\varepsilon^4$. Тогда вероятность появления ошибки на выходе схемы C равна $7\varepsilon - 29\varepsilon^2 + 57\varepsilon^3 - 45\varepsilon^4$.

x_1	x_2	$m+1$	$m+2$	$m(m+1, m+2)+1$	$f(x_1, x_2)$
0	0	1	2	0	2
0	1	2	0	0	0
0	2	0	1	2	0
1	0	2	0	0	0
1	1	2	0	0	0
1	2	0	1	2	0
2	0	0	1	2	0
2	1	0	1	2	0
2	2	0	1	2	0

Таблица 1.

2) Пусть входной набор $\tilde{a}^2$ схемы C равен одному из наборов (01), (10) или (11). Тогда при отсутствии неисправностей в схеме C на ее выходе появляется

значение 0. Вычислим вероятность появления 0 на выходе схемы C по формуле полной вероятности и получим: $P_0(C, \tilde{a}^2) = 1-3\varepsilon+2\varepsilon^2+3\varepsilon^3$. Тогда вероятность появления ошибки на выходе схемы C равна $3\varepsilon - 2\varepsilon^2 - 3\varepsilon^3$.

3) Пусть входной набор $\tilde{a}^2$ схемы C равен одному из наборов (0,2), (2,0), (1,2), (2,1) или (2,2). Тогда при отсутствии неисправностей в схеме C на ее выходе появляется значение 0. Вычислим вероятность появления 0 на выходе схемы C по формуле полной вероятности и получим: $P_0(C, \tilde{a}^2) = 1 - 7\varepsilon + 32\varepsilon^2 - 69\varepsilon^3 + 54\varepsilon^4$. Тогда вероятность появления ошибки на выходе схемы C равна $7\varepsilon - 32\varepsilon^2 + 69\varepsilon^3 - 54\varepsilon^4$.

Таким образом, ненадежность $P(C)$ схемы C равна

$P(C) = \max\{7\varepsilon-29\varepsilon^2+57\varepsilon^3-45\varepsilon^4,\ 3\varepsilon-2\varepsilon^2-3\varepsilon^3,\ 7\varepsilon-32\varepsilon^2+69\varepsilon^3-54\varepsilon^4\} =$
$= 7\varepsilon - 29\varepsilon^2 + 57\varepsilon^3 - 45\varepsilon^4$ (поскольку $\varepsilon \in (0, 1/4)$).

Очевидно, что при $\varepsilon \to 0$ ненадежность $P(C)$ асимптотически равна 7ε.

Работа выполнена при поддержке РФФИ (проекты № 14-01-00273, 14-01-31360).

Список литературы

[1] Барсукова О. Ю. Синтез надежных схем, реализующих функции двузначной и трехзначной логик : дис. ... канд. физ.-мат. наук : 01.01.09 : защищена 06.06.14 : утв. 08.12.14 / Барсукова Оксана Юрьевна. — Пенза, 2014. — 87 с. — Библиогр. : с. 84–87.

Об одном методе повышения надежности схем в базисе Россера–Туркетта

Алехина Марина Анатольевна, Каргин Степан Павлович

Пензенский государственный университет, e-mail: ama@sura.ru, dm@pnzgu.ru

Пусть $n \in \mathbf{N}$, а P_4 — множество всех функций четырехзначной логики, т. е. функций $f(x_1, ..., x_n) : \{0, 1, 2, 3\}^n \to \{0, 1, 2, 3\}$. Рассмотрим реализацию функций из множества P_4 схемами из ненадежных функциональных элементов в базисе Россера–Туркетта $\{0, 1, 2, 3, J_0(x_1), J_1(x_1), J_2(x_1), J_3(x_1), \min\{x_1, x_2\}, \max\{x_1, x_2\}\}$ ($\min\{x_1, x_2\}$ будем также обозначать через &, а $\max\{x_1, x_2\}$ — через $\vee$ [1]).

Будем считать, что схема из ненадежных элементов реализует функцию $f(\tilde{x}^n)$ ($\tilde{x}^n = (x_1, ..., x_n)$), если при поступлении на входы схемы набора $\tilde{a}^n$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a}^n)$.

Пусть схема S реализует функцию $f(\tilde{x}^n)$, $\tilde{a}^n$ — произвольный входной набор схемы S, $f(\tilde{a}^n) = \tau$. Обозначим через $P_i(S, \tilde{a}^n)$ вероятность появления значения i ($i \in \{0, 1, 2, 3\}$) на выходе схемы S при входном наборе $\tilde{a}^n$, а через $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}^n$. Ясно, что $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n) = P_{\tau+1}(S, \tilde{a}^n) + P_{\tau+2}(S, \tilde{a}^n) + P_{\tau+3}(S, \tilde{a}^n)$. (В выражениях $\tau + 1$, $\tau + 2$ и $\tau + 3$ сложение осуществляется по $\bmod 4$.)

Например, если входной набор $\tilde{a}^n$ схемы S такой, что $f(\tilde{a}^n) = 0$, то вероятность появления ошибки на этом наборе равна $P_{f(\tilde{a}^n)\neq 0}(S, \tilde{a}^n) = P_1(S, \tilde{a}^n) + P_2(S, \tilde{a}^n) + P_3(S, \tilde{a}^n)$.

Ненадежностью схемы S, реализующей функцию $f(\tilde{x}^n)$, будем называть число $P(S)$, равное наибольшей из вероятностей появления ошибки на выходе схемы S. *Надежность* схемы S равна $1 - P(S)$.

Предполагается, что элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon \in (0, 1/6)$) подвержены инверсным неисправностям на выходах, т. е. каждый базисный элемент с функцией $\varphi(\tilde{x}^k)$ ($k \in \mathbf{N}$) на любом входном наборе $\tilde{a}^k$ таком, что $\varphi(\tilde{a}^k) = \tau$, с вероятностью ε выдает значение $\tau + 1 \pmod 4$, с вероятностью ε выдает значение $\tau + 2 \pmod 4$ и с вероятностью ε выдает значение $\tau + 3 \pmod 4$. Очевидно, что ненадежность любого базисного элемента равна 3ε, а надежность — $1 - 3\varepsilon$.

Пусть $f(\tilde{x}^n)$ — функция из P_4, а S — любая схема, реализующая функцию f. Покажем, каким образом по схеме S построить схему, которая реализует ту же функцию f, но, возможно (при некоторых условиях на $P(S)$), более надежно. Для этого возьмем четыре экземпляра схемы S, два элемента с функцией $\&$ и один элемент с функцией $\vee$ и построим новую схему, как показано на рис. 1. Обозначим построенную схему через $\psi(S)$.

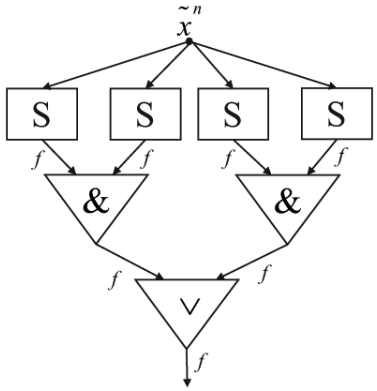

Рис. 1. Схема $\psi(S)$.

В теореме 1 найдено рекуррентное соотношение для ненадежностей схем S и $\psi(S)$.

Теорема 1. *Пусть f — произвольная функция из P_4, S — любая схема, реализующая f, а $P(S)$ — ненадежность схемы S. Тогда схема $\psi(S)$ (см. рис. 1) реализует функцию f с ненадежностью $P(\psi(S))$, удовлетворяющей неравенству*

$$P(\psi(S)) \leq 9\varepsilon + 36\varepsilon P(S) + 6P^2(S).$$

Доказательство. Пусть f — произвольная функция. Без ограничения общности можно считать, что функция f зависит от переменных $x_1, ..., x_n$. Пусть S — любая схема, реализующая f, $\tilde{a}^n$ — произвольный набор, $f(\tilde{a}^n) = \tau$. Обозначим через p вероятность появления ошибки $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$ на выходе схемы S (т. е.

$p = P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n)$) и найдем вероятность ошибки на выходе схемы $\psi(S)$ на этом же наборе, учитывая, что ненадежность подсхемы из трех элементов (двух конъюнкторов и одного дизъюнктора) не более 9ε.

$$P_{f(\tilde{a}^n)\neq\tau}(\psi(S), \tilde{a}^n) \leq (1-p)^4 \cdot 9\varepsilon + 4p(1-p)^3 \cdot 9\varepsilon + \sum_{i=2}^{4} C_4^i (1-p)^{4-i} p^i.$$

Найдем верхнюю оценку выражения $\sum_{i=2}^{4} C_4^i (1-p)^{4-i} p^i$:

$\sum_{i=2}^{4} C_4^i (1-p)^{4-i} p^i = 6p^2(1-2p+p^2) + 4p^3(1-p) + p^4 = 6p^2 - 8p^3 + 3p^4 \leq$
$\leq 6p^2$ при всех $p \in [0, 1]$.

Тогда

$$P_{f(\tilde{a}^n)\neq\tau}(\psi(S), \tilde{a}^n) \leq 9\varepsilon + 36p\varepsilon + 6p^2.$$

Следовательно,

$$P(\psi(S)) \leq 9\varepsilon + 36\varepsilon P(S) + 6P^2(S).$$

Теорема 1 доказана.

Таким образом, в базисе Россера–Туркетта при инверсных неисправностях на выходах элементов предложен метод синтеза надежных схем, реализующих четырехзначные функции, и получена рекуррентная формула, связывающая ненадежность предлагаемой схемы и ненадежность исходной схемы.

Работа выполнена при поддержке РФФИ (проект № 14-01-00273-а).

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Высш. шк., 2001. — 384 с.

О нижних оценках сложности функций многозначной логики в бесконечных базисах

Андреев Александр Андреевич

Московский государственный университет имени М. В. Ломоносова, e-mail: sanchez_14@mail.ru

Исследуется задача нахождения высоких оценок сложности для функций многозначной логики в бесконечных базисах (под базисом понимается произвольная система функций). Известно, что рост функции Шеннона сложности (и «схемной», и «формульной») и глубины булевых функций принципиально различается в случае конечных и бесконечных полных базисов. А именно, наблюдается значительное уменьшение порядка роста при переходе от конечных базисов к бесконечным. Аналогичный эффект наблюдается и для функции Шеннона глубины функций многозначной логики.

В работе приводятся два примера высоких нижних оценок функций Шеннона сложности (при реализации формулами) и глубины для случая бесконечных базисов функций многозначной логики. В обоих примерах строится бесконечный базис, для которого справедливы экспоненциальные и сверхэкспоненциальные оценки глубины и сложности соответственно. При этом в первом примере замкнутый класс, задаваемый этим базисом, не является конечно порождённым, а во втором является. Кроме того, для второго примера предъявлен конечный базис, порождающий тот же класс функций, и для которого рост функции Шеннона остаётся асимптотически таким же.

Предположим, что у нас есть конечная система функций k-значной логики и последовательность функций, сложность реализации которых формулами над этой системой нам известна. Покажем, как на основе этого примера построить бесконечный базис с такой же скоростью роста сложности для реализации некоторой последовательности функций.

Пусть $E_k = \{0, \ldots, k-1\}$; $\mathfrak{A} = \{\varphi_1(x_1, \ldots, x_{i_1}), \ldots, \varphi_m(x_1, \ldots, x_{i_m})\}$ — конечная система функций из P_k, а $f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n), \ldots$ — последовательность функций, сложность $L_{\mathfrak{A}}(f_n)$ реализации которых формулами над системой $\mathfrak{A}$ равна $h(n)$. Рассмотрим функции $(k+2)$-значной логики ψ_l и g_n, получающиеся соответственно из функций φ_l и f_n доопределением константой k на множества $E^{i_l}_{k+2}$ и E^n_{k+2} ($l \in \{1, \ldots, m\}$, $n \in \mathbb{N}$). Также определим функции $\mu_n(x_1, \ldots, x_n)$, $n = 1, 2, \ldots$, равные k, если $x_1 = \ldots = x_n = k+1$, и $k+1$ в остальных случаях.

Пусть $\mathfrak{A}' = \{\psi_1, \ldots, \psi_m, \mu_1, \mu_2, \ldots\}$. Покажем, что $L_{\mathfrak{A}'}(g_n) = h(n)$.

Если в некоторой формуле над системой $\mathfrak{A}'$ для некоторого n есть элемент μ_n, то такая формула может принимать только значения k и $k+1$. Значит, сложность реализации функций g_n над системой $\mathfrak{A}'$ не изменится, если из этой системы убрать функции μ_n. Очевидно, что $L_{\mathfrak{A}}(f_n) = L_{\mathfrak{A}'}(g_n)$.

Таким образом, если в качестве $\mathfrak{A}$ взять систему из [1], то приведённым способом мы построим бесконечный базис, сложность реализации некоторой последовательности функций над которым растёт сверхэкспоненциальным образом. Недостаток приведённого метода в том, что порождающую систему можно разделить на две практически не связанные части: одна доставляет нам необходимую оценку, а вторая делает систему бесконечной. Это делает систему сильно искусственной.

Построим бесконечный базис, удовлетворяющий следующим условиям: 1) класс, порождаемый этим базисом, конечно порождён; 2) функции Шеннона глубины и сложности в этом базисе асимптотически равны соответствующим функциям в конечном базисе (и растут экспоненциально и сверхэкспоненциально соответственно); 3) каждая функция базиса используется хотя бы в одной минимальной формуле, доставляющей такую оценку.

Для описания такого примера рассмотрим базис из работы [2]. Обозначим через E^n_k ($n \geq 1$) множество всех наборов $(\alpha_1, \ldots, \alpha_n)$, таких, что $\alpha_1, \ldots, \alpha_n \in E_k$, а через Q_n множество всех наборов из E^n_k, состоящих только из символов $3, \ldots, k-1$, причем тройки есть обязательно. Определим функции $\lambda(x, y)$,

$\mu(x,y,z)$, $\varphi_m(x,y)$, где $m \in \{3,\ldots,k-1\}$, и $f_n(y,x_1,\ldots,x_n)$, принадлежащие P_k, следующим образом.

$$\lambda(x,y) = \begin{cases} 0, & \text{если } x=0,\ y=2; \\ 1, & \text{если } x=1, y \in E_k \text{ или } x=0,\ y=3; \\ 2 & \text{в остальных случаях;} \end{cases}$$

$$\mu(x,y,z) = \begin{cases} \lambda(x,z), & \text{если } x=y; \\ 2 & \text{в противном случае;} \end{cases}$$

$$\varphi_m(x,y) = \begin{cases} 3, & \text{если } x=3,\ y=m; \\ 2 & \text{в остальных случаях;} \end{cases}$$

$$f_n(y,x_1,\ldots,x_n) = \begin{cases} 0, & \text{если } y=0,\ (x_1,\ldots,x_n) \notin Q_n; \\ 1, & \text{если } y=1, (x_1,\ldots,x_n) \in E_k^n \\ & \text{или } y=0,\ (x_1,\ldots,x_n) \in Q_n; \\ 2 & \text{в остальных случаях.} \end{cases}$$

Теорема 1 [2]. *Пусть* $\mathfrak{B} = \{\mu, \varphi_3, \ldots, \varphi_{k-1}, 2\}$. *Тогда при всех* $n \geq 1$, $k \geq 4$ *для последовательности* f_n *функций* k*-значной логики справедливо равенство*

$$L_{\mathfrak{B}}(f_n) = (n+1) \cdot 2^{n((k-3)^n-(k-4)^n)} - n.$$

При доказательстве этой теоремы в [2] установлено, что любая формула Φ, реализующая функцию f_n для некоторого n, устроена строго определённым образом. Для пояснения введём формулу $G_N = \lambda(\lambda(\ldots\lambda(\lambda(y,Z_1),Z_2),\ldots),Z_N)$, где $Z_1,\ldots,Z_N$ — формулы над $\mathfrak{B}$, N — натуральное. Формула Φ получается из формулы G_N при замене всех подформул вида $\lambda(A,B)$ формулами $\mu(A,A,B)$. Во всех минимальных формулах подформулы Z_i также устроены строго определённым образом: они все имеют вид $\varphi_{m_1}(\ldots\varphi_{m_s}(H_{s+1},H_s),\ldots,H_1)$, где $H_1,\ldots,H_{s+1}$ — переменные из множества $x_1,\ldots,x_n$, каждая встречается в формуле как минимум один раз. Кроме того, минимально возможное для реализации f_n количество таких подформул равно $N=(k-3)^n-(k-4)^n$.

Теперь зафиксируем некоторое k и построим базис $\mathfrak{C} \subseteq P_k$. Для этого возьмём базис $\mathfrak{B} \subseteq P_k$ и для всех натуральных n для всех минимальных формул над $\mathfrak{B}$ для всех подформул Z_i добавим в базис функции, реализуемые формулами Z_i. Получится бесконечный базис, в котором при реализации функций f_n каждая функция базиса используется хотя бы в одной минимальной формуле, и при этом формулы будут всё так же иметь описанные выше особенности строения. Это значит, что справедлива

Теорема 2. *При всех $n \geq 1$, $k \geq 4$ для последовательности f_n функций k-значной логики справедливо равенство*

$$L_{\mathfrak{C}}(f_n) = (n+1) \cdot 2^{n((k-3)^n-(k-4)^n)} - n.$$

Отметим, что для замкнутого класса $[\mathfrak{B}] = [\mathfrak{C}]$ функции Шеннона сложности реализации функций из этого класса формулами в базисах $\mathfrak{B}$ и $\mathfrak{C}$ растут как указанные в теоремах 1 и 2 функции.

Работа выполнена при поддержке РФФИ (проект № 14-01-00598-а) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

[1] Андреев А. А. Об одной последовательности функций многозначной логики // Вестник Московского университета. Сер. 1. Математика. Механика. — 2011. — № 6. — С. 52–57.

[2] Андреев А. А. О нижних оценках сложности для некоторых последовательностей функций многозначной логики // Вестник Московского университета. Сер. 1. Математика. Механика. — 2013. — № 6. — С. 25–30.

Эффективность доступа к данным в системе управления базами данных DIM

Антонов Дмитрий Владимирович[1], **Рублев Вадим Сергеевич**[2]

[1] Ярославский государственный университет им. П. Г. Демидова, e-mail: dmitrii.antonov@gmail.com
[2] Ярославский государственный университет им. П. Г. Демидова, e-mail: roublev@mail.ru

Введение

Архитектуры современных СУБД разнообразны, но все они имеют в своем основании одну из распространённой моделей:реляционная (Codd, 1970), объектно-ориентированная (др., 1995), объектно-реляционная (Дарвин, и др., 1996), темпоральная (Костенко, и др., 2007).

Каждая из этих систем имеет свои достоинства и недостатки [1]. Недостатки имеющихся моделей СУБД позволили задуматься о создании новой технологии СУБД, которая использует достоинства имеющихся технологий перечисленных выше систем. Новый объектный подход к созданию СУБД [1] предполагает как изменение данных объектов, так и возможность изменения типов объектов, т. е. схемы базы данных. Итоговая СУБД была названа динамической информационной моделью (DIM).

СУБД DIM будет иметь преимущества перед реляционной технологией, если: сложные запросы могут быть написаны проще и доступней; дополнительное ПО поможет генерировать запросы в сложных случаях; проигрыш реляционных запросов не будет значителен; преобразование реляционной БД в

БД DIM может быть проведен программно. В этом мы видим эффективность доступа к данным.

Формализация дискретной детерминированной модели привела к построению объектно-динамической модели (OD-модели), а для адекватного описания ее данных в DIM введены формализация схемы классов DIM и формализация статического описания OD-модели схемой классов DIM [2].

OD-моделью будем называть одиннадцатку

(O,A,$\bar{A}(o)$,$V(o)$,L_p,L_o,L_f,$\bar{A}_{L_f}(o_l^j)$,$V_{L_f}(o_l^f)$,F,T),

где

O — конечное множество объектов,

$A = \bigcup_o A_o$ — конечное множество свойств объектов с типами этих свойств (элемент этого множества пара (a,V^a) – свойство, тип свойства),

$\bar{A}(o)$ — функция кортежа свойств объекта o,

$V(o)$ — функция кортежа значений свойств объектов (упорядоченность значений свойств объекта о соответствует упорядоченности свойств этого объекта в кортеже $\bar{A}(o)$),

$L_p = \bigcup_{j \in\ L_p} \{l_j^p = \{o, o1\}\}$ — множество простых связей объектов,

L_o — множество объектов-связей ($O \cap\ L_o = \emptyset$),

$L_f = \bigcup_{j \in\ L_f} \{(l_j^f, o_l^j \in\ L_o)\}$ — множество функциональных связей объектов,

$\bar{A}_{L_f}(o_l^j)$ — функция кортежа атрибутов объекта-связи o_l^j функциональных связей L_f,

$V_{L_f}(o_l^f)$ — функция кортежа значений атрибутов объекта-связи o_l^f функциональных связей L_f,

F — конечное множество алгоритмических процедур изменения значений свойств объектов и изменения объектов,

T — дискретная шкала времени.

Постановка задачи

Поскольку существуют разные типы СУБД, то единого алгоритма для конвертирования данных из любой СУБД в DIM не написать, но можно использовать OD-модель, то есть сначала преобразовывать имеющуюся БД в OD-модель, а затем использовать имеющийся алгоритм преобразования OD-модели в структуру СУБД DIM.

Для переноса существующих БД на СУБД DIM была создана программа, которая может преобразовывать данные из реляционной СУБД. Остальные виды, такие как: темпоральная, объектно-ориентированная и объектно-реляционная, на данный момент находятся на стадии тестирования. Для такого преобразования необходимо два этапа. На первом БД конвертируется в OD-модель. Затем модель конвертируется в СУБД DIM.

Алгоритм преобразования реляционной БД в БД DIM

Для конвертирования реляционной БД в OD-модель был разработан алгоритм, который был успешно применен в описанной выше программе:

1. Выполняется запрос с целью получения перечня таблиц и соответствующих им полей, представленных в БД.
2. На основе полученных данных заполняется массив, отвечающий за множество наименований таблиц переносимой БД.
3. Заполняется двумерный массив, отвечающий за множество полей всех таблиц (в массив записывается информация о наименовании полей и их типе).
4. Выполняется серия запросов к таблицам с целью получения информации о записанных в их полях данных (при этом считываются именно наборы данных, соответствующие каждому из полей).
5. Заполняется массив, отвечающий за множество значений, записанных в таблице (каждый набор разделяется специальным тегом для возможности в дальнейшем отличить наборы друг от друга).
6. Выполняется серия запросов с целью выяснить наличие внешних индексов, следовательно, связей между таблицами.
7. Заполняется массив, отвечающий за множество связей между таблицами.

В результате формируется модель, которая соответствует описанию OD-модели [2]. Далее в специальной программе, которая была названа «Конвертер СУБД DIM», используется алгоритм, по которому эти таблицы связываются с соответствующими группами полей (как правило, каждая группа начинается с поля Id). В дальнейшем программа анализирует наименования полей на предмет частичного совпадения, и на основе этого формирует связи между соответствующими этим полям таблицами. Так как в существующей БД могут иметься свои особенности связей между таблицами, то пользователю предоставляется возможность предварительного просмотра и корректировки элементов OD-модели. Для удобства пользователю отображается предварительный список параметров, классов и связей между ними. Имеется возможность редактирования связей и остальных объектов модели.

Заключение

В итоге разработанные алгоритмы используются в созданной программе «Конвертер СУБД DIM» для преобразования реляционных БД в БД СУБД DIM. Конвертер был протестирован на БД Oracle и на данный момент программа проходит госрегистрацию. Также был проведен сравнительный анализ запросных технологий [3] и разработано ПО «Генератор ODQL-запросов». Таким образом поставленные задачи по созданию эффективных средств доступа к данным DIM достигнуты.

Список литературы

[1] Писаренко Д. С., Рублев В.С. Объектная СУБД Динамическая информационная модель и ее основные концепции // Моделирование и анализ информационных систем. — 2009. — Т. 16, № 1. — С. 62–91.

[2] Рублев В.С. Теорема о статической полноте СУБД DIM // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16 - 20 июня 2014г.). Казань: Отечество. — 2014. — С. 242–245.

[3] Антонов Д.В., Рублев В.С. Анализ технологий вычисления ODQL-запросов СУБД DIM // Ярославский педагогический вестник. — 2013. — Т. 3, № 4. — С. 93–97.

О свойстве булевых функций, гарантирующем существование логарифмических диагностических тестов относительно примитивных сдвигов переменных

Антюфеев Григорий Валерьевич

ОАО «Байкал Электроникс», e-mail: grigoriy.rus@gmail.com

Пусть $f(x_1, x_2, ..., x_n)$ — булева функция, формально зависящая от переменных $x_1, x_2, ..., x_n$ (это будет записываться так: $f(\tilde{x}^n) \in P_2^n$), E_2^k — множество всех k-разрядных двоичных наборов и пусть выбран какой-то набор $\tilde{\gamma} = (\gamma_1, \gamma_2, .., \gamma_n) \in E_2^n$. Рассмотрим источник неисправностей $U_{n,\tilde{\gamma}}^{shift}$, способный действовать на булеву функцию следующим образом. Источником выбирается число $k \in \{1, ..., n\}$, и вместо значения функции $f(\alpha_1, ..., \alpha_k, \alpha_{k+1}, ..., \alpha_n)$ вычисляется значение $f(\alpha_{k+1}, ..., \alpha_n, \gamma_1, ..., \gamma_k)$. Определим множество функций неисправности $F_{f,\tilde{\gamma}} = \{f_{k,\tilde{\gamma}}(x_1, x_2, ..., x_n) | k \in \{1, 2, ..., n\}, \tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n\}$. Назовём такой источник неисправностей $U_{n,\tilde{\gamma}}^{shift}$ *источником примитивных сдвигов влево с фиксированным параметром* $\tilde{\gamma}$ [1].

Множество T наборов значений переменных $x_1, ..., x_n$ называется *диагностическим тестом относительно примитивных сдвигов переменных функции* f *влево с фиксированным параметром* $\tilde{\gamma}$ тогда и только тогда, когда для любых двух неравных функций g, h из $F_{f,\tilde{\gamma}} \cup \{f\}$, найдётся набор $\tilde{\alpha}$ из T, для которого выполнено неравенство $g(\tilde{\alpha}) \neq h(\tilde{\alpha})$. Количество различных наборов в тесте T называется его *длиной* и обозначается через $L(T)$. Тест минимальной длины называется *минимальным*. Обозначим через $L_{\tilde{\gamma}}^{shifts,diagn}(f(\tilde{x}^n))$ длину минимального диагностического теста отсносительно примитивных сдвигов переменных функции $f(x_1, ..., x_n)$ влево с фиксированным параметром $\tilde{\gamma}$.

Таблица у которой все столбцы различны, называется *отделимой по столбцам таблицей*.

Таблицы неисправностей (относительно примитивных сдвигов переменных функции f влево с фиксированным параметром $\tilde{\gamma}$) имеют $n + 1$ столбец: n функций неисправности и исходная функция. Нумерация столбцов начинается с нуля, нулевой столбец соответствует исходной функции $f(\tilde{x}^n) \in P_2^n$, k-ый — функции $f_{\tilde{\gamma}}^k(\tilde{x}^n) \in P_2^n$, получающейся из исходной примитивным сдвигом переменных с «наползающим» набором $\tilde{\gamma}$ на k позиций, где $k \in \{1, ..., n\}$.

Функция $f(\tilde{x}^n) \in P_2^n$ обладает свойством **A1**, если для любого $\tilde{\alpha} = (\alpha_1, ..., \alpha_{n-1}, \alpha_n) \in E_2^n$ на наборах вида $(\alpha_1, ..., \alpha_{n-1}, \alpha_n)$, $(0, \alpha_1, ..., \alpha_{n-1})$, $(1, \alpha_1, ..., \alpha_{n-1})$ функция $f(\tilde{x}^n) \in P_2^n$ принимает оба значения.

Функция $f(\tilde{x}^n) \in P_2^n$ обладает свойством **A2**, если для любого $\tilde{\alpha} = (\alpha_1, ..., \alpha_{n-1}, \alpha_n) \in E_2^n$ на наборах $(0, 0, \alpha_1, ..., \alpha_{n-2})$, $(0, 1, \alpha_1, ..., \alpha_{n-2})$, $(1, 0, \alpha_1, ..., \alpha_{n-2})$, $(1, 1, \alpha_1, ..., \alpha_{n-2})$ функция $f(\tilde{x}^n) \in P_2^n$ принимает оба значения.

Лемма 1. *Свойство* A1 *является необходимым для того, чтобы для любого набора* $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ *все столбцы таблицы неисправностей* $M_{f,\tilde{\gamma}}$ *были различны.*

Лемма 2. *Свойство* A2 *является необходимым для того, чтобы для любого набора* $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ *все столбцы таблицы неисправностей* $M_{f,\tilde{\gamma}}$ *были различны.*

Из-за громоздкости подробного доказательства этой лемм опустим их.

Теорема 1. *Наличие одновременно свойств* A1 *и* A2 *необходимо и достаточно для того, чтобы для любого набора* $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ *все столбцы таблицы неисправностей* $M_{f,\tilde{\gamma}}$ *были различны.*

Доказательство. Необходимость следует из лемм 1 и 2. Докажем достаточность. Пусть выполняется A1 и $f^i_{\tilde{\gamma}} \equiv f^j_{\tilde{\gamma}}$. Тогда $f(x_i, ..., x_j, xj + 1, ..., x_n, \gamma_1, ..., \gamma_i) \equiv f(x_{j-1}, ..., x_n, \gamma_1, ..., \gamma_i, ..., \gamma_j)$ и $x_i, ..., x_j$ — фиктивные переменные. Пусть теперь $j = i + 1$. Тогда

$$f(0, x_{j+1}, ..., x_n, \gamma_1, ..., \gamma_i) = f(1, x_{j+1}, ..., x_n, \gamma_1, ..., \gamma_i, ..., \gamma_j) =$$

$$= f(x_{j+1}, ..., x_n, \gamma_1, ..., \gamma_i, ..., \gamma_j)$$

и, взяв набор $\tilde{\alpha} = (0, ..., 0) \in E_2^n$, получим противоречие: $f(0, 0, ..., 0, \gamma_1, ..., \gamma_i) = f(1, 0, ..., 0, \gamma_1, ..., \gamma_i, ..., \gamma_j) = f(0, ..., 0, \gamma_1, ..., \gamma_i, \gamma_j)$. Пусть теперь выполняется A2 и $f^i_{\tilde{\gamma}} \equiv f^j_{\tilde{\gamma}}$ и $j \geq i + 2$. Тогда $f(x_{i+1}, x_{i-2}, ..., x_{j+1}, ..., x_n, \gamma_1, ..., \gamma_i) \equiv f(x_{j+1}, ..., x_n, \gamma_1, ..., \gamma_i, ..., \gamma_j)$ и x_{i-1}, x_{i+2} — фиктивные переменные. Тогда, взяв набор $\tilde{\alpha} = (0, ..., 0) \in E_2^n$, получаем $f(x_1, x_2, 0, ..., 0, \gamma_1, ..., \gamma_i) \equiv const$. Следовательно на квадрате $(*, *, 0, ..., 0, \gamma_1, ..., \gamma_i)$ функция f принимает одно и то же занчение. Получили противоречие. **Теорема 1 доказана.**

Лемма 3. *Если функция* $f(\tilde{x}^n) \in P_2^n$ *обладает свойством* A1*, то в таблице* $M_{f,\tilde{\gamma}}$ *имеется строка вида* $\tilde{\varepsilon} = \underbrace{(\varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}, ..., \varepsilon^{'})}_{n-1}, \varepsilon^{'} = \begin{cases} \varepsilon, & n = 2k \\ \overline{\varepsilon}, & n = 2k+1 \end{cases}, k \in N.$

Лемма 4. *Если функция* $f(\tilde{x}^n) \in P_2^n$ *обладает свойством* A2*, то в таблице* $M_{f,\tilde{\gamma}}$ *имеются все возможные строки вида* $\tilde{\varepsilon} = (\varepsilon_0, ..., \varepsilon_n)$*, где либо координаты с чётными индексами выбираются произвольно, либо с нечётными.*

Из-за громоздкости подробного доказательства этих лемм опустим их.

Теорема 2. *Если функция* $f(\tilde{x}^n) \in P_2^n$ *обладает свойствами* A1 *и* A2*, то*

$$L^{shifts,diagn}_{\tilde{\gamma}}(f(\tilde{x}^n)) \lesssim 2 \log n. \quad (1)$$

Доказательство. По лемме 4 существуют строки в таблице $M_{f,\tilde{\gamma}}$, которые отличают все чётные столбцы друг от друга и все нечётные. Строка из леммы 1 отличает чётные столбцы от нечётных. Таким образом получаем следующую оценку:

$$L_{\tilde{\gamma}}^{shifts,diagn}(f(\tilde{x}^n)) \leq \log\left(\left\lfloor \frac{n+1}{2} \right\rfloor\right) + \log\left(\left\lceil \frac{n+1}{2} \right\rceil\right) + 1. \qquad (2)$$

Теорема 2 доказана.

Теорема 3. *Если для функции $f(\tilde{x}^n) \in P_2^n$ таблица неисправностей $M_{f,\tilde{\gamma}}$ для любого набора $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ отделима по столбцам, то для любого $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ длина диагностического теста определяется формулой* (1).

Доказательство следует из теорем 1 и 2.

Следствие. *Если для функции $f(\tilde{x}^n) \in P_2^n$ таблица неисправностей $M_{f,\tilde{\gamma}}$ для любого набора $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ отделима по столбцам, то для любого $\tilde{\gamma} = (\gamma_1, ..., \gamma_n) \in E_2^n$ длина диагностического теста для такой функции будет:*

$$L_{\tilde{\gamma}}^{shifts,diagn}(f(\tilde{x}^n)) = \Theta(\log n). \qquad (3)$$

Доказательство. Нижняя оценка тривиальна, см., например, [2]. Верхняя следует из теоремы 3. **Следствие доказано.**

Для полноты картины стоит отметить, что функция Шеннона [1] длины диагностического теста относительно примитивных сдвигов переменных влево с фиксированным параметром $\tilde{\gamma}$ выглядит следующим образом:

$$L_{\tilde{\gamma}}^{shifts,diagn}(n) = \Theta(n). \qquad (4)$$

Автор выражает благодарность доценту Романову Д. С. за проявленный интерес к работе.

Список литературы

[1] Романов Д. С., Антюфеев Г. В. О тестах относительно примитивных сдвигов переменных в булевых функциях // Вопросы радиоэлектроники. Серия «Электронная вычислительная техника (ЭВТ)». — 2013. — Вып. 2. — С. 64–68.

[2] Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004. — 256 с.

Операторные полиномиальные формы функций над конечными полями

Балюк Александр Сергеевич, Янушковский Григорий Викторович
Иркутский государственный университет, e-mail: sacha@hotmail.ru, grisha_ya@inbox.ru

Пусть $\mathbb{F}_q$ — конечное поле порядка q, n — натуральное число. Множество n-местных функций над $\mathbb{F}_q$ с операциями сложения и умножения на константы из $\mathbb{F}_q$ образует линейное пространство размерности $N = q^n$, которое будем обозначать $\mathbb{F}_q^N$. Пусть $\sigma^1, \ldots, \sigma^N$ — все наборы из $\mathbb{F}_q^n$, упорядоченные некоторым образом, например, лексикографически. Будем считать, что i-й компонент в векторном представлении $f \in \mathbb{F}_q^N$ равен $f(\sigma^i)$, $i \in \{1, \ldots, N\}$.

Множество ненулевых векторов из $\mathbb{F}_q^q$ будем обозначать $\dot{\mathbb{F}}_q^q$, а элементы этого множества будем называть одноместными операторами. n-местным оператором назовем вектор $\mathfrak{a} = \mathfrak{a}_1 \otimes \cdots \otimes \mathfrak{a}_n$, где $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_n\} \subseteq \dot{\mathbb{F}}_q^q$, а $\otimes$ обозначает тензорное произведение векторов.

Пусть $S = (f_1, \ldots, f_N)$ — упорядоченное множество функций из $\mathbb{F}_q^N$, а M_S — матрица, стобцы которой суть векторы $f_1, \ldots, f_N$. Определим действие оператора $\mathfrak{a}$ на множество S следующим образом: $\mathfrak{a}S = M_S\mathfrak{a}$. Если $f_1, \ldots, f_N$ — линейно независимы, то множество S будем назвать базисным.

Для заданной функции $g \in \mathbb{F}_q^N$ определим упорядоченное множество функций $S_g = (g_1, \ldots, g_N)$, где для всех $\tau \in \mathbb{F}_q^n$ и всех $i \in \{1, \ldots, N\}$ выполняется $g_i(\tau_1, \ldots, \tau_n) = g(\tau_1 - \sigma_1^i, \ldots, \tau_n - \sigma_n^i)$. Действие оператора $\mathfrak{a}$ на функцию g определим следующим образом: $\mathfrak{a}g = \mathfrak{a}S_g$. Если S_g — базисное множество, то функцию g будем также называть базисной.

Упорядоченное множество из N n-местных операторов $\mathfrak{A} = (\mathfrak{a}^1, \ldots, \mathfrak{a}^N)$ будем называть пучком размерности n. Матрицу, столбцы которой суть векторы $\mathfrak{a}^1, \ldots, \mathfrak{a}^N$ будем называть матрицей пучка и обозначать $M_{\mathfrak{A}}$. Пучок будем называть базисным, если его матрица невырожденна.

Если S — базисное множество, а $\mathfrak{A} = (\mathfrak{a}^1, \ldots, \mathfrak{a}^N)$ — базисный пучок, то тогда любую функцию $f \in \mathbb{F}_q^N$ можно единственным образом представить в виде операторной полиномиальной формы $f = \sum_{i=1}^N \alpha_i \mathfrak{a}^i S$, где $\alpha_i \in \mathbb{F}_q$. Это выражение можно записать в матричном виде: $f = M_S M_{\mathfrak{A}} \alpha$, где $\alpha = (\alpha_1, \ldots, \alpha_N)$. Число ненулевых коэффициентов вектора α будем назвать сложностью представления функции f пучком $\mathfrak{A}$ по множеству S и обозначать $L_{\mathfrak{A}}^S(f)$.

Пусть C — некоторое множество (класс) базисных пучков. Величину $L_C^S(f) = \min\{L_{\mathfrak{A}}^S(f) \mid \mathfrak{A} \in C\}$ будем называть сложностью функции f в классе C по множеству S. Классы пучков C_1 и C_2 будем называть эквивалентными, если существуют взаимно однозначное соответствие $\rho : C_1 \to C_2$ и матрица M_ρ, такие что $M_{\rho(\mathfrak{A})} = M_\rho M_{\mathfrak{A}}$ для всех $\mathfrak{A} \in C_1$.

Пусть $F \subseteq \mathbb{F}_q^N$. Величину $L_C^S(F) = \max\{L_C^S(f) \mid f \in F\}$ будем называть сложностью множества функций F в классе C по множеству S. Величину $L_C^S(\mathbb{F}_q^N)$ будем обозначать $L_C^S(n)$.

Теорема 1. *Для любых базисных множеств S_1, S_2 и любых классов базисных пучков C_1 и C_2 справедливо: 1) $L_{C_1}^{S_1}(n) = L_{C_1}^{S_2}(n)$; 2) если C_1 и C_2 эквивалентны, то $L_{C_1}^{S_1}(n) = L_{C_2}^{S_1}(n)$; 3) если $C_1 \subseteq C_2$, то $L_{C_1}^{S_1}(n) \geqslant L_{C_2}^{S_1}(n)$.*

В дальнейшем вместо $L_C^S(n)$ будем использовать обозначение $L_C(n)$.

Пусть $a \in \mathbb{F}_q$. Если для пучка $\mathfrak{A} = (\mathfrak{a}^1, \ldots, \mathfrak{a}^N)$ существует оператор $\mathfrak{b}$, такой что $\mathfrak{a}_i^j = \mathfrak{b}_i$, когда $\sigma_i^j = a$, то множество $\{\mathfrak{b}\}$ будем называть проекцией пучка $\mathfrak{A}$ по элементу a и обозначать $\mathrm{Pr}_a(\mathfrak{A})$. Если такого оператора не существует, будем считать, что $\mathrm{Pr}_a(\mathfrak{A}) = \varnothing$. Если $A \subseteq \mathbb{F}_q$, то будем считать, что $\mathrm{Pr}_A(\mathfrak{A}) = \bigcup_{a \in A} \mathrm{Pr}_a(\mathfrak{A})$ и $\mathrm{Pr}(\mathfrak{A}) = \mathrm{Pr}_{\mathbb{F}_q}(\mathfrak{A})$.

Базисный пучок $\mathfrak{A}$ назовем t-порожденным, если $|\mathrm{Pr}(\mathfrak{A})| \geqslant t$.

Пусть $(i_1, \ldots, i_n)$ — перестановка чисел $(1, \ldots, n)$. Перестановкой пучка $(\mathfrak{a}^1, \ldots, \mathfrak{a}^N)$ назовем пучок $(\mathfrak{b}^1, \ldots, \mathfrak{b}^N)$, в котором для каждого $j \in \{1, \ldots, N\}$ положим $\mathfrak{b}_k^j = \mathfrak{a}_{i_k}^m$, где m выбирается так, что $\sigma_k^j = \sigma_{i_k}^m$, $k \in \{1, \ldots, n\}$.

Пусть $n = n_1 + n_2$, $n_1 \geqslant 1$, $n_2 \geqslant 1$, $N_1 = q^{n_1}$, $N_2 = q^{n_2}$, $\mathfrak{A} = (\mathfrak{a}^1, \ldots, \mathfrak{a}^{N_1})$ — базисный пучок операторов размерности n_1, $\mathfrak{B}_1, \ldots, \mathfrak{B}_{N_1}$ — базисные пучки операторов размерности n_2, $\mathfrak{B}_i = (\mathfrak{b}^{i,1}, \ldots, \mathfrak{b}^{i,N_2})$, $i \in \{1, \ldots, N_1\}$. Слиянием пучков $\mathfrak{B}_1, \ldots, \mathfrak{B}_{N_1}$ по пучку $\mathfrak{A}$ назовем пучок $(\mathfrak{c}^1, \ldots, \mathfrak{c}^N)$ размерности n, в котором $\mathfrak{c}^{(i-1)*N_2+j} = \mathfrak{a}^i \otimes \mathfrak{b}^{i,j}$, $i \in \{1, \ldots, N_1\}$, $j \in \{1, \ldots, N_2\}$.

Операторы $\mathfrak{b}^1, \ldots, \mathfrak{b}^k$ будем называть сильно линейно независимыми, если для всех $i \in \{1, \ldots, n\}$ множества $\{\mathfrak{b}_i^1, \ldots, \mathfrak{b}_i^k\}$ — линейно независимы. Пусть $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{F}_q$, $|A| = k \geqslant 0$, $\mathfrak{b}^1, \ldots, \mathfrak{b}^k$ — сильно линейно независимые операторы. Для каждого t, $q \geqslant t \geqslant k$ определим класс $K_t(\mathfrak{b}^1, \ldots, \mathfrak{b}^k)$ t-порожденных базисных пучков, определенных операторами $\mathfrak{b}^1, \ldots, \mathfrak{b}^k$, следующим образом: $K_t(\mathfrak{b}^1, \ldots, \mathfrak{b}^k) = \{\mathfrak{A} : |\mathrm{Pr}(\mathfrak{A})| \geqslant t, \mathrm{Pr}_{a_i} = \{\mathfrak{b}^i\}, 1 \leqslant i \leqslant k\}$. Если $k = 0$, то $K_t(\mathfrak{b}^1, \ldots, \mathfrak{b}^k)$ будем обозначать просто K_t.

Рассмотрим класс $K_q(\mathfrak{b}^1, \ldots, \mathfrak{b}^q)$. Он состоит из единственного пучка. Пусть это будет пучок $\mathfrak{A} = (\mathfrak{a}^1, \ldots, \mathfrak{a}^N)$. Пусть $\mathfrak{c} = \sum_{i=1}^N \mathfrak{a}^i$. Для каждого $i \in \{1, \ldots, N\}$ определим пучок $\mathfrak{A}_i = (\mathfrak{a}^1, \ldots, \mathfrak{a}^{i-1}, \mathfrak{c}, \mathfrak{a}^{i+1}, \ldots, \mathfrak{a}^N)$. Определим классы $E(\mathfrak{b}^1, \ldots, \mathfrak{b}^q) = \{\mathfrak{A}\} \cup \{\mathfrak{A}_i \mid i \in \{1, \ldots, N\}\}$ и $E = \bigcup_{\mathfrak{b}^1, \ldots, \mathfrak{b}^q} E(\mathfrak{b}^1, \ldots, \mathfrak{b}^q)$.

Класс пучков, матрицы которых — верхние треугольные, обозначим T.

Класс пучков, которые можно построить из базисных пучков размерности 1 применением операций слияния и перестановки, обозначим FK.

Отметим, что при $q = 2$ классам $K(\mathfrak{a})$, K, $G(\mathfrak{a})$, G, $E(\mathfrak{a})$, E, FK, OF из работы [1] соответствуют классы $K_q(\mathfrak{a})$, K_q, $K_{q-1}(\mathfrak{a})$, K_{q-1}, $E(\mathfrak{a})$, E, FK, K_0, а классам ExH_i, ExH, HPE, HPD, HDE, H, NPE, NPD, NDE, N, MH, OPF из работы [2] — классы $E(\mathfrak{a})$, E, $K_q(\mathfrak{a})$, $K_q(\mathfrak{b})$, $K_q(\mathfrak{c})$, K_q, $K_{q-1}(\mathfrak{a})$, $K_{q-1}(\mathfrak{b})$, $K_{q-1}(\mathfrak{c})$, K_{q-1}, FK, K_0 для некоторых операторов $\mathfrak{a}$, $\mathfrak{b}$ и $\mathfrak{c}$.

Теорема 2 (об иерархии). *Если $\mathfrak{b}^1, \ldots, \mathfrak{b}^q$ — сильно линейно независимые операторы и $q \geqslant t_1 \geqslant t_2 \geqslant k_1 \geqslant k_2 \geqslant 0$, то справедливо следующее: 1) $K_{t_2}(\mathfrak{b}^1, \ldots, \mathfrak{b}^{k_1}) \subsetneq K_{t_1}(\mathfrak{b}^1, \ldots, \mathfrak{b}^{k_1})$; 2) $K_{t_1}(\mathfrak{b}^1, \ldots, \mathfrak{b}^{k_1}) \subsetneq K_{t_1}(\mathfrak{b}^1, \ldots, \mathfrak{b}^{k_2})$; 3) $E(\mathfrak{b}^1, \ldots, \mathfrak{b}^q) \subsetneq E$; 4) $E \subsetneq K_{q-1}$; 5) $T \subsetneq K_0$; 6) $K_q \subsetneq FK \subsetneq K_0$; 7) $K_q \subsetneq E$.*

Обзор оценок величины $L_C(n)$ для различных классов в случае $q = 2$ можно найти в [1,2]. В работе [3] для простого q приведены следующие оценки: $\frac{q-1}{q}q^n \lesssim L_{K_q \cap T}(n) \leqslant \frac{q}{q+1}q^n$. В работе [4] приведена оценка $L_{K_q}(n) \leqslant \frac{q-1}{q-q^{1-q}}q^n$.

Теорема 3. 1) *Для любых сильно линейно независимых операторов* $\mathfrak{b}^1, \ldots, \mathfrak{b}^q$ *выполняется* $L_{E(\mathfrak{b}^1,\ldots,\mathfrak{b}^q)}(n) = \frac{q-1}{q}q^n$; 2) $L_{FK}(n) = \frac{1}{q}q^n$.

Другие классы пучков при $q > 2$ исследовались, например, в работах [5, 6, 7].

Работа выполнена при поддержке РФФИ (проект № 13-01-00621).

Список литературы

[1] Baluck A. S., Vinokurov S. F. Classes of Operator Forms // 5^{th} International Workshop on Boolean Problems. — Freiberg, Germany, 2002. — P. 217–224.

[2] Избранные вопросы теории булевых функций / Под ред. Винокурова С. Ф. и Перязева Н. А. — М.: Физматлит, 2001. — 192 с.

[3] Селезнева С. Н. О сложности задания k-значных функций обобщенно-поляризованными полиномами // Дискретная математика. — 2009. — Т. 21, вып. 4. — С. 20–29.

[4] Балюк А. С. О верхней оценке сложности задания квазиполиномами функций над конечными полями // Известия Иркутского государственного университета. Серия «Математика» — 2014. — Т. 10. — С. 3–12.

[5] Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

[6] Зинченко А. С., Пантелеев В. И. Полиномиальные операторные представления функций k-значной логики // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, № 3. — С. 13–26.

[7] Башов М. А., Селезнева С. Н. О длине функций k-значной логики в классе полиномиальных нормальных форм по модулю k // Дискретная математика. — 2014. — Т. 26, вып. 3. — С. 3–9.

Истоки и неподвижные точки в дискретных динамических системах циркулянтного типа

Батуева Цындыма Чимит-Доржиевна

Институт математики им. С. Л. Соболева СО РАН, e-mail: batueva@math.nsc.ru, tsyn.batueva@gmail.com

Введение

Данная работа посвящена свойствам дискретных динамическоих систем введеных в работе [4]. Такие системы являются, например, моделями регуляторного контура генной сети [3, 5]. Вершины графа-носителя соответствуют различным химическим веществам в клетке. Метки вершин характеризуют

концентрации веществ, а контуры функционального графа описывают периодические процессы.

Пусть $G = (V, D)$ — ориентированный граф с множеством вершин $V = \{0, 1, \ldots, n-1\}$ (граф-носитель). Рассмотрим следующую дискретную динамическую систему. В каждый момент времени вершины графа G помечены элементами $v_0, v_1, \ldots, v_{n-1}$ из конечного поля F_q порядка q. Набор $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1}) \in F_q^n$ называется *состоянием системы*. В следующий момент времени (такт работы системы) состояние системы пересчитывается под действием отображения

$$A_{\varphi,q} : F_q^n \to F_q^n,$$

где $\varphi = (f_0, f_1, \ldots, f_{n-1})$. Каждая вершина приобретает новую метку, равную значению функции $f_i : F_q^k \to F_q$, где $k < n$, аргументами которой являются значения старых меток, из которых выходят дуги в вершину i.

Функциональным графом $G_{\varphi,q}$ называется ориентированный граф, вершинами которого являются элементы из F_q^n, а дуги соединяют вершины $\widetilde{v}$ и $\widetilde{u}$ тогда и только тогда, когда $A_{\varphi,q}(\widetilde{v}) = \widetilde{u}$. Структура таких графов представляет собой несколько компонент связности. Каждая компонента состоит из конечного числа деревьев, ориентированных к корням, а корни соединены в контур.

Состояние системы $\widetilde{u}$ называется *рабочим*, если существует состояние $\widetilde{v}$ такое, что $A_{\varphi,q}(\widetilde{v}) = \widetilde{u}$. В противном случае состояние называется *истоком*.

Неподвижные точки и истоки

Для описания неподвижных точек функционального графа в [1] был введен вспомогательный граф $P_{f,q}$, отдаленно напоминающий графы де Брёйна.

Пусть $f : F_q^k \to F_q$. Ориентированным графом $P_{f,q}$ обозначается граф, вершинами которого являются элементы поля F_q^k, причем дуга идет из вершины $(v_0, v_1, \ldots, v_{k-1})$ в вершину $(v_1, v_2, \ldots, v_k)$ тогда и только тогда, когда $f(v_0, \ldots, v_{k-1}) = v_k$.

В работе [2] был предложен алгоритм нахождения всех неподвижных точек отображения $A_{f,q}$ через граф $P_{f,q}$.

Обозначение $\widetilde{v} = \widetilde{\alpha}^{n/s}$, если n кратно s, означает n/s раз конкатенацию слова $\widetilde{\alpha} \in F_q^s$.

Теорема 1 [2]. *Состояние $\widetilde{v} = (v_0, v_1, \ldots, v_{l-1})^{n/l}$ с минимальным периодом l является неподвижной точкой отображения $A_{f,q}$ тогда и только тогда, когда граф $P_{f,q}$ содержит простой цикл $\widetilde{u}^0, \ldots, \widetilde{u}^{l-1}$, где вершины*

$$\widetilde{u}^i = \left(v_i, v_{i+1(\mathrm{mod}\ \ l)}, \ldots, v_{i+k-1(\mathrm{mod}\ \ l)}\right)$$

для $i \in \{0, 1, \ldots, l-1\}$.

Для описания истоков раскрасим вершины графа де Брёйна размерности k значениями функции f от этих вершин. Обозначим граф $GB_{f,q}$.

Теорема 2. *Пусть $f : F_q^k \to F_q$. Состояние $\widetilde{v} \in F_q^n$ является истоком для отображения $A_{f,q}$ тогда и только тогда, когда не существует цикла в графе $GB_{f,q}$ раскрашенного последовательностью значений состояния $\widetilde{v}$.*

Данные теоремы облегчают описание неподвижных точек и истоков дискретных динамических систем циркулянтного типа с произвольной q-значной функцией в вершинах сети.

Работа выполнена при поддержке РФФИ (проект № 14–01–00507).

Список литературы

[1] Батуева Ц. Ч.-Д. Свойства генных сетей циркулянтного типа с пороговыми функциями // Прикладная дискретная математика. Приложение. — 2013. — № 6. — С. 72–73.

[2] Батуева Ц. Ч.-Д. Дискретные динамические системы циркулянтного типа с пороговыми функциями в вершинах // Дискретный анализ и исследование операций. — 2014. — № 4. — С. 25–32.

[3] Демиденко Г. В., Колчанов Н. А., Лихошвай В. А., Матушкин Ю. Г., Фадеев С. И. Математическое моделирование регулярных контуров генных сетей // Журн. вычисл. математики и мат. физики. — 2004. — Т. 44, № 12. — С. 2276–2295.

[4] Евдокимов А. А., Пережогин А. Л. Дискретные динамические системы циркулянтного типа с линейными функциями в вершинах сети // Дискретный анализ и исследование операций. — 2011. — Т. 18, № 3. — С. 39–48. (Перевод: Evdokimov A. A., Perezhogin A. L. Discrete dynamical systems of a circulant type with linear functions at vertices of network // J. Appl. Industr. Math. — 2012. — V. 6, N 2. — P. 160–166.)

[5] Лихошвай В. А., Голубятников В. П., Демиденко Г. В., Евдокимов А. А., Матвеева И. И., Фадеев С. И. Теория генных сетей // Системная компьютерная биология. — Новосибирск: Изд-во СО РАН, 2008. — С. 397–480.

Существование асимптотики стандартного вида для сложности реализации функций алгебры логики клеточными и планарными схемами в некоторых базисах

Белышов Михаил Владимирович

Московский государственный университет имени М. В. Ломоносова, e-mail: belyshovmv@gmail.com

Предметом исследования является сложность реализации функций алгебры логики (ФАЛ) в классе планарных схем и схем из клеточных элементов. Рассматривается вопрос установления в явном виде асимптотики функции Шеннона сложности указанных схем в некоторых базисах, или классах базисов.

Схема из клеточных элементов (СКЭ) строится из элементов базиса $Б$, каждый из которых представляет собой единичный квадрат и является либо функциональным элементом, который реализует ФАЛ, либо коммутационным элементом, который передает значения булевых переменных, поданных на его

вход (входы) на выходы (выход) данного элемента. В работе будут рассматриваться двуместные базисы, функциональные и коммутационные элементы которых показаны на рис. 1 и 2 соответственно, где $f_1(x_1, x_2), ..., f_k(x_1, x_2)$ — двуместные ФАЛ, образующие полную в P_2 систему.

Рис. 1. Функциональные элементы.

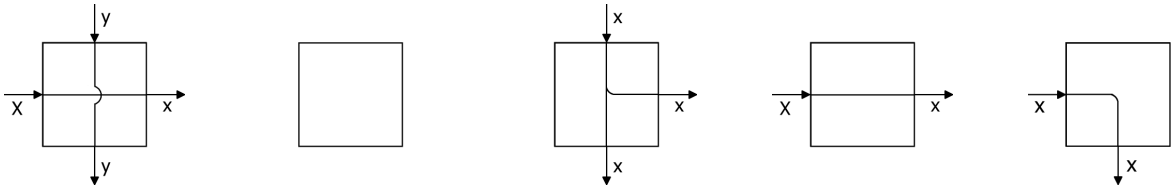

Рис. 2. Коммутационные элементы.

Схема из клеточных элементов представляет собой плоскую прямоугольную решетку, составленную из единичных квадратов, в каждой клетке которой расположен один из элементов базиса, повернутый, возможно, на угол $\pi k/2\,(k = 0, 1, 2, 3)$. Соединение элементов схемы между собой осуществляется через совпавшие входы и выходы данных элементов. При этом, с логической точки зрения, СКЭ представляет собой обычную (см., например, [4]) схему из функциональных элементов (СФЭ).

Планарная схема (ПС) над базисом *Б* представляет собой обычную СФЭ над базисом *Б*, являющуюся плоским графом, на границе внешней грани которого находятся все входы и выходы данной схемы. Предполагается, что класс СКЭ и класс ПС над рассматриваемым базисом *Б* ФАЛ, полны в том смысле, что в них можно реализовать произвольную систему ФАЛ.

Если $l(S)$ и $h(S)$ — соответственно длина и высота СКЭ S, то ее сложность $A(S)$ положим равной площади S, то есть $A(S) = h(S) \cdot l(S)$. Сложность $A_Б(f)$ реализации произвольной ФАЛ f в классе СКЭ над базисом *Б* — это наименьшее из чисел $A(S)$, где минимум берется по всем СКЭ S над базисом *Б*, которые реализуют ФАЛ f. Функция Шеннона $A_Б(n)$ — это наибольшее из чисел $A_Б(f)$, где максимум берется по всем ФАЛ, зависящим от переменных $x_1, x_2, \ldots, x_n$.

Сложность $\mathcal{L}(S)$ ПС S равна числу ее функциональных элементов. При этом для класса ПС над базисом *Б* сложность $\mathcal{L}_Б(f)$ ФАЛ f и функция Шеннона $\mathcal{L}_Б(n)$ вводится аналогично тому, как это делалось для СКЭ.

Полное описание СКЭ см., например, в [1], СФЭ — в [4] и [5], а ПС в [6].

Кравцовым С.С. в работе [3] для одного конкретного базиса $Б'$ установлены следующие асимптотические* оценки функции Шеннона для их площади:

$$\frac{1}{4}\cdot 2^n \lesssim A_{Б'}(n) \lesssim \frac{9}{2}\cdot 2^n.$$

Кроме того, Альбрехтом А. в работе [1] было установлено, что в этом же базисе $Б'$ СКЭ справедливо следующее асимптотическое равенство

$$A_{Б'}(n) \sim \sigma_{Б'} 2^n,$$

хотя значение константы $\sigma_{Б'}$ в явном виде указано не было.

Грибок С. В. в работе [2] предложил базис $Б''$ схем из клеточных элементов, в котором функция Шеннона асимптотически равна 2^n.

В данной работе получены следующие результаты.

Теорема 1. *Для класса СКЭ и класса ПС над произвольным базисом Б рассматриваемого типа существуют константы $\sigma_Б > 0$ и $\tau_Б > 0$ соответственно, такие, что*

$$A_Б(n) \sim \sigma_Б 2^n, \tag{1}$$

$$\mathcal{L}_Б(n) \sim \tau_Б 2^n. \tag{2}$$

Теорема 2. *Пусть Б — произвольный двуместный неизбыточный базис СКЭ, показанный на рис. 3, функциональные элементы которого могут реализовать как двуместные, так и одноместные ФАЛ. Тогда верны следующие асимптотические неравенства*

$$\frac{1}{\log_2 6}\cdot 2^n \lesssim A_Б(n) \lesssim 9\cdot 2^n. \tag{3}$$

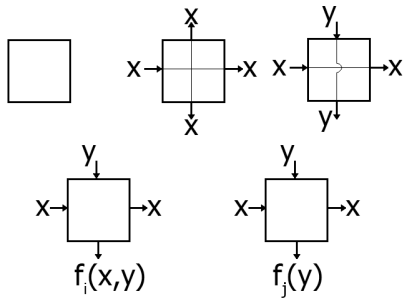

Рис. 3. Общий вид базиса для теоремы 2.

Список литературы

[1] Альбрехт А. О схемах из клеточных элементов // Проблемы кибернетики. — М.: Наука, 1975. — Вып. 33 — С. 209–214.

*Асимптотическое неравенство $a(n) \lesssim b(n)$, $n = 1, ...$, означает, что $\overline{\lim\limits_{n\to\infty}}\left(\frac{a(n)}{b(n)}\right) \le 1$, а асимптотическое равенство $a(n) \sim b(n)$ равносильно выполнению неравенств $a(n) \lesssim b(n)$ и $b(n) \lesssim a(n)$.

[2] Грибок С. В. Об одном базисе для схем из клеточных элементов // Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. — 1999. — № 4. — С. 36–39.

[3] Кравцов С. С. О реализации функций алгебры логики в одном из классов схем из функциональных и коммутационных элементов // Проблемы кибернетики. — М.: Наука, 1967. — Вып. 19. — С. 285–292.

[4] Ложкин С. А. Лекции по основам кибернетики. — М.: МАКС Пресс, 2004.

[5] Лупанов О. Б. Асимптотические оценки сложности управляющих систем // — М.: Издательство МГУ, 1984.

[6] Wegener I. The Complexity of Boolean Functions. — Wiley, 1987.

Свойства f–многочленов Эйлера, связанных со статистикой exc на перестановках

Бондаренко Леонид Николаевич[1], **Шарапова Марина Леонидовна**[2]

[1] Пензенский государственный университет, e-mail: leobond5@mail.ru

[2] Московский государственный университет имени М. В. Ломоносова, e-mail: msharapova@list.ru

Статистика $\mathrm{exc}_r(\sigma) = \#\{i \in [n] : \sigma_i \geq i + r\}$ описывает число превышений со смещением $r = 0, 1, \ldots, n$ на перестановке $\sigma = \sigma_1 \ldots \sigma_n \in S_n$ над алфавитом $[n] = \{1, \ldots, n\}$ (при использовании $r = 0$ индекс r будет опускаться).

Многочлен $A_{n,r}(z) = \sum_{k=0}^{n-r} A_{n,r,k}\, z^k$, где $A_{n,r,k} = \#\{\sigma \in S_n : \mathrm{exc}_r(\sigma) = k\}$, является многочленом попаданий треугольной доски с катетами $n - r$ и выражается через перманент по формуле $A_{n,r}(z) = \mathrm{per}(z_{ij}^{(r)})_{i,j=1}^{n}$, в которой элементы матрицы $z_{ij}^{(r)} = 1$ при $j - i < r$ и $z_{ij}^{(r)} = z$ при $j - i \geq r$, а коэффициенты $A_{n,r,k}$ удовлетворяют при $A_{r,r,k} = \delta_{0k}$, где δ_{ij} — символ Кронекера, соотношению [1]

$$A_{n,r,k} = (r + k)A_{n-1,r,k} + (n - r - k + 1)A_{n-1,r,k-1},\ n > r,\ k \in \mathbb{Z}. \quad (1)$$

С помощью (1) при $A_{r,r}(z) = r!$ получается рекуррентная формула

$$A_{n,r}(z) = ((n - r)z + r)A_{n-1,r}(z) + z(1 - z)D_z A_{n-1,r}(z),\ n > r. \quad (2)$$

z–Преобразование $Z\{f(t)\} = \sum_{k=0}^{\infty} f(k)z^k = (1 - z)^{-(n+1)}P(z)$ функции $f(t)$ определяет f–эйлеров многочлен $P(z)$ степени не выше n, а его коэффициенты называются f–эйлеровыми числами [2]. Так, $Z\left\{\binom{t+n-k}{n}\right\} = \frac{z^k}{(1-z)^{n+1}}$ и $P(z)$ при $f(t) = t^n$ является обычным многочленом Эйлера $A_n(z)$.

Использование рекуррентного соотношения (1) позволяет получить аналог тождества Ворпицкого [3] $r!t^{n-r}\binom{t}{r} = \sum_{k=0}^{n-r} A_{n,r,k}\binom{t+n-r-k}{n}$ и его обращение $A_{n,r,k} = r!\sum_{i=0}^{k}(-1)^{k-i}\binom{n+1}{k-i}(r + i)^{n-r}\binom{r+i}{r}$, которые составляют пару взаимно обратных соотношений Эйлера, т. е. $A_{n,r}(z)$ — f–эйлеров многочлен.

Записывая с помощью выражения (2) обобщенную формулу Родрига [3] $r!A_{n,r}(z) = k(z)^{-(n-r)}w(z)^{-1}H^{n-r}w(z)$, где $H = zD_z$, $k(z) = (1 - z)^{-1}$,

$w(z)=z^r(1-z)^{-(r+1)}$, по методике работы [3] можно получить выражение для производящей функции

$$A_r(z,u)=\sum_{m=0}^{\infty}A_{m+r,\,r}(z)\frac{u^m}{m!}=\frac{r!w(ze^{k(z)^{-1}u})}{w(z)}=r!\left(\frac{1-z}{1-ze^{(1-z)u}}\right)^{r+1}e^{r(1-z)u},$$

т. е. $A_r(z,u)=r!A(z,u)^{r+1}e^{r(1-z)u}$, а также следующее разложение в J–дробь $r!^{-1}\sum_{m=0}^{\infty}A_{m+r,\,r}(z)u^m=J_u[\kappa_k(z),\lambda_k(z):(0,\infty)]$, в котором параметры определены выражениями $\kappa_k(z)=(k+1)z+k+r$, $\lambda_k(z)=(k+1)(k+r+1)z$ и непрерывная J–дробь записывается в соответствующей стандартной форме $J_u[\kappa_k(z),\lambda_k(z):(0,\infty)]=\frac{1}{1-\kappa_0(z)u}-\frac{\lambda_0(z)u^2}{1-\kappa_1(z)u}-\frac{\lambda_1(z)u^2}{1-\kappa_2(z)u}-\ldots$.

Для s–й декартовой степени всех перестановок $\sigma^{(j)}=\sigma_1^{(j)}\ldots\sigma_n^{(j)}\in S_n$ над алфавитом $[n]$ определим следующую статистику превышения $\mathrm{exc}_r^{(s)}(\sigma^{(1)},\ldots,\sigma^{(s)})=\#\{i\in[n]:(\sigma_i^{(1)}\geq i+r)\&\ldots\&(\sigma_i^{(s)}\geq i+r)\}$. Производящий многочлен для $\mathrm{exc}_r^{(s)}$ имеет вид $A_{n,r}^{(s)}(z)=\sum_{k=0}^{n-r}A_{n,\,r,\,k}^{(s)}z^k$, а его коэффициенты $A_{n,\,r,\,k}^{(s)}=\#\{(\sigma^{(1)},\ldots,\sigma^{(s)})\in S_n^s:\mathrm{exc}_r^{(s)}(\sigma^{(1)},\ldots,\sigma^{(s)})=k\}$.

При изучении свойств многочленов $A_{n,r}^{(s)}(z)$ будем использовать следующее обобщение центральных факториальных чисел $T_{n,\,k}^{(s)}$ [4]

Определение 1. $T_{0,\,k}^{(s)}=\delta_{0k},\ T_{n,\,k}^{(s)}=T_{n-1,\,k-1}^{(s)}+k^sT_{n-1,\,k}^{(s)},\ n\geq 1,\ k\in\mathbb{Z}$.

Из определения 1 для многочлена $T_n^{(s)}(x)=\sum_{k=1}^{n}T_{n,\,k}^{(s)}x^k$ можно получить рекуррентное выражение $T_0^{(s)}(x)=1,\ T_n^{(s)}=xT_{n-1}^{(s)}(x)+(xD_x)^sT_{n-1}^{(s)}(x),\ n\geq 1$ и производящую функцию $\sum_{m=0}^{\infty}T_{m+k,\,k}^{(s)}u^m=((1-u)(1-2^su)\ldots(1-k^su))^{-1}$, обобщающую случай $s=1$ в [1].

Теорема 1. а) $T_{n+1,\,n+1-k}^{(s)}$ *соответствует для статистики* $\mathrm{exc}_r^{(s)}$ *определенному числу способов размещения* k *взаимно неатакующих ладей на* s *треугольных досках с катетами* n*, причем отвечающий этому ладейный многочлен* $L_n^{(s)}(x)=x^{n+1}T_{n+1}^{(s)}(x^{-1})$.

б) *Для статистики* $\mathrm{exc}_r^{(s)}$ *имеем обобщение соотношений из* [1]

$$L_{n,\,r}^{(s)}(x)=\sum_{k=0}^{n-r}T_{n-r+1,\,n-r+1-k}^{(s)}x^k,\ A_{n,\,r}^{(s)}(z)=\sum_{k=0}^{n-r}T_{n-r+1,\,n-r+1-k}^{(s)}((n-k)!)^s(z-1)^k.$$

Доказательство а) базируется на определении 1, а б) следует из а).

Производящая функция $2u(e^u+1)^{-1}=u+\sum_{n=1}^{\infty}(-1)^nG_{2n}u^{(2n)}/2n!$ задает числа Дженокки $G_{2n}=G_{2n}^{(2)}$, а их обобщение $G_{2n}^{(s)}$, $n\geq 1$, $s\geq 1$ определим аналогично [4] равенством $G_{2(n+2)}^{(s)}=B_n^{(s)}(1)$. Многочлен $B_n^{(s)}(t)=H^n1$ степени $(s-1)n$ имеет вид обобщенной формулы Родрига с оператором $H=\Delta t^s$, где $\Delta-$разностный оператор, причем $B_n^{(s)}(0)=B_{n-1}^{(s)}(1)=G_{2(n+1)}^{(s)}$, а эти числа связаны с $T_{n,\,k}^{(s)}$ выражением $G_{2(n+1)}^{(s)}=\sum_{k=1}^{n}(-1)^{n-k}(k!)^sT_{n,\,k}^{(s)}$ [4].

Определение 2. Зададим обобщенные многочлены Ганди–Карлитца $C_n^{(s)}(t)$ степени $n-1$ соотношением

$$tC_n^{(s)}(t) = \sum_{k=1}^{n}(-1)^{n-k}(k!)^s T_{n,k}^{(s)} \binom{t+k-1}{k}. \qquad (3)$$

Определение 2 мотивировано тем, что в [5] рассматривались полиномы $C_n^{(2)}(t) = B_{n-1}^{(2)}(t)$, связанные с многочленами Ганди, причем из (3) следует, что $C_n^{(1)}(t) = t^{n-1}$ и $G_{2(n+1)}^{(s)} = C_n^{(s)}(1)$. По методике работы [3] для соответствующей производящей функции можно построить J–дробь $\sum_{n=0}^{\infty} B_n^{(2)}(t)u^m = J_u[\kappa_k(t), \lambda_k(t) : (0,\infty)]$, где $\kappa_k(t) = (k+1)(2t+2k+1)$, $\lambda_k(t) = (k+1)(k+2)(t+k+1)^2$, что дает при $t=0$ и $t=1$ аналогичные разложения, связанные с числами Дженокки.

Теорема 2. $Z\{tC_n^{(s)}(t)\} = (1-z)^{-(n+1)}A_n^{(s)}(z)$ и справедливы следующие взаимно обратные соотношения Эйлера

$$tC_n^{(s)}(t) = \sum_{k=1}^{n} A_{n,k}^{(s)} \binom{t+n-k}{n}, \; A_{n,k}^{(s)} = \sum_{i=1}^{k}(-1)^{k-i}\binom{n+1}{k-i} iC_n^{(s)}(i).$$

При доказательстве теоремы 2 используется теорема 1, б) и выражение (3). В частности, теорема 2 дает еще одну комбинаторную интерпретацию обобщенных чисел Дженокки – $G_{2(n+1)}^{(s)} = A_{n,1}^{(s)}$.

Работа выполнена при поддержке РФФИ (проект № 14-01-00273).

СПИСОК ЛИТЕРАТУРЫ

[1] Риордан Дж. Введение в комбинаторный анализ. — М.: ИЛ, 1963. — 288 с.

[2] Стенли Р. Перечислительная комбинаторика. — М.: Мир, 1990. — 440 с.

[3] Бондаренко Л. Н., Шарапова М. Л. Применение обобщенной формулы Родрига в комбинаторном анализе // Известия высших учебных заведений. Поволжский регион. — 2011. — № 4. — С. 44–57.

[4] Domaratzki M. Combinatorial interpretations of a generalization of the Genocchi numbers // Journal of integer sequences. — 2004. — V. 7. — Article 04.3.6.

[5] Carlitz L. Explicit formulas for the Dumont–Foata polynomial // Discrete Mathematics. — 1980. — V. 30, N 3. — P. 211–225.

Критерии полноты аксиоматик зависимостей в табличных базах данных

Буй Дмитрий Борисович[1], **Пузикова Анна Валентиновна**[2]

[1] Киевский национальный университет имени Тараса Шевченко, e-mail: buy@unicyb.kiev.ua

[2] Киевский национальный университет имени Тараса Шевченко, e-mail: anna_inf@mail.ru

В предыдущих работах авторов приведены доказательства полноты для аксиоматики функциональных зависимостей (ФЗ) [1] и аксиоматики многозначных зависимостей (МЗЗ) [2], которые соответствуют стандартным требованиям

строгости и полноты математического доказательства [3], а именно: введены отношения семантического ($\models$) и синтаксического ($\vdash$) следований и показано их совпадение.

Анализ этих доказательств показывает, что они проведены в предположении: $|D| \geq 2$ и $|R| \geq 2$, то есть универсальный домен, использующийся при интерпретациях, содержит не менее 2 элементов, а схема R (выступающая параметром всех построений, так как рассматриваются только таблицы со схемами — подмножествами R) — как минимум 2 атрибута. Для полноты картины естественно рассмотреть совпадение отношений $\models$ и $\vdash$ в случаях $|D| < 2$ или $|R| < 2$.

Для аксиоматики ФЗ указанная задача была рассмотрена в работе [4].

Зависимость совпадения отношений синтаксического и семантического следований при разных значениях мощностей множеств R и D для аксиоматики ФЗ отображена в табл. 1. Символ “+” (соответственно “–”) в ячейке означает, что при указанных условиях отношения $\models$ и $\vdash$ совпадают (не совпадают соответственно).

Таблица 1. *Все варианты мощностей множеств R и D для аксиоматики ФЗ.*

	$\|R\| = 0$	$\|R\| = 1$	$\|R\| \geq 2$
$\|D\| = 0$	$+$	$-$	$-$
$\|D\| = 1$	$+$	$-$	$-$
$\|D\| \geq 2$	$+$	$+$	$+$

Ввиду заполнения табл. 1 имеем следующий результат.

Теорема 1 (Критерий полноты аксиоматики Армстронга для ФЗ). *Отношения семантического $\models$ и синтаксического $\vdash$ следований для аксиоматики ФЗ совпадают тогда и только тогда, когда $|D| \geq 2$ или $|R| = 0$.*

При рассмотрении МЗЗ будем говорить о двух аксиоматиках:

- аксиоматике МЗЗ, которая включает аксиому рефлексивности и три правила вывода: полноты, пополнения и транзитивности [5];
- аксиоматике МЗЗ и ФЗ, которая помимо аксиомы рефлексивности и правил вывода для ФЗ, а также указанных выше аксиомы и правил вывода для МЗЗ, включает в себя два общих правила для ФЗ и МЗЗ [5].

Зависимость совпадения отношений синтаксического и семантического следований в случаях $|D| < 2$ или $|R| < 2$ для аксиоматики МЗЗ указана в табл. 2. Обозначения те же, что и для табл. 1.

Таблица 2. *Все варианты мощностей множеств R и D для аксиоматики МЗЗ.*

	$\|R\| = 0$	$\|R\| = 1$	$\|R\| \geq 2$
$\|D\| = 0$	$+$	$+$	$-$
$\|D\| = 1$	$+$	$+$	$-$
$\|D\| \geq 2$	$+$	$+$	$+$

Анализ заполнения табл. 1 и 2 для аксиоматик ФЗ и МЗЗ позволяет предположить, что условия совпадения отношений $\models$ и $\vdash$ для аксиоматики ФЗ и МЗЗ такие же, как и для аксиоматики ФЗ. Это подтверждается строгим доказательством, результат которого приведен в табл. 3. Обозначения те же, что и для табл. 1.

Таблица 3. *Все варианты мощностей множеств R и D для аксиоматики ФЗ и МЗЗ.*

	$\lvert R\rvert = 0$	$\lvert R\rvert = 1$	$\lvert R\rvert \geq 2$
$\lvert D\rvert = 0$	$+$	$-$	$-$
$\lvert D\rvert = 1$	$+$	$-$	$-$
$\lvert D\rvert \geq 2$	$+$	$+$	$+$

Ввиду заполнения табл. 2 и 3 имеем следующие основные результаты.

Теорема 2 (Критерий полноты для аксиоматики МЗЗ). *Отношения семантического $\models$ и синтаксического $\vdash$ следований для аксиоматики МЗЗ совпадают тогда и только тогда, когда $|R| \leq 1$ или $|R| \geq 2$ и при этом $|D| \geq 2$.*

Теорема 3 (Критерий полноты для аксиоматики МЗЗ и ФЗ). *Отношения семантического $\models$ и синтаксического $\vdash$ следований для аксиоматики МЗЗ и ФЗ совпадают тогда и только тогда, когда $|D| \geq 2$ или $|R| = 0$.*

Одна из следующих естественных задач — установление взаимной независимости компонент (т.е. аксиом и правил вывода) рассмотренных аксиоматик.

Полученные же результаты составляют фрагмент математической теории нормализации и целостности табличных баз данных.

Список литературы

[1] Буй Д. Б., Пузикова А. В. Полнота аксиоматики Армстронга // Вестник Киевского национального университета им. Т. Шевченко. Серия: физ.-мат. науки. — 2011. — № 3. — С. 103–108. (На украинском языке).

[2] Буй Д. Б., Пузикова А. В. Аксиоматика многозначных зависимостей табличных баз данных: полнота и её критерий // Theoretical and applied aspects of program systems development — TAAPSD'2014 (Украина, Киев, 15–17 декабря 2014 года). — С. 35–43. (На украинском языке).

[3] Линдон Р. Заметки по логике. — М.: Мир, 1968. — 128 с.

[4] Буй Д. Б., Пузикова А. В. Критерий полноты аксиоматики Армстронга // Theoretical and applied aspects of program systems development — TAAPSD'2011 (Украина, Ялта, 19-23 сентября 2011 года). — С. 30–34. (На украинском языке).

[5] Beeri C., Fagin R., Howard J. A complete axiomatization for functional and multivalued dependencies // Proceedings of the ACM-SIGMOD Conference, August 3–5, 1977, Toronto, Canada. — P. 47–61.

Субэкспоненциальные алгоритмы распознавания сохранения некоторых центральных предикатов функциями, заданными полиномами

Бухман Антон Владимирович

Московский государственный университет имени М. В. Ломоносова, e-mail: antvbx@gmail.com

Введение

Пусть $E_k = \{0, \dots, k-1\}$. Произвольное отображение $f : E_k^n \to E_k$ называется *функцией k-значной логики*. Будем рассматривать задание функций k-значной логики в виде полиномов. *Мономом* над переменными $x_1, \dots, x_n$ назовём 1 или любое выражение вида $x_{i_1}^{j_1} \dots x_{i_l}^{j_l}$, где $l \geq 1, 1 \leq i_1 < \dots < i_l \leq n, 1 \leq j_1, \dots, j_l \leq k-1$. *Полиномом* назовём сумму по модулю k конечного числа различных мономов с ненулевыми коэффициентами из E_k или просто 0. *Длиной* полинома называется число его слагаемых. Любая k-значная функция задаётся полиномом по модулю k, причём однозначно тогда и только тогда, когда k — простое число. Далее в работе будем предполагать, что k — простое число [1].

Предикат называется *центральным* [2], если он

1. тотально симметричен
2. тотально рефлексивен
3. обладает центром.

Центральные предикаты (или предикаты семейства C) интересны тем, что они описывают предполные классы в k-значной логике [2].

Пусть задан некоторый центральный предикат. Рассмотрим следующую задачу: на вход алгоритма подаётся полином некоторой функции k-значной логики, требуется определить сохраняет ли эта функция двухместный центральный предикат. В качестве исполнителя алгоритма будем рассматривать RAM-машину. Заметим, что полином длины l от n переменных будет записываться словом длины nl.

Отметим, что полиномиальные алгоритмы для распознавания сохранения функциями, заданными полиномами, предикатов из других семейств были рассмотрены в работах С. Н. Селезневой [3,4].

Заметим, что в общем случае в описанной алгоритмической модели проверка того, что функция, заданная полиномом, сохраняет заданный центральный предикат, может занять экспоненциальное время.

Основной результат

В данной работе показано, как можно ограничить перебор и снизить сложность до субэкспоненциальной. *Расстоянием* (по Хэммингу) между парой наборов из E_k^n назовём количество различных компонент в них. Идея состоит в том, чтобы перебирать близкие в смысле расстояния Хэмминга наборы.

Пусть функция не сохраняет предикат, тогда выберем наборы $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in E_k^n$, на которых условие сохранения

предиката нарушается, причём будем их выбирать так, что расстояние между ними минимальное (среди всех пар наборов, на которых условие сохранения предиката функцией нарушается). Тогда нетрудно показать, что для любого набора $\gamma \in E_k^n$ такого, что $\gamma_i \in \{\alpha_i, \beta_i\}$ и $\gamma \neq \alpha, \gamma \neq \beta$ верно, что $f(\gamma) \in C$.

Будем говорить, что функция f удовлетворяет на наборах $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n)$ условию (*) если: $f(\alpha) \neq 0, f(\beta) \neq 0$ и для любого набора $\gamma \in E_p^n$ такого, что $\gamma_i \in \{\alpha_i, \beta_i\}$ и $\gamma \neq \alpha, \gamma \neq \beta$ верно, что $f(\gamma) = 0$.

Лемма 1. *Пусть k — простое число, если функция k-значной логики f удовлетворяет условию (*) для некоторых наборов α, β то верно что длина полинома функции f больше либо равна $2^{\rho/2-1}$, где ρ — расстояние между наборами α, β.*

Теорема. *Пусть k — простое число. Для любого двухместного центрального предиката ρ существует RAM-машина, которая по записи полинома функции k-значной логики, проверяет, сохраняет ли эта функция предикат ρ, причём сложность работы этой машины равна $2^{O(\log^2(N))}$, где $N = nl$, и l — длина полинома, а n — число переменных.*

Доказательство.

Пусть $C = \{c_1, \ldots, c_q\}$ — центр предиката ρ. Если для функции $F = (f - c_1) \ldots (f - c_q)$ выполнено условие (*) на некоторых наборах, и на этих наборах значения функции f не удовлетворяют предикату ρ, то функция f не сохраняет предикат ρ.

Положим $s = 2(\log(l) + 1)$. Идея алгоритма состоит в том, чтобы перебирать всевозможные наборы, которые удовлетворяют предикату и находятся на расстоянии не более s. Заметим, что по лемме 1, если существуют наборы, на которых нарушается предикат, то обязательно найдётся такая пара наборов на расстоянии меньше s.

Приведём описание алгоритма.

Проводим перебор по всевозможным числам $1 \leq i_1 < \cdots < i_s \leq n$. Для каждых $i_1, \ldots, i_s$ переберём всевозможные пары $(\alpha = (\alpha_1, \ldots, \alpha_s), \beta = (\beta_1, \ldots, \beta_s))$ такие, что $\rho(\alpha_i, \beta_i) = 1$. Рассмотрим функции f_1, f_2 от $n - s$ переменных; f_1 получается из f подстановкой вместо переменных $x_{i_1}, \ldots, x_{i_s}$ констант $\alpha_1, \ldots \alpha_s$ соответственно. А функция f_2 получается из f подстановкой вместо переменных $x_{i_1}, \ldots, x_{i_s}$ констант $\beta_1, \ldots \beta_s$ соответственно.

Проверяем полином функции $\rho(f_1, f_2)(f_1 - c_1) \ldots (f_1 - c_q)(f_2 - c_1)(f_2 - c_q)$ на тождественное равенство 0. Если не равен, то завершаем алгоритм и выдаём ответ НЕТ, функция f не сохраняет ρ.

Если алгоритм окончил работу и не выдал ответ НЕТ, то функция сохраняет предикат — выдаём ДА.

Сложность алгоритма $2^{O(\log^2(N))}$.

Работа выполнена при поддержке РФФИ (проект № 13-01-00684-а).

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2010. — 384 с.

[2] Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд-во МЭИ, 1997. — 144 с.

[3] Селезнева С. Н. Полиномиальный алгоритм распознавания свойства функций многозначных логик, представленных полиномом, сохранять рефлексивный и транзитивный предикат // Тезисы докладов XII Международной конференции "Проблемы теоретической кибернетики". — М.: МГУ, 1999. — 207 с.

[4] Селезнева С. Н. Полиномиальный алгоритм распознавания принадлежности реализованной полиномом функции k-значной логики предполным классам самодвойственных функций // Дискретная математика. — 1998. — Т. 10, № 3. — С. 64–72.

О равномерных кодах Грея

Быков Игорь Сергеевич

Новосибирский государственный университет, e-mail: patrick.no10@gmail.com

n-Мерный код Грея — это последовательность всех 2^n бинарных слов длины n такая, что два соседних слова отличаются ровно в одном символе. Альтернативным видом записи кода Грея (помимо перечисления всех слов) является переходная последовательность кода. *Переходная последовательность* кода C — это циклическое слово $\tau = (\tau_1, \tau_2, \ldots, \tau_{2^n})$ над алфавитом $\{1, 2, \ldots, n\}$ такая, что i-ое и $(i+1)$-ое слово в коде C отличаются в позиции τ_i. При изучении кодов Грея основной интерес представляет поиск кодов Грея обладающих заданными свойствами ([1]).

Рассматриваются коды Грея, обладающие свойством равномерности. Пусть $l(C)$ — такое минимальное число, что в каждом подслове переходной последовательности кода C встречаются все буквы из алфавита $\{1, 2, \ldots, n\}$. Наименьшее значение, которое параметр $l(C)$ принимает на множестве всех n-мерных кодов Грея обозначим $l(n)$. Для получения верхней оценки на параметр равномерности $l(n)$ используется конструкция, приведенная в [2].

Линейная оценка сверху для числа $l(n)$

Смежная перестановка вершин в $V(Q_n)$ — это перестановка вершин Q_n такая, что каждая вершина переходит в одну из соседних. Список смежных перестановок $\pi_1, \pi_2, \ldots, \pi_k$ и начальная вершина v задают путь в Q_n:

$$W(v; \pi_1, \pi_2, \ldots, \pi_k) = v\ v^{\pi_1}\ v^{\pi_1\pi_2} \ldots v^{\pi_1\pi_2\ldots\pi_k}.$$

Тогда потоком в Q_n, порожденным последовательностью смежных перестановок $\pi_1, \pi_2, \ldots, \pi_k$ назовем совокупность 2^n путей:

$$S(\pi_1, \pi_2, \ldots, \pi_k) = \{W(v; \pi_1, \pi_2, \ldots, \pi_k) : v \in V(Q_n)\}.$$

Мы построим код Грея в декартовом произведении $Q_a \times Q_b \cong Q_{a+b}$ из потока в Q_a и кода Грея в Q_b. Пусть (X, Y) — разбиение $V(Q_a)$ на слова четного и нечетного веса соответственно.

Пусть S — поток длины 2^b в Q_a такой, что X — орбита $\pi(S)$ ($\pi(S)$ — перестановка, порождаемая потоком на множестве $V(Q_a)$). Поток $S' = S^{2^{a-1}}$, полученный в результате конкатенации исходного потока 2^{a-1} раз, определяет замкнутый путь W в Q_a с начальной вершиной $w_0 \in X$:

$$W = W(w_0, S') = w_0, w_1, \ldots, w_{2^{a+b-1}}, w_0.$$

Пусть $Z = z_0, z_1, \ldots, z_{2^b-1}, z_0$ — код Грея в Q_b. Рассмотрим маршрут C в Q_a, который имеет следующий вид:

$$\begin{aligned} C = {} & (w_0, z_0)(w_1, z_0)(w_1, z_1)(w_2, z_1)(w_2, z_2)\ldots(w_{2^b-1}, z_{2^b-1})(w_{2^b}, z_{2^b-1}) \\ & (w_{2^b}, z_0)(w_{2^b+1}, z_0)(w_{2^b+1}, z_1)\ldots(w_{2\cdot 2^b-1}, z_{2^b-1})(w_{2\cdot 2^b}, z_{2^b-1}) \\ & (w_{2\cdot 2^b}, z_0)(w_{2\cdot 2^b+1}, z_0)(w_{2\cdot 2^b+1}, z_1)\ldots(w_{3\cdot 2^b-1}, z_{2^b-1})(w_{3\cdot 2^b}, z_{2^b-1}) \\ & (w_{3\cdot 2^b}, z_0) \\ & \ldots \\ & (w_{(2^{a-1}-1)\cdot 2^b}, z_0)(w_{(2^{a-1}-1)\cdot 2^b+1}, z_0)\ldots(w_{(2^{a-1})\cdot 2^b-1}, z_{2^b-1})(w_0, z_{2^b-1}) \\ & (w_0, z_0). \end{aligned}$$

Согласно [2], такой маршрут является гамильтоновым циклом в Q_{a+b}. Легко видеть, что $l(C) \leq 2\max\{l(S), l(Z)\}$.

Теперь перейдем к построению потока в Q_a, обладающего необходимыми свойствами: длиной 2^b и «хорошим» значением $l(S)$. Сначала докажем лемму:
Лемма 1. *Существует поток в Q_a длины $2a+2$ такой, что X — орбита $\pi(S)$, и $l(S) \leq a+2$.*

В справедливости этого утверждения легко убедиться, рассмотрев поток, порожденный последовательностью перестановок

$$\sigma_G, \sigma_G, \tau_1, \tau_2, \ldots, \tau_{a-1}, \tau_a, \tau_1, \tau_2, \ldots, \tau_{a-1}\tau_a,$$

где σ_G — перестановка, сдвигающая по циклу вершины некоторого кода Грея G в Q_a, а τ_i — перестановка, меняющая местами вершины, отличающиеся в координате i. С помощью следующей леммы мы сможем увеличивать длину полученного потока, с сохранением свойства $l(S)$.
Лемма 2. *Для любого четного целого $d \geq 2a^2+2$, существует поток S' в Q_a длины d такой, что X — орбита $\pi(S')$, и $l(S') \leq a+2$.*
Доказательство. Пусть $d = 2a+2+2t$, где $t \geq a(a-1)$. Известно, что тогда существуют неотрицательные α и β такие, что

$$t = \alpha a + \beta(a+1).$$

Рассмотрим поток $S' = ST^{2\beta}R^{2\alpha}$, где S — поток, построенный в предыдущей лемме,

$$\begin{aligned} T &= \tau_a, \tau_1, \tau_2, \ldots, \tau_{a-1}, \tau_a; \\ R &= \tau_1, \tau_2, \ldots, \tau_{a-1}, \tau_a. \end{aligned}$$

Легко заметить, что перестановки $\pi(T)$ и $\pi(R)$ оставляют вершины на местах. Значит, X — орбита $\pi(S')$.

Очевидно, длина S' равна d. Для того, чтобы показать, что $l(S') \leq a+2$, нужно рассмотреть $l(TS)$, $l(RS)$, $l(ST)$, $l(SR)$. Рассмотрев все случаи, легко убедиться, что каждое из этих значений не превосходит $a+2$. **Лемма 2 доказана.**

Следствие 1. *Если* $2a^2+2 \leq 2^b$, *то*

$$l(a+b) \leq 2\max\{a+2, l(b)\}.$$

Ранее, с использованием компьютерного перебора было показано, что $l(n) \leq 2n$ при $n \leq 16$.

Представим n в виде $n = a+b$, где

$$a = \left\lceil \frac{n}{2} \right\rceil, \qquad b = \left\lfloor \frac{n}{2} \right\rfloor.$$

Легко убедиться, что условия следствия выполняются, начиная с $n = 17$. Простая индукция доказывает теорему:

Теорема 1. *Для любого* $n \geq 3$ *справедливо неравенство*: $t(n) \leq 2n$.

Улучшение оценки

Добавляя в качестве третьего потока в лемме 2 поток $P = \tau_{a-1}, \tau_a, \tau_1, \tau_2, \ldots, \tau_{a-1}, \tau_a$ длины $a+2$, получим диофантово уравнение от трех переменных:

$$t = \alpha a + \beta(a+1) + \gamma(a+2).$$

С использованием известных результатов о неотрицательных решениях диофантовых уравнений с тремя неизвестными было доказано следующее утверждение:

Теорема 2. *Если для всех* $3 \leq n < 27$ *выполнено* $l(n) \leq n + 3\lfloor log\ n \rfloor$, *то это неравенство верно для любого* $n \geq 3$.

Список литературы

[1] Carla D. Savage. A Survey of Combinatorial Gray Codes // SIAM Review. — 1997. — V. 39, Iss. 4. — P. 605–629.

[2] Luis Goddyn, Pavol Gvozdjak. Binary Gray codes with long bit runs // The Electronic Journal of Combinatorics. — 2003. — V. 10, Research paper R27. — P. 1–10.

О циклах графов функционирования генных сетей циркулянтного типа с пороговыми функциями

Быков Игорь Сергеевич

Новосибирский государственный университет, e-mail: patrick.no10@gmail.com

В данной работе рассматривается функционирование дискретных моделей генных сетей ([1]). Как и в работе [2], рассматриваются симметрические пороговые функции в вершинах с произвольным пороговым значением T.

Состоянием генной сети назовем кортеж $(s_0, s_1, \ldots, s_{n-1})$, где $s_i \in \{0, 1, \ldots, p-1\}$. Тогда функционированием такой системы будем называть последовательное изменение состояний

$$S, A(S), A^2(S), A^3(S), \ldots,$$

где S — некоторое состояние, A — отображение, действующее на множестве всех состояний.

Отображение A задается пороговой функцией с двумя параметрами k и T следующим образом: пусть $S = (s_0, s_1, \ldots, s_{n-1})$, тогда $A(S) = (s'_0, s'_1, \ldots, s'_{n-1})$, где

$$s'_i = \begin{cases} s_i + 1, & \text{если } \sum\limits_{j=1}^{k} s_{i+j} < T \text{ и } s_i < p-1; \\ s_i - 1, & \text{если } \sum\limits_{j=1}^{k} s_{i+j} \geq T \text{ и } s_i > 0; \\ s_i, & \text{иначе.} \end{cases}$$

(Здесь и далее операции в индексах выполняются по модулю n).

В данной работе рассматривается функционирование системы при $p = 2$. В этом случае:

$$s'_i = \begin{cases} 0, & \text{если } \sum\limits_{j=1}^{k} s_{i+j} \geq T; \\ 1, & \text{иначе.} \end{cases}$$

Графом функционирования называют ориентированный граф $G(V, D)$, где V — множество всех состояний, а

$$D = \{(S_1, S_2) \mid S_1, S_2 \in V; A(S_1) = S_2\}.$$

Задачей анализа функционирования называется задача описания качественных характеристик графа функционирования по заданным параметрам n,k,T.

Одной из таких задач является изучение свойств состояний, входящих в циклы графа функционирования. Рассматривая полученные свойства, можно получать оценки на количество циклов (компонент связности) графа функционирования, а также перечислять некоторые из циклов.

Выделим среди множества всех состояний два подмножества: состояния с длинными сериями и состояния с короткими сериями.

Состояния с длинными сериями

Состояние S будем называть *состоянием с длинными сериями*, если длина каждой серии из нулей не меньше $k - T + 1$, а длина каждой серии из единиц не меньше T.

Теорема 1. *Любое состояние с длинными сериями лежит в цикле графа функционирования. Все состояния этого цикла также являются состояниями с длинными сериями.*

В силу предыдущего утверждения, подсчитав количество состояний с длинными сериями, можно получить, например, следующую оценку на количество циклов в графе функционирования:

Теорема 2. *Количество циклов в графе функционирования системы с параметрами n, k, T не менее*

$$1 + \sum_{i=1}^{\left\lfloor \frac{n}{k+1} \right\rfloor} \widetilde{P}(n - (k-1)i, 2i).$$

где $\widetilde{P}(a, b)$ — число циклических разбиений a на b слагаемых.

Состояния с короткими сериями

Состояние S будем называть *состоянием с короткими сериями*, если длина каждой серии из нулей не больше $k - T$, а длина каждой серии из единиц не больше $T - 1$.

Теорема 3. *Если состояние лежит в цикле графа функционирования, то оно является либо состоянием с длинными сериями, либо состоянием с короткими сериями.*

Обозначим вес состояния (количество ненулевых компонент) как $W(S)$.

Состояния с короткими сериями в системах с большими параметрами можно строить из подходящих систем с меньшими параметрами, используя одну из следующих двух конструкций.

Теорема 4. *Пусть имеется q систем. S_i — состояние с длинными сериями в системе с параметрами n_i, k_i, T_i и отображением A_i. Тогда если для некоторых k и T и любого $0 \le j \le q - 1$ выполняются все условия:*

$$k = k_j + \sum_{i=0}^{q-1} n_i - n_j, \quad T = T_j + \sum_{i=0}^{q-1} W(S_i) - W(S_j), \quad W(S) = W(A_j(S_j)),$$

то состояние $S = S_0\ S_1\ \ldots\ S_{q-1}$ лежит в цикле графа функционирования системы с параметрами

$$n = \sum_{i=0}^{q-1} n_i, \quad k = k_0 + \sum_{i=0}^{q-1} n_i - n_0, \quad T = T_0 + \sum_{i=0}^{q-1} W(S_i) - W(S_0)$$

и является состоянием с короткими сериями.

Теорема 5. *Пусть состояние S' лежит в цикле графа функционирования системы с параметрами n', k', T' и отображением A'. И выполнено условие:*

$$W(S) = W(A'(S')),$$

тогда состояние

$$S = \underbrace{S'\ S'\ \dots\ S'\ S'}_{m}$$

лежит в цикле графа функционирования системы с параметрами

$$n = mn', \quad k = k' + ln', \quad T = T' + lW(S')$$

и является состоянием с короткими сериями для всех $0 < l < m$.

Список литературы

[1] Евдокимов А. А., Лиховидова Е. О. Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник ТГУ. — 2008. — № 2. — С. 18–21.

[2] Быков И. С. Функционирование дискретных моделей генных сетей циркулянтного типа с пороговыми функциями // Материалы IX молодежной научной школы по дискретной математике и ее приложениям. — М.: Изд-во ИПМ РАН, 2013. — С. 26–31.

Полные системы одноместных предикатов для классов Поста

Быковская Светлана Викторовна

Московский государственный университет имени М. В. Ломоносова, e-mail: bykovskaya.svetlana@gmail.com

Рассматривается множество $\mathfrak{P}(V)$ одноместных предикатов, определенных на некотором непустом конечном множестве V и принимающих значения 0 и 1 (определения см. в [1]). Пусть $\mathfrak{A}$ — некоторое конечное множество предикатов, F — некоторое множество булевых функций. Определим понятие *предикатной формулы* над $(\mathfrak{A}, F)$: 1) выражения $P(x)$, где $P(x) \in \mathfrak{A}$, являются (атомными) формулами над $(\mathfrak{A}, F)$; 2) пусть $f(x_1, \dots, x_n) \in F$ и пусть $A_1, \dots, A_n$ — формулы над $(\mathfrak{A}, F)$, тогда выражение $f(A_1, \dots, A_n)$ — формула над $(\mathfrak{A}, F)$. Замыканием системы предикатов $\mathfrak{A} \subseteq \mathfrak{P}(V)$ над системой булевых функций F (обозначение $[\mathfrak{A}]_F$) называется множество всех предикатов, которые выражаются формулами над $(\mathfrak{A}, F)$.

Система предикатов $\mathfrak{A}$ называется *полной над системой функций F*, если $[\mathfrak{A}]_F = \mathfrak{P}_V$. Известна теорема (см. [1]) о том, что система предикатов $\mathfrak{A} = \{A_1(x), ..., A_s(x)\}$ является полной над системой $F = \{\ x \vee y,\ x\&y,\ \overline{x}, x \to y\}$ тогда и только тогда, когда для любых двух различных элементов a и b множества V найдется предикат $A_i(x), 1 \leq i \leq s$, такой, что $A_i(a) \neq A_i(b)$.

В данной работе в качестве систем функций F рассматриваются произвольные системы булевых функций. Для любой системы булевых функций F получен критерий полноты произвольной системы предикатов над F.

Легко видеть, что если системы булевых функций F и H порождают один и тот же замкнутый класс, то произвольная система предикатов $\mathfrak{A}$ полна над F тогда и только тогда, когда $\mathfrak{A}$ полна над H. Поэтому в качестве систем булевых функций достаточно рассматривать только замкнутые классы.

Пусть $P(x) \in \mathfrak{P}(V)$, пусть $V' \subseteq V, V' \neq \emptyset$. Через $P(x)|_{V'}$ будем обозначать ограничение предиката $P(x)$ на множество V'. Далее, пусть $\mathfrak{A} \subseteq \mathfrak{P}(V)$, через $\mathfrak{A}|_{V'}$ будем обозначать множество всех ограничений предикатов из $\mathfrak{A}$ на множество V'.

Пусть $\mathfrak{A}$ — произвольная система предикатов, определенных на множестве V, такая, что $|V| \geq m$, где $m \geq 2$, и пусть $F \subseteq P_2$. Будем говорить, что система $\mathfrak{A}$ является $m-$*полной* над F, если для любого $V' \subseteq V$, такого, что $|V'| = m$, система $\mathfrak{A}|_{V'}$ полна над F.

Введем понятие порядка замкнутого класса булевых функций. Порядок функции f — число ее существенных переменных (обозначение $ord(f)$). Порядок конечной системы функций A — максимум из порядков входящих в нее функций (обозначение $ord(A)$). Порядком замкнутого класса F с конечным базисом называется такое натуральное число $ord(F)$, что

$$ord(F) = \min_{A} ord(A),$$

где минимум берется по всевозможным базисам A класса F.

Далее будем рассматривать все замкнутые классы булевых функций (описание замкнутых классов см. в [2]). Классы констант (порядок 0) и одноместных функций (порядок 1) не могут порождать новых предикатов, отличных от констант и отрицаний предикатов, поэтому ограничимся рассмотрением замкнутых классов порядка p, где $p \geq 2$. Их можно разбить на несколько групп, для каждой из которых сформулирован свой критерий полноты.

Теорема 1. *Пусть F — один из классов $M, M_0, M_1, M_{01}, T_0, T_1, T_{01}, S, S_{01}, SM, O^p, MO^p, O_0^p, MO_0^p, I^p, MI^p, I_1^p, MI_1^p$, где $p \geq 2, ord(F) = m$, V — произвольное конечное множество, $|V| \geq m$. Тогда система предикатов $\mathfrak{A}$ полна над классом F тогда и только тогда, когда она является $m-$полной над F.*

Будем обозначать тождественно ложный предикат через P^0, тождественно истинный предикат — через P^1.

Пусть $a \in V$, определим предикат $P_a(x)$ следующим образом:

$$P_a(x) = \begin{cases} 1, & \text{если } x = a; \\ 0, & \text{иначе.} \end{cases}$$

Теорема 2. *Пусть $F \in \{D, D_0\}$, V — произвольное конечное множество, такое, что $|V| \geq 2$. Тогда система предикатов $\mathfrak{A}$ полна над классом F тогда*

и только тогда, когда для любого элемента $a \in V$ выполняется соотношение $P_a(x) \in \mathfrak{A}$.

Теорема 3. *Пусть $F \in \{K, K_1\}$, V — произвольное конечное множество, такое, что $|V| \geq 2$. Тогда система предикатов $\mathfrak{A}$ полна над классом F тогда и только тогда, когда для любого элемента $a \in V$ выполняется соотношение $\overline{P}_a(x) \in \mathfrak{A}$.*

Для классов $O^\infty, MO^\infty, MO_0^\infty, O_0^\infty, D_1, D_{01}$ имеет место следующий критерий полноты.

Теорема 4. *Пусть $F \in \{P_2, M, M_0, T_0, D, D_0\}$, V — произвольное конечное множество, $|V| \geq 2$. Тогда система предикатов $\mathfrak{A}$ полна над классом $F \cap O^\infty$ тогда и только тогда, когда $P^0 \in \mathfrak{A}$ и система $\mathfrak{A}$ полна над F.*

Для классов $I^\infty, MI^\infty, MI_1^\infty, I_1^\infty, K_0, K_{01}$ имеет место следующий критерий полноты.

Теорема 5. *Пусть $F \in \{P_2, M, M_1, T_1, K, K_1\}$, V — произвольное конечное множество, $|V| \geq 2$. Тогда система предикатов $\mathfrak{A}$ полна над классом $F \cap I^\infty$ тогда и только тогда, когда $P^1 \in \mathfrak{A}$ и система $\mathfrak{A}$ полна над F.*

Пусть $\mathfrak{A} = \{A_1(x), ..., A_n(x)\}$ — произвольная система предикатов, определенных на V. Будем говорить, что система $\mathfrak{A}$ *линейно независима*, если из равенства

$$c_1 \cdot A_1(x) + \cdots + c_n \cdot A_n(x) + c_{n+1} \cdot P^1 = 0,$$

где $c_1, c_2, ..., c_n, c_{n+1} \in \{0, 1\}$, следует, что $c_1 = c_2 = ... = c_n = c_{n+1} = 0$.

Теорема 6. *Пусть $F \in \{L, L_0, L_1, L_{01}, SL\}$, V — произвольное конечное множество, $|V| \geq 2$. Тогда система предикатов $\mathfrak{A}$ полна над классом F тогда и только тогда, когда существует линейно независимая система предикатов $\mathfrak{A}' \subseteq \mathfrak{A}$, такая, что $|\mathfrak{A}'| = |V| - 1$, и $P^0, P^1 \in [\mathfrak{A}]_F$.*

Задача была поставлена профессором Угольниковым А. Б.

Список литературы

[1] Конспект лекций О. Б. Лупанова по курсу «Введение в математическую логику» / Отв. ред. Угольников А. Б. — М.: Изд-во ЦПИ при мех.-матем. ф-те МГУ им. М. В. Ломоносова, 2008. — 192 с.

[2] Угольников А. Б. Классы Поста. — Изд-во ЦПИ при мех.-матем. ф-те МГУ им. М. В. Ломоносова, 2008. — 64 с.

К вопросу о существовании доказуемо стойких систем облачных вычислений

Варновский Николай Павлович[1], **Захаров Владимир Анатольевич**[2], **Шокуров Александр Владимирович**[3]

[1] Московский государственный университет имени М. В. Ломоносова, e-mail: barnaba.np@gmail.com
[2] Московский государственный университет имени М. В. Ломоносова, e-mail: zakh@cs.msu.su
[3] Институт системного программирования РАН, e-mail: shok@ispras.ru

Информационная защита конфиденциальных данных в облачных вычислениях (ОВ) невозможна без гомоморфного шифрования. И хотя в 2009 г. К. Джентри [1] разработал стойкую систему вполне гомоморфного шифрования (FHE), в статье [2] было показано, что для некоторых схем ОВ одной лишь FHE недостаточно для их информационной защиты. Чтобы обойти этот отрицательный результат, нами в [3] была предложена модель ОВ, дополненная специальными криптографическими серверам. В этой модели предполагается, что противник может контролировать лишь часть этих серверов. Это предположение делает результат работы [2] неприменимым к нашей модели.

Предложенная нами система ОВ строится на основе ограниченной гомоморфной пороговой криптосистемы (TSHE) и включает в себя облачный вычислитель (СР), центр аутентификации (АС), криптосерверы, пользователей и клиентов. Все пользователи, клиенты и криптосерверы соединены каналами связи с СР. АС имеет каналы связи с СР, а также с каждым из криптосерверов. Сеть связи между криптосерверами представляет собой полный граф. Все каналы связи предполагаются защищенными.

На этапе инициализации схемы ОВ криптосерверы генерируют свои доли секретного ключа TSHE $sk_1, \ldots, sk_N$, и на их основе создают и опубликовывают общий для всех пользователей открытый ключ pk. Пользователи зашифровывают свои данные на этом ключе и предоставляют полученные шифртексты СР. Запросы на вычисления выдают клиенты. АС проверяет каждый такой запрос, руководствуясь политикой контроля доступа, и санкционирует или запрещает его выполнение.

СР выполняет вычисления над зашифрованными данными. В системах FHE [1] при ее выполнении «шум» зашифрованных промежуточных результатов вычисления возрастает. Поэтому всякий раз, когда этот «шум» приближается к критической величине, СР обращается к криптосерверам для выполнения ускоренной процедуры перешифрования, чтобы снизить уровень «шума». По окончании облачного вычисления криптосерверы выполняют финальное расшифрование результата.

Наша модель ОВ призвана защищать данные от пассивного противника, который следует протоколу вычислений, но может использовать полученную информацию для нарушения конфиденциальности. Противник может контролировать СР, пользователей, клиентов, а также часть криптосерверов, однако, при этом количество контролируемых противником криптосерверов не превосходит некоторого порога t, $t < N$. АС противнику недоступен.

В нашей схеме ОВ задействованы следующие протоколы и алгоритмы: 1) описанный выше протокол генерации ключей пороговой не вполне гомоморфной системы шифрования (TSHE), 2) протокол аутентификации запроса клиента, 3) алгоритм шифрования TSHE, 4) протокол дешифрования TSHE, 5) алгоритм вычисления над зашифрованными данными, 6) протокол ускоренного перешифрования TSHE, выполняемый криптосерверами.

Протокол аутентификации запроса клиента выполняется при получении АС запроса вида $(C_j, pk_j, \langle f_j \rangle)$, где C_j — идентификатор клиента, pk_j — его открытый ключ криптосистемы с открытым ключом, $\langle f_j \rangle$ — описание функции f_j, которую хочет вычислить клиент. Данный протокол выполняют АС и криптосерверы, каждый из которых должен убедиться, что АС санкционирует вычисление заданной функции. СР в этом протоколе не участвует.

Алгоритм шифрования Enc выполняется пользователем перед отправкой конфиденциальных данных СР. Он ничем не отличается от алгоритма шифрования обычной (непороговой) криптосистемы с открытым ключом.

Протокол дешифрования Dec выполняется криптосерверами. У каждого из них есть конфиденциальный вход — доля секретного ключа. Общим входом служит шифртекст результата вычисления, а выходом — открытый текст этого результата. Пример такого протокола для TSHE приведен в [4].

Входом процедуры вычислений $Eval$ служат хранящиеся в СР шифртексты. Гомоморфные вычисления выполняются обычным для FHE способом, за одним исключением: для «уменьшения» накопившегося в криптограмме «шума», вместо затратной и сложной процедуры скрытного перешифрования, выполняется протокол ускоренного перешифрования TSHE с использованием криптосерверов.

Если АС санкционировал вычисление запроса $(C_j, pk_j, \langle f_j \rangle)$ клиента C_j, то алгоритм $Eval$ получает на входе описания вычисляемой функции f_j, шифртексты ее аргументов $c(x_{i_1}), \ldots, c(x_{i_k})$, а также открытый ключ pk_j клиента C_j. Все данные зашифрованы на открытом ключе pk TSHE. Процедура $Eval$ вычисляет значение $Enc(Enc(f_j(x_{i_1}, \ldots, x_{i_k}), pk_j), pk)$, используя возможности гомоморфного шифрования. Криптосерверы расшифровывают это значение, используя доли секретного ключа $sk_1, \ldots, sk_N$, и отправляют клиенту C_j шифртекст $Enc(f_j(x_{i_1}, \ldots, x_{i_k}), pk_j)$. Клиент C_j расшифровывает его при помощи секретного ключ sk_j и извлекает значение функции.

Протокол ускоренного перешифрования выполняют криптосерверы. Общим входом служат криптограмма $c(b, e) = Enc(b, pk)$ бита b с «длинным шумом» e и открытый ключ TSHE pk. У каждого криптосервера есть дополнительный конфиденциальный вход — доля секретного ключа sk_i. Выходом является криптограмма $c(b, e')$ того же бита b с «коротким шумом» e'.

На этих входах i-й сервер выбирает случайный бит σ_i и шифрует его на открытом ключе pk TSHE. На основе полученных криптограмм вычисляется шифртекст $c(\sigma)$, где $\sigma = \sum_{i=1}^{N} \sigma_i$, а затем и шифртекст $c(b \oplus \sigma)$. Для этой цели используется алгоритм вычисления над зашифрованными данными. Далее

выполняется протокол дешифрования этого шифртекста. Полученный бит $b \oplus \sigma$ вновь шифруется с «коротким шумом» e', и полученный шифртекст еще раз складывается с $c(\sigma)$.

Таким образом, для скрытного перешифрования СР вместо выполнения сложной процедуры над зашифрованными данными, известной под названием bootstrapping [1], выполняет лишь очень простое суммирование. Поэтому введение в схему ОВ вспомогательных криптосерверов не только решает задачу информационной защиты для некоторых приложений, но и значительно повышает эффективность гомоморфных вычислений.

Список литературы

[1] Gentry C. Computing Arbitrary Functions of Encrypted Data // Communications of the ACM. — 2010. — V. 53, No. 3. — P. 97–105.

[2] van Dijk M., Juels A. On the impossibility of cryptography alone for privacy preserving cloud computing // Hot Topics in Security (HotSec'10), USENIX Association. — 2010. — P. 1–8.

[3] Варновский Н. П., Мартишин С. А., Храпченко М. В., Шокуров А. В. Методы пороговой криптографии для защиты облачных вычислений // Труды Института системного программирования РАН. — 2014. — Т. 26, вып. 2. — С. 269–274.

[4] Asharov G., Jain A., Lopez-Alt A., Tromer E., Vaikuntanathan V., Wichs D. Multiparty computation with low communication, computation and interaction via threshold FHE // Lecture Notes in Computer Science. — 2012. — V. 7237. — P. 483–501.

Минимизация коллизий при квантовом хешировании

Васильев Александр Валерьевич[1], **Зиятдинов Мансур Тагирович**[2]

[1] Казанский федеральный университет, e-mail: Alexander.KSU@gmail.com

[2] Казанский федеральный университет, e-mail: gltronred@gmail.com

Квантовое хеширование

В работе [1] нами предложен метод криптографического квантового хеширования, позволяющий представлять классическую информацию в виде квантовой суперпозиции следующего вида:

$$|\psi_{q,B}(w)\rangle = \frac{1}{\sqrt{|B|}} \sum_{i=1}^{|B|} |i\rangle \left(\cos \frac{2\pi b_i w}{q} |0\rangle + \sin \frac{2\pi b_i w}{q} |1\rangle \right).$$

Предложенный нами метод хеширования включает множество параметров B, от которых зависит вероятность коллизий. Точнее, вероятность коллизий зависит от максимального по всем парам входных сообщений $w \neq w'$ значения

$|\langle\psi(w)\,|\,\psi(w')\rangle|$, которое мы обозначим δ. В работе [1] показали для произвольного $\delta \in (0,1)$ существование такого множества полилогарифмического размера (от длины входных сообщений n).

Оптимизационная задача

Легко проверить, что для функции $\psi_{q,B}(x)$ имеем

$$|\langle\psi(w)\,|\,\psi(w')\rangle| = \left|\frac{1}{d}\sum_{i=1}^{d}\cos\frac{2\pi b_i(w-w')}{q}\right|,$$

и нам необходимо, чтобы данное выражение не превосходило δ для любого значения $(w-w')$ кроме 0. Таким образом, возникает следующая оптимизационная задача.

Для фиксированного q необходимо найти минимум целевой функции

$$\delta(q,B) = \max_{x\neq 0}\left|\frac{1}{d}\sum_{i=1}^{d}\cos\frac{2\pi b_i x}{q}\right|$$

по всем $B \subset \mathbb{Z}_q$, $d = |B|$.

Наилучшее решение всегда существует и равно $B = \mathbb{Z}_q$, т.к. $\delta(q,\mathbb{Z}_q) = 0$. Однако при этом размер хеша будет превосходить размер прообраза, что означает отсутствие второго ключевого свойства квантового хеширования, связанного с его размером и возможностью восстановления прообраза. Поэтому дополнительно требуется, чтобы $d \ll q$.

Для описанной выше задачи нами разработано два эвристических алгоритма, позволяющих получать хорошие множества параметров за приемлемое время.

Генетический алгоритм

Генетический алгоритм описан, например, в книге [2]. Исследования в этой области начаты ещё в 1954 году и стали широко распространены в 1970–1980-х годах.

В применении к нашей задаче генотипом будет являться само множество, упорядоченное по неубыванию; функцией приспособленности задается $\delta(q,C)$; мутацией — изменение произвольного элемента множества на единицу; скрещиванием — разбиение множеств-родителей на две части и обмен этими частями.

Для того, чтобы найти искомое множество, случайным образом генерируется набор множеств, размер которого является одним из параметров алгоритма. Далее на этом наборе моделируется эволюция следующим образом. В наборе производятся случайные “мутации” — произвольный элемент множества меняется на единицу. Для каждого множества набора вычисляется максимальное значение вероятности коллизий, которое достигается на этом наборе. После этого, множества из той половины, у которой вычисленное значение меньше медианы, “производит потомство”: выбираются случайные пары множеств; каждое множество из пары разбивается на две части случайным образом так, чтобы элементы первой части любого из множеств были меньше элементов

второй части; происходит обмен этими частями и “потомство” добавляется к набору. И, наконец, из набора удаляются множества с наихудшими показателями до тех пор, пока набор не станет первоначального размера, после чего проводится следующая итерация алгоритма, уже с новым набором множеств.

Алгоритм прекращается либо по выполнению заданного количества итераций, либо по нахождению искомого множества.

Алгоритм имитации отжига

Алгоритм имитации отжига описан, например, в главе “Section 10.12. Simulated Annealing Methods” книги [3].

Применительно к нашей задаче *энергией* будет максимальное значение δ на данном множестве; *соседними* множествами будут множества, отличающиеся значением одного элемента.

Алгоритм заключается в моделировании физического процесса, происходящего при кристаллизации. При этом атомы уже находятся в кристаллической решетке, но ещё могут переходить из одной ячейки в другую, если при этом уменьшается потенциальная энергия. Вероятность подобных переходов падает с понижением температуры.

Вначале генерируется случайное множество. Каждое возможное в рамках задачи множество представляет собой вариант кристаллической решетки.

Далее происходит переход в соседний вариант кристаллической решетки (множество, отличающееся значением одного элемента) с вероятностью, определенной распределением Гиббса, зависящим от температуры (которая зависит от максимального значения δ на данном множестве и от номера итерации).

Эти итерации повторяются, при этом температура постепенно уменьшается.

Алгоритм останавливается либо при достижении нужного значения δ, либо после превышения указанного времени работы.

Для ускорения работы алгоритма, а также для того, чтобы избегать локальных минимумов, вместо одного множества рассматривается набор множеств, размер которого является одним из параметров алгоритма. Данный алгоритм легко параллелизуем, поскольку поведение каждого множества из набора может быть промоделировано в отдельном потоке.

Работа выполнена при поддержке РФФИ (проект № 14-07-00878-а).

Список литературы

[1] Ablayev F. M., Vasiliev A. V. Cryptographic quantum hashing // Laser Physics Letters. — 2014. — V. 11, N 2. — P. 025202.

[2] Michalewicz Z. Genetic Algorithms + Data Structures = Evolution Programs. — Springer-Verlag, London, 1996. — 387 p.

[3] Press W. H., Teukolsky S. A., Vetterling W. T., Flannery B. P. Numerical Recipes: The Art of Scientific Computing. — Cambridge University Press, 2007. — 1256 p.

Об асимптотике для числа помеченных эйлеровых графов

Воблый Виталий Антониевич
Московский государственный технический университет им. Н. Э. Баумана, e-mail: vitvobl@yandex.ru

Эйлеров граф — это связный граф, у которого каждая вершина имеет четную степень. Рид [1] перечислил помеченные эйлеровы графы с заданными числами вершин и ребер. В [2, 3] получены явные формулы и асимптотика для числа помеченных бициклических и трициклических, а также тетрациклических эйлеровых графов.

В докладе получена асимптотика для числа помеченных эйлеровых графов с фиксированным цикломатическим числом и большим количеством вершин.

Включением вершины w степени 2 в ребро $e = uv$ графа G (равенство $u = v$ допускается) называется замена e на два новых ребра $e_1 = uw$ и $e_2 = wv$. Обратная операция называется исключением вершины степени 2 из ребра. В результате применения этой операции в графе могут появиться кратные ребра или петля. Гомеоморфным типом (топологическим графом) называется общий граф (допускаются петли и кратные ребра), не содержащий вершин степени 2, из которого с помощью операций включения вершин степени 2 могут быть получены все графы данного класса гомеоморфных графов [4, 5]. Граф является эйлеровым только тогда, когда его гомеоморфный тип — эйлеров граф.

Цикломатическим числом (циклическим рангом) связного графа называется увеличенная на 1 разность между числом ребер и числом вершин графа. Цикломатическое число связного графа совпадает с цикломатическим числом соответствующего данному графу гомеоморфного типа, так как при исключении вершины степени 2 из графа число вершин и ребер графа уменьшается на 1.

Теорема. *Пусть $E_n(k)$ — число помеченных эйлеровых графов с n вершинами и фиксированным цикломатическим числом k, тогда при $k \geq 1$ и $n \to \infty$ верна асимптотическая формула*

$$E_n(k) \sim c_k n^{2k-3} n!.$$

Доказательство. Пусть H — гомеоморфный тип с a вершинами, b ребрами, b_0 петлями (b — общее число ребер, петля — тоже ребро), $A(H)$ — порядок вершинно-реберной группы автоморфизмов графа H, причем H является связным гладким графом, отличным от изолированной вершины или петли. Тогда для числа помеченных связных графов C_n с n вершинами и гомеоморфным типом H при $n \to \infty$ верна асимптотика [4, лемма 4]:

$$C_n = \frac{n! n^{b-1}}{2^{b_0} A(H)(b-1)!}(1 + O(1/n)).$$

Заметим, что связный граф с фиксированным цикломатическим числом имеет конечное число гомеоморфных типов. Действительно, для графа, яв-

ляющегося гомеоморфным типом, по определению цикломатического числа: $k = b - a + 1$ или $b = a + k - 1$. А в силу «леммы о рукопожатиях», которая верна и для общих графов, $\sum_{i=1}^{a} d_i = 2b$, где d_i — степень i-й вершины. Кроме того, для эйлерового гомеоморфного типа $d_i \geq 4$, поэтому $2(a + k - 1) \geq 4a$, $a \leq k - 1$, $b \leq 2k - 2$. Следовательно, при фиксированном k гомеоморфный тип — это граф с фиксированным числом вершин и ребер, а таких графов — конечное число.

Теперь видим, что при $k \geq 2$ $E_n(k) = P_{b-1}(n)n!$, где $P_{b-1}(n)$ — многочлен степени $b - 1$ от n. Степень старшего члена этого многочлена максимальна при $b = 2k - 2$ и при этом равна $2k - 3$. Причем этот максимум достигается, в частности, для гомеоморфного типа, являющегося циклом с $k - 1$ вершинами, у которого все ребра — двойные.

Следовательно, при $k \geq 2$ и $n \to \infty$ $E_n(k) \sim c_k n^{2k-3} n!$.

Поскольку при $k = 1$ эйлеров граф является простым циклом, а число таких циклов n с вершинами равно $(n - 1)!/2$, то утверждение теоремы верно и в этом случае ($c_1 = 1/2$). **Теорема доказана.**

Величина константы c_k известна только для эйлеровых графов с малым цикломатическим числом. Значения $c_2 = 1/8$, $c_3 = 1/72$ найдены в работе [2], а значение $c_4 = 11/11520$ — в работе [3].

Список литературы

[1] Read R. C. Euler graphs on labelled nodes // Canad. J. Math. — 1962. — V. 14. — P. 482–486.

[2] Воблый В. А. Перечисление помеченных бициклических и трициклических эйлеровых графов // Матем. заметки. — 2012. — Т. 92, № 5. — С. 678–683.

[3] Воблый В. А., Мелешко А. К. Перечисление помеченных эйлеровых тетрациклических графов // Дискретный анализ и исследование операций. — 2014. —Т. 21, № 5. — С. 17–22.

[4] Степанов В. Е. О некоторых особенностях строения случайного графа вблизи критической точки // Теория вероятн. и ее примен. — 1987. — Т. 32, вып. 4. — С. 633–657.

[5] Ford G. W., Uhlenbeck G. E. Combinatorial problems in theory graphs, IV // Proc. Nat. Acad. Sci. U. S. A. — 1957.– V. 43. — P. 163–167.

Перечисление помеченных двудольных кактусов

Воблый Виталий Антониевич[1], **Мелешко Анна Константиновна**[2]

[1] Московский государственный технический университет им. Н. Э. Баумана, e-mail: vitvobl@yandex.ru

[2] Московский государственный технический университет им. Н. Э. Баумана, e-mail: akmeleshko@gmail.com

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей ребрами граф становится несвязным. Блок — связный граф без точек сочленения, а также максимальный связный нетривиальный подграф, не имеющий точек сочленения [1, с. 41]. Кактусом

называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [2, с. 93]. Все блоки кактуса — ребра или простые циклы. Двудольный граф G — это граф, множество вершин V которого можно разбить на два подмножества V_1 и V_2 таким образом, что каждое ребро графа G соединяет вершины из разных множеств V_1 и V_2 [1, с. 31].

Форд и Уленбек перечислили помеченные кактусы с заданным распределением числа вершин по циклам [3]. Из их результата следует формула для числа помеченных кактусов с заданным числом вершин, но она содержит суммирование по всем разбиениям целого числа. Более простые формулы получены в [4] и [5]. Г. Н. Багаев и Е. Ф. Дмитриев без доказательства дали асимптотику для числа помеченных двудольных кактусов с заданным цикломатическим числом [6].

Теорема. *Пусть D_n число помеченных двудольных кактусов с n вершинами, тогда при $n \geq 4$ верна формула*

$$D_n = n^{n-2} + (n-1)! \sum_{i=1}^{[(n-1)/3]} \sum_{j=0}^{[(n-3i-1)/2]} \binom{i+j-1}{j} \frac{n^{n-2i-2j-2}}{2^i i!(n-3i-2j-1)!} .$$

Доказательство. По теореме Кёнига граф является двудольным только тогда, когда все его простые циклы четны [1, с. 32]. Пусть C_n — число помеченных связных графов с n вершинами, а B_n — число помеченных блоков с n вершинами. Введем производящую функцию $B(z) = \sum_{n=3}^{\infty} B_n \frac{z^n}{n!}$.

В работах [4, 7] выведено соотношение

$$C_n = \frac{(n-1)!}{n}[z^{n-1}] \exp(nB'(z)) = \frac{(n-1)!}{n}[z^{-1}] \exp(nB'(z)) z^{-n} .$$

Обозначим через $\bar{B}(z)$ экспоненциальную производящую функцию для числа блоков помеченных двудольных кактусов. Так как число циклов с n помеченными вершинами равно $(n-1)!/2$, получим

$$\bar{B}(z) = \frac{z^2}{2} + \sum_{n=2}^{\infty} \frac{1}{2}(2n-1)! \frac{z^{2n}}{(2n)!}, \bar{B}'(z) = z + \frac{z^3}{2(1-z^2)}.$$

Следовательно, имеем

$$D_n = \frac{(n-1)!}{n}[z^{-1}] \exp\left(nz + \frac{nz^3}{2(1-z^2)}\right) z^{-n} .$$

Разлагая экспоненту в степенной ряд, найдем

$$D_n = n^{n-2} + \frac{(n-1)!}{n}[z^{-1}]\Big(\sum_{k=0}^{\infty} \frac{n^k z^k}{k!} \sum_{i=1}^{\infty} \frac{n^i z^{3i-n}}{2^i i!(1-z^2)^i}\Big).$$

С помощью известного ряда [8, с. 141],

$$(1-z)^{-i} = \sum_{j=0}^{\infty} \binom{j+i-1}{i-1} z^j,$$

имеем

$$D_n = n^{n-2} + (n-1)![z^{-1}] \sum_{k=0}^{\infty} \frac{n^{k-1} z^k}{k!} \sum_{i=1}^{\infty} \frac{n^i z^{3i-n}}{2^i i!} \sum_{j=0}^{\infty} \binom{i+j-1}{j} z^{2j} =$$

$$= n^{n-2} + (n-1)! \sum_{i=1}^{\infty} \sum_{j=0}^{\infty} \binom{i+j-1}{j} \frac{n^{n-2i-2j-2}}{2^i i!(n-3i-2j-1)!}.$$

Учитывая, что факториал обнуляет слагаемые при $n - 3i - 2j - 1 < 0$, получим утверждение теоремы. **Теорема доказана.**

Список литературы

[1] Харари Ф. Теория графов. — М.: Мир, 1973. — 302 с.

[2] Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1977. — 326 с.

[3] Ford G. W., Uhlenbeck G. E. Combinatorial problems in theory graphs, I // Proc. Nat. Acad. Sci. U. S. A., 1956. — V. 42. — P. 122–128.

[4] Воблый В. А. Об одной формуле для числа помеченных связных графов // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 4. — С. 48–59.

[5] Воблый В. А., Мелешко А. К. Новая формула для числа помеченных кактусов с заданным числом вершин // Тез. докл. Международной науч. конфер. «Дискретная математика, теория графов и их приложения». — Минск, 2013. — С. 9–11.

[6] Багаев Г. Н., Дмитриев Е. Ф., Перечисление связных отмеченных двудольных графов // Докл. АН БССР. — 1984. — Т. XXVIII, № 12. — С. 1061–1063.

[7] Воблый В. А. О перечислении помеченных связных графов по числу точек сочленения // Дискретная математика. — 2008. — Т. 20, № 1. — С. 14–23.

[8] Риордан Дж. Комбинаторные тождества. — М.: Наука, 1982. — 256 с.

О подсчете числа совершенных паросочетаний в графе

Вялый Михаил Николаевич

ВЦ РАН, e-mail: vyalyi@gmail.com

Как известно, задача подсчета числа совершенных паросочетаний в графе $\#P$-трудна [1]. Она остается $\#P$-трудной даже для 2-дольных 3-регулярных графов [2].

Для графов общего вида все известные на данный момент алгоритмы работают не быстрее $O^*(2^n)$, где n — число вершин в графе, $O^*(\cdot)$ обозначает асимптотическую оценку с точностью до полиномиального по n множителя.

Для многих классов графов известны более быстрые алгоритмы. В частности, для разреженных графов, в которых число ребер невелико, известен

алгоритм М. Фюрера [3], который работает за время $O^*(1.4656^{m-n})$. Здесь и далеее n и m — это количество вершин (соответственно, рёбер) графа.

Ицуми и Вадаяма [4] предложили алгоритм подсчета числа совершенных паросочетаний в разреженных двудольных графах, который работает за время $O^*(2^{\frac{1}{2}(1-1/(5\Delta\log\Delta))n})$. Здесь и далее Δ — средняя степень вершины.

В данной работе мы исследуем возможности метода Ицуми–Вадаяма применительно к недвудольным графам.

Метод Ицуми–Вадаяма основан на выражении числа совершенных паросочетаний как коэффициента в весовом многочлене пространства циклов графа. Метод применим только к графам, в которых все вершины имеют нечетную степень. Добавлением 2 вершин и $\leq n$ рёбер из любого графа легко конструируется граф с нечетными степенями, имеющий то же количество совершенных паросочетаний.

Обозначим $f_G(x,y)$ однородный весовой многочлен пространства циклов графа G, а через $[k]f_G$ — его коэффициент при мономе $x^k y^{m-k}$.

Лемма 1 ([4]). *Пусть в графе G степени всех вершин нечетны. Тогда число совершенных паросочетаний равно $[m-n/2]f_G$.*

Как известно, пространство циклов ортогонально пространству разрезов. Поэтому в силу тождества Мак-Вильямс подсчет числа совершенных паросочетаний сводится к нахождению весового многочлена $h_G(x,y)$ пространства разрезов графа.

Для каждого ребра e графа G введем переменные t_{e0} и t_{e1}. С каждой вершиной свяжем моном $D_u = \prod_{e\in\Gamma(u)} t_{e0} + \prod_{e\in\Gamma(u)} t_{e1}$ и определим *многомерный многочлен разрезов* как $D_G = \prod_{u\in V(G)} D_u$.

Коэффициенты $h_G(x,y)$ выражаются через коэффициенты многочлена D_G. Связь задается линейным отображением $\varphi\colon \Bbbk[(t_{e\alpha})_{e\in E(G),\alpha\in\{0,1\}}] \to \Bbbk[x,y]$, которое на мономе $\prod_{e\in E,\alpha\in\{0,1\}} t_{e\alpha}^{s(e,\alpha)}$, где $s(e,\alpha)\in\{0,1\}$, равно $x^a y^b$, если для ровно a рёбер выполняется равенство $s(e,0)+s(e,1)=1$. На остальных мономах отображение φ может быть каким угодно.

Из определений легко следует, что $\varphi(D_G) = 2^c h_G(x,y)$, где c — количество компонент связности графа G. Множитель 2^c связан с тем, что отображение разрезов из пространства вершин в пространство ребер имеет ядро размерности c.

Вычисление D_G «по определению» занимает время $O^*(2^n)$. Ускорение вычислений основано на слабой мультипликативности отображения

$$\varphi\colon \prod_{e\in E',\alpha} t_{e\alpha} \prod_{e\in E'',\alpha} t_{e\alpha} \mapsto \varphi\Big(\prod_{e\in E',\alpha} t_{e\alpha}\Big)\varphi\Big(\prod_{e\in E'',\alpha} t_{e\alpha}\Big), \quad \text{если } E'\cap E''=\varnothing.$$

По линейности последнее равенство продолжается на любые многочлены, в которых переменные не пересекаются.

Для алгоритмических приложений важно, что арифметика в кольце $\Bbbk[x,y]$ выполняется быстро, так как это кольцо многочленов от двух переменных.

Соотношения слабой мультипликативности позволяют сокращать вычисление образа $\varphi(D_G)$ путём выбора порядка раскрытия скобок.

Мы приведем три способа ускорения вычислений многочлена разрезов. Все они основаны на оценке числа мономов в промежуточных многочленах, возникающих при подходящем раскрытии скобок в многомерном многочлене разрезов.

Первый способ оценивает число мономов через ширину линейного представления графа (pathwidth). Эффективно достижимые оценки ширины линейного представления графов из [5] дают следующие результаты.

Теорема 1. *Существует алгоритм нахождения числа совершенных паросочетаний в графе, который работает за время* $O^*(2^{m/5.769})$. *Для графов со средней степенью* $\Delta = 3$ *время работы алгоритма улучшается до* $O^*(2^{n/6})$. *Для графов с* $\Delta = 4$ *время работы алгоритма* $O^*(2^{n/3})$.

Второй способ ускорения вычислений состоит в нахождении независимого множества и раскрытии скобок по дополнению к этому множеству. В полученных многочленах переменные не пересекаются и потому применимы соотношения слабой мультипликативности.

Теорема Турана гарантирует существование независимого множества размера не менее $\frac{n}{\Delta+1}$. Как показано в [6], эта оценка достигается жадным алгоритмом построения независимого множества.

Отсюда получаем более быстрый алгоритм для разреженных графов произвольной средней степени.

Теорема 2. *Существует алгоритм нахождения числа совершенных паросочетаний в графе, который работает за время* $O^*(2^{(1-1/(\Delta+1))n})$.

Третий способ сокращения вычислений состоит в нахождении вершинных сепараторов в графе.

Алон и др. [7] доказали, что в графах с запрещенными минорами размера h есть $2/3$-сепаратор размера $h^{3/2}n^{1/2}$, причем поиск такого сепаратора занимает полиномиальное время. Отсюда получаем следующий результат.

Теорема 3. *Существует субэкспоненциальный алгоритм нахождения числа совершенных паросочетаний в графах с фиксированным списком запрещенных миноров.*

Работа выполнена при поддержке РФФИ (проект № 14-01-00641-а).

Список литературы

[1] Valiant L. G. The complexity of computing the permanent // Theoretical Computer Science. — 1979. — V. 8. — P. 189–201.

[2] Dagum P., Luby M. Approximating the permanent of graphs with large factors // Theoretical Computer Science. — 1992. — V. 102. — P. 283–305.

[3] Fürer M. Counting perfect matchings in graphs of degree 3 // FUN 2012, LNCS 7288. — 2012. – P. 189–197.

[4] Izumi T., Wadayama T. A new direction for counting perfect matchings // FOCS'53. — 2012. — P. 591–598.

[5] Gaspers S. Exponential time algorithms: structures, measures, and bounds. — VDM Verlag Dr. Mueller e.K. — 2010. — 208 p.

[6] Halldórsson M. M. , Radhakrishnan J. Greed is good: approximating independent sets in sparse and bounded-degree graphs // Algorithmica. — 1997. — V. 18. — P. 145–163.

[7] Alon N., Seymour P., Thomas R. Separator theorem for graphs with an excluded minor and its applications // STOC'90. — 1990. — P. 293–299.

Аддитивная сложность матриц НОД и НОК

Гашков Сергей Борисович[1], **Сергеев Игорь Сергеевич**[2]

[1] Московский государственный университет им. М. В. Ломоносова, e-mail: sbgashkov@gmail.com
[2] ФГУП «НИИ «Квант», e-mail: isserg@gmail.com

В настоящей работе рассматривается задача об аддитивной сложности матриц, составленных из степеней наибольших общих делителей (НОД) или наименьших общих кратных (НОК) номеров строк и столбцов.

Под сложностью $L_B(A)$ матрицы A понимается сложность реализации линейного оператора с матрицей A схемами над базисом B (подробнее о понятиях схемы и сложности см. в [1, 2]).

В работе [3] Ж. Моргенштерн предложил метод нижней оценки сложности матрицы через ее определитель. В упрощенном виде его результат формулируется так: сложность матрицы A над базисом $B = \{x \pm y\} \cup \{ax \mid |a| \le 2\}$ удовлетворяет соотношению $L_B(A) \ge \log_2 |\det A'|$ для любой квадратной подматрицы A' матрицы A.

Оказалось, что для многих известных матриц метод дает точные по порядку оценки. Примеры: матрица дискретного преобразования Фурье [3], матрица Сильвестра–Адамара, матрицы из комбинаторных чисел (Паскаля, Стирлинга, Гаусса) [4, 5].

Здесь мы приводим аналогичный результат для матриц, составленных из натуральных степеней НОД и НОК. Далее все матрицы по умолчанию имеют размер $n \times n$.

Обозначим через $\text{НОД}^{[r]}$ и $\text{НОК}^{[r]}$ матрицы, составленные из r-х степеней НОД и, соответственно, НОК номеров строк и столбцов.

Теорема. (i) *В базисе* $B_+ = \{x + y\}$ *при* $n \to \infty$

$$L_{B_+}\left(\text{НОД}^{[r]}\right) \sim rn \log_2 n.$$

(ii) *В базисе* $B_\pm = \{x + y, -x\}$ *при* $n \to \infty$

$$L_{B_\pm}\left(\text{НОК}^{[r]}\right) \sim 2rn \log_2 n.$$

Нижние оценки теоремы вытекают из значений определителей матриц, найденных Г. Смитом [6].

Матрицу НОД$^{[r]}$ можно разложить в произведение

$$\text{НОД}^{[r]} = E \times J_r(D) \times E^T, \tag{1}$$

где E — булева матрица, определяемая правилом $E(i,k) = (k \mid i)$; $J_r(D)$ — диагональная матрица с числами $J_r(1), J_r(2), \ldots, J_r(n)$ на главной диагонали; J_r — функция Жордана

$$J_r(n) = n^r \prod_{p\in\mathbb{P},\, p|n} \left(1 - p^{-r}\right),$$

$\mathbb{P}$ — множество простых чисел.

Для матрицы НОК$^{[r]}$ справедливо аналогичное представление

$$\text{НОК}^{[r]} = D^r \times E \times J_{-r}(D) \times E^T \times D^r, \tag{2}$$

где D^r — диагональная матрица с числами $1^r, 2^r, \ldots, n^r$ на главной диагонали.

Формулы (1) и (2) позволяют легко найти определители матриц НОД$^{[r]}$ и НОК$^{[r]}$, поскольку матрица E — треугольная с единичной диагональю (поэтому $\det E = 1$), а остальные матрицы в разложениях — диагональные.

Верхние оценки теоремы тоже доказываются построением подходящих разложений матриц.

Для доказательства п. (i) достаточно воспользоваться формулой (1), из которой следует

$$L_{B_+}\left(\text{НОД}^{[r]}\right) \le 2L_{B_+}(E) + L_{B_+}(J_r(D)).$$

Асимптотически оптимальный способ вычисления матрицы $J_r(D)$ состоит в покомпонентном применении метода Брауэра [7], а сложность матрицы E мала: можно проверить, что $L_{B_+}(E) = O(n \log\log n)$.

Для вывода верхней оценки п. (ii) формула (2) не подходит: в ней используются матрицы с нецелыми коэффициентами. Мы применяем другое разложение, в котором все матрицы имеют неотрицательные целые коэффициенты. Справедливо

$$\text{НОК}^{[r]} = E \times J_r(\gamma(D)) \times \Phi^{[r]} \times G \times D^r,$$

где через $\gamma(n)$ обозначается произведение всех простых делителей числа n; $J_r(\gamma(D))$ — диагональная матрица с числами $J_r(\gamma(1)), J_r(\gamma(2)), \ldots, J_r(\gamma(n))$ на главной диагонали; G — булева матрица, определемая правилом: $G(m,k) = 1$ равносильно $\gamma(m) = \gamma\left(\frac{m}{\text{НОД}(m,k)}\right)$; матрица $\Phi^{[r]}$ определяется как

$$\Phi^{[r]}(d,m) = \begin{cases} J_r\left(\frac{d}{m}\right), & m \mid d,\ \ \gamma(d) = \gamma(m), \\ 0, & \text{иначе.} \end{cases}$$

Тогда

$$L_{B_\pm}\left(\text{НОК}^{[r]}\right) \le L_{B_\pm}(E) + L_{B_\pm}(J_r(\gamma(D))) + L_{B_\pm}\left(\Phi^{[r]}\right) + L_{B_\pm}(G) + L_{B_\pm}(D^r).$$

Асимптотическая сложность матрицы $\text{НОК}^{[r]}$ сосредоточена в сложности матриц $J_r(\gamma(D))$ и D^r, которые могут быть вычислены оптимально методом Брауэра. Сложность остальных матриц мала: в частности, $L_{B_+}\left(\Phi^{[r]}\right) = O(rn)$.

Матрицу G можно разложить дальше как

$$G = U \times \mu^*(D) \times E^T,$$

где U — булева матрица, определяемая правилом: $U(m,d) = 1$ равносильно $d \mid m$ и $\text{НОД}(d, m/d) = 1$; $\mu^*(D)$ — диагональная матрица с числами $\mu^*(1), \mu^*(2), \ldots, \mu^*(n)$ на главной диагонали; $\mu^*(n)$ — унитарная функция Мёбиуса, определяемая как $\mu^*(n) = (-1)^{l(n)}$, где $l(n)$ — число различных простых делителей n.

Теперь можно проверить, что $L_{B_+}(U) = O(n \log\log n)$, $L_{B_\pm}(\mu^*(D)) = O(n)$, следовательно, $L_{B_\pm}(G) = O(n \log\log n)$.

Единственная в схеме для матрицы $\text{НОК}^{[r]}$ операция отрицания $-x$ используется при вычислении матрицы $\mu^*(D)$. Вопрос о том, можно ли обойтись без отрицаний и получить оценку п. (ii) в базисе B_+, остается открытым.

Работа выполнена при поддержке РФФИ (проект № 14-01-00671-а).

Список литературы

[1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984. — 138 с.

[2] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986. — 384 с.

[3] Morgenstern J. Note on a lower bound of the linear complexity of the fast Fourier transform // J. ACM. — 1973. — V. 20. — P. 305–306.

[4] Гашков С. Б. Об арифметической сложности вычисления линейных преобразований // Вестник МГУ. Серия 1. Математика. Механика. — 2014. — № 6. — С. 24–31.

[5] Гашков С. Б. Арифметическая сложность преобразований Стирлинга // Дискретная математика. — 2014. — Т. 26, № 4. — С. 23–35.

[6] Smith H. J. S. On the value of a certain arithmetical determinant // Proc. LMS. — 1875/76. — V. 7. — P. 208–212.

[7] Brauer A. On addition chains // Bull. AMS. — 1939. — V. 45. — P. 736–739.

Одно обобщение алгоритма Шеннона–Фано для кодирования дискретных множеств сообщений

Герасимов Михаил Александрович
Санкт-Петербургский государственный университет, e-mail: ge@star.math.spbu.ru

Предлагается обобщение алгоритма Шеннона–Фано, которое позволяет не только находить оптимальные коды для заданного конечного множества сообщений за полиномиальное время, но и дает возможность кодировать сообщения приближенно, в зависимости от имеющихся ресурсов (времени и памяти). Оценки сложности сделаны для детерминированной одноленточной машины Тьюринга с входной и выходной лентой.

Машина Тьюринга

Для оценки сложности алгоритмов рассматривается одноленточная одноголовочная машина Тьюринга с входной и выходной лентой для записи результата. Предполагается, что входные данные записываются на входной ленте, обрабатываются на рабочей ленте и результат записывается на выходной ленте. При работе машины Тьюринга используется алфавит, состоящий из четырех символов $\{\#, b, 0, 1\}$. Результатом работы алгоритма считается битовая последовательность, кодирующая исходное множество сообщений, и соответствующее дерево кодирования, позволяющее однозначно восстановить исходную последовательность. В дальнейшем будем считать, что входные данные (натуральные числа) записаны в виде битовой последовательности на входной ленте между маркерами ‘#’. В качестве разделителя входных битовых последовательностей используется пустой символ ‘b’. Считывание второго маркера означает конец цепочки входных данных. Входная лента позволяет считывать входные данные произвольное количество раз. Выходная лента позволяет только записать результат вычисления в виде последовательности символов рабочего алфавита. Каждый символ выходной цепочки записывается только один раз и больше не изменяется.

Алгоритм Шеннона–Фано

Рассматривается общий вид алгоритма Шеннона–Фано, а именно, предполагается наличие некоторого множества сообщений $X = \{x_1, \ldots, x_M\}$ и некоторого распределения p, как функции из множества X во множество рациональных чисел от 0 до 1, обладающей тем свойством, что $\sum_{i=1}^{M} p(x_i) = 1$. Для простоты будем предполагать наличие алфавита A, состоящего из 2-х символов $\{0, 1\}$. Результатом работы алгоритма будет считаться набор цепочек, кодирующих сообщения множества X в алфавите A, таким образом, что существует обратное однозначное отображение, восстанавливающее по цепочке из алфавита A соответствующее сообщение из множества X. Оптимальность понимается в обычном смысле, т. е. средняя длина полученных кодирующих цепочек (математическое ожидание) отличается от энтропии множества X, при заданном распределении p, на минимальную величину, обычно близкую или

равную 0.
Предполагается также, что алгоритм производит следующие шаги:

Шаг 1. Строит дерево кодирования для множества X по следующим правилам:

Шаг 1.1. Если $|X| = 1$, то алгоритм останавливается, помещая это множество в лист дерева кодирования.
Шаг 1.2. Если $|X| > 1$, то исходное множество разбивается на два непустых подмножества X_1, X_2 таким образом, что сумма вероятностей сообщений одного множества отличается от суммы вероятностей сообщений другого множества не более чем на некоторое δ, большее или равное 0. К множествам X_1, X_2 рекурсивно применяется шаг 1.1.
Шаг 2. Используя построенное дерево, листьями которого являются одноэлементные множества, строится код $K : X \to A^*$ естественным образом: левой ветви дерева соответствует символ ‘0’, правой ветви дерева соответствует ‘1’. Путь из корня дерева в лист, соответствующий элементу x, будет определять код этого элемента.
Шаг 3. Полученные коды сообщений множества X записываются на выходную ленту машины Тьюринга.
Данный алгоритм завершает свою работу не более чем за $|X|$ шагов, при любом множестве X, поскольку на шаге 1.2 мощность любого из получаемых подмножеств X_1, X_2 меньше мощности X. Полученный в результате работы алгоритма код может не быть оптимальным и может иметь относительную погрешность, зависящую от выбора δ.

Теорема 1. *Для любого множества X существует $\delta(X) > 0$, которое применимо к любому подмножеству множества X на шаге* 1.2 *обобщенного алгоритма Шеннона–Фано.*

Теорема 2. *Существует полиномиальный по времени алгоритм, кодирующий любое множество сообщений X цепочками двоичного алфавита $A = \{0, 1\}$ с любым распределением p обобщенным алгоритмом Шеннона–Фано с $\delta(X) = \max_{x \in X} p(x) - \min_{x \in X} p(x)$.*

Замечание 1. *Данное определение, теорему* 1 *и теорему* 2 *можно обобщить до случая, когда мощность алфавита A больше* 2.
Замечание 2. *Обобщенный алгоритм Шеннона–Фано работает и в тех случаях, когда существуют x_1, x_2 из X, для которых $p(x_1) = p(x_2)$.*

Список литературы

[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

[2] Fischetti M., Martello S. Wost-case analysis of the differencing method for the partition problem // Math. Programming. — 1987. — V. 37, N 1. — P. 117–120.

[3] Минский М. Вычисления и автоматы. — М., 1971.

[4] Huffman. D. A method for construction of minimum redundancy codes // Proceeding of IRE. — 1952. — V. 40, N 9. — P. 1098–1101.

[5] Horowits E., Sahni S. Fundamentals of Computer Algorithms. — Computer Science Press, 1978.

[6] Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. — July 1948. — V. 27. — P. 373–423.

Верхняя оценка ненадежности неветвящихся программ в базисах, содержащих нелинейную функцию двух переменных

Грабовская Светлана Михайловна

Пензенский государственный университет, e-mail: swetazin@mail.ru

Рассматривается реализация булевых функций неветвящимися программами с оператором условной остановки [1] в полном конечном базисе, содержащем нелинейную функцию двух переменных, т. е. некоторую функцию вида $(x_1^{\alpha_1}\&x_2^{\alpha_2})^{\alpha_3}(\alpha_1,\ \alpha_2,\ \alpha_3 \in \{0,\ 1\})$. Программы с оператором условной остановки характеризуются наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы программы при поступлении единицы на вход оператора условной остановки (стоп-оператора).

Будем считать, что все вычислительные операторы независимо друг от друга с вероятностью ε ($\varepsilon \in (0, 1/2)$) подвержены однотипным константным неисправностям либо типа 0, либо типа 1 на выходах. Константные неисправности типа 0 характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему булеву функцию φ, а в неисправном — функцию 0. Неисправности типа 1 на выходах вычислительных операторов определяются аналогично.

Предполагается, что операторы условной остановки ненадежны и независимо друг от друга подвержены неисправностям двух типов [2]: первого и второго рода. Неисправность первого рода характеризуется тем, что при поступлении единицы на вход стоп-оператора он с вероятностью δ ($\delta \in (0, 1/2)$) не срабатывает, и, следовательно, работа программы продолжается. Неисправность второго рода такова, что при поступлении нуля на вход стоп-оператора он с вероятностью η ($\eta \in (0, 1/2)$) срабатывает, и, следовательно, работа программы прекращается. Обозначим $\mu = \max\{\varepsilon,\ \delta,\ \eta\}$.

Заметим, что схему из функциональных элементов (ФЭ) можно считать частным случаем неветвящихся программ, а именно, неветвящейся программой, в которой нет стоп-операторов.

Ненадежностью $N_\mu(Pr)$ программы Pr назовем максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах. Надежность программы Pr равна $1 - N_\mu(Pr)$.

Для нелинейной функции двух переменных $(x_1^{\alpha_1}\&x_2^{\alpha_2})^{\alpha_3}$ $(\alpha_1,\ \alpha_2,\ \alpha_3 \in \{0,\ 1\})$ возможны 2 случая:

1. $\alpha_3 = 0$, тогда функция принимает вид $x_1^{\alpha_1} \vee x_2^{\alpha_2}$ и будем называть ее обобщенной дизъюнкцией;
2. $\alpha_3 = 1$, тогда функция принимает вид $x_1^{\alpha_1} \& x_2^{\alpha_2}$ и будем называть ее обобщенной конъюнкцией.

Константные неисправности типа 0

В данном разделе будем считать, что вычислительные операторы подвержены константным неисправностям типа 0 на выходах. Получены следующие результаты.

Теорема 1. *В полном конечном базисе, содержащем функцию вида* $x_1^{\alpha_1} \vee x_2^{\alpha_2}$ $(\alpha_1,\ \alpha_2 \in \{0,\ 1\})$*, любую булеву функцию* f *можно реализовать такой неветвящейся программой* Pr_f*, что при всех* $\varepsilon \in (0,\ 1/960]$ *справедливо неравенство* $N_\mu(Pr_f) \leq \varepsilon + 78\mu^2$.

Теорема 2. *В полном конечном базисе, содержащем функцию вида* $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1,\ \alpha_2 \in \{0,\ 1\})$*, любую булеву функцию* f *можно реализовать такой неветвящейся программой* Pr_f*, что при всех* $\varepsilon \in (0,\ 1/960]$ *справедливо неравенство* $N_\mu(Pr_f) \leq 80\mu^2$.

Таким образом, в полном конечном базисе, содержащем нелинейную функцию двух переменных, любую булеву функцию f можно реализовать неветвящейся программой при константных неисправностях типа 0 на выходах вычислительных операторов и неисправностях первого и второго рода стоп-операторов с ненадежностью не больше $\varepsilon + 78\mu^2$ при всех $\varepsilon \in (0,\ 1/960]$ и $\mu = \max\{\varepsilon,\ \delta,\ \eta\}$. Однако, если базис содержит обобщенную конъюнкцию, эта оценка составляет $80\mu^2$ при всех $\varepsilon \in (0,\ 1/960]$.

Константные неисправности типа 1

В данном разделе будем считать, что вычислительные операторы подвержены константным неисправностям типа 1 на выходах. Получены следующие результаты.

Теорема 3. *В полном конечном базисе, содержащем функцию вида* $x_1^{\alpha_1} \vee x_2^{\alpha_2}$ $(\alpha_1,\ \alpha_2 \in \{0,\ 1\})$*, любую булеву функцию* f *можно реализовать такой неветвящейся программой* Pr_f*, что при всех* $\varepsilon \in (0,\ 1/960]$ *справедливо неравенство* $N_\mu(Pr_f) \leq 80\mu^2$.

Теорема 4. *В полном конечном базисе, содержащем функцию вида* $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1,\ \alpha_2 \in \{0,\ 1\})$*, любую булеву функцию* f *можно реализовать такой неветвящейся программой* Pr_f*, что при всех* $\varepsilon \in (0,\ 1/960]$ *справедливо неравенство* $N_\mu(Pr_f) \leq \varepsilon + 78\mu^2$.

Таким образом, в полном конечном базисе, содержащем нелинейную функцию двух переменных, любую булеву функцию f можно реализовать неветвящейся программой при константных неисправностях типа 1 на выходах вычислительных операторов и неисправностях первого и второго рода стоп-операторов с ненадежностью не больше $\varepsilon + 78\mu^2$ при всех $\varepsilon \in (0,\ 1/960]$ и $\mu = \max\{\varepsilon,\ \delta,\ \eta\}$. Однако, если базис содержит обобщенную дизъюнкцию, эта оценка составляет $80\mu^2$ при всех $\varepsilon \in (0,\ 1/960]$.

В качестве сравнения, для схем из ФЭ известно [3], что в произвольном полном конечном базисе любую булеву функцию f можно реализовать схемой из ФЭ при тех же типах неисправностей с ненадежностью не больше $3\varepsilon+100\varepsilon^2$ при всех $\varepsilon \in (0,\ 1/960]$. Однако в некоторых базисах данную верхнюю оценку можно улучшить. Например, в базисе $\{x_1 \vee x_2,\ \bar{x}_1\}$ она составляет $2\varepsilon + 42\varepsilon^2$ при всех $\varepsilon \in (0,\ 1/140]$; в базисе $\{x_1 \& \bar{x}_2,\ x_1 \sim x_2\}$ имеем $\varepsilon + 6\varepsilon^2$ при всех $\varepsilon \in (0,\ 1/320]$. Тогда как для неветвящихся программ верхняя оценка ненадежности составляет $\varepsilon + 78\mu^2$ при всех $\varepsilon \in (0,\ 1/960]$ и $\mu = \max\{\varepsilon,\ \delta,\ \eta\}$, а в некоторых базисах $80\mu^2$, что в общем случае лучше, чем для схем из ФЭ.

Работа выполнена при поддержке РФФИ (проект № 14-01-31360).

Список литературы

[1] Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — Январь–март, 1997. — Т. 4, № 1. — С. 60–78.

[2] Грабовская С. М. Асимптотически оптимальные по надежности неветвящиеся программы с оператором условной остановки : дис. . . . канд. физ.-мат. наук : 01.01.09 : защищена 31.05.12 : утв. 18.03.13 / Грабовская Светлана Михайловна. — Пенза, 2012. — 89 с. — Библиогр. : С. 9–10.

[3] Алехина М. А. Синтез асимптотически оптимальных по надежности схем : моногр. — Пенза: ИИЦ ПГУ, 2006. — 156 с.

Ширина некоторых классов политопов и задача поиска целой точки

Грибанов Дмитрий Владимирович[1], **Веселов Сергей Иванович**[2]

[1] НИУ ВШЭ, Нижний Новгород; ННГУ им. Н. И. Лобачевского, e-mail: dimitry.gribanov@gmail.com

[2] Нижегородский госуниверситет им. Н. И. Лобачевского, e-mail: ves20@yandex.ru

Пусть матрица $A \in Z^{m\times n}$ имеет ранг n, будем называть A Δ-*модулярной* матрицей если максимальное абсолютное значение $n \times n$ миноров A не превосходит Δ. Ссылаясь на работу [1], будем говорить, что A *почти унимодулярна*, если она 2-*модулярна* и абсолютное значение $(n-1)\times(n-1)$ миноров A не превосходит 1. В работе [2] 2-*модулярные* матрицы названы *бимодулярными*. Будем говорить, что A *строго* Δ-*модулярна* если любой её $n \times n$ минор есть в точности $-\Delta$, 0 или Δ.

Шириной выпуклого тела P будем называть следующую величину: $width(P) = \min_{c\in Z^n\setminus\{0\}}\{\max\{c^\top x : x \in P\} - \min\{c^\top x : x \in P\}\}$. Хинчиным [3] был установлен следующий факт: если P не содержит точек из Z^n, тогда $width(P) \leq f(n)$, где величина $f(n)$ зависит только от размерности. Существует много оценок на величину $f(n)$. Наилучшая оценка $O(n^{3/4}\log^c n)$ дана в работе [4]. Наилучшая оценка для симплексов $O(n\log n)$ дана в работе [5].

Результаты работы:

1) Показано, что задача целочисленного программирования с *почти унимодулярной* матрицей ограничений принадлежит классу P.

2) Показано, что ширина симплекса, не содержащего целых точек, не превосходит $\Delta - 1$, если симплекс порожден системой неравенств с Δ-*модулярной* матрицей. Целая точка в симплексе ширины большей чем $\Delta - 1$ может быть найдена за полиномиальное время. Также было показано, что для задачи целочисленной оптимизации на таких симплексах применимы алгоритмы групповой минимизации предложенные Гомори и Ху [6, 7], откуда следует существование полиномиального при фиксированном Δ алгоритма. В данном результате существенно используются свойства *углового многогранника* [6, 8]. Введением в изучение симплексов без целых точек могут послужить работы [9, 10].

3) В более общем случае показано, что ширина политопа размерности n без целых точек не превосходит $(\Delta - 1)(n + 1)$, если политоп порожден системой неравенств со *строго* Δ-*модулярной* матрицей. Иначе целая точка может быть найдена за полиномиальное время. Доказательство опубликовано в сборнике [11].

4) Приведен пример конуса заданного *бимодулярной* матрицей ограничений и порожденного экспоненциальным числом образующих. Данный пример важен, потому что из противоположного утверждения о полиномиальности числа рёбер в любом *бимодулярном* конусе следовала бы полиномиальность задачи целочисленного программирования на политопе с бимодулярной матрицей ограничений.

Работа выполнена при поддержке лаборатории алгоритмов и анализа сетевых структур НИУ ВШЭ, грант правительства РФ дог. 11.G34.31.0067 и при поддержке РФФИ, грант 15-01-06249.

Список литературы

[1] Cornuéjols G., Zuluaga L. F. On Padberg's conjecture about almost totally unimodular matrices // Oper. Res. Lett. — 2000. — V. 27, N 3. — P. 97–99.

[2] Veselov S. I., Chirkov A. J. Integer program with bimodular matrix // Discrete Optimization. 2009. — V. 6, N 2. — P. 220–222.

[3] Khinchine A. A quantitative formulation of Kronecker's theory of approximation. Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya. — 1948. — V. 12, N 2. — P. 113–122 [in Russian].

[4] Rudelson M. Distances between non-symmetric convex bodies and the MM^*-estimate // Positivity. — 2000. — V. 4, N 2. — P. 161–178.

[5] Banaszczyk W., Litvak A. E., Pajor A., Szarek S. J. The flatness theorem for non-symmetric convex bodies via the local theory of Banach spaces // Mathematics of operations research. — 1999. — V. 24, N 3. — P. 728–750.

[6] Gomory R. E. On the relation between integer and non-integer solutions to linear programs // Proc. Natl. Acad. Sci. — USA. — 1965. — V. 53, N 2. — P. 260–265.

[7] Hu T. C. On the Asymptotic Integer Algorithm. — MRC Report 946. — University of Wisconsin, Madison, 1968.

[8] Shevchenko V. N. Qualitative Topics in Integer Linear Programming (Translations of Mathematical Monographs). — AMS, 1996.

[9] Haase C., Ziegler G. On the maximal width of empty lattice simplices // Europ. J. Combinatorics. — 2000. — V. 21. — P. 111–119.

[10] Sebö A. An introduction to empty lattice simplexes // Cornuéjols G., Burkard R. R., Woeginger R. E. LNCS. — V. 1610. — 1999. — P. 400–414.

[11] Gribanov D. V. The flatness theorem for some class of polytopes and searching an integer point // Springer Proceedings in Mathematics & Statistics. Models, Algorithms and Technologies for Network Analysis. — 2013. — V. 104. — P. 37–45.

Асимптотическое поведение ранговой функции базиса для модели обобщенной целочисленной глубины схем из функциональных элементов

Данилов Борис Радиславович

Московский государственный университет имени М. В. Ломоносова, e-mail: brdanilov@gmail.com

Рассматривается модель [1] обобщенной глубины схем из функциональных элементов (СФЭ) в произвольном конечном полном базисе $\text{Б} = \{\mathcal{E}_1, \ldots, \mathcal{E}_b\}$, в которой глубина $D_{i,j,s}$ базисного функционального элемента (ФЭ) $\mathcal{E}_i$ по одному из его k_i входов с номером j является положительной целочисленной величиной и складывается из двух компонент: глубины межэлементного соединения входа номер j элемента $\mathcal{E}_i$ с выходом подсоединённого элемента $\mathcal{E}_s$ и внутренней глубины самого элемента $\mathcal{E}_i$. Глубина СФЭ определяется через глубину её цепей — подсхем, в которых выходы ФЭ ветвятся не более одного раза и ровно один вход каждого ФЭ за исключением одного ФЭ соединён с выходом другого ФЭ данной подсхемы. Будем называть инициальной цепь, в которой выделен вход того единственного ФЭ, все входы которого являются входами схемы. Мы предполагаем, что выделенному входу инициальной цепи приписан тип некоторого ФЭ базиса Б, тогда глубина $D(\omega)$ инициальной цепи ω равна сумме глубин всех её ФЭ по соединяющим их входам и глубины ФЭ с выделенным входом по этому входу. Приписывая входам СФЭ Σ типы ФЭ базиса Б, определим её глубину $D(\Sigma)$ как наибольшую глубину её главных цепей, т. е. таких цепей, которые идут от входов схемы к её выходам.

Обозначим через $P_2(n)$ множество всех функций алгебры логики (ФАЛ), зависящих от заданных на множестве $B = \{0, 1\}$ булевых переменных (БП) $x_1, \ldots, x_n$. Пусть базисный ФЭ $\mathcal{E}_i$ реализует ФАЛ $\varphi_i \in P_2(k_i)$, которая в случае $k_i \geqslant 2$ существенно зависит от всех своих переменных. Определим глубину $D_{\text{Б}}(f)$ ФАЛ f как наименьшую из глубин СФЭ над Б, реализующих f. Функция Шеннона $D_{\text{Б}}(n)$ для глубины ФАЛ из $P_2(n)$ в классе СФЭ над Б определяется обычным образом как наибольшая глубина ФАЛ указанного множества. В работе [1] доказано, что асимптотика функции $D_{\text{Б}}(n)$ имеет

вид $D_{\text{Б}}(n) \sim \tau_{\text{Б}} n$ и определяется константой $\tau_{\text{Б}}$ — так называемой приведённой глубиной базиса Б:

$$\tau_{\text{Б}} = \lim_{t \to +\infty} \frac{t}{\log R_{\text{Б}}(t)}, \tag{1}$$

где $R_{\text{Б}}(t)$ — ранговая функция базиса, равная наибольшему рангу[†] СФЭ над Б глубины, не превосходящей t. Приведённая выше асимптотика функции $D_{\text{Б}}(n)$ извлекается с использованием методов [3] из асимптотического соотношения для ранговой функции, вытекающего из определения (1) и фактически доказанного в той же работе [1]:

$$R_{\text{Б}}(t) = 2^{\frac{t}{\tau_{\text{Б}}} \pm o(t)}. \tag{2}$$

Для базисов, в которых глубины ФЭ удовлетворяют некоторым дополнительным ограничениям, могут быть установлены [1, 3] более точные оценки:

$$R_{\text{Б}}(t) = c(t) 2^{\frac{t}{\tau_{\text{Б}}}} + o\big(2^{\frac{t}{\tau_{\text{Б}}}}\big), \tag{3}$$

где $c(t) = O(1)$, с использованием которых методы [3] дают для функции Шеннона $D_{\text{Б}}(n)$ асимптотические оценки высокой степени точности: $D_{\text{Б}}(n) = \tau_{\text{Б}}(n - \log\log n) \pm O(1)$. В настоящей заметке оценки (3) ранговой функции $R_{\text{Б}}(t)$ распространены на базисы Б произвольного вида без дополнительных ограничений на глубины составляющих Б элементов. Следующая теорема позволяет с привлечением методов [3] получать асимптотические оценки функции $D_{\text{Б}}(n)$ вида $D_{\text{Б}}(n) = \tau_{\text{Б}} n - O(\log\log n)$.

Теорема. *Для ранговой функции $R_{\text{Б}}(t)$ произвольного конечного полного базиса* Б *выполняются соотношения* (3)*, в которых $c(t) = O(t^q)$ при некотором целом неотрицательном q.*

Заметим, что поднятие ветвлений выходов ФЭ к входам схемы не изменяет её глубины, поэтому аналогично [2] отсюда вытекает, что для любой одновыходной СФЭ Σ над Б найдётся схема формульного типа (т. е. СФЭ без ветвлений выходов ФЭ, далее для краткости просто формула) над Б, глубина которой совпадает с глубиной Σ. Последнее означает, что $R_{\text{Б}}(t)$ также равно наибольшему рангу формул над Б и мы без ограничения общности можем рассматривать лишь формулы.

Для доказательства основной теоремы мы пользуемся подходом [1] к определению аналогичных (3) асимптотических оценок ранговой функции подмножеств множества всех формул над Б определённого вида, которыми описывается множество формул последовательности определяющей значение предела (1). Ранговая функция $R_{\mathfrak{S}}(t)$ множества $\mathfrak{S}$ формул над Б определяется аналогично $R_{\text{Б}}(t)$ за тем уточнением, что указанные в её определении СФЭ пробегают лишь множество $\mathfrak{S}$. Само множество формул $\mathfrak{S}$ описывается нами как множество корневых поддеревьев бесконечного информационного (ориентированного

[†]Ранг СФЭ — это количество дуг, исходящих из её входов. Это и другие используемые нами понятия можно найти, например, в [2].

корневого) дерева, узлами которого являются ФЭ базиса Б. Указанное информационное дерево упрощается при помощи операции отождествления эквивалентных вершин до конечного или бесконечного ориентированного упорядоченного графа $\mathcal{S}$, который мы называем шаблоном подключений. В случае, когда количество вершин r шаблона $\mathcal{S}$ счётно мы называем его однородным. Вершины шаблона $\mathcal{S}$ нумеруются натуральными числами так, чтобы корню информационного дерева соответствовала вершина с номером один. Выделяя в $\mathcal{S}$ вершину с номером i мы порождаем множество формул $\mathfrak{S}_i$, причем $\mathfrak{S} = \mathfrak{S}_1$. Функции $R_{\mathfrak{S}_1}(t), R_{\mathfrak{S}_2}(t), \ldots$ связаны между собой системой линейных однородных конечноразностных уравнений

$$R_{\mathfrak{S}_i}(t) = \sum_{j=1}^{k_i} \sum_{s=1}^{r} \varepsilon_{ij}^{(s)} R_{\mathfrak{S}_s}\big(t - D_{\eta_i,j,\eta_s}\big) \qquad (t \geqslant \max_{i,j,s} D_{i,j,s}), \tag{4}$$

где η_i — номер ФЭ вершины с номером i, а $\varepsilon_{ij}^{(s)} = 1$, если в $\mathcal{S}$ дуга с номером j ведёт из вершины номер i в вершину номер s, и $\varepsilon_{ij}^{(s)} = 0$ иначе. Для однородных шаблонов подключений и целочисленных глубин асимптотическое поведение решения системы (4) может быть найдено [4] при помощи спектральной теории Перрона неотрицательных матриц. Для неоднородного шаблона $\mathcal{S}$ асимптотическое поведение системы (4) находится аналогично [4] с использованием обобщения [5, 6] теории неотрицательных матриц.

Работа выполнена при поддержке РФФИ (проект № 15-01-07474-а).

Список литературы

[1] Данилов Б. Р. О поведении функции Шеннона для задержки схем в модели, где задержка соединений определяется типами соединяемых элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2014. — Т. 3, № 31. — С. 78–100.

[2] Ложкин С. А. Основы кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004. — 256 с.

[3] Ложкин С. А., Данилов Б. Р. О задержке схем из функциональных элементов в модели с произвольным распределением задержек элементов базиса по входам // Прикладная математика и информатика. № 39. — М.: МАКС Пресс, 2011. — С. 107–129.

[4] Любич Ю. И. Замечание о пропускной способности дискретного канала связи без шумов // Успехи математических наук. — 1962. — Т. 17, вып. 1. — С. 191–198.

[5] Vere-Jones D. Ergodic properties of nonnegative matrices // Pacific Journal of Mathematics. — 1967. — V. 22, N 2 — P. 361–386.

[6] Seneta E. Non-negative matrices and Markov chains. — Springer, 2006. — P. 199–220.

О свойствах конечно-порожденных классов монотонных функций k-значной логики

Дудакова Ольга Сергеевна

Московский государственный университет имени М. В. Ломоносова, e-mail: olga.dudakova@gmail.com

Известно, что все предполные классы функций k-значной логики кроме классов монотонных функций являются конечно-порожденными, кроме того, при $k \leq 7$ все предполные классы монотонных функций k-значной логики также являются конечно-порожденными [1], а начиная с $k = 8$, существуют предполные классы монотонных функций, не имеющие конечного базиса [2] (см. также [1]); полного описания конечно-порожденных предполных классов монотонных функций к настоящему времени не получено. Ранее в работах автора были получены различные условия конечной порожденности классов монотонных функций, в частности, условия существования конечных порождающих систем специального вида в этих классах. В работе [3] получены условия существования в классе монотонных функций функции выбора, которая вместе с константами образует порождающую систему класса. В данной работе исследуются свойства монотонных функций выбора.

Пусть $E_k = \{1, 2, \ldots, k\}$, $\preccurlyeq$ — частичный порядок на множестве E_k. Положим $\mathcal{P} = (E_k, \preccurlyeq)$. Через $\mathcal{M}_\mathcal{P}$ будем обозначать класс всех монотонных функций над множеством $\mathcal{P}$.

Функцию $\lambda(x_0, x_1, \ldots, x_k)$ будем называть *функцией выбора*, если для каждого набора $(i, a_1, \ldots, a_k) \in \mathcal{P}^{k+1}$ выполняется равенство

$$\lambda(i, a_1, \ldots, a_k) = a_i. \tag{1}$$

Легко видеть, что если замкнутый класс функций k-значной логики содержит все константы из E_k и функцию выбора, то он является конечно-порожденным.

Далее положим

$$\mathcal{P}_\lambda = \{(a, b_1, \ldots, b_k) \in \mathcal{P}^{k+1} \mid \text{ если } i \preccurlyeq j, \text{ то } b_i \preccurlyeq b_j\}.$$

Легко видеть, что функция λ монотонна на множестве $\mathcal{P}_\lambda$. Назовем *монотонной функцией выбора* функцию $\nu(x_0, x_1, \ldots, x_k)$ из $\mathcal{M}_\mathcal{P}$, совпадающую на множестве $\mathcal{P}_\lambda$ с функцией $\lambda(x_0, x_1, \ldots, x_k)$.

Следует отметить, что если частичный порядок на множестве $\mathcal{P}$ отличен от тривиального (то есть в $\mathcal{P}$ содержится хотя бы одна пара сравнимых элементов), то $\lambda(x_0, x_1, \ldots, x_k) \notin \mathcal{M}_\mathcal{P}$. Тем не менее, если класс $\mathcal{M}_\mathcal{P}$ содержит монотонную функцию выбора, то он является конечно-порожденным.

Пусть $\mathcal{Q} \subseteq \mathcal{P}$, $\mathcal{Q} \neq \emptyset$. Множество $\mathcal{Q}$ будем называть *стягиванием* множества $\mathcal{P}$, если существует монотонное отображение $\varphi : \mathcal{P} \to \mathcal{Q}$, такое, что $\varphi(x) = x$ для всех $x \in \mathcal{Q}$. При этом отображение φ будем называть *стягивающим отображением*.

Основным результатом данной работы является следующее утверждение.

Теорема. *Пусть $\mathcal{P}$ — частично упорядоченное множество, $\mathcal{Q}$ — стягивание множества $\mathcal{P}$, и пусть в классе $\mathcal{M}_{\mathcal{P}}$ содержится монотонная функция выбора. Тогда в классе $\mathcal{M}_{\mathcal{Q}}$ содержится монотонная функция выбора.*

Доказательство. Пусть $\mathcal{P} = \{1, \ldots, k\},\ \mathcal{Q} = \{q_1, \ldots, q_n\} \subset \{1, \ldots, k\},\ n < k$, пусть φ — стягивающее отображение $\mathcal{P} \to \mathcal{Q}$ и пусть $\nu(x_0, x_1, \ldots, x_k)$ — монотонная функция выбора, определенная на множестве $\mathcal{P}^{k+1}$. Определим функцию $\widehat{\nu}(x_0, x_{q_1}, \ldots, x_{q_n})$ следующим образом: для каждого набора $(a_0, a_{q_1}, \ldots, a_{q_n}) \in \mathcal{Q}^{n+1}$ положим

$$\widehat{\nu}(a_0, a_{q_1}, \ldots, a_{q_n}) = \varphi(\nu(a_0, a_{\varphi(1)}, a_{\varphi(2)}, \ldots, a_{\varphi(k)})).$$

Нетрудно показать, что так определенная функция $\widehat{\nu}$ является монотонной на множестве $\mathcal{Q}^{n+1}$ и на подмножестве $\mathcal{Q}_\lambda$ для нее выполняется соотношение (1). Таким образом, $\widehat{\nu}$ — монотонная функция выбора. **Теорема доказана.**

Список литературы

[1] Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Springer Monographs in Mathematics. Berlin. Springer, 2006. — 668 p.

[2] Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

[3] Дудакова О. С. О порождающих системах в классах монотонных функций многозначной логики // Учен. зап. Казан. ун-та. Серия Физ.-матем. науки. — 2014. — Т. 156, кн. 3. — С. 49–54.

Переходные явления в неразложимых стохастических КС-грамматиках

Дурандин Олег Владимирович[1], **Жильцова Лариса Павловна**[2]

[1] Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: oleg.durandin@gmail.com
[2] Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: larzhil@rambler.ru

В работе исследуются переходные явления, возникающие в неразложимых стохастических КС-грамматиках. Переходные явления возникают в случае, когда перронов корень r матрицы первых моментов грамматики стремится слева к единице, т.е. происходит переход от докритического случая $(r < 1)$ к критическому $(r = 1)$ [1]. Для рассматриваемого случая получена асимптотика условного математического ожидания $M(t, \tau)$ числа вершин, помеченных нетерминальными символами на ярусе τ, в деревьях вывода высоты t. Определен интервал для ярусов дерева вывода, на которых величина $M(t, \tau)$ близка к асимптотическому значению. Установлена зависимость полученных характеристик от величины $\varepsilon = 1 - r$, определяющей близость к критическому случаю.

Стохастической КС-грамматикой называется система $G =< V_N, V_T, R, S >$, где V_N — конечное множество нетерминальных

символов; V_T — конечное множество терминальных символов; S — аксиома грамматики, $S \in V_N$; R — конечное множество правил, представимое в следующем виде: $R = \cup_{i=1}^{k} R_i$, где k — мощность V_N и $R_i = \{r_{i1}, \ldots, r_{i,n_i}\}$. Каждое правило r_{ij} имеет следующий вид:

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij}, \qquad j = 1, \ldots, n_i,$$

где $A_i \in V_N$, $\beta_{ij} \in (V_N \cup V_T)^*$ и p_{ij} — вероятность применения правила r_{ij}, причём $0 < p_{ij} \leq 1$, $\sum_{j=1}^{n_i} p_{ij} = 1$.

Для $\alpha, \gamma \in (V_N \cup V_T)^*$ будем говорить, что γ непосредственно выводимо из α (обозначать $\alpha \Rightarrow \gamma$), если существуют $\alpha_1, \alpha_2 \in (V_N \cup V_T)^*$, для которых $\alpha = \alpha_1 A_i \alpha_2$, $\gamma = \alpha_1 \beta_{ij} \alpha_2$ и в грамматике имеется правило $A_i \xrightarrow{p_{ij}} \beta_{ij}$.

Через $\Rightarrow_*$ обозначим рефлексивное транзитивное замыкание отношения $\Rightarrow$. Множество слов $L_G = \{\alpha : s \Rightarrow_* \alpha, \alpha \in V_T^*\}$ образует КС-язык, порожденный грамматикой G. Каждому слову α КС-языка соответствует последовательность правил грамматики (вывод), с помощью которой α выводится из аксиомы S.

Левым выводом слова α называется вывод, при котором каждое правило в процессе вывода слова α из аксиомы S применяется к самому левому нетерминальному символу в слове. Последовательность правил в левом выводе обозначим как $\omega(\alpha)$. Левому выводу соответствует дерево вывода [2].

Ярусы дерева нумеруются следующим образом. Корень дерева располагается на нулевом ярусе. Вершины дерева, смежные с корнем, образуют первый ярус и т. д. Таким образом, дуги, выходящие из вершин j-го яруса, ведут к вершинам $(j+1)$-го яруса.

Пусть $\alpha \in L_G, \omega(\alpha) = r_{i_1 j_1} r_{i_2 j_2} \ldots r_{i_n j_n}$ — некоторый вывод слова $\alpha \in L_G$, а d — соответствующее этому слову дерево вывода. Вероятность дерева вывода d определим как $p(d) = p_{i_1 j_1} p_{i_2 j_2} \ldots p_{i_n j_n}$. Будем обозначать $D(L_G)$ множество всех деревьев вывода для слов из L_G. Стохастическая КС-грамматика называется согласованной, если $\sum_{d \in D(L_G)} p(d) = 1$ [3].

В работе рассматриваются согласованные стохастические КС-грамматики с одним нетерминальным символом.

Введем понятие производящей функции. Производящая функция $F(s)$ строится по множеству правил R. При рассмотрении грамматик с одним нетерминалом, правила грамматики можно записать в виде: $S \xrightarrow{p_j} \beta_j$. Для каждого правила $S \xrightarrow{p_j} \beta_j$ (где $S \in V_N, \beta_j \in (V_T \cup V_T)^*$) выписывается слагаемое $p_j s^l$, где l — число вхождений нетерминального символа S в правую часть правила. Тогда $F(s) = \sum\limits_{j=1}^{n} p_j s^l$.

Положим

$$r = \frac{\partial F(s)}{\partial s}|_{s=1}, \; B = \frac{\partial^2 F(s)}{\partial s^2}|_{s=1}, \; C = \frac{\partial^3 F(s)}{\partial s^3}|_{s=1}, \; \varepsilon = 1 - r. \qquad (1)$$

Обозначим через $M(t, \tau)$ условное математическое ожидание числа нетерминальных символов на ярусе τ в деревьях вывода высоты t.

Теорема 1. При $\tau \to \infty$ *и* $t - \tau \to \infty$

$$M(t,\tau) \sim 1 + \frac{B}{\varepsilon \cdot r}.$$

Положим

$$d = \max\left\{\frac{2\varepsilon \cdot r + B}{12B},\ \frac{\varepsilon \cdot (2\varepsilon \cdot r + B) \cdot (1+r)}{6(3B^2 + 2B \cdot (1+r) + C)}\right\},$$

где B и C определены в (1).

Теорема 2. *Пусть* $0 < \delta < 1$. *Тогда*

$$\left| M\left(t,\tau\right) - \left(1 + \frac{B}{\varepsilon \cdot r}\right)\right| < \delta$$

при $\tau \in [\tau_1, \tau_2]$, *где*

$$\tau_1 = \left\lceil \left(\ln\delta + \ln\frac{B + \varepsilon \cdot r}{3B}\right) / \ln r \right\rceil,$$

$$\tau_2 = t - \left\lceil \left(\ln\delta + \ln d\right) / \ln r \right\rceil.$$

Отметим, что оценки, полученные в теореме 2, справедливы для любого значения r $(r < 1)$, и поэтому относятся не только к переходным явлениям.

СПИСОК ЛИТЕРАТУРЫ

[1] Севастьянов Б. А. Ветвящиеся процессы. — М.: Наука, 1971.

[2] Фу К. Структурные методы в распознавании образов. — М.: Мир, 1977.

[3] Жильцова Л. П. Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. — Вып. 9. — М.: Физматлит, 2000. — С. 101–126.

Линейные порядки на множестве дискретных случайных величин: использование в комбинаторной оптимизации

Емец Олег Алексеевич[1], **Барболина Татьяна Николаевна**[2]

[1] Полтавский университет экономики и торговли, e-mail: yemetsli@mail.ru

[2] Полтавский национальный педагогический университет имени В. Г. Короленко, e-mail: tn_b@rambler.ru

Актуальным направлением исследований в области оптимизации является изучение задач с неопределенностью различного характера. Один из подходов к решению оптимизационных задач интервальной и нечеткой оптимизации [1],

[2] основан на введении отношения порядка. В докладе предлагается развитие этих идей на случай вероятностной неопределенности.

Будем рассматривать конечнозначные дискретные случайные величины, обозначая сами величины большими латинскими буквами (X, Y, Z), их возможные значения — малыми (x_i, y_i, z_i), а соответствующие вероятности через p_i^x, p_i^y, p_i^z. Через $M(X)$ и $D(X)$ будем обозначать соответственно математическое ожидание и дисперсию случайной величины X.

Определение 1. *Будем называть две дискретные случайные величины X и Y упорядоченными в возрастающем порядке $\prec$ (и обозначать этот факт $X \prec Y$), если выполнено одно из следующих условий:* 1) $M(X) < M(Y)$; 2) $M(X) = M(Y)$ *и* $D(X) > D(Y)$; 3) $M(X) = M(Y)$, $D(X) = D(Y)$ *и найдется такой индекс t, что $x_i = y_i$, $p_i^x = p_i^y$ для всех $1 \le i < t$, и при этом:* 3.1) *либо $x_t < y_t$,* 3.2) *либо $x_t = y_t$ и $p_t^x > p_t^y$.*

Определение 2. *Будем называть две дискретные случайные величины X и Y упорядоченными в неубывающем порядке $\preceq$ (и обозначать этот факт $X \preceq Y$), если $X \prec Y$ или $X = Y$.*

Непосредственной проверкой свойств бинарного отношения $\preceq$ несложно убедиться в справедливости следующего утверждения.

Утверждение 1. *Отношение $\preceq$ на множестве дискретных случайных величин является линейным порядком.*

Линейное упорядочение конечного множества дискретных случайных величин позволяет говорить его о минимальных и максимальных элементах: среди величин $X^1, \ldots, X^s$, удовлетворяющих соотношению $X^1 \preceq \ldots \preceq X^s$, минимумом является X^1, а максимумом — X^s.

Рассмотрим некоторые постановки оптимизационных задач. Пусть D — конечное множество дискретных случайных величин; $(X^1, \ldots, X^n)$ — многомерная случайная величина, где $X^i \in D$; случайная величина R, рассматриваемая как функция $F(X^1, \ldots, X^n)$, принадлежит множеству D, какими бы ни были величины $X^i \in D$. Тогда достаточно общая задача оптимизации на множестве D может быть сформулирована следующим образом: найти минимум функции $F(X^1, \ldots, X^n)$ в некоторой области S n-мерных случайных величин, компоненты которых принадлежат D: $F(X^1, \ldots, X^n) \to \min_{(X^1, \ldots, X^n) \in S}$.

В частности, если S является евклидовым комбинаторным множеством (соответствующую терминологию см. в [3]), будем говорить о безусловной евклидовой задаче комбинаторной стохастической оптимизации. Данная задача может рассматриваться как математическая модель различных практических задач, например, простейших задач упаковки [3]. В таких задачах естественно требовать выполнения свойства введенного порядка и суммы, сформулированного в следующем утверждении.

Утверждение 2. *Если для дискретных случайных величин X и Y выполняется условие $X \prec Y$, и случайные величины X и Z, Y и Z — независимы, то также имеет место $X + Z \prec Y + Z$.*

Доказательство. Обозначим $\bar{X} = X + Z$, $\bar{Y} = Y + Z$. Если имеет место условие 1 или 2 определения 1, то с учетом свойств математического ожидания и дисперсии получаем, что также $\bar{X} = X + Z \prec Y + Z = \bar{Y}$.

Пусть теперь для индекса t выполняется условие 3 определения 1. Тогда для любых j и для всех $i < t$ выполняются равенства $x_i + z_j = y_i + z_j$, $p_i^x p_j^z = p_i^y p_j^z$, откуда $\bar{x}_k = \bar{y}_k$ для всех $k < s$, где $\bar{x}_s = x_t + z_1$, $\bar{y}_s = y_t + z_1$. С другой стороны, для всех $i > t$ и произвольного j имеем $x_i + z_j > x_t + z_j \geq x_t + z_1 = \bar{x}_s$, $y_i + z_j > \bar{y}_s$. Значит, для всех $k < s$ в суммах

$$p_k^{\bar{x}} = \sum_{i,j:x_i+z_j=\bar{x}_k} p_i^x p_j^z,\ p_k^{\bar{y}} = \sum_{i,j:y_i+z_j=\bar{y}_k} p_i^y p_j^z$$

все $i < t$, а значит, $p_k^{\bar{x}} = p_k^{\bar{y}}$. Если $x_t < y_t$, то также $\bar{x}_s < \bar{y}_s$, откуда $\bar{X} \prec \bar{Y}$. Если $x_t = y_t$, то $p_t^x > p_t^y$. Так как для индексов в суммах $x_i + z_j = \bar{x}_s$, $y_i + z_j = \bar{y}_s$ выполняется условие $i \leq t$ (причем если $i = t$, то $j = 1$), то

$$p_s^{\bar{x}} = \sum_{i,j:x_i+z_j=\bar{x}_s, i<t} p_i^x p_j^z + p_t^x p_1^z > \sum_{i,j:y_i+z_j=\bar{y}_s, i<t} p_i^y p_j^z + p_t^y p_1^z = p_s^{\bar{y}},$$

то есть $\bar{X} \prec \bar{Y}$. **Утверждение 2 доказано.**

Следствие 1. *Если для дискретных случайных величин X и Y выполняется условие $X \preceq Y$, и случайные величины X и Z, Y и Z — независимы, то также имеет место $X + Z \preceq Y + Z$.*

Следствие 2. *Если для попарно независимых случайных величин $A_1, \ldots, A_n$, $B_1, \ldots, B_n$ выполняются условия $A_i \preceq B_i$ для всех $i = \overline{1,n}$, то $A_1 + \ldots + A_n \preceq B_1 + \ldots + B_n$.*

Доказательство. Так как случайные величины попарно независимы, то в соответствии со следствием 1 из $A_1 \preceq B_1$ и $A_2 \preceq B_2$ следует, что $A_1 + A_2 \preceq B_1 + A_2 \preceq B_1 + B_2$. Продолжая аналогичные рассуждения для $i = \overline{3,n}$, получим, что $A_1 + \ldots + A_n \preceq B_1 + \ldots + B_n$. **Следствие 2 доказано.**

Отметим, что в зависимости от потребностей моделирования для постановки оптимизационных задач с вероятностной неопределенностью могут использоваться и другие порядки на множестве дискретных случайных величин, в частности,на основе сравнения моментов [4].

Осуществим разбиение заданного конечного множества попарно независимых дискретных случайных величин на классы эквивалентности следующим образом: случайные величины X и Y принадлежат одному классу тогда и только тогда, когда равны их начальные моменты по k-й включительно, то есть $\mu_i(X) = \mu_i(Y)$ для всех $i = \overline{1,n}$ (здесь $\mu_i(X)$ обозначает начальный момент i-го порядка случайной величины X). Классы с представителями X и Y будем называть упорядоченными по неубыванию, если первая отличная от нуля разность $\mu_i(X) - \mu_i(Y)$ является отрицательной.

Доказано, что данное отношение является линейным порядком, причем для него выполняется свойство, аналогичное утверждению 2.

Таким образом, в докладе предложены два подхода к введению порядка на множестве дискретных случайных величин, которые могут использоваться для решения оптимизационных задач с вероятностной неопределенностью.

Список литературы

1. Сергиенко И. В., Емец О. А., Емец А. О. Задачи оптимизации с интервальной неопределенностью: метод ветвей и границ // Кибернетика и системный анализ. — 2013. — № 5. — С. 38–50.
2. Ємець О. О., Ємець Ол-ра О. Розв'язування задач комбінаторної оптимізації на нечітких множинах : монографія. — Полтава : ПУЕТ, 2011. — 239 с. — Электронный вариант доступен: http://dspace.puet.edu.ua/handle/123456789/352.
3. Стоян Ю. Г., Ємець О. О. Теорія і методи евклідової комбінаторної оптимізації. — К.: Інститут системних досліджень освіти, 1993. — 188 с. — Электронный вариант доступен: http://dspace.puet.edu.ua/handle/123456789/487.
4. Емец О.А., Барболина Т.Н. Об оптимизационных задачах с вероятностной неопределенностью // Доповіді Національної академії наук України. — 2014. — № 11. — С. 40–45.

О ключевых предикатах k-значной логики

Жук Дмитрий Николаевич

Московский государственный университет имени М. В. Ломоносова, e-mail: zhuk@intsys.msu.ru

Известно, что может быть построено естественное соответствие Галуа между клонами и замкнутыми множествами предикатов [1], где клон — замкнутый относительно суперпозиции класс функций, содержащий все селекторы, а замыкание на множестве предикатов — замыкание относительно позитивных примитивных формул, то есть формул, содержащих только конъюнкции и кванторы существования. Следовательно любой клон может быть задан некоторым множеством предикатов, и для описания решётки клонов достаточно описать решётку замкнутых множеств предикатов.

Возникает естественный вопрос: нужны ли все предикаты для задания любого клона? Легко убедиться, что без некоторых предикатов можно обойтись, например, нам не нужны предикаты, которые можно представить в виде конъюнкции предикатов меньшей арности. Предикаты, которые не могут быть разложены на более простые таким образом, мы будем называть существенными. Эта простая идея может быть очень полезной, например, она позволяет получить короткое доказательство теоремы Поста о решётке замкнутых классов двухзначной логики [2] и найти для каждого минимального клона трёхзначной логики мощность множества всех надклассов [3]. Более того, мы можем определить оператор замыкания на множестве существенных предикатов, и используя его описывать фрагменты решётки замкнутых классов [4]. С помощью этой идеи был найден самый большой известный фрагмент решётки замкнутых классов трёхзначной логики [5], [6] — удалось описать подрешетку

всех замкнутых классов самодвойственных функций, содержащую континуум классов.

Нужны ли нам все существенные предикаты для описания всех клонов? Оказывается, нет. Пусть предикат представляется в виде конъюнкции предикатов $\rho_1, \ldots, \rho_n$ той же арности, таких что $\rho_i \supset \rho$ и каждый предикат ρ_i может быть получен из ρ с помощью позитивной примитивной формулы. В этом случае предикат может быть разложен на бóльшие предикаты той же арности, а значит без него можно обойтись при описании клонов. Предикаты, которые не могут быть разложены таким образом называются максимальными в [5] и критическими в [7]. Это понятие оказывается очень полезным, так как теперь мы ещё больше сократили множество предикатов, которые нам нужно рассматривать. При этом определение достаточно сложное и даже в двухзначном случае не так просто описать все критические предикаты.

В данной работе мы вводим другое определение. Мы полагаем, что все предикаты определены на конечном множестве A. При этом мы не различаем предикаты и отношения, и говорим, что набор принадлежит предикату, если предикат на нём принимает значение 1. Мы говорим, что вектор функция $\Psi = (\psi_1, \ldots, \psi_h)$ сохраняет предикат ρ если $(\psi_1(a_1), \ldots, \psi_h(a_h)) \in \rho$ для любого набора $(a_1, \ldots, a_h) \in \rho$. Предикат ρ арности h называется *ключевым*, если существует набор $\beta \in A^h \setminus \rho$, такой что для любого набора $\alpha \in A^h \setminus \rho$ существует вектор-функция Ψ, которая сохраняет предикат ρ и отображает α в β. Набор β называется *ключевым* для ρ.

Можно показать, что любой критический предикат является ключевым, а следовательно нам достаточно ключевых предикатов для задания всех клонов. Подтверждением того, что понятие ключевого предиката является очень удобным, является следующее описание всех ключевых предикатов двузначной логики.

Теорема 1. *Пусть ρ — предикат двузначной логики. Тогда ρ — ключевой предикат тогда и только тогда, когда $\rho(x_1, \ldots, x_n) = L_1 \vee L_2 \vee \ldots \vee L_m$ для линейных уравнений $L_1, L_2, \ldots, L_m$, где $L_i = (a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n = a_0)$.*

Оказалось, что уже в трёхзначном случае ключевые предикаты не имеют такого красивого описания. В данной работе было получено описание всех ключевых предикатов в k-значном случае, которые сохраняются слабой функцией почти единогласия.

Функция f называется *идемпотентной*, если $f(x, x, \ldots, x) = x$. *Слабая функция почти единогласия* (СФПЕ) — идемпотентная функция f, удовлетворяющая следующему условию:

$$f(x, y, y, \ldots, y) = f(y, x, y, \ldots, y) = \cdots = f(y, y, \ldots, y, x).$$

Легко убедиться, что в двухзначном случае функцией почти единогласия являются конъюнкция, дизъюнкция, функция голосования, а также функция $x + y + z$. Таким образом, любой замкнутый класс, содержащий существенную функцию, также содержит функцию почти единогласия. Нечто похожее можно доказать и для k-значного случая, что оправдывает рассмотрение только таких ключевых предикатов.

Для предиката ρ арности n мы определяем бинарное отношение на множестве $\{1, 2, \ldots, n\}$, которое будем называть шаблоном предиката. Мы полагаем по определению $i \overset{\rho}{\sim} i$ для любого $i \in \{1, 2, \ldots, n\}$. Для $i \neq j$ мы говорим, что $i \overset{\rho}{\sim} j$, если не существует $a_1, \ldots, a_n, b_i, b_j \in A$, таких, что

$$\begin{pmatrix} a_1 \\ \cdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \cdots \\ a_{j-1} \\ a_j \\ a_{j+1} \\ \cdots \\ a_n \end{pmatrix} \notin \rho, \begin{pmatrix} a_1 \\ \cdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \cdots \\ a_{j-1} \\ b_j \\ a_{j+1} \\ \cdots \\ a_n \end{pmatrix}, \begin{pmatrix} a_1 \\ \cdots \\ a_{i-1} \\ b_i \\ a_{i+1} \\ \cdots \\ a_{j-1} \\ a_j \\ a_{j+1} \\ \cdots \\ a_n \end{pmatrix}, \begin{pmatrix} a_1 \\ \cdots \\ a_{i-1} \\ b_i \\ a_{i+1} \\ \cdots \\ a_{j-1} \\ b_j \\ a_{j+1} \\ \cdots \\ a_n \end{pmatrix} \in \rho.$$

Теорема 2. *Пусть ρ — ключевой предикат, сохраняемый СФПЕ. Тогда шаблон предиката ρ — отношение эквивалентности. При этом не более одного класса эквивалентности содержит более одного элемента.*

Теорема 3. *Пусть ρ — ключевой предикат арности n, сохраняемый СФПЕ, чей шаблон равен $\{\{1, 2, \ldots, r\}, \{r+1\}, \{r+2\}, \ldots, \{n\}\}$. Тогда для любого ключевого набора $(a_1, \ldots, a_n)$ существуют $\boldsymbol{B} = B_1 \times B_2 \times \cdots \times B_n$, простое число p и биективные отображения $\phi_i : B_i \to \mathbb{Z}_p$ для $i = 1, 2, \ldots, r$, такие что $(a_1, \ldots, a_n) \in \boldsymbol{B}$, $B_i = \{a_i, b_i\}$ for $i = r+1, \ldots, n$,*

$$\rho \cap \boldsymbol{B} = (\phi_1(x_1) + \ldots + \phi_r(x_r) = 0) \vee (x_{r+1} = b_{r+1}) \vee \cdots \vee (x_n = b_n),$$

и каждый набор $\gamma \in \boldsymbol{B} \setminus \rho$ — ключевой набор для ρ.

Это означает, что в каждом ключевом предикате, сохраняемом СФПЕ, можно найти часть, которая устроена некоторым регулярным образом. Эта часть определяется как дизъюнкция линейных уравнений, среди которых только одно может быть нетривиальным.

Работа выполнена при поддержке РФФИ (проект № 13-01-00684-а).

Список литературы

[1] Бондарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста I-II // Кибернетика. — 1969. — № 3, с. 1–10; № 5, с. 1–9.

[2] Жук Д. Н. Предикатный метод построения решетки Поста // Дискретная математика. — 2011. — Т. 23, вып. 2. — С. 115–128.

[3] Zhuk D. The cardinality of the set of all clones containing a given minimal clone on three elements // Algebra universalis. — 2012. — V. 68. — P. 295–320.

[4] Zhuk D., Moiseev S. On the clones containing a near-unanimity function // IEEE 43rd International Symposium on Multiple-Valued Logic, Japan 2013.

[5] Zhuk D. The lattice of all clones of self-dual functions in three-valued logic // Journal of Multiple-Valued Logic and Soft Computing. — 2015. — V. 24(1–4). — P. 254–316.

[6] Жук Д. Н. Решетка замкнутых классов самодвойственных функций трехзначной логики. М.: Издательство МГУ, 2011.

[7] Kearnes K. A., Szendrei Á. Clones of algebras with parallelogram terms // Internat. J. Algebra Comput. — 2012. — V. 22, N 1.

Асимптотическая сложность и глубина обратимых схем из элементов NOT, CNOT и 2-CNOT

Закаблуков Дмитрий Владимирович

Московский государственный технический университет им. Н. Э. Баумана, e-mail: dmitriy.zakablukov@gmail.com

Теория схемной сложности берет свое начало с работы Шеннона [1], в которой было предложено в качестве меры сложности булевой функции рассматривать сложность реализующей ее минимальной схемы из функциональных элементов. На сегодняшний день доказана асимптотическая сложность $L(n) \sim 2^n/n$ для булевых функций от n переменных [2] в базисе классических функциональных элементов, таких как инвертор, дизъюнктор, конъюнктор и др.

Вычисления с ограниченной памятью были рассмотрены в работе [3]. Карповой Н. А. было доказано, что асимптотика функции Шеннона сложности схем в базисе из функциональных элементов, соответствующих всем p-местным булевым функциям, зависит только от p и никак не зависит от количества t используемых регистров памяти при $t \geq 3$. Также в этой работе было показано, что для любой булевой функции существует реализующая ее схема, использующая всего два регистра памяти.

Лупановым О. Б. в работе [4] были рассмотрены схемы из функциональных элементов с задержками. Было доказано, что в регулярном базисе функциональных элементов, имеющих равные единичные задержки, любая булева функция от n переменных может быть реализована схемой, имеющей задержку n. При этом такая схема будет иметь асимптотически наилучшую сложность. Однако до сегодняшнего дня не рассматривался вопрос зависимости задержки схемы от количества используемых регистров памяти.

Определение обратимых функциональных элементов было впервые введено Фейнманом в работе [5]. Обратимые функциональные элементы NOT и k-CNOT, а также синтез схем из этих элементов были рассмотрены, к примеру, в работе [6].

Через N_j^n обозначается функциональный элемент NOT (инвертор) с n входами, инвертирующий значение на j-м выходе. Через $C^n_{i_1,\ldots,i_k;j} = C^n_{I;j}$, $j \notin I$, обозначается функциональный элемент k-CNOT с n входами (контролируемый инвертор, обобщенный элемент Тоффоли с k контролирующими входами), инвертирующий значение на j-м выходе тогда и только тогда, когда значения на всех входах $i_1, \ldots, i_k$ равно 1. Обозначим через Ω_n^2 множество всех функциональных элементов NOT, 1-CNOT (CNOT) и 2-CNOT с n входами.

Будем рассматривать обратимые схемы, состоящие из элементов множества Ω_n^2. В таких схемах запрещено ветвление и произвольное подключение входов и выходов функциональных элементов. В ориентированном графе, описывающем обратимую схему, все вершины, соответствующие функциональным элементам, имеют ровно n занумерованных входов и выходов. Эти вершины нумеруются

от 1 до l, при этом i-й выход m-й вершины, $m < l$, соединяется только с i-м входом $(m+1)$-й вершины. Входами обратимой схемы являются входы первой вершины, а выходами — выходы l-й вершины.

Всем i-м входам и выходам вершин графа приписывается символ r_i из некоторого множества $R = \{ r_1, \ldots, r_n \}$, который можно интерпретировать как имя регистра памяти (номер ячейки памяти). В этих ячейках памяти хранится текущий результат работы схемы. В один момент времени (один такт работы схемы) может быть инвертированно значение не более, чем в одном регистре памяти. В этом заключается существенное отличие обратимых схем от схем из классических функциональных элементов, рассмотренных Лупановым О. Б. и Карповой Н. А. в своих работах.

Основными свойствами обратимой схемы $\mathfrak{S}$ являются ее сложность и глубина. Сложность схемы $L(\mathfrak{S})$ — количество функциональных элементов в схеме. Глубина схемы $D_i(\mathfrak{S})$ по i-му входу — количество элементов схемы, у которых либо i-й вход является контролирующим, либо i-й выход является контролируемым. Глубина схемы $D(\mathfrak{S}) = \max_i D_i(\mathfrak{S})$.

Обозначим через $P_2(n,n)$ множество всех булевых отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Обозначим через $F(n,m) \subseteq P_2(n,n)$ множество всех отображений, которые могут быть реализованы обратимой схемой с $(n+m)$ входами.

Обозначим через $L(f,N)$ и $D(f,N)$ минимальную сложность и глубину, соответственно, обратимой схемы, состоящей из функциональных элементов множества Ω_{n+N}^2 и реализующей некоторое отображение $f \in F(n,N)$ с использованием N дополнительных входов. Определим функции Шеннона $L(n,N)$ и $D(n,N)$ для сложности и глубины обратимой схемы, соответственно:

$$L(n,N) = \max_{f \in F(n,N)} L(f,N), \qquad D(n,N) = \max_{f \in F(n,N)} D(f,N).$$

Для величин $L(n,N)$ и $D(n,N)$ можно доказать следующие теоремы.
Теорема 1. *Нижняя оценка сложности и глубины обратимой схемы:*

$$L(n,N) \gtrsim \frac{n2^n - \log_2 A_{n+N}^n - N}{2\log_2(n+N)},$$
$$D(n,N) \gtrsim \frac{n2^n - \log_2 A_{n+N}^n - N}{2(n+N)\log_2(n+N)}.$$

Теорема 2. *Верхняя оценка сложности и глубины обратимой схемы, не использующей дополнительные входы:*

$$L(n,0) \lesssim 52n2^n/\log_2 n,$$
$$D(n,0) \lesssim 36n2^n/\log_2 n.$$

Теорема 3. *Верхняя оценка сложности и глубины обратимой схемы, использующей дополнительные входы:*

$$L(n, N_0) \lesssim 2^n \text{ при } N_0 \sim n2^{n-n/\log_2 n},$$
$$D(n, N_1) \lesssim 4n \text{ при } N_1 \sim 2^{n+1},$$
$$D(n, N_2) \lesssim 2,5n \text{ при } N_2 \sim 2^{n+2},$$
$$D(n, N_3) \lesssim 2n \text{ при } N_3 \sim \frac{5n2^n}{\log_2 n}.$$

Доказательство некоторых оценок для $L(n, N)$ было опубликовано в работе [7].

Из теорем (1)–(3) следует, что использование дополнительных входов в рассматриваемых обратимых схемах почти всегда позволяет снизить сложность и глубину обратимой схемы, чего нельзя утверждать про схемы, состоящие из классических необратимых функциональных элементов.

Список литературы

[1] Shannon C. E. The Synthesis of Two-Terminal Switching Circuits // Bell System Technical Journal. — 1949. — V. 28, N 8. — P. 59–98.

[2] Яблонский С. В. Введение в дискретную математику. — М.: Высш. шк., 2003. — 384 с.

[3] Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. — Вып. 2. — М.: Наука, 1989. — С. 131–144.

[4] Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. — Вып. 23. — М.: Наука, 1970. — С. 43-81.

[5] Feynman R. Quantum Mechanical Computers // Optic News. — 1985. — V. 11, N 2. — P. 11–20.

[6] Закаблуков Д. В. Быстрый алгоритм синтеза обратимых схем на основе теории групп подстановок // Прикладная дискретная математика. — 2014. — № 2. — С. 101–109.

[7] Закаблуков Д. В. Вентильная сложность обратимых схем как мера сложности четных подстановок // Вестник МГТУ им. Н. Э. Баумана. Серия «Приборостроение». Готовится к публикации в первом номере 2015 года.

Существенные точки и разрешающие множества k-пороговых функций

Замараева Елена Михайловна

Нижегородский госуниверситет им. Н. И. Лобачевского, e-mail: elena.zamaraeva@gmail.com

Рассматриваются функции $f : E_n^d = \{0, 1, \ldots, n-1\}^d \to \{0, 1\}, n \geq 2, d \geq 1$. Обозначим $M_\nu(f) = \{x \in E_n^d : f(x) = \nu\}$ для $\nu = 0, 1$.

Функция $f : E_n^d \to \{0, 1\}$ называется *k-пороговой*, $k \geq 1$, если существуют вещественные числа $a_{10}, a_{11}, \ldots, a_{kd}$ такие, что

$$M_1(f) = \left\{ x \in E_n^d : \sum_{j=1}^{d} a_{ij} x_j \leq a_{i0} \text{ для } i = 1, \ldots, k \right\}, \tag{1}$$

при этом неравенства $\sum\limits_{j=1}^{d} a_{ij} x_j \leq a_{i0}$ для $i = 1, \ldots, k$ называются *пороговыми*. В случае $k = 1$ функция называется *пороговой*.

Для функций, заданных на множестве E_n^d, обозначим через $\mathfrak{T}(d, n, k)$ — множество всех k-пороговых функций при фиксированном k, а через $\mathfrak{T}(d, n, *)$ — множество всех k-пороговых функций по всем k, то есть $\mathfrak{T}(d, n, *) = \bigcup\limits_{k \geq 1} \mathfrak{T}(d, n, k)$.

Если f — k-пороговая функция над E_n^d, то существуют пороговые функции $f_1, \ldots, f_k$ такие, что $f(x) = f_1(x) \& \ldots \& f_k(x)$. Будем говорить, что f *задана* набором функций $f_1, \ldots, f_k$.

Разрешающим множеством функции $f \in C$ относительно класса C называется множество точек T такое, что если для некоторой функции $g \in C, f(x) = g(x)$ для всех $x \in T$, то $f \equiv g$. Минимальное по включению разрешающее множество называется *тупиковым*. Минимальное по мощности разрешающее множество для функции f назовем *наименьшим*.

Точка x называется *существенной* для функции $f \in C$ относительно класса C, если существует некая функция $h \in C$ такая, что $f(x) \neq h(x)$ и $f(y) = h(y)$ для любых $y \neq x$. Множество существенных точек функции относительно класса C обозначим через $S(f, C)$. Известно, что тупиковое разрешающее множество пороговой функции представляет собой множество всех ее существенных точек. В общем случае множество существенных точек не является разрешающим для k-пороговой функции при фиксированном k. Кроме того, в общем случае тупиковое разрешающее множество не единственно для k-пороговой функции при фиксированном k.

Пусть $\sigma(f, C)$ — мощность наименьшего разрешающего множества для $f \in C$ относительно класса C. *Длиной обучения* в классе функций C называется

$$\sigma(C) = \max_{f \in C} \sigma(f, C).$$

Известна оценка длины обучения в классе пороговых функций при фиксированном d (см. [1, 2]):

$$\sigma(\mathfrak{T}(d, n)) = \Theta(\log_2^{d-2} n).$$

В данной работе описывается связь между множеством существенных точек и тупиковым разрешающим множеством в классе $\mathfrak{T}(d, n, *)$ (утверждение 1) и дается оценка мощности тупикового разрешающего множества для нетривиальных функций из $\mathfrak{T}(2, n, *)$ (утверждение 3). Также оценивается мощность

разрешающего множества 2-пороговых функций для $d = 2$ при некоторых специальных условиях (утверждение 4).

Выпуклую оболочку точек множества $X \subseteq \mathbb{R}^d$ обозначим через $\mathrm{Conv}(X)$. Множество вершин политопа P обозначим через $\mathrm{Vert}(P)$. Для произвольного выпуклого многоугольника P и его вершины v через $q(v, P)$ обозначим угол при вершине v в этом многоугольнике, а через $\mathcal{P}(P)$ — периметр P. Для $f \in \mathfrak{T}(d, n, *)$ обозначим $P(f) = \mathrm{Conv}(M_1(f))$.

Утверждение 1. *Для любой функции $f \in \mathfrak{T}(d, n, *)$ множество $S(f, \mathfrak{T}(d, n, *))$ является разрешающим множеством, и*

$$S(f, \mathfrak{T}(d, n, *)) = \begin{cases} E_n^d, & M_1(f) = \emptyset; \\ \mathrm{Vert}(P(f)) \cup D(f), & M_1(f) \neq \emptyset; \end{cases}$$

где $D(f) = \{x \in M_0(f) : \mathrm{Conv}(P(f) \cup \{x\}) \cap M_0(f) = \{x\}\}$.

Следствие 2. *$\sigma(\mathfrak{T}(d, n, k)) = n^d$ для любого $k > 1$.*

Обозначим $B(E_n^2) = \{x \in E_n^2 : x_1 = 0 \vee x_2 = 0 \vee x_1 = n - 1 \vee x_2 = n - 1\}$.

Рассмотрим некоторую функцию $f \in \mathfrak{T}(2, n, *)$ такую, что $P(f)$ имеет ненулевую площадь. Пусть $a_1x_1 + a_2x_2 = a_0$ является уравнением прямой, на которой лежит некоторое ребро из $P(f)$. Не теряя общности, можем считать, что НОД$(a_1, a_2) = 1$. Из двух неравенств $a_1x_1 + a_2x_2 \leq a_0$ и $a_1x_1 + a_2x_2 \geq a_0$ назовем *реберным* то, которое удовлетворяется во всех точках $P(f)$.

Пусть $f \in \mathfrak{T}(2, n, *)$, $P(f)$ имеет ненулевую площадь и реберные неравенства: $a_{i1}x_1 + a_{i2}x_2 \leq a_{i0}, i = 1, \ldots, |\mathrm{Vert}(P(f))|$.

Пусть $P'(f) = \{x = (x_1, x_2) : a_{i1}x_1 + a_{i2}x_2 \leq a_{i0} + 1\}$ и пусть $\Delta P(f) = P'(f) \setminus P(f)$.

Тогда имеет место следующее

Утверждение 3. *Пусть $f \in \mathfrak{T}(2, n, *)$ и $P(f)$ имеет ненулевую площадь. Тогда*

$$S(f, \mathfrak{T}(2, n, *)) = (\Delta P(f) \cap M_0(f)) \cup \mathrm{Vert}(P(f))$$

и

$$|S(f, \mathfrak{T}(2, n, *))| = O\left(\min\left(n, \mathcal{P}(P(f)) + \frac{1}{q_{min}(P(f))}\right)\right),$$

где $q_{min}(P(f))$ — наименьший угол при вершинах $P(f)$, не входящих в $B(E_n^2)$.

Пусть $\mathfrak{A}$ — множество всех пар пороговых неравенств f, одновременно превращающихся в равенства в какой-то точке из $\mathrm{Conv}(E_n^2)$. Обозначим эту точку через $o(A)$ для $A \in \mathfrak{A}$. Рассмотрим лучи с началом в точке $o(A)$, лежащие на пороговых прямых и заключающие между собой $M_1(f)$. Точки пересечения этих лучей с $\mathrm{Conv}(E_n^2)$ обозначим через $a_1(A)$ и $a_2(A)$. Также обозначим $p_{max}(f) = \max\limits_{A \in \mathfrak{A}} \angle(a_1(A), o(A), a_2(A))$.

Утверждение 4. *Пусть $f \in \mathfrak{T}(2, n, 2) \setminus \mathfrak{T}(2, n, 1)$, $|M_1(f)| > 1$, $B(E_n^2) \cap M_1(f) \neq \emptyset$, $M_1(f) \not\subseteq B(E_n^2)$ и f может быть задана как минимум двумя разными множестами пороговых функций. Тогда существует разрешающее*

множество T такое относительно $\mathfrak{T}(2, n, 2)$, что:

$$|T| = O\left(\frac{1}{\pi - p_{max}(f)} + \frac{1}{\max\left(p_{max}(f) - \arctan\frac{1}{l_1-1} - \arctan\frac{1}{l_2-1}, \frac{1}{4(l_1+l_2)^2}\right)}\right),$$

где $l_i = |o(A) - a_i(A)|$, $A \in \mathfrak{A}$ и $\angle(a_1(A), o(A), a_2(A)) = p_{max}(f)$.

СПИСОК ЛИТЕРАТУРЫ

[1] Шевченко В. Н., Золотых Н. Ю. О нижней оценке сложности расшифровки пороговых функций k-значной логики // Журн. вычисл. матем. и матем. физики. — 1999. — Т. 39, № 2. — С. 346–352.

[2] Золотых Н. Ю., Чирков А. Ю. Сложность расшифровки пороговых функций многозначной логики // Материалы XI Международного семинара «Дискретная математика и ее приложения» (18–23 июня 2012 г.). — Москва: Изд-во механико-матем. факультета МГУ. — 2012. — С. 63–67.

[3] Zamaraeva E. On teaching sets of k-threshold functions // arXiv:1502.04340v1 [math.CO], Feb. 15, 2015.

Аксиоматизируемость наследственных классов графов и матроидов

Ильев Артем Викторович[1], **Ильев Виктор Петрович**[2]

[1] Институт математики им. С. Л. Соболева СО РАН, e-mail: artyom_iljev@mail.ru

[2] Омский государственный университет им. Ф. М. Достоевского, e-mail: iljev@mail.ru

Введение

Класс алгебраических систем — это семейство однотипных систем сигнатуры Σ. Класс $\boldsymbol{K}$ алгебраических систем называется *аксиоматизируемым*, если существует такое множество предложений Z сигнатуры Σ, что произвольная система $\mathcal{M}$ принадлежит $\boldsymbol{K}$, если и только если любое предложение $\varphi \in Z$ истинно в $\mathcal{M}$. Множество предложений Z называется *множеством аксиом* для $\boldsymbol{K}$. Если для класса $\boldsymbol{K}$ существует конечное множество аксиом, то класс $\boldsymbol{K}$ называется *конечно аксиоматизируемым*.

Предложение φ называется *универсальным предложением* или $\forall$*-предложением*, если $\varphi = \forall x_1 \ldots \forall x_n \psi$, где ψ — бесквантороная формула, содержащая только переменные $x_1, \ldots, x_n$. Если для класса $\boldsymbol{K}$ существует множество аксиом, состоящее только из $\forall$-предложений, то класс $\boldsymbol{K}$ называется *универсально аксиоматизируемым* или $\forall$*-аксиоматизируемым*.

В данной работе методами теории моделей исследуются некоторые классы графов и матроидов. Рассмотрены вопросы универсальной аксиоматизируемости и конечной аксиоматизируемости наследственных классов графов. Предложены различные способы аксиоматизации класса матроидов предписанного ранга на языке исчисления предикатов первого порядка с равенством.

1. Наследственные классы графов

Граф в терминах теории моделей [1] — это алгебраическая система $G = \langle V, \Sigma \rangle$, носитель которой V — непустое множество вершин, а сигнатура $\Sigma = \langle E, = \rangle$ состоит из бинарного предиката смежности вершин и предиката равенства, причем предикат смежности $E(x, y)$ *иррефлексивен и симметричен*, т. е. удовлетворяет условию:

$$\forall x \forall y \; [\neg E(x, x) \wedge (E(x, y) \to E(y, x))].$$

Таким образом, класс графов является конечно $\forall$-аксиоматизируемым.

Граф *конечен*, если множество его вершин конечно. Граф $H = \langle V_H, \Sigma \rangle$ является *подграфом* графа $G = \langle V_G, \Sigma \rangle$, если $V_H \subseteq V_G$ и любая пара смежных вершин графа H смежна в графе G.

Пусть $\boldsymbol{H}$ — некоторый класс графов. Тогда класс $Forb(\boldsymbol{H})$, состоящий из всех графов, не содержащих подграфов из $\boldsymbol{H}$, является абстрактным классом, т. е. замкнут относительно изоморфизма. Этот класс может быть определен заданием графов $H \in \boldsymbol{H}$ в качестве *запрещенных подграфов*. *Наследственный класс* графов — это абстрактный класс, замкнутый относительно взятия подграфов. Показано, что для наследственных классов графов справедливы утверждения.

Теорема 1. *Любой наследственный класс графов, который может быть определен в терминах конечных запрещенных подграфов, является $\forall$-аксиоматизируемым.*

Теорема 2. *Наследственный класс графов, который не может быть определен в терминах конечного множества запрещенных подграфов, не является конечно аксиоматизируемым.*

Теорема 3. *Наследственный класс графов аксиоматизируем тогда и только тогда, когда он может быть определен в терминах конечных запрещенных подграфов.*

2. Аксиоматизируемость классов матроидов

Впервые понятие матроида было введено Уитни в работе [2] и охватывало только конечный случай.

Матроид — это пара $M = (U, \mathcal{I})$, где U — непустое конечное множество, $\mathcal{I}$ — непустое семейство его подмножеств (называемых *независимыми*), удовлетворяющее аксиомам:

(A1) $I \in \mathcal{I},\ J \subseteq I \Rightarrow J \in \mathcal{I}$ (аксиома наследственности);

(A2) для любых $I, J \in \mathcal{I}$ таких, что $|J| = |I| + 1$, существует элемент $j \in J \setminus I$, для которого $I \cup \{j\} \in \mathcal{I}$ (аксиома пополнения).

Максимальные независимые подмножества множества $A \subseteq U$ называются *базами* множества A. Максимальные независимые подмножества множества U называются *базами матроида* M. Напомним, что в матроиде все базы любого множества равномощны. *Рангом* $r(A)$ множества A называется мощность любой базы A. Число $r(M) = r(U)$ называется *рангом матроида* M.

Пусть $k \in \mathbb{N}$ — фиксированное число. Тогда в бесконечном случае *матроид ранга, не превосходящего* k, — это пара $M = (U, \mathcal{I})$, где U — непустое множе-

ство, $\mathcal{I}$ — непустое семейство его независимых подмножеств, удовлетворяющее аксиомам (A1), (A2), а также аксиоме (A3):

(A3) $|I| \leq k$ для всех $I \in \mathcal{I}$.

Чтобы определить класс *матроидов ранга* $k \in \mathbb{N}$, в приведенном выше определении аксиому (A3) нужно заменить на аксиому (A3′):

(A3′) $r(M) = k$.

Класс матроидов ранга, не превосходящего k, аксиоматизируем следующим образом.

Матроид M ранга, не превосходящего k, — это алгебраическая система $M = \langle U, \Sigma_I \rangle$, где U — непустое множество, а сигнатура $\Sigma_I = \langle I_0, I_1, ..., I_k, = \rangle$ состоит из $k+1$ предикатов независимости, местность каждого из которых совпадает с его порядковым номером, и предиката равенства, причем предикаты независимости удовлетворяют условиям *неупорядоченности и неповторения элементов, наследственности* и *пополнения*:

1) $\forall x_1 \ ... \ \forall x_n \ [I_n(x_1, ..., x_n) \rightarrow \bigwedge\limits_{\pi} I_n(\pi(x_1), ..., \pi(x_n))]$, где π пробегает по всем перестановкам элементов $x_1, ..., x_n$, $n \in \{1, ..., k\}$;

2) $\forall x_1 \ ... \ \forall x_n \ [I_n(x_1, ..., x_n) \rightarrow \bigwedge\limits_{i \neq j} (x_i \neq x_j)]$, $n \in \{1, ..., k\}$;

3) $\forall x_1 \ ... \ \forall x_n \ [(I_n(x_1, ..., x_n) \rightarrow I_{n-1}(x_2, ..., x_n) \wedge \ ... \ \wedge I_{n-1}(x_1, ..., x_{n-1})) \wedge I_0]$, $n \in \{2, ..., k\}$;

4) $\forall x_1 \ ... \ \forall x_n \ \ \forall y_1 \ ... \ \forall y_{n+1} \ \ [I_n(x_1, ..., x_n) \ \wedge \ I_{n+1}(y_1, ..., y_{n+1}) \ \rightarrow \bigvee\limits_{i \in \{1,...,n+1\}} I_{n+1}(x_1, ..., x_n, y_i)]$, $n \in \{1, ..., k-1\}$.

Чтобы определить *матроид ранга* $k \in \mathbb{N}$, в приведенное выше определение нужно добавитить пятую аксиому:

5) $\exists x_1 \ ... \ \exists x_k \ I_k(x_1, ..., x_k)$.

Класс матроидов ранга k аксиоматизируем также в терминах баз.

Матроид M ранга k — это алгебраическая система $M = \langle U, \Sigma_B \rangle$, где U — непустое множество, а сигнатура $\Sigma_B = \langle B, = \rangle$ состоит из k-местного предиката баз матроида и предиката равенства, причем предикат баз удовлетворяет условиям:

1) $\forall x_1 \ ... \ \forall x_k \ [B(x_1, ..., x_k) \rightarrow \bigwedge\limits_{\pi} B(\pi(x_1), ..., \pi(x_k))]$, где π пробегает по всем перестановкам элементов $x_1, ..., x_k$;

2) $\forall x_1 \ ... \ \forall x_k \ [B(x_1, ..., x_k) \rightarrow \bigwedge\limits_{i \neq j} (x_i \neq x_j)]$;

3) $\forall x_1 \ ... \ \forall x_k \ \forall y_1 \ ... \ \forall y_k \ [B(x_1, ..., x_k) \wedge B(y_1, ..., y_k) \rightarrow \bigwedge\limits_{i \in \{1,...,k\}} (B(x_i, y_2, ..., y_k) \vee B(y_1, x_i, y_3, ..., y_k) \vee \ ... \ \vee B(y_1, ..., y_{k-1}, x_i))]$;

4) $\exists x_1 \ ... \ \exists x_k \ B(x_1, ..., x_k)$.

Список литературы

[1] Ершов Ю. Л., Лавров И. А., Тайманов А. Д., Тайцлин М. А. Элементарные теории // Успехи мат. наук. — 1965. — Т. 20, № 4. — С. 37–108.

[2] Whitney H. On the abstract properties of linear dependence // American Journal of Mathematics. — 1935. — V. 57. — P. 509–533.

Избыточность конструктивных описаний (r, s)-деревьев

Иорданский Михаил Анатольевич

Мининский университет, e-mail: iordanski@mail.ru

Рассматриваются обыкновенные неориентированные графы. Используется конструктивный подход к представлению графов, при котором одни графы строятся из других с помощью бинарных *операций склейки*, реализуемых путем отождествления изоморфных подграфов графов-операндов. Подграф результирующего графа операции склейки, соответствующий отождествлённым подграфам графов-операндов, называется *подграфом склейки*. Конструктивные описания графов обладают *избыточностью*, поскольку подграфы склейки, соответствующие каждой операции склейки, задаются двумя их изоморфными копиями в графах-операндах. Эта избыточность позволяет формулировать условие наследования результирующими графами операций склейки характеристических свойств графов-операндов в терминах ограничений на вид отождествляемых подграфов, их выбор в графах-операндах и способ отождествления [1].

Избыточность конструктивного описания можно оценивается с помощью вершинной и (или) реберной компоненты. Вершинная избыточность находится по формуле

$$I_v^c(G) = \frac{\sum\limits_{i=1}^{q} |V(\tilde{G}_i)|}{|V(G)|}, \tag{1}$$

где q — число операций склейки в суперпозиции c, реализующей граф G, $\tilde{G}_i$ — подграф склейки i-ой операции.

Для реберной избыточности используется формула

$$I_e^c(G) = \frac{\sum\limits_{i=1}^{q} |E(\tilde{G}_i)|}{|E(G)|}. \tag{2}$$

Формула (1) определяет среднее число операций склейки, в которых участвуют вершины графа G, а формула (2) — среднее число операций склейки, в которых участвуют рёбра графа G.

В [2] получены оценки для величины вершинной избыточности (1) конструктивных описаний эйлеровых графов. В [3] получены оценки для величины реберной избыточности (2) конструктивных описаний гамильтоновых планарных графов.

В работе рассматриваются (r, s)-деревья, которые можно построить из графов K_r путём склейки по подграфам K_s, $s < r$. Поскольку для задания полного графа достаточно перечислить его вершины, то рассматривается вершинная избыточность (r, s)-деревьев. Пусть $T_n^{r,s}$ - множество всех (r, s)-деревьев, каж-

дое из которых содержит по n-вершин. Обозначим $\max\limits_{G\in T_n^{r,s}} I_v^c(G)$ через $I_v(T_n^{r,s})$. Справедлива

Теорема 1. $I_v(T_n^{r,s}) < \frac{n}{4}$.

Доказательство. Из конструктивного описания (r,s)-деревьев следует, что $n \equiv r \pmod{(r-s)}$ и число операций склейки равно $(n-r)/(r-s)$. При этом для числа вершин во всех подграфах склейки графа $G \in T_n^{r,s}$ справедливо равенство

$$\sum_{i=1}^{q} |V(\tilde{G}_i)| = s\frac{n-r}{r-s}. \tag{3}$$

Для любого фиксированного $1 \le s \le n-2$ функция $f(r,s) = s(n-r)/(r-s)$ растёт при уменьшении r от $r = n-1$ до величины $r = s+1$. При этом получаем функцию $f(r) = (r-1)(n-r)$, имеющую максимум при $r = (n+1)/2$. Учитывая (3), получаем

$$I_v(T_n^{r,s}) = \frac{(n-1)^2}{4n} < \frac{n}{4}.$$

Теорема 1 доказана.

Список литературы

[1] Иорданский М. А. Избыточность конструктивных описаний эйлеровых графов // Материалы XVII международной конференции «Проблемы теоретической кибернетики» (Казань, 16–20 июня 2014 г.). Под редакцией Ю. И. Журавлёва. — Казань: Отечество, 2014. — С. 115–116.

[2] Иорданский М. А. Избыточность конструктивных описаний гамильтоновых планарных графов // Материалы XI международного семинара «Дискретная математика и её приложениия» (МГУ, 18–22 июня 2012 г.). — М.: Издательство механико-математического факультета МГУ, 2012. — С. 285–288.

Автоматы с задержкой и отображения на $\mathbb{Z}_2$

Карандашов Максим Валерьевич

Саратовский государственный университет им. Н. Г. Чернышевского, e-mail: norg113@gmail.com

В данной работе будет рассмотрен вопрос сохранения меры автоматными отображениями с задержкой, ассоциированными с детерминированными автоматами, на словах из алфавита $\{0,1\}$.

Будем определять *детерминированный автомат* как пятёрку $A = (S, X, Y, \delta, \lambda)$, где S — множество состояний, X — входной алфавит, Y — выходной алфавит, $\delta : S \times X \to S$ — функция переходов, $\lambda : S \times X \to Y$ — функция выходов. Для рассматриваемых, в данной работе, автоматов, $X = Y = \{0, 1, \ldots, (p-1)\}$.

Инициальный автомат будем обозначать за A_s, где s — начальное состояние автомата. С каждым инициальным автоматом A_s будем связывать автоматное

отображение f_{A_s} такое, что $f_{A_s}(p) = \lambda(s, p)$. В дальнейшем, если автомат ясен из контекста, будем обозначать автоматное отображение f_{A_s} за f_s или же просто за f (если и начальное состояние автомата следует из контекста или не важно).

Каждому бесконечному слову $\ldots x_2 x_1 x_0$, где $x_i = \{0, 1, \ldots, (p-1)\}$, можно поставить в соответствие целое p-адическое чило $x_0 + x_1 p + x_2 p^2 + \ldots$, являющееся элементом кольца $\mathbb{Z}_p$, где p — простое число. Таким образом, можно рассматривать автоматное отображение f_s как отображение на $\mathbb{Z}_p$.

Пространство $\mathbb{Z}_p$ измеримо относительно вероятностной меры μ_p (мера Хаара), нормированной так, что $\mu_p(\mathbb{Z}_p) = 1$.

Шаром будем называть такое μ_p-измеримое множество p-адических чисел, которое определено как $(a + p^k\mathbb{Z}_p)$, где $a \in \mathbb{Z}_p$. Радиус шара равняется p^{-k} и для шара $B_{p^{-k}}(a) = (a + p^k\mathbb{Z}_p)$ мера вычисляется как $\mu_p(a + p^k\mathbb{Z}_p) = p^{-k}$.

Будем обозначать через $B_r(x)$ шар с центром в $x \in \mathbb{Z}_p$ радиуса r.

Преобразование $f : S \to S$, измеримое относительно μ_p, называется *сохраняющим меру*, если $\mu_p(f^{-1}(T)) = \mu_p(T)$ для любого измеримого $T \subseteq S$.

Под *автоматным отображением с задержкой* $v \in \mathbb{N}$ будем понимать такую функцию $D[f_s, v]$, для которой справедливо

$$\forall m \in \mathbb{N}\ \forall p \in X^{m+v} : f(p) = x_{i_1} x_{i_2} \ldots x_{i_{m+v}}\ \wedge\ D[f, v](p) = x_{i_{v+1}} x_{i_{v+2}} \ldots x_{i_{m+v}},$$

где f определяется некоторым инициальным автоматом. В силу приведённого выше представления p-адических чисел, любое отображение $D[f, v]$ будет отображением вида $\mathbb{Z}_p \to \mathbb{Z}_p$.

Будем называть *состоянием с потерей* [1] такое состояние s, что $\exists x_1, x_2 \in X : x_1 \neq x_2\ \wedge\ \lambda(s, x_1) = \lambda(s, x_2)$.

Теорема 1. [2] *Автоматное отображение $f_{A_s} : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2^k\mathbb{Z}$ биективно на $\mathbb{Z}/2^k\mathbb{Z}$ тогда и только тогда, когда автомат A_s не содержит состояний с потерей (достижимых из s).*

Известно, что автоматное отображение сохраняет меру тогда и только тогда, когда оно биективно [3]. Найдём условия сохранения меры для автоматных отображений с задержкой.

	0	1
0*	0/0	0/1

Таблица 1: Автомат A_1.

	0	1
0*	1/0	2/0
1	3/0	3/0
2	2/0	2/1
3	3/0	3/1

Таблица 2: Автомат A_2.

Для этого, в первую очередь, выясним соотношение между сохраняющими меру автоматными отображениями и автоматными отображениями с задержкой.

Теорема 2. *Если отображение f_s сохраняет меру, то $\forall v \in \mathbb{N}$ отображение $D[f_s, v]$ так же будет сохранять меру на $\mathbb{Z}_2$.*

Доказательство. Возьмём произвольный шар $B_{2^{-m}}(w)$ и построим множество $R = D[f_s, v]^{-1}(B_{2^{-m}}(w))$.

Каждое слово $\alpha \in X^v$ переведёт автомат A_s (определяющий отображение f_s) в некоторое состояние $s_{\delta(s,\alpha)}$, которое, в свою очередь, будет определять биективный автомат $A_{\delta(s,\alpha)}$ функционирующий без задержки.

В силу биективности $A_{\delta(s,\alpha)}$, будет существовать лишь одно входное слово $w_{\delta(s,\alpha)}$ такое, что $\lambda(\delta(s,\alpha), w_{\delta(s,\alpha)}) = w$. Следовательно,

$$\forall \alpha \in X^v \; D[A_s, v](B_{2^{-(m+v)}}(\alpha + 2^v \cdot w)) \in P_w, \text{ откуда}$$

$$R = \cup_{\alpha \in X^v} D[A_s, v](B_{2^{-(m+v)}}(\alpha + 2^v \cdot w)) \qquad (1)$$

Оценим $\mu_p(R)$. В силу счётно-аддитивности μ_p, получаем, что $\mu_p(R) = \sum_{\alpha \in X^v} \mu_p(B_{2^{-(m+v)}}(\alpha + 2^v \cdot w))$. Но $B_{2^{-(m+v)}}(\alpha + 2^v \cdot w)$ есть шар радиуса $(v+m)$. Тогда справедливо, что $\forall \alpha \in X^v \; \mu_p(B_{2^{-(m+v)}}(\alpha + 2^v \cdot w)) = 2^{-(v+m)}$.

Откуда следует, что $\sum_{\alpha \in X^v} \mu_p(B_{2^{-(m+v)}}(\alpha + 2^v \cdot w)) = 2^{-m} = \mu_p(B_{2^{-m}}(w))$.
Теорема 2 доказана.

Примером автомата, удовлетворяющего условиям теоремы 2, может служить автомат A_1.

Будем называть *значимой частью автомата* A_s, ассоциированного с отображением $D[f_s, v]$, такое множество состояний $H \subseteq S$, что каждое состояние из H достижимо за v или более шагов из состояния s.

Теорема 3. *Если значимая часть автомата A_s не содержит состояний потерей для задержки v, то отображение $D[f_s, v]$ сохраняет меру.*

Справедливость теоремы 3 следует из теоремы 2.

Таким образом, мы рассмотрели случай, когда автомат A_s не содержит состояний с потерей в своей значимой части (для некоторой задержки v).

Рассмотрим случай, когда состояния с потерей будут присутствовать в значимой части автомата.

Из доказательства теоремы 2 мы знаем, что мера множества $R = D[f_s, v]^{-1}(B_{2^{-m}}(w))$ определяется соотношением (1). Причём, в случае, когда f_s сохраняет меру, каждое из слагаемых в (1) равняется $2^{-(m+v)}$.

Рассматривая действие состояний с потерей, можно прийти к следущющим выводам:

- Каждое состояние с потерей либо увеличивает меру соответствующего шара (который определяется через α) в 2 раза, либо обнуляет её.
- Увеличение меры происходит в том случае, если происходит совпадение соответствующего символа из w с $\lambda(\widehat{s}, x)$, где $\widehat{s}$ — состояние с потерей.
- Обнуление слагаемого происходит в том случае, если символ из w не совпадает с генерируемым $\lambda(\widehat{s}, x)$ выходным символом.

Теорема 4. *Для того чтобы отображение $D[f_s, v]$ сохраняло меру необходимо и достаточно, чтобы $\forall w \in X^m$ мощность множества $\{\omega \mid s_v \in S_v, f_{s_v}(\omega) = w\}$ равнялась 2^m, где $S_v = \{\delta(s,p) \mid p \in X^v\}$.*

Примером автомата, не удовлетворяющего условию теоремы 4, может служить автомат A_2.

Список литературы

1. Гилл А. Введение в теорию конечных автоматов. — М.: «Наука», 1966. — 272 с.
2. Карандашов М. В. Исследование биективных автоматных отображений на кольце вычетов по модулю 2^k // Компьютерные науки и информационные технологии : Материалы Междунар. науч. конф. — Саратов: Издат. центр «Наука», 2014. — С. 148–152.
3. Anashin V. The non-archimedian theory of discrete systems // Mathematics in Computer Science. — 2012. — V. 6, No 4. — P. 375–393.

Обращение дифференцируемых перестановок над группой

Карпов Артем Валерьевич

Томский государственный университет, e-mail: karpov@isc.tsu.ru

Пусть заданы группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$ и подмножество $\Psi \subseteq End(\mathbb{G})$ эндоморфизмов группы $\mathbb{G}$, переводящих подгруппы из нормального ряда $\{H_k\}$ в себя.

Определение. Функция $f : \mathbb{G} \to \mathbb{G}$ называется *дифференцируемой* в точке $a \in \mathbb{G}$ относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, если существует эндоморфизм $\psi_{f(a)} \in \Psi$, такой что для любого члена нормального ряда H_k и любого элемента $h \in H_k$ выполняется равенство

$$f(a + h) \equiv f(a) + \psi_{f(a)}(h) \pmod{H_{k+1}}.$$

Функция называется дифференцируемой, если она дифференцируема в каждой точке группы $\mathbb{G}$. Эндоморфизм $\psi_{f(a)}$ называется производной функции f в точке a.

Дифференцируемые функции над группой являются обобщением полиномиальных функций над примарным кольцом вычетов $\mathbb{Z}_{p^m}$, где в роли производной выступает умножение на значение формальной производной полинома.

Пример. Пусть $\mathbb{G} = (\mathbb{Z}_{p^n}^m, +)$ — группа векторов длины m с компонентами из кольца $\mathbb{Z}_{p^n}$ и покомпонентным сложением по модулю p^n, $H_k = p^k\mathbb{Z}_{p^n}^m$. Определим функцию $f : \mathbb{G} \to \mathbb{G}$ как набор $(f_1, \ldots, f_m)$ полиномов из кольца $\mathbb{Z}_{p^n}[x_1, \ldots, x_m]$. Зафиксируем точку $a \in \mathbb{G}$ и придадим ей приращение $h \in H_k$, тогда $f(a + h) \equiv f(a) + h * J_f(a) \pmod{H_k}$, где J_f — матрица Якоби функции f, и f — дифференцируема.

Естественно называть дифференцируемую биективную функцию *дифференцируемой перестановкой*. Будем говорить, что g *— обратная (по модулю H_k)* к f дифференцируемая перестановка, если для всех $x \in \mathbb{G}$ выполняется

$$g(f(x)) = x \ \ (g(f(x)) \equiv x \pmod{H_k}).$$

Данная работа обобщает результаты, полученные в [1], а именно решается задача обращения дифференцируемой перестановки элементов группы в случаях абелевой, нильпотентной и разрешимой групп. Нормальный ряд в группе $\mathbb{G}$ задает структуру, аналогичную последовательности модулей $p,\ p^2, \ldots, p^m$ в случае примарного кольца, что дает возможность применять схожие методы обращения перестановок, и имеет место следующая теорема.

Теорема. *Пусть f — перестановка элементов разрешимой группы $\mathbb{G}$, дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, g_k — обратная перестановка к f по модулю H_k. Тогда обратной к f по модулю H_{k+1} является перестановка*

$$g_{k+1}(x) = 2g_k(x) - g_k(f(g_k(x))) - [-g_k(x) + g_k(f(g_k(x))), g_k(x)].$$

Следствие. *Если в условиях теоремы группа $\mathbb{G}$ абелева или нильпотентна, то*

$$g_{k+1}(x) = 2g_k(x) - g_k(f(g_k(x))).$$

Таким образом, если известно обращение заданной дифференцируемой перестановки элементов абелевой, нильпотентной или разрешимой группы $\mathbb{G}$ по модулю H_k, то можно получить обращение и над всей группой $\mathbb{G}$, строя обратную перестановку рекурсивно по теореме.

Список литературы

[1] Карпов А. В. Перестановочные многочлены над примарными кольцами // Прикладная дискретная математика. — 2013. — № 4(22). — С. 16–21.

Построение транзитивных полиномов над кольцом $\mathbb{Z}_{p^2}$

Ковалевская Анастасия Олеговна

Томский государственный университет, e-mail: aokovalevskaya@gmail.com

Пусть $\alpha = a_0 a_1 \ldots$ — рекуррентная последовательность, полученная с помощью полинома $f(x) \in \mathbb{Z}_{p^n}[x]$ по правилу: $a_{i+1} = f(a_i) \mod p^n, i = 0, 1, 2, \ldots$, где $a_0 \in \mathbb{Z}$, p простое, $n \in \mathbb{N}$. Такие последовательности находят применение в различных областях математики. В частности, они используются в генераторах псевдослучайных последовательностей. В связи с этим, возникает проблема построения таких $f(x)$, для которых указанная последовательность имеет наибольший период.

Полином $f(x) \in \mathbb{Z}_{p^n}[x]$ назовем транзитивным по модулю p^n, если последовательность α, полученная с помощью $f(x)$, имеет период p^n.

Полином $f(x)$ назовем тождеством по модулю p^n, если $f(a) = 0 \mod p^n$ для любого $a \in \mathbb{Z}$.

В [1] показано, что для любого $p \notin \{2,3\}$ и $n \in \mathbb{N}$ каждый полином, транзитивный по модулю p^2, является транзитивным по модулю p^n. Кроме того, транзитивные полиномы по модулю p^n могут быть получены из транзитивных по модулю p^2 путём добавления тождества. Таким образом, важным является случай $n = 2$.

Рассмотрим задачу получения всех транзитивных полиномов по модулю p^2.

Известны различные формы представления полиномиальных функций. Любая полиномиальная функция над $\mathbb{Z}_{p^2}$, в соответствии с [2], может быть представлена многочленом

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)f_2(x), \tag{1}$$

где $f_0(x), f_1(x), f_2(x)$ — полиномы степени меньше p над кольцом $\mathbb{Z}_p$.

Из формы (1) несложно получить другую, которая будет использована далее:

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)(f_0^{'}(x) - f^{'}(x)) \tag{2},$$

где $f^{'}(x)$ и $f_0^{'}(x)$ — производные для $f(x)$ и $f_0(x)$ с коэффициентами, приведёнными по модулю p.

Обозначим $f^{(1)}(x) = f(x)$ и для $k \geq 2$, $f^{(k)}(x) = f(f^{(k-1)}(x))$.

В [1] сформулировано необходимое и достаточное условие транзитивности. Полином $f(x)$, для которого $\prod\limits_{x \in \mathbb{Z}_p} f^{'}(x) = 1 \mod p$, транзитивен по модулю p^2, если и только если

$$f^{(p)}(a) \neq a \mod p^2 \text{ for some } a \in \mathbb{Z}_{\nmid p}. \tag{3}$$

В [1] показано, что если полином $f(x)$ транзитивен по модулю p^2, то $\prod\limits_{x \in \mathbb{Z}_p} f^{'}(x) = 1 \mod p$.

Пусть

L_0 — множество всех транзитивных по модулю p полиномов из $\mathbb{Z}_p[x]$; $|L_0| = (p-1)!$ [1];

L — множество всех полиномов $h(x) \in \mathbb{Z}_p[x]$, удолетворяющих равенству $\prod\limits_{x \in \mathbb{Z}_p} h(x) \mod p = 1$; очевидно, $|L| = (p-1)^{p-1}$;

$L1$ — множество всех полиномов из $\mathbb{Z}_p[x]$ степеней $0, 1, \cdots, p-1$; очевидно, $|L| = p^p$.

Метод построения всех транзитивных по модую p^2 полиномов $f(x)$ заключается в том, чтобы для каждой тройки $(f_0, h, f_1) \in L0 \times L \times L_1$, выполнить следующие шаги:

1. Построить полином $f(x) = f_0(x) + pf_1(x) + (x^p - x)(f_0^{'}(x) - h(x))$.
2. Проверить, удовлетворяет ли $f(x)$ условию (3).

Теорема 1. *Все транзитивные по модулю p^2 полиномы могут быть получены этим методом.*

Метод требует перебора $(p-1)!(p-1)^{p-1}p^p$ полиномов $f(x)$. Количество полиномов, транзитивных по модулю p^2 равно $(p-2)!(p-1)^{p+1}p^{p-1}$ [1]. Таким образом, доля нетранзитивных составляет $1/p$. При больших значениях p эта доля очень мала, что обеспечивает хорошую работу метода.

При реализации алгоритма в системе компьютерной алгебры `Sage` все 15360000 транзитивных по модулю 25 полиномов были построены за 32 мин. Эксперименты проводились на компьютере с процессором Intel Core i7-3770 и оперативной памятью 15,4 Гб.

Если рассматривать задачу нахождения не всех, а какого-либо одного или нескольких транзитивных полиномов, то возможно улучшение этого метода. Оно заключается в следующем.

Пусть выбранный случайным образом полином $f_1(x)$ не привёл к транзитивному $f(x)$. Тогда выберем такой полином $g(x)$, для которого $g(x) = 0$ при всех значениях x, кроме одного. Затем подставим в формулу (2) вместо $f_1(x)$ сумму $f_1(x) + g(x)$. В соответствии со следующей теоремой, такое построение гарантирует, что $F(x) = f(x) + pg(x)$ транзитивен по модулю p^2.

Теорема 2. *Пусть полином $f(x) \in \mathbb{Z}_p^2[x]$ транзитивен по модулю p и не транзитивен по модулю p^2. Полином $g(x)$ удовлетворяет условию: $|x : x \in \mathbb{Z}_p, g(x) \neq 0| = 1$. Тогда полином $F(x) = f(x) + pg(x)$ транзитивен по модулю p^2.*

Список литературы

[1] Larin M. V. Transitive polynomial transformations of residue class rings // Diskr. Mat. — 2002. — V. 14, N 2. — P. 20–32. [In Russian].

[2] Frisch S., Krenn D. Sylow p-groups of polynomial permutations on the integers mod p^n // J. Number Th. — 2013. — V. 133. — P. 4188–4199.

Алгоритмы построения расписаний обслуживания линейно рассредоточенных объектов с учётом временны́х характеристик

Коган Дмитрий Израилевич[1], **Федосенко Юрий Семенович**[2]

[1] Московский государственный университет приборостроения и информатики, e-mail: `kdi_41@mail.ru`

[2] Волжский государственный университет водного транспорта, e-mail: `fds@vgavt-nn.ru`

В рассматриваемой модели M (она возникает, в частности, при рассмотрении задач снабжения топливом группы дизель-электрических добывающих комплексов, дислоцированных в крупномасштабном русловом полигоне и осуществляющих донную выемку нерудных строительных материалов) считается заданной расположенная в одномерной рабочей зоне L совокупность $O_n = \{o_1, o_2, \ldots, o_n\}$ подлежащих однократному обслуживанию стационарных объектов. Начальная точка A зоны является базовой для обслуживающего процессора; объекты пронумерованы в порядке возрастания их расстояний от точки A; конечная точка B зоны является местом расположения объекта o_n. Из

точки A, начиная от момента $t = 0$, процессор поступательно перемещается в точку B (прямой рейс λ_+), а затем, достигнув ее, также поступательно возвращается в точку A (обратный рейс λ_-). При реализации указанных рейсов процессор выполняет однократное, без прерываний обслуживание объектов группы O_n; часть объектов обслуживается в рейсе λ_+, все остальные — в рейсе λ_-.

Принимаются обозначения: $1, 2, \ldots, n$ — точки отрезка L, в которых расположены объекты $o_1, o_2, \ldots, o_n$ соответственно (точки n и B совпадают); $\gamma_{j-1,j}$ и $\gamma_{j,j-1}$ — затраты времени на перемещения процессора между точками $j-1$ и j в рейсах λ_+ и λ_- соответственно, $j = \overline{1,n}$; при этом $\gamma_{0,1}$ и $\gamma_{1,0}$ — затраты времени на перемещение процессора между точкой A и точкой 1 в рейсах λ_+ и λ_-. Для каждого объекта o_j считаются заданными: τ_j — продолжительность обслуживания процессором; $\varphi_j(t)$ — функция индивидуального штрафа (если обслуживание объекта завершается в момент времени t, то $\varphi_j(t)$ — соответствующая величина штрафа); r_j — момент готовности объекта к обслуживанию; d_j — директивный срок завершения обслуживания ($j = \overline{1,n}$). Считаем параметры τ_j, $\gamma_{j-1,j}$, $\gamma_{j,j-1}$, d_j принимающими только натуральные значения, параметр r_j может принимать только целые неотрицательные значения.

Стратегией обслуживания называем произвольную упорядоченную по возрастанию последовательность индексов $V = (i_1, i_2, \ldots, i_k)$ из $N = \{1, 2, \ldots, n\}$. Объекты o_{i_k}, где $i_k \in V$, в реализации стратегии обслуживаются в прямом рейсе; все остальные объекты — в обратном рейсе. Последовательность обслуживания объектов в обратном рейсе записываем в виде $V^- = (i_{k+1}, i_{k+2}, \ldots, i_n)$, здесь индексы объектов перечислены по убыванию.

Расписаниями обслуживания, реализующими стратегию V, именуем кортежи вида $\rho = \langle (i_1, a_1, b_1), (i_2, a_2, b_2), \ldots, (i_n, a_n, b_n) \rangle$, где a_k и b_k — соответственно моменты начала и завершения обслуживания объекта o_{i_k}, $k = \overline{1,n}$. Момент завершения обслуживания произвольного объекта o_j при реализации расписания ρ обозначим $C_j(\rho)$. Расписание r-допустимо, если при его реализации соблюдаются все предписанные объектам ранние сроки начала обслуживания. Расписание d-допустимо, если при его реализации соблюдаются все предписанные объектам директивные сроки. Расписание (r,d)-допустимо, если оно r-допустимо и d-допустимо одновременно. Через M_r, M_d и M_{r-d} соответственно будем обозначать множества r-допустимых, d-допустимых и (r,d)-допустимых в рассматриваемой модели расписаний. Критерии оценки расписаний: $K_1(\rho) = \sum\limits_{j=1}^{n} \varphi_j(C_j(\rho))$, $K_2(\rho) = \max\limits_{j} \varphi_j(C_j(\rho))$.

$T_1(\rho)$ — момент возвращения процессора в базовую точку после реализации расписания ρ; $T_2(\rho)$ — момент завершения обслуживания последнего в расписании ρ объекта, $T_2(\rho) = b_n$.

Рассмотрены следующие задачи.

Задача 1. $\min\limits_{\rho \in M_r} K_1(\rho)$.

Задача 2. $\min\limits_{\rho \in M_r} K_2(\rho)$.

Задача 3. По имеющимся исходным данным модели $\boldsymbol{M}$ определить, является ли множество d-допустимых в ней расписаний непустым.

Задача 4. По имеющимся исходным данным модели $\boldsymbol{M}$ определить, является ли множество (r, d)-допустимых в ней расписаний непустым.

Задача 5. $\min\limits_{\rho \in M_r} T_1(\rho)$.

Задача 6. $\min\limits_{\rho \in M_r} T_2(\rho)$.

Задача 7. $\min\limits_{\rho \in M_r} (K_1(\rho), T_1(\rho))$.

Задача 8. $\min\limits_{\rho \in M_r} (K_2(\rho), T_1(\rho))$.

Задача 9. $\min\limits_{\rho \in M_r} (T_1(\rho), T_2(\rho))$.

При рассмотрении бикритериальных задач 7–9 принимается концепция Парето, предусматривающая синтез полных совокупностей эффективных оценок [1].

Результаты выполненного исследования следующие.

Теорема 1. *Задача* 1, *в которой существует индекс* $j = \overline{1, n}$ *такой, что* $r_j > 0$ *и функции индивидуального штрафа* $\varphi_i(t)$ *линейны для любого индекса* $i = \overline{1, n}$, *NP-трудна.*

Теорема 2. *Задача* 2, *в которой существует индекс* $j = \overline{1, n}$ *такой, что* $r_j > 0$ *и функции индивидуального штрафа* $\varphi_i(t)$ *линейны для любого индекса* $i = \overline{1, n}$, *NP-трудна.*

Теорема 3. *Задача* 4 *NP-полна.*

Перечисленные результаты о труднорешаемости получены путём полиномиального сведения к рассматриваемым задачам 2 и 4 NP-полной задачи «Разбиение» [2].

Из теорем 1 и 2 вытекают следующие два факта.

Теорема 4. *Проблема определения по исходным данным задачи* 7 *и натуральным константам* C_1 *и* C_2, *имеется ли в этой задаче расписание* ρ *такое, что одновременно* $K_1(\rho) \le C_1$ *и* $T_1(\rho) \le C_2$, *NP-полна.*

Теорема 5. *Проблема определения по исходным данным задачи* 8 *и натуральным константам* C_1 *и* C_2, *имеется ли в этой задаче расписание* ρ *такое, что одновременно* $K_2(\rho) \le C_1$ *и* $T_1(\rho) \le C_2$, *NP-полна.*

Для задач 3, 5 и 6 построены алгоритмы решения с не более чем квадратично зависящими от n верхними оценками числа выполняемых элементарных операций. Построен функционирующий в квадратично зависящем от n времени алгоритм отыскания полной совокупности эффективных оценок в задаче 9. Алгоритмы решения задач 7 и 8 основаны на рекуррентных соотношениях бикритериального динамического программирования [3, 4]; они имеют псевдополиномиальные оценки вычислительной сложности [2]. Благодаря указанным соотношениям решаются также задачи 1, 2 и 4 (ввести для однокритериальных задач 1 и 2 скалярную функцию Беллмана не представляется возможным).

Работа выполнена при поддержке РФФИ (проект № 15-07-03141-а).

Список литературы

[1] Подиновский В. В., Ногин В. Д. Парето-оптимальные решения многокритериальных задач. — М.: Физматлит, 2007. — 256 с.

[2] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: «Мир», 1982. — 419 с.

[3] Villareal B., Karwan M. Multicriteria Dynamic Programming with an Application to the Integer Case // Journal of optimization theory and applications. — 1982. — V. 38, N 1. — P. 43–69.

[4] Коган Д. И. Динамическое программирование и дискретная многокритериальная оптимизация. — Н. Новгород: Изд-во Нижегородского госуниверситета, 2004. — 150 с.

Исправления и дополнения одного алгоритма в перечислительной комбинаторике и биоинформатике

Коганов Леонид Маркович

Научный центр нелинейной волновой механики и технологии РАН, Москва, e-mail: lenya_85@mail.ru

Памяти профессора Г. П. Гаврилова, ученика и соавтора С. В. Яблонского.

1. Цель настоящей работы заключается в исправлении и уточнении алгоритма, предложенного автором в [1], а также в выводе необходимых следствий. Сохраняется терминология, принятая в [1]. Мы, как и в [1], работаем с определёнными в указанном источнике так называемыми $\{3\}$-деревьями с помеченными начальным отрезком $[n] = \{1, \ldots, n\}$ натурального ряда всеми без исключения висячими вершинами. Все внутренние вершины имеют одну и ту же степень 3 и не имеют никаких пометок.

По известной *лемме о рукопожатиях* их число в этом случае есть $n - 2$. Тогда общее число вершин равно $2n - 2$, а число рёбер — $2n - 3$. Параметр n ниже является *перечисляющим параметром*.

Рёбра будем метить скобочным символом $(l)_{\text{рим}}$ (читается как «l в римской нумерации» или, сокращённо, «l-римское»: так, например, $(27)_{\text{рим}} = \text{XXVII}$, $(3)_{\text{рим}} = \text{III}$ и т. д.).

2. Главное в построении алгоритма, доставляющего искомую универсальную посистемную биекцию из [1; теор. 1], заключается в строгой линейной (тотальной в смысле порядка) пошаговой римской нумерации добавляемых на каждом шаге рёбер. Эту (пере)нумерацию мы, если так можно выразиться, будем «отгонять» к правому концу опорной геодезической, а именно к вершине 2.

Для пошагового построения алгоритма наращения спэйсов-рёбер (ср. с [1]) мы будем вынуждены ввести следующее

Определение 1. *Гроздь*, соответствующая геодезической (в данном случае — в $\{3\}$-дереве), включает в себя саму геодезическую, а также все ветви, растущие из всех, *кроме концевых*, вершин геодезической. Указанные ветви-поддеревья не содержат рёбер самой геодезической (простой несамопересекающейся цепи), а также *каких-либо рёбер из базисной или опорной геодезической* (см. ниже).

Мы будем работать исключительно с геодезическими, соединяющими *ребро*, подразбиваемое стеблем по Ф. Харари на данном шаге алгоритма, с висячей *вершиной* 2 — условно *правым концом* в горизонтальном положении *базисной или опорной геодезической*, соединяющей вершины 1 и 2.

3. **Алгоритм** (исправленный: ср. с [1]) заключается в следующем:

3.1. Начальным данным алгоритма является ребро с концами 1 и 2, помеченное римской единицей I, — как вырожденное $\{3\}$-дерево без внутренних вершин.

3.2. На каждом последующем шаге при последовательном встраивании стебля в условную середину каждого из рёбер в соответствии с их (римской) нумерацией, мы производим перенумерацию рёбер следующим образом.

Пусть ребро, куда встраиваем новый стебель, до шага алгоритма имело пометку $(l)_{\text{рим}}$. Тогда при естественной нумерации вершины – свободного конца стебля, отличного от подразбивающей «стрелки», мы делаем следующее:

a) фиксируем (до шага) геодезическую, соединяющую ребро $(l)_{\text{рим}}$ с вершиной 2;

b) на самом шаге полуребро подразбиения, содержащее (дальний от 2) конец геодезической, сохраняет метку $(l)_{\text{рим}}$;

c) встраиваемое ребро-стебель получает метку $(l+1)_{\text{рим}}$;

d) все без исключения рёбра *грозди, соответствующей* указанной выше в пункте a) геодезической, получают метки

$$(\mathrm{Y})_{\text{рим}} := (\mathrm{Y})_{\text{рим}} + \mathrm{II},$$

или, что — то же самое,

$$(\mathrm{Y})_{\text{рим}} := (\mathrm{Y}+2)_{\text{рим}};$$

e) метки не указанных выше рёбер не меняются.

Таким образом, при последовательном посистемном построении (класса) $\{3\}$-деревьев римские метки *рёбер* накапливаются и увеличиваются вдоль соответствующих геодезических к правой вершине 2 базисной цепи.

4. Теперь мы обратимся к диаграммам связей (д. с.) в виде систем полуокружностей в верхней полуплоскости, соединяющих пары точек — концы диаметров — на действительной горизонтальной прямой [2] (см. также переложение, осуществлённое в основном трудами Н. Б. Васильева в [3]). Рассматривая случаи перечисляющего параметра $n = 2$ и, соответственно, $n = 3$, мы видим, что им соответствуют случаи значений ранга ($rank$ = число полуокружностей) $n = 0$ и, соответственно, $n = 1$ для д. с. При этом левому бесконечно удалённому концу $-\infty$ действительной прямой соответствует левый конец 1 опорной

геодезической, а правому бесконечно удалённому концу $+\infty$ прямой — соответствует её (геодезической) правый конец 2. Это соответствие универсально (стабильно) и не зависит от значения n перечисляющего параметра.

Теорема 1. *Системе всех без исключения $\{3\}$-деревьев с перечисляющим параметром n, $n \geq 3$, биективно соответствует (при $n = 2$ — пустая) система д. с. ранга $n - 2$. При этом соответствие концам опорной геодезической, указанной выше, бесконечно удалённых точек действительной прямой постоянно и универсально. Что задаёт в совокупности универсальную посистемную биекцию класса $\{3\}$-деревьев* [1] *и класса д. с. — диаграмм связей* [2]; [4].

Следствие 1. *Число $\{3\}$-деревьев порядка n, $n \geq 3$, (с перечисляющим параметром — числом висячих вершин n) даётся выражением:*

$$[2 \cdot (n-2) - 1]!!.$$

Следствие 2. *Согласно настоящей теореме 1 и в силу результата из* [1; Следствие 1, с. 165] *система $\{3\}$-деревьев порядка n кодируется при $n \geq 4$ словами вида*

$$(\alpha_{n-2},\ \ldots,\ \alpha_2),$$

где $\alpha_2 \in [3]$, $\alpha_3 \in [5]$, $\ldots$, $\alpha_{n-2} \in [2 \cdot (n-2) - 1]$ (скобочный символ начальных отрезков натурального ряда по Стенли — просьба не путать с литературными ссылками!).

Отметим, что из Следствия 2 также вытекает Следствие 1 настоящей работы.

5. **Замечание 1.** В указанной совместной статье Н. Б. Васильева и автора [3], посвящённой памяти Н. Я. Виленкина, для последнего кодового символа (суффикса) α_1 в кодовом слове:

$$(\alpha_n,\ \ldots,\ \alpha_2),$$

в котором реверсная нумерация индексов даётся «по разборке», имеем (ниже вертикальная черта — знак подстановки по Лейбницу):

$$\alpha_1 \leq 2n - 1|_{n=1} = 1. \qquad (*)$$

И, поскольку

$$\alpha_1 \geq 1, \qquad (**)$$

так как все символы α_i, $1 \leq i \leq n$, *суть натуральные числа*, то из $(**)$ и $(*)$ необходимо следует, что

$$\alpha_1 \equiv 1$$

тождественно во всех кодовых словах.

Таким образом, крайний справа символ α_1 без ущерба может быть отброшен. Что и было осуществлено автором в основной для понимания работе [2], опубликованной в УМН.

В заключение автор выражает признательность коллегам: Л. Н. Бондаренко (Пенза) и Д. С. Романову (Москва) за постоянную моральную, информационную и иную поддержку настоящей работы.

Список литературы

[1] Коганов Л. М. Ещё одна биекция в перечислительной комбинаторике // Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014 г.) / Под ред. Ю. И. Журавлёва. — Казань: Отечество, 2014. — С. 124–127.

[2] Коганов Л. М. Универсальная биекция между перестановками Гесселя – Стенли и диаграммами связей соответствующих рангов // УМН. — 1996. — Т. 51, вып. 2 (308). — С. 165–166.

[3] Васильев Н. Б., Коганов Л. М. Разбиения, ГС-перестановки и деревья // В кн.: Васильев Н. Б. Статьи из журнала «Квант». Часть 2. — М.: Издательство МЦНМО, 2013 (Библиотечка «Квант». Вып. 126). — С. 140–148.

[4] Коганов Л. М. Универсальная биекция между частично помеченными бинарными свободными деревьями и плоскими монотонными деревьями // Формальные степенные ряды и алгебраическая комбинаторика. 12-я Международная конференция, FPSAC'00: дополнительные тезисы. — М.: МАКС Пресс, 2000. — С. 40–41.

О решётке конгруэнций полигонов над прямоугольными связками

Кожухов Игорь Борисович[1], **Халиуллина Айгуль Римзиловна**[2]

[1] Национальный исследовательский университет "МИЭТ", e-mail: kozhukhov_i_b@mail.ru
[2] Национальный исследовательский университет "МИЭТ", e-mail: haliullinaar@gmail.com

В работе [1] были описаны полигоны над прямоугольной связкой. Используя это описание, в [2] были охарактеризованы полигоны над прямоугольной связкой, являющиеся подпрямо неразложимыми. Важными частными случаями прямоугольной связки являются полугруппы левых и правых нулей. Все конгруэнции полигонов над полугруппами левых и правых нулей были описаны в [3], а в [4] — инъективные и проективные полигоны, а также инъективные оболочки и проективные накрытия полигонов над полугруппами левых и правых нулей. Наконец, в [5] были найдены необходимые и достаточные условия того, что заданный полигон над полугруппой левых или правых нулей будет иметь модулярную, дистрибутивную решётку конгруэнций или решётка конгруэнций будет являться цепью.

Цель данной работы — получить необходимые и достаточные условия модулярности произвольного полигона над прямоугольной связкой. Наибольший порядок такого полигона оказался равным 9.

В работе будут приняты следующие обозначения. Если $\varphi : A \to B$ — отображение множеств, то ядро $\ker\varphi = \{(a, a') \mid a\varphi = a'\varphi\}$, а образ $\operatorname{im}\varphi = A\varphi$. Через $\operatorname{Eq} A$ мы обозначаем решётку отношений эквивалентности на множестве A. Если $\rho \in \operatorname{Eq} A$ и $a \in A$, то $a\rho$ — класс отношения ρ, содержащий a. Фактор-множество $A/\rho = \{a\rho \mid a \in A\}$ — множество всех ρ-классов.

Полигоном над полугруппой S называется (см. [6]) множество X, на котором действует полугруппа S, т. е. определено отображение $X \times S \to X$, $(x, s) \mapsto xs$, удовлетворяющее условию $x(st) = (xs)t$ при всех $x \in X$, $s, t \in S$. Хорошо известно, что полигон над полугруппой является алгебраической моделью автомата (см. [7]). Полигон X называется *копроизведением* своих подполигонов X_i $(i \in I)$, если $X = \cup_{i\in I} X_i$ и $X_i \cap X_j = \emptyset$ при $i \neq j$. В этом случае мы пишем $X = \sqcup_{i\in I} X_i$. Для некоторых классов полугрупп все полигоны над ними могут быть описаны Так, в [1] были описаны полигоны над вполне простыми и вполне 0-простыми полугруппами.

Полугруппа L называется полугруппой левых нулей, если $ab = a$ для всех $a, b \in L$, а R — полугруппа правых нулей, если $ab = b$ для всех $a, b \in R$. *Прямоугольной связкой* называется полугруппа $S \cong L \times R$, где L — полугруппа левых, а R — полугруппа правых нулей.

Будем записывать элементы прямоугольной связки $S = L \times R$ в виде $s = \langle l, r\rangle$, где $l \in L$, $r \in R$. Умножение в S осуществляется по правилу $\langle l, r\rangle \cdot \langle l', r'\rangle = \langle l, r'\rangle$.

Следующее утверждение является частным случаем теоремы 5 из [1].

Предложение 1. *Пусть $S = L \times R$ — прямоугольная связка (L — полугруппа левых, R — полугруппа правых нулей), X и Q — множества, для каждых $l \in L$, $r \in R$ заданы отображения $\kappa_r : Q \to X$, $\pi_l : X \to Q$ такие, что $\kappa_r\pi_l = 1_Q$ при всех $l \in L$, $r \in R$. Для $x \in X$, $\langle l, r\rangle \in S$ положим $x \cdot \langle l, r\rangle = x\pi_l\kappa_r$. Тогда X будет являться полигоном над S. Кроме того, любой полигон над прямоугольной связкой изоморфен полигону, построенному таким образом.*

Пусть $S = L \times R$ — прямоугольная связка и X — полигон над S. Положим $Y = XS$. Нетрудно проверить, что $Y = \cup_{r\in R} \operatorname{im}\kappa_r$. Положим $\tau = \cap_{l\in L} \ker\pi_l$ и $\sigma = \tau|_Y$. Очевидно, $\tau \in \operatorname{Eq} X$, а $\sigma \in \operatorname{Eq} Y$. Пусть $X = \sqcup_{i\in I} X_i$ — разбиение X на σ-классы и $Y_i = X_i \cap Y$.

Далее, проверяется, что $(\ker\pi_l)|_Y$ не зависит от l, а также что $y \cdot \langle l, r\rangle \in Y_i$ при $y \in Y_i$ и $y \cdot \langle l, r\rangle$ не зависит от l. Ввиду этого мы можем Y считать полигоном над полугруппой R, где действие определено формулой $y{\cdot}r = y{\cdot}\langle l, r\rangle$ для $y \in Y$, $r \in R$, $l \in L$. Подмножество Y_i — подполигон R-полигона Y, а так как Y_i — σ-класс, то $|Y_ir| = 1$ при любом $r \in R$. Отсюда $Y_ir = \{y_{ir}\}$ при некотором $y_{ir} \in Y_i$. Положим $A = X \setminus Y$.

Далее, если $a \in A$, $l \in L$, $r \in R$, то $a \cdot \langle l, r\rangle = y_{ir}$ при некотором $i \in I$. Следовательно, для каждого $l \in L$ мы имеем отображение $\varphi_l : A \to I$, а именно, $a\varphi_l = I \Leftrightarrow a \cdot \langle l, r\rangle = y_{ir}$ при всех $r \in R$.

Нетрудно заметить, что $Y_i = \{y_{ir} \mid r \in R\}$ при любых $i \in I$ и $y_{ir} \cdot r' = y_{ir'}$ при $r, r' \in R$.

Теперь мы можем переформулировать описание полигонов над прямоугольной связкой $S = L \times R$, приведённое в предложении 1, в несколько ином виде, более удобном для дальнейшего.

Предложение 2. *Пусть Y — множество, разбитое некоторым отношением эквивалентности σ следующим образом: $Y = \cup_{i\in I} Y_i$. Пусть $\{y_{ir} \mid i \in I, r \in R\}$ — семейство элементов из Y таких, что $y_{ir} \in Y_i$ при всех $i \in I$, $r \in R$ и*

$Y_i = \{y_{ir} \mid r \in R\}$. Пусть A — множество такое, что $A \cap Y = \emptyset$, и для каждого $l \in L$ задано отображение $\varphi_l : A \to I$. Положим $X = Y \cup A$ и определим умножение элементов из X на элементы полугруппы S следующим образом: $y \cdot \langle l, r\rangle = y_{ir}$, если $y \in Y_i$; $a \cdot \langle l, r\rangle = y_{ir}$, если $a \in A$ и $a\varphi_l = i$. Тогда X — полигон над полугруппой $S = L \times R$, причём любой S-полигон изоморфен полигону, построенному таким образом.

Для элементов $i, j \in I$ таких, что $i \neq j$, введём в рассмотрение двудольный граф Γ_{ij}, у которого вершинами являются элементы множества $Y_i \cup Y_j$, а рёбрами — пары (y_{ir}, y_{jr}) при $r \in R$.

Теперь мы можем привести описание полигонов X над прямоугольными связками, у которых решётка $\mathrm{Con}\, X$ модулярна. Пусть X — полигон над прямоугольной связкой $S = L \times R$, $Y = XS$, $A = X \setminus Y$, подполигоны Y_i $(i \in I)$, графы Γ_{ij} $(i, j \in I)$ и отображения φ_l $(l \in L)$ имеют тот же смысл, что и выше. По лемме 8 $|A| \leq 2$.

Теорема 1. *Пусть X — полигон над прямоугольной связкой $S = L \times R$. Тогда решётка $\mathrm{Con}\, X$ модулярна в том и только том случае, если $|A| \leq 2$ и выполнены условия:*

(i) $|I| \leq 3, |Y_i| \leq 3$ при $i \in I$, графы Γ_{ij} связны при $i \neq j$;

при $A = \{a\}$ выполнено условие (i), а также условие

(ii) если $a\varphi_l = i$ при некотором $i \in I$ и всех $l \in L$, то $|Y_i| \leq 2$;

при $A = \{a, b\}$ выполнено условие (i), а также условия

(iii) $a\varphi_l = b\varphi'_l$ при некоторых $l, l' \in L$;

(iv) если одно из множеств $\{a\varphi_l | l \in L\}$, $\{b\varphi_l | l \in L\}$ состоит из одного элемента i, а в другом более одного элемента, то $|Y_i| \leq 2$;

(v) если $\{a\varphi_l | l \in L\} = \{b\varphi_l | l \in L\} = \{i\}$, то $|Y_i| = 1$.

Список литературы

[1] Avdeyev A. Yu., Kozhukhov I. B. Acts over completely 0-simple semigroups // Acta Cybernetica. — 2000. — V. 14. N 4. — P. 523–531.

[2] Кожухов И. Б, Халиуллина А. Р. Характеризация подпрямо неразложимых полигонов // Прикладная дискретная математика (в печати).

[3] Халиуллина А. Р. Конгруэнции полигонов над полугруппами правых нулей // Чебыш. сборник. — 2013. — Т. 14, вып. 3. — С. 142–146.

[4] Кожухов И. Б, Халиуллина А. Р. Инъективность и проективность полигонов над сингулярными погруппами // Электронные информационные системы. — 2014. — № 2, ч. 2. — С. 45–56.

[5] Халиуллина А. Р. Условия модулярности решётки конгруэнций полигона над полугруппой правых или левых нулей // Дальневосточный математический журнал (в печати).

[6] Kilp M., Knauer U., Mikhalev A. V. Monoids, acts and cathegories. — W. de Gruyter, N. Y., Berlin. — 2000. — 529 p.

[7] Лаллеман Ж. Полугруппы и комбинаторные приложения. — М.: Мир, 1985. — 440 с.

Эволюционная модель покрытия графа звездами

Козин Игорь Викторович, Перепелица Виталий Афанасьевич[1], Рябенко Антон Евгеньевич[2]

[1] Запорожский национальный университет, e-mail: ainc00@gmail.com, perepel2@yandex.ru
[2] Запорожский национальный технический университет, e-mail: rjabenkoae@mail.ru

Задача покрытия графа звездами имеет многочисленные практические приложения как в технике (оптимальное размещение элементов конструкций), так и в экономике (задача оптимального размещения производства).

Звездой в графе называется его связный подграф диаметра не более чем 2 без циклов. Покрытием (реберным покрытием) графа звездами будем называть такой набор вершинно непересекающихся звезд графа, который содержит все вершины графа. Пусть в графе $G = (V, E)$ каждому ребру $e \in E$ приписан вес $\rho(e) \in R_1$ и пропускная способность $\mu(e) \in R_1$.

Весом звезды будем называть сумму весов ее ребер, а весом покрытия, соответственно, сумму весов звезд, составляющих покрытие. Пропускной способностью звезды будем называть минимальную из пропускных способностей ее ребер. Соответственно, пропускной способностью покрытия называется минимальная из пропускных способностей звезд, входящих в это покрытие.

Двукритериальная задача покрытия графа звездами состоит в отыскании покрытия $P(G)$ с минимальным весом $\rho(P)$ и максимальной пропускной способностью $\mu(P)$. Как правило, в задаче присутствуют дополнительные ограничение на число ребер составляющих покрытие звезд или количество звезд этого покрытия.

Даже в однокритериальном случае с критерием $\rho(P)$ задача относится к разряду NP-трудных [1]. Для многокритериальной задачи покрытия звездами доказано свойство полноты [2]. То есть в худшем случае множество Парето задачи может содержать все допустимые решения.

Метод, описанный ниже, позволяет отыскивать подмножества множества допустимых решений, которые могут рассматриваться как приближения множества Парето.

Задача покрытия графа звездами может быть представлена как задача с фрагментарной структурой [3]. Элементарным фрагментом в данном случае является ребро графа. Порядок присоединения фрагментов задается перестановкой размерности m, каждый элемент которой является номером ребра.

Фрагментарный алгоритм позволяет определить покрытие по заданной перестановке s по следующему правилу. Составляется список V_1 центров звезд покрытия, список E_1 ребер покрытия и список V_2 вершин, участвующих в покрытии. На начальном в списки V_1 и V_2 добавляются все изолированные вершины графа, а список E_1 — пустой. Перестановка ребер просматривается слева направо и на каждом шаге выполняется следующая процедура:

а) если очередное ребро $e = (v_1, v_2)$ инцидентно двум вершинам списка V_2, то переходим к следующему шагу;

b) если ребро инцидентно лишь одной вершине списка V_2 (например вершина v_1) и эта вершина входит в список V_1, то ребро добавляется в список ребер E_1, а вторая вершина v_2 добавляется в список V_2;

c) если ребро e инцидентно лишь одной вершине списка V_2 (например вершина v_1) и эта вершина не входит в список V_1, то вершина v_2 добавляется в списки V_1 и V_2;

d) если ребро e не инцидентно ни одной из вершин списка, то одна из вершин (v_1) добавляется в список вершин V_1, ребро e добавляется в список ребер E_1 и обе вершины ребра e добавляются в список вершин V_2.

Алгоритм заканчивает работу, когда все вершины из перестановки s просмотрены. Результатом работы алгоритма является набор звезд с центрами из множества V_1 и ребрами из множества E_1.

Таким образом, определено отображение $F : S_n \to \{P\}$ множества перестановок ребер S_n в множество допустимых решений $\{P\}$ задачи покрытия. Заметим, что отображение F является сюръекцией, то есть каждое допустимое решение задачи может быть построено фрагментарным алгоритмом при надлежащем выборе перестановок элементарных фрагментов.

Наличие фрагментарной структуры позволяет построить универсальную эволюционно-фрагментарную модель [4] для задачи покрытия графов звездами.

На начальном шаге эволюционного алгоритма с помощью оператора начальной популяции строится множество решений Y_0. На каждом очередном шаге предполагается заданным некоторое множество допустимых решений — текущая популяция. На первом шаге это множество $Y = Y_0$. Для каждого из элементов множества Y вычисляется значение критериев селекции. Далее с помощью оператора отбора в текущей популяции Y выбирается множество пар для кроссовера. К каждой паре из выбранного множества пар применяется оператор кроссовера, а затем к результату кроссовера применяется оператор мутации. Таким путем находится множество элементов — потомков $\tilde{Y}$. К промежуточной популяции $Y \cup \tilde{Y}$, которая является объединением текущей популяции и множества потомков, применяется оператор эволюции, который выделяет на этом множестве новую текущую популяцию. Процесс эволюции повторяется до тех пор, пока не будет выполнено условие остановки эволюционного алгоритма.

Оператор кроссовера K определяется следующим образом. Пусть $U = (u_1, u_2, ..., u_n)$ и $V = (v_1, v_2, ..., v_n)$ — две произвольные перестановки. Перестановка-потомок строится следующим образом. Последовательности U и V просматриваются слева направо. На k-м шаге выбирается наименьший из первых элементов последовательностей и добавляется в новую перестановку-потомок. Затем этот элемент удаляется из двух последовательностей-родителей. Например,

$$K((2,3,4,7,8,1,6,5),(3,4,6,2,1,5,8,7)) = (2,3,4,6,1,5,7,8)$$

Оператор мутации выполняет случайную транспозицию (замену местами двух элементов) в перестановке.

Обычное правило остановки — количество поколений достигло предельной границы L. Лучшие по Парето перестановки из последней построенной популяции определяют приближенное решение задачи.

СПИСОК ЛИТЕРАТУРЫ

[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М. : Мир, 1982. — 416 с.

[2] Емеличев В. А., Перепелица В. А. О некоторых алгоритмических проблемах многокритериальной оптимизации на графах // Журн. вычисл. математики и мат. физики. — 1989. — Т. 29, № 2. — С. 171–183.

[3] Козин И. В. Фрагментарные алгоритмы в системах поддержки принятия решений // Питання прикладної математики і математичного моделювання : зб. наук. праць; [ред. кол.: О. М. Кисельова (відп. редактор) та ін.]. — Д.: Вид-во Дніпропетр. нац. ун-ту, 2006. — С. 131–137.

[4] Козин И. В. Фрагментарные структуры и эволюционные алгоритмы // Питання прикладної математики і математичного моделювання : зб. наук. праць; [ред. кол.: О. М. Кисельова (відп. редактор) та ін.]. — Д.: Вид-во Дніпропетр. нац. ун-ту, 2008. — С. 138–146.

Зрительная среда и образы в ней

Козлов Вадим Никитович

Московский государственный университет имени М. В. Ломоносова, e-mail: vnkozlov@mail.ru

В рамках темы этой работы показывается, как плоская среда «порождает» образы, и что в этом случае есть распознавание образов. Истоки работы — в моделировании опытов Л. В. Крушинского по изучению так называемой элементарной рассудочной деятельности у животных [1]. Основные результаты изложены в статье [2]. Здесь мы рассмотрим свойства кодов среды.

Изображение — конечное множество точек на плоскости. Кодом изображения A называем пару $\langle M_A, T_A\rangle$. Здесь M_A — множество номеров точек изображения, T_A — множество всех чисел вида $\rho_{mnu,ksp} = S_{mnu}/S_{ksp}$, где S_{mnu} и S_{ksp} — площади треугольников в вершинах с точками соответственно m, n, u и k, s, p. При $S_{ksp} = 0$ полагаем $\rho_{mnu,ksp}$ неопределенным. Изображения A и B с кодами $\langle M_A, T_A\rangle$ и $\langle M_B, T_B\rangle$ называем эквивалентными, если существует такая биекция $\psi : M_A \to M_B$, что $\rho_{mnu,ksp} = \rho_{\psi(m)\psi(n)\psi(u),\psi(k)\psi(s)\psi(p)}$. Если все точки изображения не лежат на одной прямой или двух параллельных прямых, то изображение называем плоским.

Теорема 1 [2]. *Два плоских изображения эквивалентны тогда и только тогда, когда они аффинно эквивалентны.*

Содержательно теорема 1 означает, в частности, что код изображения задает его с точностью до аффинных преобразований.

Пусть B есть часть изображения A. Если код для A есть $\langle M_A, T_A\rangle$, то, очевидно, код $\langle M_B, T_B\rangle$ можно получить, если собрать в M_B номера из M_A

всех точек, вошедших в B, и собрав в T_B все те $\rho_{mnu,ksp}$ из T_A, для которых m, n, u, k, s, p вошли в M_B. Говорим в этом случае, что код $\langle M_B, T_B\rangle$ есть часть кода $\langle M_A, T_A\rangle$.

Известно, что для построения изображения A по коду $\langle M_A, T_A\rangle$ достаточно таких элементов $\rho_{mnu,ksp}$ из T_A, у которых тройки mnu и ksp разнятся только одним номером. Возникает вопрос: какова может быть роль других элементов $\rho_{mnu,ksp}$ в коде?

Назовем изображения A и B эквидистантными, если существует такая биекция $\psi : M_A \to M_B$, при которой для любых точек с номерами m, n, u из M_A (не лежащих на одной прямой), число $\rho_{mnu,\psi(m)\psi(n)\psi(u)}$ есть константа, не зависящая от выбора точек m, n, u.

Название «эквидистантные изображения» объясняется следующей аналогией с более простым случаем. Пусть A и B есть изображения, совместимые параллельным переносом. Тогда, очевидно, существует биекция $\psi : M_A \to M_B$ такая, что все расстояния $r(a, \psi(a))$ между соответствующими точками двух изображений есть константа. Отрезки $r(a, \psi(a))$ для всех a из M_A в этом случае не только равны, но и параллельны. Очевидно, имеет место и обратное: если все эти отрезки равны и параллельны, то A и B совместимы параллельным переносом.

Теорема 2. *Два плоских изображения эквидистантны тогда и только тогда, когда они аффинно эквивалентны.*

Доказательство. Пусть A и B аффинно эквивалентны. Тогда существует такая биекция $\psi : M_A \to M_B$, что B переводится в B', совмещенное с A, т. е. при этом каждая точка a из A совмещена с точкой $\psi(a)$. Ясно, что при этом для каждой тройки m, n, u из A (не лежащих на одной прямой) и соответствующей тройки k', s', p' из B' (здесь $k' = \psi(m)$, $s' = \psi(n)$, $p' = \psi(u)$) имеем $\rho_{mnu,k's'p'} = S_{mnu}/S_{k's'p'} = q$. Вернем теперь обратным преобразованием B' в B. При этом площадь каждого треугольника с вершинами $k's'p'$ из B' при переводе в треугольник ksp с вершинами из B умножится на одну и ту же для всех треугольников величину q. Следовательно $\rho_{mnu,ksp} = S_{mnu}/S_{ksp} = S_{mnu}/(qS_{k's'p'}) = 1/q$.

Пусть теперь A и B эквидистантны. Если B' получено из B аффинным преобразованием, то нетрудно видеть, A и B' тоже эквидистантны. Выберем некоторые три точки (не на одной прямой) m, n, u на A, и пусть преобразованное B' таково, что его точки k', s', p', соответствующие точкам m, n, u, совпали с ними, т. е. площади треугольников mnu и $k's'p'$ равны. Но тогда, с учетом эквидистантности, должны быть равны площади и всех остальных соответствующих друг другу треугольников из A и B'. Однако это значит, что коды $\langle M_A, T_A\rangle$ и $\langle M_{B'}, T_{B'}\rangle$ эквивалентны, и, значит, в силу теоремы 1, изображения A и B' аффинно эквивалентны. Но тогда аффинно эквивалентны и изображения A и B. Теорема доказана.

Итак, прояснена роль элементов $\rho_{mnu,ksp}$ кода с полностью различными тройками mnu и ksp. Роль элементов с двумя различиями в этих тройках пока не ясна.

Список литературы

[1] Крушинский Л. В., Кудрявцев В. Б., Козлов В. Н. О некоторых результатах применения математики к моделированию в биологии // Математические вопросы кибернетики. — 1988. — Вып. 1. — С. 52–88.

[2] Козлов В. Н. Введение в математическую теорию зрительного восприятия. — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2007. — 136 с.

Асимптотические оценки высокой степени точности для сложности булевых формул в некоторых базисах, состоящих из элементов с прямыми и итеративными входами

Коноводов Владимир Александрович

Московский государственный университет имени М. В. Ломоносова, e-mail: vkonovodov@gmail.com

Пусть $X = \{x_1, x_2, \ldots\}$ и $Y = \{y_1, y_2, \ldots\}$ — счетные множества булевых переменных, причем переменные из множества X (из Y) будем называть *прямыми* (соответственно, *итеративными*). Для каждого множества переменных Z обозначим через $P_2(Z)$ множество всех функций алгебры логики (в дальнейшем — просто функций), зависящих от переменных из Z. Функции, не имеющие общих существенных переменных, будем называть *независимыми*.

На множестве $P_2(X \cup Y)$, согласно [1], определим следующие операции суперпозиции: переименование (с отождествлением) прямых переменных; подстановка констант 0, 1 вместо переменных; переименование (без отождествления) итеративных переменных; подстановка одной из двух независимых функций вместо итеративной переменной другой функции; замена итеративных переменных прямыми переменными; отождествление итеративных переменных.

Пусть $A \subseteq P_2(X \cup Y)$ — некоторое конечное множество базисных функций. В соответствии с введенными операциями суперпозиции будем рассматривать одновыходные схемы из функциональных элементов (см., например, [2]) над базисом A, в которых прямые входы любого элемента либо присоединяются к входам схемы, либо являются константными входами (вход называется константным, если вместо него в базисный элемент подставлена константа 0 или 1); итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами; неконстантным входам схемы сопоставлены некоторые переменные из множества X. Под формулами будем понимать те одновыходные схемы, в которых выход любого элемента либо поступает на вход ровно одного (другого) элемента, либо является выходом схемы.

Систему функций A, $A \subseteq P_2(X \cup Y)$, будем называть *полной*, если для любой функции f, $f \in P_2(X)$, существует формула над A указанного вида, реализующая функцию f.

Рассмотрим произвольный базис $A = \{\mathcal{E}_1, \ldots, \mathcal{E}_b\}$, $A \subseteq P_2(X \cup Y)$. Будем считать, что каждый элемент $\mathcal{E}_i$, $i = 1, \ldots, b$, имеет вес L_i, и k_i входов, при этом k_i' из них прямые, а $k_i'' = k_i - k_i'$ итеративны. *Приведенным весом* элемента $\mathcal{E}_i$, $i = 1, \ldots, b$, такого, что $k_i > 1$, назовем величину $\rho_i = \frac{L_i}{k_i - 1}$.

Макроблоком в базисе A назовем схему из функциональных элементов в этом базисе, состоящую из одного элемента $\mathcal{E}_j \in A$, $j \in \{1, \ldots, b\}$, такого, что $k_j'' > 1$, и m, $m = (k_j'' - 1)$, элементов $\mathcal{E}_{i_1}, \ldots, \mathcal{E}_{i_m}$, выходы которых подаются на итеративные входы элемента $\mathcal{E}_j$, и для которых $k_{i_t}'' = 0$, $t = 1, \ldots, m$. Итеративным входом макроблока будем считать его свободный (т. е. тот, на который не подаются выходы других элементов макроблока) входов элемента $\mathcal{E}_j$, остальные входы макроблока будем считать прямыми. *Приведенным весом* макроблока M указанного вида назовем величину

$$\rho_M = \frac{L_j + L_{i_1} + \ldots + L_{i_m}}{k_{i_1} + \ldots + k_{i_m} + k_j - m - 1}.$$

Приведенным весом ρ_A базиса A назовем минимальный приведенный вес среди всех элементов с хотя бы одним итеративным входом и всех макроблоков в этом базисе. Пусть $\hat{A}$ — множество элементов базиса A с итеративными входами, которые либо имеют приведенный вес, равный ρ_A, либо входят в макроблоки этого базиса с приведенным весом ρ_A.

Сложностью $\mathcal{L}(\mathcal{F})$ формулы $\mathcal{F}$ в базисе A будем называть сумму весов всех входящих в нее элементов. Функцией Шеннона $\mathcal{L}_A(n)$ для сложности формул в базисе A, как обычно, будем называть максимальное значение $\mathcal{L}_A(f)$ среди всех функций f, $f \in P_2(\{x_1, \ldots, x_n\})$, где $\mathcal{L}_A(f)$ — минимальная сложность формулы из рассматриваемого класса, реализующей функцию f.

Пусть $A \subseteq P_2(X \cup Y)$. Множество тех функций, которые можно получить из функций системы A в результате применения операций суперпозиции, описанных выше, обозначим через $[A]$. Множество всех функций множества $[A]$, зависящих только от итеративных переменных, обозначим $\delta(A) = [A] \cap P_2(Y)$ и будем называть *итеративным замыканием* [1, 3] базиса A. Множество $\delta(A)$ представляет собой «обычный» замкнутый класс (см., например, [2]) в $P_2(Y)$, и поэтому совпадает с одним из классов системы $\Delta = \{B, I, O, D, K, L, M, P_2(Y)\}$, где $B = \{0, 1\}$, $I = Y \cup B$, $O = I \cup \{\bar{y} : y \in Y\}$, класс D (класс K) содержит константы и дизъюнкции (соответственно, конъюнкции) переменных Y, а классы L и M состоят из линейных и монотонных функций от переменных Y соответственно.

В [4] показано, что для любой системы функций A, $A \subseteq P_2(X \cup Y)$, такой, что $\delta(A) \in \{M, P_2(Y)\}$, справедливо соотношение[‡] $\mathcal{L}_A(n) \sim \rho_A \cdot \frac{2^n}{\log n}$,, а в [5] получены асимптотические оценки высокой степени точности для сложности формул такого класса, а именно для любого базиса A такого, что

[‡]Все логарифмы в данной работе рассматриваются по основанию 2.

$\delta(\hat{A}) \in \{P_2(Y), M\}$, показана справедливость соотношения[§]

$$\mathcal{L}_A(n) = \rho_A \cdot \frac{2^n}{\log n} \cdot \left(1 \pm \frac{O(1)}{\log n}\right). \qquad (1)$$

В работе [3] указано, что для каждого δ, $\delta \in \{I, O, D, K, L\}$, существует базис A такой, что $\delta(A) = \delta$ и при этом $\mathcal{L}_A(n) = \Theta\left(2^n\right)$. Следует отметить, что для аналогичной функции Шеннона для сложности схем из функциональных элементов асимптотика и оценки высокой степени точности получены в [6].

В данной работе расширен класс базисов, для которых доказаны оценки высокой степени точности функции Шеннона для сложности формул. А именно получены следующие результаты.

Теорема 1. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис, такой, что $\delta(A) \supseteq M$, а $\delta(\hat{A}) \in \{L, D, K\}$. Тогда, если множество $\hat{A}$ либо является полным, либо содержит функцию f вида $(\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0$, где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых переменных, что $\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0$, то при растущем значении натурального аргумента n, $n \geqslant 2$, справедливо соотношение (1). Если же множество $\hat{A}$ содержит функцию, зависящую хотя бы от одной прямой переменной, то справедлива оценка*

$$\mathcal{L}_A(n) \leqslant \rho_A \cdot \frac{2^n}{\log n} \cdot \left(1 + \frac{\log\log\log n + O(1)}{\log n}\right).$$

Теорема 2. *Пусть*

$$A_1 = \{y_1 \cdot \ldots \cdot y_{k_1}, x_1 \vee \ldots \vee x_{k_2}, \bar{y}_1\},$$
$$A_2 = \{y_1 \vee \ldots \vee y_{k_1}, x_1 \cdot \ldots \cdot x_{k_2}, \bar{y}_1\},$$

где $k_1, k_2 \geqslant 2$, при этом минимальный приведенный вес каждого из базисов достигается только на макроблоках. Тогда для $i = 1, 2$ имеет место соотношение:

$$\mathcal{L}_{A_i}(n) = \rho_{A_i} \cdot \frac{2^n}{\log n} \cdot \left(1 + \frac{\frac{1}{k_2}\log\log n \pm O(1)}{\log n}\right).$$

Работа выполнена при поддержке РФФИ (проект № 15-01-07474-а).

Список литературы

[1] Ложкин С. А. О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 1999. — № 3. — С. 35–41.

[§]Запись $f(n) = O(g(n))$ для неотрицательных функций $f(n)$ и $g(n)$ натурального аргумента n означает, что найдется константа $c > 0$ такая, что $f(n) \leqslant c \cdot g(n)$. Запись $f(n) = \Theta(g(n))$ означает одновременное выполнение равенств $f(n) = O(g(n))$ и $g(n) = O(f(n))$.

[2] Яблонский С. В. Введение в дискретную математику.— М.: Высшая школа, 2003. — 384 с.

[3] Коноводов В. А. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными переменными // Учёные записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, кн. 3. — С. 76–83.

[4] Ложкин С. А., Коноводов В. А. О сложности формул алгебры логики в некоторых полных базисах, состояших из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 1 (в печати).

[5] Ложкин С. А., Коноводов В. А. Оценки высокой степени точности для сложности булевых формул в некоторых базисах из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 2 (в печати).

[6] Ложкин С. А. О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными входами // Труды III Международной конференции «Дискретные модели в теории управляющих систем» (Красновидово, 1998 г.). — М., 1998. — С. 72–73.

О сравнении поведения автоматов, порождаемых локальными преобразованиями ОД-k-эталона

Копытова Ольга Михайловна

Донецкий национальный технический университет, e-mail: omkop@list.ru

Введение

В работе исследуется влияние переброски одной дуги на поведение инициального приведенного автомата. Целью работы является: 1) поиск меры близости поведения автомата-эталона и автомата, полученного из эталона переброской одной дуги; 2) оценка этой меры близости; 3) описание класса автоматов с заданной степенью близости.

Под автоматом понимаем инициальный приведенный (в частном случае, определенно-диагностируемый порядка k) автомат Мили $A = (S, X, Y, \delta, \lambda, s_0)$, где S, X, Y — конечные множества состояний, входных и выходных символов соответственно, δ, λ — функции переходов и выходов, а s_0 — начальное состояние. Автомат A называется ОД-k-автоматом, если $k \geq 1$ — наименьшее целое такое, что для любого входного слова p длины k и любой пары различных состояний $s, t \in S$ выполняется неравенство $\lambda(s, p) \neq \lambda(t, p)$. Неопределяемые понятия можно найти в [1].

Будем говорить, что вход-выходное слово $w = (p, q)$ порождается состоянием s автомата A, если $\lambda(s, p) = q$. Два состояния s и t одного и того же автомата A или двух разных автоматов A и B соответственно, называются эквивалентными, если для всякого входного слова $p \in X^*$ выполняется $\lambda(a, p) \neq \lambda'(b, p)$, где λ' - функция выходов автомата A или B. Автомат называется приведенным, если все его состояния попарно неэквивалентны. Каждому состоянию s поставим в соответствие множество λ_s всех вход-выходных слов, порождаемых этим состоянием. Под поведением автомата A будем понимать множество λ_{s_0} вход-выходных слов, порождаемых его начальным состоянием.

Автомат удобно задавать в виде графа переходов, вершины которого соответствуют состояниям из S, а дугами являются четверки (s, x, y, t), где $t = \delta(s, x), y = \lambda(s, x)$. Пара (x, y) называется отметкой дуги, s — ее началом, а t — концом. Пусть $e = (t, x, y, u)$ — дуга в графе переходов автомата A. Переброской дуги, исходящей из состояния t, назовём замену её некоторой другой дугой (t, x, y, v), где $v \neq u$.

Пусть автомат A' получен из A переброской произвольной дуги. Назовём A' автоматом, локально порождённым из эталона A. Обозначим через $K(A)$ класс всех автоматов, локально порождённых из A, включая сам эталон. Для указанного класса выполним следующее: 1) введём метрику, позволяющую вычислить расстояние между любой парой автоматов; 2) найдём достижимую нижнюю оценку для этого расстояния; 3) опишем подклассы автоматов, находящиеся на заданном расстоянии от эталона.

Основные результаты

Введем на классе автоматов бэровскую метрику [2] следующим образом. Пусть i — длина некоторого кратчайшего входного слова p, различающего начальные состояния s_0 и s'_0 автоматов A и A' соответственно, т. е. такого слова, для которого $\lambda(s_0, p) \neq \lambda'(s'_0, p)$. Здесь состояния автомата A' и его функции помечены штрихом. Зададим расстояние между A и A':

$$\rho(A, A') = \begin{cases} 0, & \text{если } \lambda_{s_0} = \lambda'_{s'_0}; \\ 1/i, & \text{если } \lambda_{s_0} \neq \lambda'_{s'_0}. \end{cases} \tag{1}$$

Ясно, что с ростом длины различающего слова p расстояние $\rho(A, A')$ между A и A' уменьшается. Пусть $|X| = m$ и $|S| = n$. Каждую из mn дуг можно перебросить в одно из $(n - 1)$ состояний. Тогда количество возможных переброс равно $mn(n - 1)$, и, значит, класс $K(A)$ состоит из $(mn(n - 1) + 1)$ автоматов, включая эталон. Исследуем разбиение $K(A)$ на подклассы $K_i(A)$ автоматов, находящихся на одинаковом расстоянии $1/i$ от эталона.

Рассмотрим классы $K_0(A)$ и $K_1(A)$. По определению, $\rho(A, A) = 0$, и, значит, $A \in K_0(A)$ и $K_0(A) \neq \varnothing$. Если же $A \neq A'$, то легко видеть, что равенство $\lambda_{s_0} = \lambda'_{s'_0}$ выполняется в единственном случае — когда состояние t, из которого произошла переброска, не достижимо из s_0. Заметим, что при переброске дуги её отметка не изменяется, т. е. состояния s_0 и s'_0 выдают одну и ту же реакцию на каждый входной символ. Следовательно, длина различающего их слова

больше или равна 2. Отсюда $K_1(A) = \varnothing$ и $\rho(A, A') \le 1/2$. С другой стороны, пара состояний (s_0, s_0') всегда различима некоторым входным словом длины, не превосходящей $(2n-1)$, поэтому $\rho(A, A') \ge 1/(2n-1)$. Таким образом, $1/(2n-1) \le \rho(A, A') \le 1/2$, и разбиение класса $K(A)$ на подклассы имеет вид:

$$K(A) = \bigcup_{i=0}^{2n-1} K_i(A). \tag{2}$$

Задача состоит в том, чтобы для любой переброски оценить $\rho(A, A')$ и описать классы $K_i(A)$ для $i \ge 2$.

В дальнейшем рассматриваются инициально связные автоматы, в которых каждое состояние достижимо из начального. Обозначим через d длину кратчайшего входного слова w, для которого $\delta(s_0, w) = t$.

Теорема 1. *Пусть $A = (S, X, Y, \delta, \lambda, s_0)$ — произвольный инициальный приведенный автомат и A' получен из A переброской дуги из состояния t. Тогда* $\rho(A, A') \ge \dfrac{1}{d+n}$.

Теорема 2. *Пусть $A = (S, X, Y, \delta, \lambda, s_0)$ — инициальный приведенный ОД-k-автомат и A' получен из A переброской дуги из состояния t. Тогда* $\rho(A, A') \ge \max\left(\dfrac{1}{d+k+1}, \dfrac{1}{d+n}\right)$.

Полученные нижние оценки в теоремах 1 и 2 достижимы. Пусть A' есть результат переброски дуги (t, x, y, u) в состояние v и c — длина кратчайшего слова, различающего состояния u и v в автомате A.

Теорема 3. *Класс $K_i(A)$ состоит из всех тех автоматов A', для которых выполняется условие: $d + c + 1 = i$, где $2 \le i \le 2n-1$.*

По этой теореме $A' \in K_i(A)$ тогда и только тогда, когда состояние t достижимо из s_0 по кратчайшему слову длины d, состояния u и v различимы кратчайшим словом длины c, и при этом $d + c = i - 1$. Поскольку $c \le n-1$, то d и c для подкласса $K_i(A)$ изменяются синхронно следующим образом.

В случае $i \le n$:

$$\begin{array}{cccccc} d = 0, & 1, & 2, & , ..., & i-2 \\ c = i-1, & i-2, & i-3, & , ..., & 1. \end{array}$$

В случае $i = n + j$, где $1 \le j \le n-1$:

$$\begin{array}{cccccc} d = j, & j+1, & j+2, & , ..., & n-1 \\ c = n-1, & n-2, & n-3, & , ..., & j. \end{array}$$

Данное в теореме 3 описание структуры классов может быть положено в основу алгоритма их построения.

Список литературы

[1] Грунский И. С., Козловский В. А. Синтез и идентификация автоматов. — Киев: Наукова думка, 2004. — 246 с.

[2] Кудрявцев В. Б., Грунский И. С., Козловский В. А. Анализ и синтез абстрактных автоматов // Фундамент. и прикл. матем. — 2009.— Т. 15, вып. 4. — С. 101–175.

О первообразных корнях из языков специального вида

Корабельщикова Светлана Юрьевна[1], **Чесноков Алексей Игоревич**[2], **Тутыгин Андрей Геннадьевич**[3]

[1] Северный (Арктический) федеральный университет им. М. В. Ломоносова, e-mail: kmv@atnet.ru
[2] Северный (Арктический) федеральный университет им. М. В. Ломоносова, e-mail: cleric_air@mail.ru
[3] ООО «Лаборатория информационно-аналитических систем», г. Архангельск, e-mail: andgt64@yandex.ru

Пусть Σ — произвольный алфавит. Рассмотрим задачу извлечения корня из заданного языка: для заданного языка $A \subseteq \Sigma^*$ и заданного $n \in \mathbb{N}$ требуется найти все языки B, такие что $A = B^n$.

Мы рассмотрим некоторый специальный класс языков, для которого эта задача легко решается.

Исследуем вопрос извлечения корня заданной степени из языков вида:

$$\bigcup_{t_1 \leqslant i \leqslant t_2} \Sigma^i, \text{ где } t_1, t_2 \in \mathbb{N},\ t_1 \leqslant t_2. \tag{1}$$

Как было отмечено в [1], операция извлечения корня не является однозначной функцией. Отметим вполне очевидный факт: для того, чтобы корень n-й степени из языка вида (1) извлекался, необходимо и достаточно, чтобы t_1 и t_2 делились на n. Справедлива следующая теорема.

Теорема 1. *Пусть Σ — произвольный алфавит. Язык $\bigcup\limits_{i \in M} \Sigma^i$ является корнем n-й степени из языка $\bigcup\limits_{n \cdot n_1 \leqslant i \leqslant n \cdot n_2} \Sigma^i$ тогда и только тогда, когда M — подмножество множества $\{n_1, n_1 + 1, \ldots, n_2\}$, удовлетворяющее условию:*

$$(\forall i)(n \cdot n_1 \leqslant i \leqslant n \cdot n_2 \to i = a_1 + a_2 + \cdots + a_n), \tag{2}$$

где a_1, a_2, …, a_n — некоторые элементы из M (не обязательно различные).

При этом между корнями n-й степени из языка $\bigcup\limits_{n \cdot n_1 \leqslant i \leqslant n \cdot n_2} \Sigma^i$ и корнями n-й степени из языка $\bigcup\limits_{n \leqslant i \leqslant n \cdot n_2 - n \cdot n_1 + n} \Sigma^i$ имеется взаимно однозначное соответствие. Множеству индексов M корня из языка $\bigcup\limits_{n \leqslant i \leqslant n \cdot n_2 - n \cdot n_1 + n} \Sigma^i$ соответствует множество индексов $L = M + (n_1 - 1)$ корня из языка $\bigcup\limits_{n \cdot n_1 \leqslant i \leqslant n \cdot n_2} \Sigma^i$. Число корней n-й степени зависит от n и от разности $n_2 - n_1$ граничных значений множества индексов корня.

Обозначим $k = n_2 - n_1 + 1$ — это мощность множества $\{n_1, n_1 + 1, \ldots, n_2\}$. Нами реализован алгоритм нахождения всех корней по заданным n, t_1 и

t_2. Сложность вычислений полученной реализации равна $O\left(2^{(k-4)} \cdot n^2 \cdot k^2\right)$, что позволяет находить все корни для $k \leqslant 30$. Ниже в таблице приведено количество корней для некоторых n и k. При k от 1 до 3 значения равны 1.

n/k	4	5	6	7	8	9	10	11	12	13	14
2	1	2	3	5	9	15	28	50	95	174	337
3	1	2	4	7	13	25	49	95	185	365	721
4	1	2	4	8	15	29	57	113	225	447	889
5	1	2	4	8	16	31	61	121	241	481	961
6	1	2	4	8	16	32	63	125	249	497	993
7	1	2	4	8	16	32	64	127	253	505	1009

Первообразные корни

Пусть S — семейство всех множеств индексов корней n-й степени из языка $\bigcup\limits_{n\cdot n_1 \leqslant i \leqslant n\cdot n_2} \Sigma^i$. Корень вида $\bigcup\limits_{i\in M}\Sigma^i$ назовём *первообразным*, если M — минимальное по включению множество из S.

Мощность множества индексов назовём *весом* корня.

Пример 1. Из языка $\bigcup\limits_{2\leqslant i\leqslant 14} \Sigma^i$ извлекаются 5 квадратных корней с множествами индексов $\{1,2,3,4,5,6,7\}$, $\{1,2,3,4,6,7\}$, $\{1,2,4,5,6,7\}$, $\{1,2,4,6,7\}$ и $\{1,2,3,5,6,7\}$. Из них 2 последних множества индексов — минимальные, им соответствуют два первообразных корня веса 5 и 6 соответственно.

Отметим вполне очевидные свойства первообразных корней.

1. Если $M \in S$ и M — множество индексов минимальной мощности, то соответствующий M корень — первообразный. Обратное утверждение в общем случае неверно. Первообразный корень не обязан иметь минимальный вес (см. пример 1).
2. Пусть $\bigcup\limits_{i\in M}\Sigma^i$ — первообразный корень n-й степени из языка $\bigcup\limits_{n\cdot n_1 \leqslant i \leqslant n\cdot n_2} \Sigma^i$ с множеством индексов M, и $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ — двоичный характеристический вектор подмножества M множества $\{n_1, n_1+1, \ldots, n_2\}$. Тогда симметричный вектор $(\alpha_k, \alpha_{k-1}, \ldots, \alpha_1)$ также задаёт множество индексов первообразного корня.
3. Если первообразный корень из языка единственен, то характеристический вектор его множества индексов симметричен.
4. Пусть $\bigcup\limits_{i\in M}\Sigma^i$ — первообразный корень n-й степени из языка $\bigcup\limits_{n\cdot n_1 \leqslant i \leqslant n\cdot n_2} \Sigma^i$ с множеством индексов M. Тогда для любого множества M', такого что $M \subseteq M' \subseteq \{n_1, n_1+1, \ldots, n_2\}$, $\bigcup\limits_{i\in M'}\Sigma^i$ — корень n-й степени из этого же языка.
5. Из свойства 4 вытекает следующее свойство: если вес первообразного корня $w \leqslant k$, и он единственен, то общее число корней из языка равно 2^{k-w}.

Как следует из свойств первообразных корней, чтобы получить все корни n-й степени из языка $\bigcup\limits_{n\cdot n_1 \leqslant i \leqslant n\cdot n_2} \Sigma^i$, достаточно знать первообразные корни, или, что то же самое, их множества индексов.

Пример 2. Найдем все корни третьей степени из языка $\bigcup\limits_{27 \leqslant i \leqslant 42} \Sigma^i$.

Множество индексов корня является подмножеством в $\{9, 10, 11, 12, 13, 14\}$, то есть $k = 6$. При $n = 3$, $k = 6$ первообразный корень один, и он имеет характеристический вектор (110011). Поэтому получим всего 4 корня с множествами индексов: $\{9, 10, 13, 14\}$, $\{9, 10, 11, 13, 14\}$, $\{9, 10, 12, 13, 14\}$ и $\{9, 10, 11, 12, 13, 14\}$.

Выводы

Исходная задача свелась, по сути, к задаче представления натуральных чисел из заданного интервала $[t_1, t_2]$ в виде суммы n натуральных слагаемых из интервала $[t_1/n, t_2/n]$, что можно рассматривать как частный случай задачи о рюкзаке, применяемой авторами ранее в [2]. Множество первообразных корней n-й степени позволяет найти все корни из языков вида (1). С другой стороны, если множество всех корней из языка достаточно велико, выделение первообразных корней является более-менее экономным его описанием.

Список литературы

[1] Корабельщикова С. Ю., Мельников Б. Ф. Максимальные префиксные коды и проблема равенства в разных классах языков // Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014г.) — Казань: Отечество, 2014. — С. 143–146.

[2] Зяблицева Л. В., Корабельщикова С. Ю., Чесноков А. И. Линейные коды, исправляющие ошибки, и алгоритмы их подсчета // Эвристические алгоритмы и распределённые вычисления. — 2014. — Т. 1, вып. 3. — С. 47–59.

О многоэтапных задачах оптимизации

Коротченко Анатолий Григорьевич[1], **Сморякова Валентина Михайловна**[2]

[1] Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: koangr@yandex.ru
[2] Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: smorykov@mail.ru

Рассматривается многошаговая система, описываемая соотношениями:

$$Y^{j+1} = F(Y^j, Y^{j-1}, ..., Y^{j-k}, \tau_{j+1}, \tau_j, \tau_{j-1}, ..., \tau_{j-k}),$$

где $Y^j \in R^n$, $\tau_j \in R$, $j = 0, 1, ...$, $k \geq 1$. При этом состояния $Y^0, Y^{-1}, ..., Y^{-k}$ и параметры $\tau_0, \tau_{-1}, ..., \tau_{-k}$ задаются априори. Система начинает функционировать из начального состояния $Y^0 \in R^n$. Переход системы из j-ого состояния в $j+1$-ое состояние определяется путём задания значения параметра τ_{j+1}. Качество перевода определяется некоторой функцией $q_{j+1}(\tau_{j+1})$. Данную функцию можно трактовать как локальный критерий, который характеризует переход системы из одного состояния в другое. Наряду с локальными критериями система

характеризуется интегральным (глобальным) критерием, который оценивает поведение системы в целом:

$$Q(\tau_1, \tau_2, ..., \tau_m) = \sum_{j=1}^{m} q_j(\tau_j), \tag{1}$$

где m не предполагается известным, а определяется в процессе функционировании системы. Поскольку значение m априори не задано, то мы можем осуществлять только локальное управление, задавая его в виде соответствующего параметра τ_{j+1}. При этом мы хотим выбирать эти управления так, чтобы для любого $m = 1, 2, ...$ максимизировать интегральный критерий.

В рамках данного описания может быть сформулирована задача о минимизации числа узлов конечно-разностной формулы численного интегрирования обыкновенных дифференциальных уравнений, которая сводится к следующей задаче математического программирования:

$$Q_m(\tau_1, ..., \tau_m) = \sum_{j=1}^{m} c_j \tau_j \Rightarrow \max,$$

$$T(m) = (\tau_1, ..., \tau_m) \in D_m,$$

$$D_m = \{T(m) \in P_m \subseteq R^m \mid f_j(\tau_{j-1}, \tau_j) \leq 0,\ j = 1, ..., m\},$$

где значение m не предполагается известным, а определяется в процессе её решения, а τ_j — значения шагов интегрирования, соответствующей конечно-разностной формулы. Здесь $q_j(\tau_j) = c_j \tau_j$ — локальный критерий, задаваемый на множестве, определяемом условиями $f_j(\tau_{j-1}, \tau_j) \leq 0,\ j = 1, ..., m$, а $Q_m(\tau_1, ..., \tau_m) = \sum\limits_{j=1}^{m} q_j(\tau_j)$ — интегральный критерий, определённый на множестве D_m.

Рассмотрим задачу (1), когда $c_j > 0$, а $f_j(\tau_{j-1}, \tau_j)$ дифференцируемы на R^2_+, $j = 1, ..., m$. Обозначим производную функции $f_j(\tau_{j-1}, \tau_j)$ по τ_j через $\varphi_j(\tau_{j-1}, \tau_j)$, а через $g_j(\tau_{j-1}, \tau_j)$ производную функции $f_j(\tau_{j-1}, \tau_j)$ по τ_{j-1}, $j = 1, ..., m$.

Пусть $T'(k) = (\tau'_1, ..., \tau'_k)$ — решение задачи (1) при $m = k$, а $T''(k+1) = (\tau''_1, ..., \tau''_{k+1})$ — решение задачи (1) при $m = k + 1$ (при условии, что они существуют).

Потребуем, чтобы выполнялись следующие соотношения:

$$\tau'_j = \tau''_j, j = 1, ..., k, \tag{2}$$

для любого $k = 1, ..., m$, $m = 1, 2....$

Данные соотношения гарантируют, что решение m задач с локальными критериями:

$$q_j(\tau_j) = c_j \tau_j \Rightarrow \max,$$

$$f_j(\tau_{j-1}, \tau_j) \le 0, j = 1, ..., m,$$

τ_0 — заданная величина, даёт решение задачи с интегральным критерием для любого $m = 1, 2....$ Пусть функции $f_j(\tau_{j-1}, \tau_j)$, $j = 1, ..., m$, удовлетворяют следующим условиям:

Условие 1. *Для любого фиксированного* $\tau_{j-1} \in [0, \bar{\tau}_{j-1}]$ *уравнение*

$$f_j(\tau_{j-1}, \tau_j) = 0 \tag{3}$$

имеет единственный положительный корень $\bar{\tau}_j$, *а* $f_j(\tau_{j-1}, 0) < 0$ *при* $\tau_{j-1} > 0$ *и* $f_j(\tau_{j-1}, 0) \ge 0$ *при* $\tau_j \ge \bar{\tau}_j$, $j = 1, ..., m$.

Условие 2. *Для всех* $\tau_{j-1} \ge 0$, $\tau_j > 0$, *удовлетворяющих равенству* (3), *справедливы соотношения*

$$g_j(\tau_{j-1}, \tau_j) > 0, j = 1, ..., m,$$

$$0 < 1 - \frac{c_j}{c_{j-1}} \cdot \frac{\varphi_j(\tau_{j-1}, \tau_j)}{g_j(\tau_{j-1}, \tau_j)} \le 1, j = 2, ..., m.$$

Пусть $\bar{\tau}_j$ — *единственный положительный корень уравнения* (3), *существующий в силу условия* 1, $j = 1, ..., m$ *и пусть*

$$\bar{T}(m) = (\bar{\tau}_1, ..., \bar{\tau}_m).$$

Теорема 1. *Если выполнены условия* 1 *и* 2, *то вектор*

$$\bar{T}(m) = (\bar{\tau}_1, ..., \bar{\tau}_m)$$

является решением задачи (1), когда $c_j > 0$, *при* $\bar{\tau}_0 > 0$ *и имеют место соотношения* (2), *где* $f_j(\bar{x}_{j-1}, \bar{x}_j) = 0$, $j = 1, ..., m$.

Для задачи математического программирования вида (1), основанной на использовании конечно-разностной схемы численного интегрирования, описанная в [1], справедлива теорема 1.

Список литературы

[1] Коротченко А. Г., Лапин А. В. О построении построении приближенно оптимального алгоритма численного интегрирования // Вестник нижегородского государственного университета им. Н. И. Лобачевского. Сер. «Математическое моделирование и оптимальное управление». — 2003. — Вып. 1 (26). — С. 189–195.

[2] Коротченко А. Г. О задачах математического программирования, имеющих многоэтапный характер // Вестник Нижегородского государственного университета им. Н. И. Лобачевского. — 2011. — № 1. — С. 183–187.

[3] Коротченко А. Г., Сморякова В. М. Об одном классе задач, имеющих многоэтапный характер // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 146.

Применение неполной выводимости в исчислении предикатов для решения ряда задач искусственного интеллекта

Косовская Татьяна Матвеевна

Санкт-Петербургский государственный университет, e-mail: kosovtm@gmail.com

В рамках логико-предметного подхода к решению задач искусственного интеллекта (ИИ) рассматриваются задачи распознавания объектов с неполной информацией, выделения информативных обобщённых признаков и создание метрики для объектов, описанных на языке исчисления предикатов. Решение этих задач базируется на понятии неполной выводимости формул в исчислении предикатов.

Введение

При логико-предметном подходе, в отличие от логико-алгебраического, каждый исследуемый объект представлен как множество его частей, а признаками объекта являются свойства этих частей и отношения между ними, задаваемые одноместными и многоместными предикатами соответственно [1]. Имеется множество Ω конечных множеств $\omega = \{\omega_1, \ldots, \omega_t\}$. На элементах ω задан набор предикатов $p_1, \ldots, p_n$, характеризующих свойства и отношения между элементами объекта ω. Задано разбиение множества Ω на K (возможно пересекающихся) классов $\Omega = \bigcup_{k=1}^{K} \Omega_k$.

Логическим описанием $S(\omega)$ объекта ω называется набор всех истинных постоянных формул вида $p_i(\overline{\tau})$ или $\neg p_i(\overline{\tau})$, выписанных для всех возможных упорядоченных наборов $\overline{\tau}$ элементов объекта ω.

Логическим описанием класса Ω_k называется бесквантворная формула $A_k(\overline{x})$ со свободными переменными $\overline{x}$, представленная в виде дизъюнкции элементарных конъюнкций атомарных формул, и такая, что если для некоторого списка $\overline{\omega}$ всех элементов множества ω истинна формула $A_k(\overline{\omega})$, то $\omega \in \Omega_k$.

Решение многих задач ИИ основано на доказательстве логического следования $S(\omega) \Rightarrow \exists \overline{x}_{\neq} A(\overline{x})$, где A(x) — элементарная конъюнкция.

В [2] доказаны оценки числа шагов алгоритмов, решающих сформулированные задачи. Доказана NP-трудность рассматриваемых задач.

Неполная выводимость

Рассматривается задача проверки того, что из истинности всех формул множества $S(\omega)$ следует истинность $A(\overline{x})$ или некоторой её максимальной подформулы $A'(\overline{x'})$ на наборе различных констант из ω. Пусть a и a' — количества атомарных формул в формулах $A(\overline{x})$ и $A'(\overline{x'})$, m и m' — количества переменных формул в формулах $A(\overline{x})$ и $A'(\overline{x'})$ соответственно. Параметры q и r определяются соответственно по формулам $q = a'/a$, $r = m'/m$. В этом случае формула $A'(\overline{x'})$ называется (q, r)-фрагментом формулы $A(\overline{x})$.

Кроме того, для двух элементарных конъюнкций $A(\overline{x})$ и $B(\overline{y})$ посредством проверки неполной выводимости $A(\overline{x}) \Rightarrow \exists \overline{y}_{\neq} B(\overline{y})$ можно выделить их максимальную (с точностью до имён переменных) подформулу.

Понятие неполной выводимости позволяет разработать алгоритмы для решения таких задач, как «Распознавание объектов с неполной информацией», «Выделение существенных признаков», «Разработка метрики в пространстве логико-предметных описаний».

Решение задач с неполной информацией об объекте

Задача распознавания объекта в условиях неполной информации заключается в том, что задано не полное описание объекта $S(\omega)$, содержащее все истинные на ω атомарные формулы или их отрицания, а лишь некоторое его подмножество $S'(\omega) \subset S(\omega)$. При этом ставится задача проверки справедливости логического следования вида $S'(\omega) \Rightarrow \exists \overline{x'}_{\neq} A'(\overline{x'})$ для некоторого максимального (q, r)фрагмента $A'(\overline{x'})$ формулы $A(\overline{x})$.

Однако только нахождение такого максимального (q, r)-фрагмента не достаточно для того, чтобы с некоторой степенью уверенности утверждать, что элементы объекта ω удовлетворяют формуле $A(\overline{x})$. Введено понятие дополнения $D(A'(\overline{x}))$ формулы $A'(\overline{x'})$ до формулы $A(\overline{x})$, определяемого как результат замены в конъюнктивных членах, входящих в $A(\overline{x})$, но не вошедших в $A'(\overline{x'})$, всех переменных из $\overline{x'}$ на их значения, определённые при доказательстве следствия $S'(\omega) \Rightarrow \exists \overline{x'}_{\neq} A'(\overline{x'})$. Необходимо также потребовать, чтобы $S'(\omega)$ не противоречило формуле $A(\overline{x})$, т. е. $S'(\omega) \Rightarrow \neg \exists \overline{x}_{\neq} D(A'(\overline{x'}))$. При этом со степенью уверенности q можно утверждать, что объект ω содержит r-ую часть объекта, удовлетворяющего формуле $A(\overline{x})$.

Многоуровневые описания классов

В [1] описано построение многоуровневого описания классов, позволяющее существенно уменьшить число шагов алгоритмов, решающих каждую из трёх сформулированных задач. Такое построение основано на выделении «часто» встречающихся в описаниях классов подформул $P_i^1(y_i^1)$ «небольшой сложности» и заменой их на новые предикаты $p_i^1(x_i^1)$, где x_i^1 — новые переменные первого уровня. При повторении этой процедуры с выделенными подформулами можно получить 2-уровневое, 3-уровневое, ... , L-уровневое описание с равносильностями вида $p_i^l(x_i^l) \Leftrightarrow P_i^l(\overline{y}_i^l)$ и описаниями классов, в которых подформулы $P_i^l(\overline{y}_i^l)$ заменены на новые предикаты $p_i^l(x_i^l)$ с переменными для списков переменных более низкого уровня.

Понятие неполной выводимости формулы позволяет разработать алгоритм выделения подформул с требуемыми свойствами.

1. Для каждой пары элементарных конъюнкций, входящих в описания классов, выделяем их максимальную подформулу.
2. Повторяем процесс выделения общих подформул для каждой пары уже выделенных подформул. Процесс завершится, так как на каждой итерации длины подформул уменьшаются.

3. Выберем среди выделенных подформулминимальные. Это общие подформулы 1го уровня.
4. Формулы более высоких уровней строятся из выделенных ранее подформул.

Метрика в пространстве логико-предметных описаний

Пусть ω_1 и ω_2 — два объекта с описаниями $S(\omega_1)$ и $S(\omega_2)$ соответственно. Проверка неполной выводимости для формулы, полученной из $S(\omega_2)$ заменой различных констант на различные переменные и расстановкой знака $\&$ между атомарными формулами позволяет выделить их максимальный общий (q, r)-фрагмент.

Если a_1 и a_2 — количества атомарных формул в формулах $S(\omega_1)$ и $S(\omega_2)$ соответственно, то $\rho(\omega_1, \omega_2) = (a_1 - q) + (a_2 - q)$ задаёт расстояние между объектами.

Более адекватной является функция $d(\omega_1, \omega_2) = \rho(\omega_1, \omega_2)/(a_1 + a_2)$. Однако для последней не выполняется неравенство треугольника, поэтому её можно назвать степенью похожести объектов.

Работа выполнена при поддержке РФФИ (проект № 14-08-01276-а).

Список литературы

[1] Косовская Т. М. Многоуровневые описания классов для уменьшения числа шагов решения задач распознавания образов, описываемых формулами исчисления предикатов // Вестн. С.-Петербург. ун-та. Сер. 10. — 2008. — Вып. 1. — С. 64–72.

[2] Косовская Т. М. Некоторые задачи искусственного интеллекта, допускающие формализацию на языке исчисления предикатов, и оценки числа шагов их решения // Труды СПИИРАН. — 2010. — Вып. 14. — С. 58–75.

NP-полнота задачи проверки совместности в отрезке целых чисел систем целочисленных линейных уравнений и дизуравнений

Косовский Николай Кириллович[1], **Косовский Николай Николаевич**[2]

[1] Санкт-Петербургский государственный университет, e-mail: kosov@nk1022.spb.edu
[2] Санкт-Петербургский государственный университет, e-mail: kosovnn@pdmi.ras.ru

В сообщении предлагаются серии задач с явно выделенными параметрами и доказываются условия на параметры, при выполнении которых каждая задача серии NP-полна.

Введение

Ценность формулировки и доказательств NP-полноты теоретико-числовых задач связана с тем, что для таких задач в настоящее время (и, по-видимому, в будущем) отсутствуют полиномиальные по времени (числу шагов машины Тьюринга) решающие их алгоритмы (см., например, [1]).

Основные результаты

Пусть целые числа m и m' таковы, что $m < m'$.

Система линейных 3-уравнений на отрезке целых чисел $[m, m']$

УСЛОВИЕ. Задана система, состоящая из линейных уравнений вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) = 0$, в которой каждое уравнение содержит ровно 3 различные переменные и все коэффициеты в уравнениях при переменных принадлежат $\{-1, 1\}$.

ВОПРОС. Совместна ли система в целых числах из отрезка $[m, m']$?

Теорема 1. *Каковы бы ни были целые числа m и m' ($m < m'$) задача* **Система линейных 3-уравнений на отрезке целых чисел** $[m, m']$ *является NP-полной.*

Идея доказательства. То, что задача принадлежит классу NP, очевидно.

Для доказательства того, что задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ из [1] полиномиально сводится к рассматриваемой задаче, прежде всего заметим, что

$$\exists\, y(x + t = y) \Longleftrightarrow m \le x + t \le m'. \tag{1}$$

Уравнение из (1) $x + m' - m - 1 = y$ имеет решение в числах из отрезка $[m, m']$ тогда и только тогда, когда $x \in \{m, m + 1\}$. Уравнения такого вида добавим к системе для каждой переменной. Поскольку в каждом уравнении этой системы только 2 переменные, то добавим тождественно равную нулю фиктивную переменную w в качестве слагаемого в левые части систем вида (1) и два уравнения, обеспечивающие равенство её нулю.

Теорема 1 допускает геометрическую интерпретацию.

Утверждение 1. *Пусть заданы многомерный куб, каждая координата вершин которого принадлежит множеству $\{m, m'\}$, и гиперплоскости, высекающие на произвольных трех осях равные отрезки и параллельные всем остальным осям. Тогда задача проверки того, что внутри многомерного куба имеется целочисленная точка пересечения всех гиперплоскостей, NP-полна.*

Пусть заданы целые числа m и m', такие что $m < m'$

Система линейных 3-дизуравнений на отрезке целых чисел $[m, m']$

УСЛОВИЕ. Задана система, состоящая из линейных дизуравнений вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \neq 0$, в которой каждое дизуравнение содержит ровно 3 различные переменные и все коэффициеты в уравнениях при переменных принадлежат $\{-1, 1\}$.

ВОПРОС. Совместна ли система в целых числах из отрезка $[m, m']$?

Теорема 2. *Каковы бы ни были различные целые числа m и m' ($m < m'$) задача* **Система линейных 3-дизуравнений на отрезке целых чисел** $[m, m']$ *является NP-полной.*

Идея доказательства. То, что задача принадлежит классу **NP**, очевидно.

Сведём задачу 3-ВЫП из [1] к рассматриваемой задаче. Действительно, истинность ровно одного литерала в дизъюнкции $x_1 \vee x_2 \vee x_3$ (где x_1, x_2, x_3 — переменные или их отрицания) может быть записана с помощью дизуравнения

$x_1 + x_2 + x_3 \neq 3m$ при $m > 2$. Константа *ложь* кодирутся числом m, константа *истина* кодирутся числом $m + 1$ При этом вместо $\neg u_i$ подставляем $2m + 1 - u_i$.

Теорема 2 допускает геометрическую интерпретацию. Точнее, она может быть сформулирована в виде утверждения.

Утверждение 2. *Пусть заданы многомерный куб, каждая координата вершин которого принадлежит множеству* $\{m, m'\}$*, и гиперплоскости, высекающие на произвольных трех осях равные отрезки и параллельные всем остальным осям. Тогда задача проверки того, что внутри многомерного куба имеется целочисленная точка, не покрытая этими гиперплоскостями, NP-полна.*

Теорема 2 может быть обобщена с многомерного куба на ограниченную многомерную фигуру, содержащую заданный куб той же размерности.

Система линейных дизуравнений на ограниченной фигуре с параметрами n**,** m_1**, ...,** m_n**,** m**,** m'

УСЛОВИЕ. Задана система, состоящая из линейных дизуравнений вида $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \neq 0$, в которой каждое дизуравнение содержит ровно 3 различные переменные и все коэффициенты при неизвестных равны 1 или -1.

Фигура в n-мерном пространстве, содержащая n-мерный куб, все целочисленные точки которого имеют координаты из отрезка $[m, m']$, и содержащаяся в n-мерном параллелепипеде $[-m_1, m_1] \times \cdots \times [-m_n, m_n]$.

ВОПРОС. Совместна ли система в целочисленных точках фигуры?

Теорема 3. *Каковы бы ни были целые числа* n, m_1, ..., m_n, m, m' $(m_1, ..., m_n > 0)$ *задача* **Система линейных дизуравнений на ограниченной фигуре с параметрами** n**,** m_1**, ...,** m_n**,** m**,** m' *с параметрами* n, m_1, ..., m_n, m, m' *является NP-полной.*

Заключение

Доказанные теоремы показывают, что решение систем линейных как уравнений, так и дизуравнений в целых числах на ограниченном множестве не может быть полиномиальным по числу шагов машины Тьюринга, решающей такие системы, если **P**$\neq$**NP**.

NP-полнота задачи **Система линейных 3-дизуравнений на отрезке целых чисел** $[m, m']$ имеет практическое значение. Теорема 1 показывает, что использование в линейных уравнениях переменных для компьютерного типа *integer* ставит под сомнение все коммерческие якобы эффективные (полиномиальные по времени) алгоритмы для решения систем таких уравнений. Что, впрочем, исключается при использовании средств программирования, имеющих встроенные операции со сколь угодно длинными целыми числами. Такими средствами обладают все диалекты языка рефал (см., например, [2]). Поэтому после применения любой программы по решению системы уравнений в числах типа *integer* необходима подстановка решения в систему с последующей проверкой.

Список литературы

[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

[2] Бабаев И. О., Герасимов М. А., Косовский Н. К., Соловьев И. П. Интеллектуальное программирование. Турбо-Пролог и Рефал-5 на персональных компьютерах. — СПб.: Изд-во СПбГУ, 1992. — 167 с.

Дискретная модель колебания длины низкоприоритетной очереди в тандеме систем обслуживания при циклическом алгоритме с продлением

Кочеганов Виктор Михайлович[1], **Зорин Андрей Владимирович**[2]

[1] Нижегородский госуниверситет им. Н. И. Лобачевского, e-mail: kocheganov@gmail.com
[2] Нижегородский госуниверситет им. Н. И. Лобачевского, e-mail: zoav1602@gmail.com

Пусть в систему с одним обслуживающим устройством поступают потоки Π_1, Π_2, Π_3 и Π_4. Требования по потоку Π_j становятся в соответствующую очередь O_j с неограниченной вместимостью, $j = \overline{1,4}$. Для $j = \overline{1,3}$ дисциплина очереди O_j, имеет тип FIFO. Таким образом, для обслуживания из соответствующей очереди выбирается то требование, которое пришло раньше. Дисциплина очереди O_4 будет описана ниже. Входные потоки Π_1 и Π_3 формируются внешней средой, которая имеет только одно состояние, то есть вероятностная структура потоков не меняется с течением времени. Требования потоков Π_1 и Π_3 формируют независимые между собой неординарные пуассоновские потоки. Интенсивность простейшего потока Π_j будем обозначать λ_j, а распределение числа заявок в группе по потоку Π_j будем описывать производящей функцией $f_j(z) = \sum_{\nu=1}^{\infty} p_\nu^{(j)} z^\nu$, $j \in \{1,3\}$, которая предполагается аналитической при любом z из внутренности круга $|z| < (1+\varepsilon)$, $\varepsilon > 0$. Величина $p_\nu^{(j)}$ определяет вероятность того, что по потоку Π_j число требований в группе равно ν. Обслуженные требования потока Π_1 поступают на повторное обслуживание, формируя при этом поток Π_4. Потоки Π_2 и Π_3 являются конфликтными, что означает запрет на одновременное обслуживание требований этих потоков и, следовательно, исследование системы не может быть сведено к задаче с меньшим числом потоков. В каждый момент времени обслуживающее устройство находится в одном из конечного множества состояний $\Gamma = \{\Gamma^{(k,r)} : k = \overline{0,d}; r = \overline{1,n_k}\}$. Здесь d, n_0, n_1, …, n_d суть заданные натуральные числа. В каждом состоянии $\Gamma^{(k,r)}$ обслуживающее устройство находится в течение неслучайного времени $T^{(k,r)}$.

Предполагается, что длительности обслуживания различных требований могут быть зависимыми и иметь различные законы распределения, поэтому вместо классического способа, состоящего в указании функции распределения длительности обслуживания произвольного требования, будут использованы потоки насыщения. Поток насыщения $\Pi_j^{\text{нас}}$, $j = \overline{1,4}$, определяется как виртуальный выходной поток из очереди O_j при условии максимального использования ресурсов обслуживающего устройства, а для $j = \overline{1,3}$ еще и при неограниченно

больших длинах соответствующих очередей. Поток насыщения $\Pi_j^{\text{нас}}$, $j = \overline{1,3}$, будет содержать неслучайное число $\ell_{k,r,j}$ требований, обслуженных в течение времени $T^{(k,r)}$, если обслуживается очередь O_j, и будет содержать 0 требований в противном случае.

Для задания информации о системе введем следующие величины и элементы, а также укажем множества их возможных значений. Пусть $\mathbb{Z}_+$ — множество целых неотрицательных чисел. В качестве дискретной временнòй шкалы выберем последовательность $\tau_0 = 0$, τ_1, τ_2, ... моментов смены состояний обслуживающего устройства. Обозначим $\Gamma_i \in \Gamma$ состояние обслуживающего устройства в промежутке $(\tau_{i-1}, \tau_i]$, количество $\varkappa_{j,i} \in \mathbb{Z}_+$ требований в очереди O_j в момент времени τ_i, количество $\eta_{j,i} \in \mathbb{Z}_+$ требований, поступивших в очередь O_j по потоку Π_j за промежуток $(\tau_i, \tau_{i+1}]$, количество $\xi_{j,i} \in \mathbb{Z}_+$ требований по потоку насыщения $\Pi_j^{\text{нас}}$ за промежуток $(\tau_i, \tau_{i+1}]$, количество $\overline{\xi}_{j,i} \in \mathbb{Z}_+$ реально обслуженных требований по потоку Π_j в промежутке $(\tau_i, \tau_{i+1}]$, $j = \overline{1,4}$.

Закон изменения состояния обслуживающего устройства будем предполагать заданным соотношением $\Gamma_{i+1} = h(\Gamma_i, \varkappa_{3,i})$, где отображение $h(\cdot,\cdot)$ определено следующим образом. Зададим непересекающиеся множества состояний $C_k = \{\Gamma^{(k,r)} \colon r = 1, 2, \dots n_k\} \in \Gamma$, $k = \overline{1,d}$, называемые далее *циклами*. При $k = 0$ состояния $\Gamma^{(0,r)}$, $r = \overline{0,n_0}$ будем называть состояниями продления. Положим $r \oplus_k 1 = r + 1$ для $r < n_k$ и $r \oplus_k 1 = 1$ при $r = n_k$, $k = 0$, 1, ..., d. В цикле C_k выделим подмножества C_k^{O} выходных состояний, C_k^{I} входных состояний и $C_k^{\text{N}} = C_k \setminus (C_k^{\text{O}} \cup C_k^{\text{I}})$ нейтральных состояний. При этом, будем предполагать, что все циклы имеют ровно одно входное и одно выходное состояние. Наконец, все состояния продления образуют один цикл. Пусть задано положительное целое число L, множество $N_0 = \{1, 2, \dots, n_0\}$ и заданы отображения $h_1(\cdot) \colon \bigcup_{k=1}^d C_k^{\text{O}} \to N_0$, $h_2(\cdot) \colon N_0 \to N_0$ и $h_3(\cdot) \colon N_0 \to \bigcup_{k=1}^d C_k^{\text{I}}$. Тогда $h(\Gamma^{(k,r)}, y)$ принимает значение $\Gamma^{(k,r\oplus_k 1)}$ при $\Gamma^{(k,r)} \in C_k \setminus C_k^{\text{O}}$, значение $\Gamma^{(k,r\oplus_k 1)}$ при $\Gamma^{(k,r)} \in C_k^{\text{O}}$ и $y > L$, значение $\Gamma^{(0,h_1(\Gamma^{(k,r)})}$ при $\Gamma^{(k,r)} \in C_k^{\text{O}}$ и $y \leqslant L$, значение $\Gamma^{(0,h_2(r))}$ при $k = 0$ и $y \leqslant L$, наконец, значение $h_3(r)$ при $k = 0$ и $y > L$.

Для определения длительности T_{i+1} состояния обслуживающего устройства в течение времени $(\tau_i, \tau_{i+1}]$ удобно ввести функцию $h_T(\cdot,\cdot)$: $h_T(\Gamma_i, \varkappa_{3,i}) = T^{(k,r)}$, где $\Gamma^{(k,r)} = h(\Gamma_i, \varkappa_{3,i})$. Далее, функциональная зависимость

$$\overline{\xi}_{j,i} = \min\{\varkappa_{j,i} + \eta_{j,i}, \xi_{j,i}\}, \quad j = \overline{1,3}, \tag{1}$$

между величиной $\overline{\xi}_{j,i}$ и величинами $\varkappa_{j,i}$, $\eta_{j,i}$, $\xi_{j,i}$ реализует стратегию механизма обслуживания требований. Из равенства $\varkappa_{j,i+1} = \varkappa_{j,i} + \eta_{j,i} - \overline{\xi}_{j,i}$ и соотношения (1) следует соотношение $\varkappa_{j,i+1} = \max\{0, \varkappa_{j,i} + \eta_{j,i} - \xi_{j,i}\}$ для $j = \overline{1,3}$. Из формулировки поставленной задачи также следуют соотношения для потока Π_4: $\eta_{4,i} = \min\{\xi_{1,i}, \varkappa_{1,i} + \eta_{1,i}\}$, $\varkappa_{4,i+1} = \varkappa_{4,i} + \eta_{4,i} - \eta_{2,i}$ и $\xi_{4,i} = \varkappa_{4,i}$.

Функцию $\psi(\cdot,\cdot,\cdot)$ зададим формулой $\psi(k; y, u) = C_y^k u^k (1-u)^{y-k}$, $k, y \in Z_+$, $u \in [0,1]$. Для $j \in \{1,3\}$ и $t \in \mathbb{R}$ функцию $\varphi_j(\cdot,\cdot)$ введем из разложения $\sum_{\nu=0}^{\infty} z^\nu \varphi_j(\nu, t) = \exp\{\lambda_j t (f_j(z) - 1)\}$. Пусть $a = (a_1, a_2, a_3, a_4) \in \mathbb{Z}_+^4$

и $x = (x_1, x_2, x_3, x_4) \in \mathbb{Z}_+^4$ и $\Gamma^{(\tilde{k},\tilde{r})} = h(\Gamma^{(k,r)}, x_3)$. Индикатор равенства двух величин x и y будем выражать символом Кронекера $\delta_{x,y}$. Тогда из постановки задачи на содержательном уровне следует, что при фиксированном значении пары $(\Gamma_i; \varkappa_i)$ вероятность $\varphi(a, k, r, x)$ одновременного выполнения равенств $\eta_{1,i} = a_1$, $\eta_{2,i} = a_2$, $\eta_{3,i} = a_3$, $\eta_{4,i} = a_4$ есть $\varphi_1(a_1, h_T(\Gamma^{(k,r)}, x_3)) \times \psi(a_2, x_4, p_{\tilde{k},\tilde{r}}) \times$ $\times\, \varphi_3(a_3, h_T(\Gamma^{(k,r)}, x_3)) \times \delta_{a_4, \min\{\ell(\tilde{k},\tilde{r},1), x_1+a_1\}}$. Пусть $b = (b_1, b_2, b_3, b_4) \in \mathbb{Z}_+^4$. Из содержательной постановки задачи также следует, что вероятность $\zeta(b, k, r, x)$ одновременного выполнения равенств $\xi_{1,i} = b_1$, $\xi_{2,i} = b_2$, $\xi_{3,i} = b_3$, $\xi_{4,i} = b_4$ при фиксированном значении $(\Gamma_i; \varkappa_i)$ есть $\delta_{b_1,\ell(\tilde{k},\tilde{r},1)} \times \delta_{b_2,\ell(\tilde{k},\tilde{r},2)} \times \delta_{b_3,\ell(\tilde{k},\tilde{r},3)} \times \delta_{b_4,x_4}$.

Указанные функциональные соотношения и свойства условных распределений позволяют построить веростноятное пространство $(\Omega, \mathcal{F}, \mathbf{P}(\cdot))$ и конструктивно задать на нем марковскую случайную последовательность $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{2,i}, \varkappa_{3,i}, \varkappa_{4,i}); i \geqslant 0\}$. Основной результат настоящей работы содержится в следующих теоремах

Теорема 1. *Пусть* $\Gamma_0 = \Gamma^{(k,r)} \in \Gamma$ *и* $\varkappa_{3,0} = x_{3,0} \in \mathbb{Z}_+$ *фиксированы. Тогда последовательность* $\{(\Gamma_i, \varkappa_{3,i}); i \geqslant 0\}$ *является счетной цепью Маркова.*

Теорема 2. *Пусть* x_3, $\tilde{x}_3 \in \mathbb{Z}_+$ *и* $\Gamma^{(k,r)}$, $\Gamma^{(\tilde{k},\tilde{r})} = h(\Gamma^{(k,r)}, x_3)$. *Тогда условная вероятность* $\mathbf{P}(\{\Gamma_{i+1} = \Gamma^{(\tilde{k},\tilde{r})}, \varkappa_{3,i+1} = \tilde{x}_3\} | \{\Gamma_i = \Gamma^{(k,r)}, \varkappa_{3,i} = x_3\})$ *равна* $\delta_{\tilde{x}_3,0} \sum_{a=0}^{\ell(\tilde{k},\tilde{r},3)-x} \varphi_3(a, h_T(\Gamma^{(k,r)}, x_3)) + (1-\delta_{\tilde{x}_3,0}) \varphi_3(\tilde{x}_3 + \ell(\tilde{k}, \tilde{r}, 3) - x_3, h_T(\Gamma^{(k,r)}, x_3))$.

Теорема 3. *Пусть для* $r = \overline{1, n_0}$ *определено множество* $S_{0,r}^3 = \{(\Gamma^{(0,r)}, x_3) \colon x_3 \in Z_+, L \geqslant x_3 > L - \max\{\sum_{t=0}^{n_k} \ell_{k,t,3} \colon k = \overline{1,d}\}\}$ *и для* $k = \overline{1,d}$, $r = \overline{1, n_k}$ *обозначено* $S_{k,r}^3 = \{(\Gamma^{(k,r)}, x_3) \colon x_3 \in Z_+, x_3 > L - \sum_{t=0}^{r-1} \ell_{k,t,3}\}$. *Тогда множество существенных состояний марковской цепи* $\{(\Gamma_i, \varkappa_{3,i}); i \geqslant 0\}$ *есть* $\bigcup_{k=0}^{d} \big(\bigcup_{r=1}^{n_k} S_{k,r}^3\big)$.

Работа выполнена в рамках фундаментальной НИР «Математическое моделирование и анализ стохастических эволюционных систем и процессов принятия решений» (номер госрегистрации: 01201456585) и государственной программы «Поддержка ведущих универсистетов РФ в целях повышения их конкурентноспособности среди ведущих мировых научно-образовательных центров».

О средней сложности конечных абелевых групп

Кочергин Вадим Васильевич

Московский государственный университет имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

Пусть G — конечная абелева группа (групповую операцию будем называть умножением). Подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы будем называть *базисом* в группе G, если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B:

$$G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q},$$

где u_i — порядок элемента a_i, $i = 1, \ldots, q$.

Для каждого элемента g группы G определим его *сложность реализации над базисом* B, обозначаемую через $L(g;B)$ как минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B, при этом все уже вычисленные элементы могут быть использованы многократно.

Сложность $L(G,B)$ *конечной абелевой группы* G *над базисом* B определим так:

$$L(G,B)=\max_{g\in G}L(g;B).$$

Далее положим

$$LM(G)=\max_{B\colon B-\text{базис } G}L(G,B),\quad Lm(G)=\min_{B\colon B-\text{базис } G}L(G,B).$$

Наконец, введем функции $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, характеризующие средние значения соответствующих мер сложности абелевых групп порядка n, определив их равенствами:

$$M_{\text{ср}}(n)=\frac{\sum LM(G)}{A(n)},\quad m_{\text{ср}}(n)=\frac{\sum Lm(G)}{A(n)},$$

где суммы берутся по всем различным (с точностью до изоморфизма) абелевым группам G порядка n, а $A(n)$ — количество попарно неизоморфных абелевых групп порядка n.

Исследуется задача о поведении функций $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$ при растущих значениях n.

Функцию $h(n)$ натурального аргумента будем называть *допустимой*, если выполняется следующее свойство — для любых двух последовательностей натуральных чисел $\{d_n^{(1)}\}$ и $\{d_n^{(2)}\}$, удовлетворяющих условиям:

1) $d_n^{(1)}\to\infty$;

2) $d_n^{(1)}/2\le d_n^{(1)}\le 2d_n^{(2)}$ для всех достаточно больших значениях n,

при $n\to\infty$ справедливо асимптотическое равенство $h\left(d_n^{(1)}\right)\sim h\left(d_n^{(2)}\right)$.

Заметим, что замена коэффициентов $1/2$ и 2, фигурирующих во втором условии определения, на произвольные константы $1/c$ и c, где $c>1$, приводит к эквивалентному определению допустимой функции.

Теорема. *При* $n\to\infty$ *выполняются соотношения*

$$\frac{\log_2 n}{\log_2\log_2 n}\lesssim m_{cp}(n)\le M_{cp}(n)\lesssim\log_2 n,$$

причем для любых допустимых функций $h_1(n)$ *и* $h_2(n)$*, удовлетворяющих при* $n\to\infty$ *условиям*

$$\frac{\log_2 n}{\log_2\log_2 n}\lesssim h_1(n)\lesssim h_2(n)\lesssim\log_2 n,$$

найдется последовательность $\{n_s\}$*, удовлетворяющая условию* $n_s \to \infty$ *при* $s \to \infty$*, для которой справедливы соотношения*

$$m_{cp}(n_s) \sim h_1(n_s); \quad M_{cp}(n_s) \sim h_2(n_s).$$

Схема доказательства. Без ограничения общности можно считать, что функции $h_1(n)$ и $h_2(n)$ при всех достаточно больших n удовлетворяют неравенствам

$$\frac{\log_2 n}{\log_2 \log_2 n} \le h_1(n) \le h_2(n) \le \log_2 n + \frac{\log_2 n}{\log_2 \log_2 n}.$$

Положим

$$H_1 = H_1(s) = \left\lceil \max \left\{ h_1(2^s) - \frac{s}{\log_2 s},\ \frac{s}{(\log_2 s)^2} \right\} \right\rceil;$$

$$H_2 = H_2(s) = \left\lceil \max \left\{ h_2(2^s) - \frac{s}{\log_2 s},\ \frac{s}{(\log_2 s)^2} \right\} \right\rceil.$$

Пусть p_1 — максимальное простое число, меньшее 2^{H_1}, p_2 — предшествующее числу p_1 простое число (т. е. p_2 — максимальное простое число, меньшее p_1), p_3 — предшествующее числу p_2 простое число и т. д. Определим параметр $d = d(s)$ из условия

$$p_1 p_2 \dots p_{d-1} < 2^{H_2} \le p_1 p_2 \dots p_{d-1} p_d.$$

Обозначим через p'_d наименьшее из простых чисел x, отличных от двойки и удовлетворяющих условию

$$p_1 p_2 \dots p_{d-1} x \ge 2^{H_2}.$$

Тем самым, справедливы неравенства

$$2^{H_2} \le p_1 p_2 \dots p_{d-1} p'_d < 3 \cdot 2^{H_2}.$$

Теперь положим

$$t = t(s) = s - H_2,$$
$$n_s = 2^t p_1 p_2 \dots p_{d-1} p'_d.$$

Тогда выполняются неравенства

$$2^s \le n_s < 3 \cdot 2^s.$$

Корректность введения параметров и справедливость оценок из теоремы устанавливаются с использованием результатов из [1, 2] и некоторых фактов из теории чисел (о распределении простых чисел) и комбинаторики (теории разбиений).

Работа выполнена при финансовой поддержке РФФИ (проект № 14–01–00598).

Список литературы

[1] Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики, вып. 4. — М.: Наука, 1992. — С. 178–217.

[2] Кочергин В. В. Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискретный анализ и исследование операций. — 2014. — Т. 21, № 6. — С. 51–72.

К вопросу о сложности сборки двоичных слов схемами конкатенации

Кочергин Вадим Васильевич[1], **Кочергин Дмитрий Вадимович**[2]

[1] Московский государственный университет имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

[2] Московский государственный университет имени М. В. Ломоносова, e-mail: kochdv@yandex.ru

Асимптотическая постановка задачи синтеза управляющих систем [1] связана с изучением поведения той или иной функции Шеннона при растущем значении ее натурального аргумента. О. Б. Лупановым найдена асимптотика роста функции Шеннона для сложности булевых функций во всех основных модельных классах управляющих систем, включая классы формул и схем из функциональных элементов над произвольным конечным полным базисом (см., например, [1]). С. А. Ложкиным [2] многие из этих результатов усилены — в частности, установлены асимптотические соотношения, названные автором асимптотическими оценками высокой степени точности (которые условно можно трактовать как оценки через функции заданного вида, дающие не только асимптотику функции Шеннона, но и асимптотику остаточного члена) для класса формул, а также для схем из функциональных элементов в базисах специального вида. В случае класса схем из функциональных элементов над полным конечным базисом B установлены следующие нижняя и верхняя оценки функции Шеннона $L_B(n)$:

$$\rho_B \frac{2^n}{n}\left(1+(1+o(1))\frac{\log_2 n}{n}\right) \le L_B(n) \le \\ \le \rho_B \frac{2^n}{n}\left(1+(1+\varkappa_B+o(1))\frac{\log_2 n}{n}\right), \qquad (1)$$

где ρ_B — приведенный вес базиса [1], а $\varkappa_B = 1$ в случае, когда базис B симметричный [2] и $\varkappa_B = 0$ в остальных случаях.

Приведенные оценки не дают ответа на вопрос, может ли коэффициент при $(\log n)/n$ в нижней оценке быть асимптотически равен 2 (или хотя бы асимптотически превышать $1+\varepsilon$ для некоторого $\varepsilon > 0$). В настоящей работе для похожей задачи — задачи сборки слов схемами конкатенации — такая возможность выявлена.

Определим меру сложности порождения (сборки) слов с помощью операции конкатенации (приписывания к одному слову другого), которая с небольшими

модификациями известна и как длина цепочек слов, и как мультипликативная сложность слов, и как аддитивная сложность слов.

Последовательность S слов (наборов) из конечного алфавита A

$$\tilde{\tau}_1, \quad \tilde{\tau}_2, \quad \ldots, \quad \tilde{\tau}_r = \tilde{\alpha}$$

назовем *схемой конкатенации* [3, 4], реализующей (вычисляющей) слово (набор) $\tilde{\alpha}$, если для каждого i, $i = 1, 2, \ldots, r$, слово $\tilde{\tau}_i$ можно представить в виде $\tilde{\tau}_i = \tilde{\beta}_{i_1}\tilde{\beta}_{i_2}$, где для $j = 1, 2$ либо β_{i_j} — буква из алфавита A, либо $\beta_{i_j} = \tau_m$ для некоторого m, удовлетворяющего условию $m \leq i - 1$. *Сложностью* $L^c(S)$ данной схемы S, реализующей слово $\tilde{\alpha}$, назовем число r. Положим $L^c(\tilde{\alpha}) = \min L^c(S)$, где минимум берется по всем схемам конкатенации, реализующим слово $\tilde{\alpha}$ в алфавите A. Отметим, что схему конкатенации в алфавите A можно рассматривать как схему из функциональных элементов, имеющую $|A|$ входов, на которые подаются, соответственно, буквы из алфавита A, а каждый элемент схемы реализует конкатенацию наборов, подаваемых на его входы.

Обозначим через $W_A(n)$ множество всех слов в алфавите A длины n. Положим

$$L^c_A(n) = \max_{\tilde{\alpha} \in W_A(n)} L^c(\tilde{\alpha}).$$

Задача нахождения асимптотики роста функции Шеннона $L^c_A(n)$, характеризующей сложность сборки самого сложного слова длины n в алфавите A, является по существу «фольклорной», а ее решение впервые опубликовано, по-видимому, в [5]. При аккуратном применении известных методов можно получить следующие нижнюю и верхнюю оценки, которые запишем в удобном для сравнения виде:

$$d_A \frac{\log_2 |W_A(n)|}{\log_2 \log_2 |W_A(n)|} \left(1 + (1 + o(1)) \frac{\log_2 \log_2 \log_2 |W_A(n)|}{\log_2 \log_2 |W_A(n)|}\right) \leq L^c_A(n) \leq$$
$$\leq d_A \frac{\log_2 |W_A(n)|}{\log_2 \log_2 |W_A(n)|} \left(1 + (2 + o(1)) \frac{\log_2 \log_2 \log_2 |W_A(n)|}{\log_2 \log_2 |W_A(n)|}\right), \quad (2)$$

где $d_A = \log_2 |A|$.

Если в формулах из (1) заменить n на $\log_2 \log_2 |P(n)|$ (здесь $P(n)$ — множество всех булевых функций от n фиксированных переменных), то соотношения (1) и (2) примут похожий вид, причем в обоих случаях нижняя и верхняя оценки отличаются лишь коэффициентами при втором слагаемом в скобках — асимптотически равными 1 и 2 соответственно (для соотношений (1) рассматривается вариант симметричного базиса). В настоящей работе установлено, что для функции Шеннона сложности сборки слов схемами конкатенации этот «зазор» может быть устранен.

Теорема. *При $n \to \infty$ для функции Шеннона сложности сборки слов схемами конкатенации в алфавите $A_2 = \{0, 1\}$ справедливо равенство*

$$L^c_{A_2}(n) = \frac{n}{\log_2 n} \left(1 + (2 + o(1)) \frac{\log_2 \log_2 n}{\log_2 n}\right).$$

Получение усиленной нижней оценки основано на двух соображениях. Во-первых, на применении мощностного метода для оценки сложности класса всех слов де Брёйна (см., например, [6]) заданной длины — с одной стороны, таких слов достаточно много, а с другой, бóльшая часть любой минимальной схемы, реализующей слово де Брёйна, имеет вид дерева, структуру которго можно без ограничения общности жестко зафиксировать (использование такого подхода позволяет увеличить соответствующий коэффициент в нижней оценке с единицы до полутора). Во-вторых, на существовании в любой минимальной схеме, реализующей слово де Брёйна, достаточного количества «связей» между частью схемы, имеющей вид дерева, и остальной частью.

Замечание. *Утверждение теоремы может быть обобщено на случай произвольного конечного алфавита.*

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 14–01–00598).

Список литературы

[1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.

[2] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. — Вып. 6. — М.: Наука, 1996. — С. 189–214.

[3] Мерекин Ю. В. Нижняя оценка сложности для схем конкатенации слов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 1. — С. 52–56.

[4] Кочергин В. В. О мультипликативной сложности двоичных слов с заданным числом единиц // Математические вопросы кибернетики. — Вып. 8. — М.: Наука, 1999. — С. 63–76.

[5] Strassen V. Berechnungen in partiellen Algebren endlichen Typs // Computing. — 1973. — V. 11. — P. 181–196.

[6] Холл М. *Комбинаторика*. — М.: Мир, 1970. — 424 с.

Об одном алгоритме вычисления матрицы смежности графа Кэли

Кузнецов Александр Алексеевич, Кузнецова Александра Сергеевна

Сибирский государственный аэрокосмический университет, e-mail: alex_kuznetsov80@mail.ru, alexakuznetsova85@gmail.com

Определение графа Кэли было дано известным английским математиком Артуром Кэли в 1878 году для представления алгебраической группы, заданной фиксированным множеством порождающих элементов.

В последние десятилетия теория графов Кэли развивается как отдельная большая ветвь теории графов. Графы Кэли находят применение как в математике, так и за ее пределами. Заметим, что известная задача по определению так называемого «числа Бога» кубика Рубика $3 \times 3 \times 3$, т. е. минимального количества поворотов граней кубика за которое его можно «собрать» из любого начального положения, сводится к исследованию соответствующего графа Кэли.

Неожиданное применение графы Кэли нашли в информационных технологиях после пионерской работы 1986 года С. Эйкерса и Б. Кришнамурти [1], которые впервые предложили применять указанные графы для представления компьютерных сетей, в том числе для моделирования топологий многопроцессорных вычислительных систем (МВС) — суперкомпьютеров. С тех пор данное направление активно развивается. Это связано с тем, что графы Кэли имеют много привлекательных свойств, из которых выделим их регулярность, вершинно-транзитивность, малые диаметр и степень при достаточно большом количестве вершин в графе. Кстати, такие базовые топологии сети, как «кольцо» и «гиперкуб», являются графами Кэли.

Вычисление матрицы смежности графа Кэли большой конечной группы является хотя и разрешимой, но достаточно сложной проблемой. Это связано с тем, что в общем случае задача по определению минимального слова в группе, как показали С. Ивен и О. Голдрейх в 1981 году [2], является NP-трудной. Так, при вычислениии в 2010 году упомянутого выше «числа Бога», которое равно диаметру соответсвующего графа Кэли, Т. Рокики, Г. Коцемба, М. Дэвидсон и Д. Детридж доказали, что любая конфигурация кубика Рубика может быть решена не более чем в 20 ходов. Для установления данного факта потребовалось около 35 «процессоро-лет» распределенных вычислений. Поэтому для эффективного решения задач на графах Кэли, имеющих большое количество вершин, необходимо применять МВС. В связи с этим представляется актуальной проблема разработки параллельных алгоритмов для исследования графов Кэли частных классов групп.

Пусть X — порождающее множество группы G, т. е. $G = \langle X \rangle$. Графом Кэли $\Gamma = Cay(G, X) = (V, E)$ называют ориентированный граф, в котором множество вершин $V(\Gamma)$ соответствуют элементам группы G, а множество ребер $E(\Gamma)$ состоит из всех упорядоченных пар (g, xg), где $g \in G$ и $x \in X$.

В дальнейшем будем считать порождающее множество X симметричным и свободным от единичного элемента группы, т. е. $x \in X \Rightarrow x^{-1} \in X$ и $e \notin X$. Поскольку X является свободным от единичного элемента, то граф Γ не содержит петель. Симметричность порождающего множества означает, что граф будет неориентированным и без кратных ребер, т. е. если в графе имеется ребро из g в xg, то оно совпадает с ребром из xg в $x^{-1}(xg) = g$.

Ниже будет представлен базовый алгоритм для вычисления матрицы смежности $M = [m(i, j)]$ графа Кэли произвольной конечной группы, где $m(i, j) = 1$, если вершина i соединена ребром с вершиной j, и $m(i, j) = 0$ в противном случае.

Алгоритм A-I

Вход: $X = \{x_1 \prec \ldots \prec x_n\}$ — упорядоченное порождающее множество G.
Выход: матрица смежности M графа Кэли группы G.
1. $K = \{e\}$, $T = K$, $M_{|G|\times|G|}$ — нулевая матрица.
2. $c = |K| - |T|$, $P = \varnothing$, $i = 1$.
3. $j = 1$.
4. $g = x_i \cdot t_j$.
5. Если $\begin{cases} g \notin K, \text{ то } m(c+j, |K|+1) = 1,\ K = K \cup g,\ P = P \cup g; \\ g = k_r \in K, \text{ то } m(c+j, r) = 1. \end{cases}$
6. Если $\begin{cases} j < |T|, \text{ то } j = j+1, \text{ переход в пункт 4}; \\ j = |T|, \text{ то переход в пункт 7}. \end{cases}$
7. Если $\begin{cases} i < |X|, \text{ то } i = i+1, \text{ переход в пункт 3}; \\ i = |X|, \text{ то переход в пункт 8}. \end{cases}$
8. Если $\begin{cases} P \neq \varnothing, \text{ то } T = P, \text{ переход в пункт 2}; \\ P = \varnothing, \text{ то переход в пункт 9}. \end{cases}$
9. Выход.

Проиллюстрируем работу алгоритма на примере вычисления матрицы смежности графа Кэли симметрической группы $S_3\langle a, b\rangle$, заданной транспозициями $a = (1\ 2)$ и $b = (2\ 3)$, причем $a \prec b$.

В результате получим:
$K = \{e,\ a = (1\ 2),\ b = (2\ 3),\ ab = (1\ 3\ 2),\ ba = (1\ 2\ 3),\ aba = (1\ 3)\}$,

$$M = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

При вычислении матриц смежности графов Кэли различных частных классов групп алгоритм A-I можно эффективно распараллелить для его реализации на МВС. Например, при вычислении матриц смежности симметрических групп $S_n = \langle X_n\rangle$ множество K разбивается на $z = n(n-1)(n-2)\ldots(n-y+1)$ непересекающихся классов элементов (подстановок):

$$K = \bigcup_{i=1}^{z} K_i\,, \quad K_i \cap K_j = \varnothing \text{ при } i \neq j.$$

Каждый класс K_i будет однозначно определяться фиксированным набором значений $(i_1, i_2, \ldots, i_k)$, т. е.

$$\forall g \in K_i \Rightarrow g = \begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{pmatrix}.$$

Аналогичным образом массив T также делится на z непересекающихся классов элементов и дальнейшая обработка данных для каждой пары множеств T_i и K_i (пункты 3–7 алгоритма A-I) производится независимо. Нетрудно заметить, что рассмотренное разделение массивов не влияет на корректность работы алгоритма. Параметр y определяется экспериментально и зависит от n, а также характеристик МВС. Указанная процедура, как показали реальные расчеты, дает ощутимый прирост скорости вычислений.

Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14), а также гранта Президента РФ (проект МД-3952.2015.9).

СПИСОК ЛИТЕРАТУРЫ

[1] Akers S., Krishnamurthy B. A group theoretic model for symmetric interconnection networks // Proceedings of the International Conference on Parallel Processing. — 1986. — P. 216–223.

[2] Even S., Goldreich O. The Minimum Length Generator Sequence is NP–Hard // Journal of Algorithms. — 1981. — V. 2. — P. 311–313.

О применении частотного анализа для решения некоторых групповых уравнений индукции действия группы Джевонса и её подгрупп на множестве булевых функций

Кукарцев Анатолий Михайлович[1], **Кузнецов Александр Алексеевич**[2]

[1] Сибирский федеральный университет, e-mail: amkukarcev@yandex.ru

[2] Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнёва, e-mail: alex_kuznetsov80@mail.ru

Постановка задачи

Пусть $E = \{0, 1\}$ — булево множество и n — целое неотрицательное число. Булевой функцией, далее БФ, местности n будем называть $f\colon E^n \to E$. Всё множество таких отображений обозначим как $B(n)$. Группу инвертирования переменных БФ (группу сдвигов) и перестановок переменных БФ (симметрическую группу) обозначим как E_n и S_n, соответственно [1]. Группу Джевонса (полупрямое произведение $E_n \leftthreetimes S_n$) обозначим как D_n [1]. Пусть $f, g \in B(n)$ и $(z\pi) \in D_n, z \in E_n, \pi \in S_n$ и рассмотрим уравнение $f^{(z\pi)} = g$ относительно $(z\pi)$. Решение такого уравнения является классической алгебраической задачей. Для множества БФ и группы Джевонса, в силу конечности обеих, данная проблема тривиально разрешима. Но это требует перебора всех значений группы D_n при её порядке $|D_n| = 2^n n!$ и экспоненциального времени получения решения.

Поиск решения связан с понятием инварианта группы, действующей на множестве [1]. Инвариант определяет, пусто или не пусто множество решений, и косвенно помогает в отыскании решений. С. В. Голомб показал, что для D_n существует полный инвариант [2]. Но для расчёта такого инварианта нужно

экспоненциальное время. Э. А. Якубайтис [2] также предложил инвариант группы Джевонса, но он не полон.

Целью настоящего изложения является создание математического аппарата на основе которого строится алгоритм, решающий указанное уравнение за время много меньшее, чем экспоненциальное.

Математическое обоснование алгоритма

Алгоритм базируется на двух доказанных суждениях. Во-первых, любой элемент $(z\pi) \in D_n$ может быть единственным образом (канонически) представлен в виде упорядоченного произведения элементов D_n порядка 2:

$$(z\pi) = (z_{n-1}, (n-1, j_{n-1})) \cdots (z_i, (i, j_i)) \cdots (z_0, (0, j_0)), \tag{1}$$

где $i \leqslant j_i$, z_i есть порождающие группы E_n, и номера точек в транспозициях (i, j_i) строго убывают. В силу ограничений на объём изложения алгоритм формирования транспозиций не приводится. Если элемент в виде (1) действует на БФ $f(x_{n-1}, \ldots, x_0)$, то каждый множитель будет действовать последовательно, причём в обратном к (1) порядке:

$$f^{(z\pi)} = \left(\left(\left(\left(f^{(z_0,(0,j_0))} \right)^{\cdots} \right)^{(z_i,(i,j_i))} \right)^{\cdots} \right)^{(z_{n-1},(n-1,j_{n-1}))}. \tag{2}$$

Во-вторых, каждой БФ f местности n можно биективно поставить информационное сообщение $y_f \in E^{2^n}$ из нулей и единиц длины 2^n. Биты в таком сообщении есть значения БФ в точках соответствующих номерам битов (столбец значений в таблице истинности). Далее требуется ряд определений.

Определение 1. Алфавит A_i — множество E^{2^i}.

Определение 2. Символ алфавита — элемент алфавита A_i, встречаемый в последовательности y_f. y_f может быть построена на любом из алфавитов A_i, где i пробегает все значения $[0; n]$.

Определение 3. Частота символа — количество случаев встречи заданного символа из алфавита в последовательности y_f.

Определение 4. Частотное распределение y_f (спектр) над алфавитом A_i — отношение $Q_i(y_f) \subset A_i \times [0; k]$ или множество пар символ-частота. Частотное распределение инвариантно, если оно не меняется при изменении информационного сообщения.

Определение 5. Спектральное распределение y_f над алфавитом A_i — отношение $R_i(y_f) \subset [0; k] \times [0; k]$ — производное множество из $Q_i(y_f)$, элементы которого показывают как часто повторяются частоты в y_f. Спектральное распределение инвариантно, если оно не меняется при изменении информационного сообщения.

Определим $c_{n-1}, \ldots, c_0 \in E^n$, причём c_i имеет на позиции i значение 1, а на остальных — 0, т. е. все c_i есть порождающие множества группы E_n.

Теорема 1 (об инвариантности частотных спектров при действии E_n). *Действие элемента $c_i \in E_n$ на БФ $f^{c_i} = g$ инвариантно для частотных распре-*

делений y_f относительно y_g для алфавитов $A_{i'}\colon i' \leqslant i$ и инвариантно для спектральных распределений y_f относительно y_g для всех алфавитов.

Следствие 1. *Энтропия информации (по Шеннону) является функцией спектрального распределения, поэтому энтропия инвариантна для y_f и y_g при действии группы E_n во всех алфавитах сразу.*

Теорема 2 (об инвариантности частотных спектров при действии S_n). *Действие элемента $(i,j)\colon i < j$ группы S_n на БФ $f^{(i,j)} = g$ инвариантно для частотных распределений y_f относительно y_g для алфавитов $A_{i'}\colon i' \leqslant i$ и инвариантно для спектральных распределений y_f относительно y_g для алфавитов $A_{j'}\colon j' > j$ и A'_i.*

Следствие 2. *Энтропия информации (по Шеннону) является функцией спектрального распределения, поэтому энтропия инварианта для y_f и y_g при действии группы S_n в алфавитах индексов до i включительно и больше j.*

Описание алгоритма. Теоремы 1 и 2 определяют необходимые условия присутствия порождающих элементов группы Джевонса в решении уравнения в виде (1). Алгоритм сводится к анализу частотных спектров после действия порождающих группы Джевонса в (2) на каждый аргумент БФ, последовательно от x_0 к x_{n-1}. Теоремы позволяют отбросить порождающие и гипотезы их содержащие не являющиеся решениями. Последний шаг алгоритма работает с БФ как с символом алфавита A_n. Откуда заключается сходимость алгоритма.

Выводы

Для БФ, имеющих нечётное количество единиц в столбце значений (половина всех БФ), теоремы определяют достаточные условия присутствия порождающих группы Джевонса в (1). Для них максимальная сложность алгоритма определяется количеством порождающих или $O(n^2)$. Вторая половина БФ на некоторых шагах алгоритма может давать паразитный рост сложности. Количество таких функций максимально для алфавита A_1 и может быть оценено по нормальному множителю группы Джевонса как (3):

$$\epsilon(n) = \sum_{x=0}^{2^{n-2}} 2^{(2^{n-1}-2x)} \frac{2^{n-1}!}{(2^{n-1}-2x)!(x!)^2}. \tag{3}$$

Из (3) нетрудно увидеть, что количество таких функций пренебрежимо мало в общей совокупности БФ. Ведутся дополнительные исследования по предварительному анализу таких БФ с целью снижения сложности до $O(n^2)$.

Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14), а также гранта Президента РФ (проект МД-3952.2015.9).

Список литературы

[1] Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.

[2] Глухов М. М., Ремизов А. В., Шапошников В. А. Обзор по теории k-значных функций. Часть 1. Справочное пособие. — М., 1988. — 153 с.

О динамической активности схем из функциональных элементов в стандартном базисе, реализующих мультиплексорную функцию

Кулешов Олег Владимирович, Шуплецов Михаил Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: KuleshovOlega@yandex.ru, mikle.shupletsov@gmail.com

Введение

Разработка математических моделей и получение теоретических оценок энергопотребления интегральных схем, реализующие заданные функции алгебры логики (ФАЛ), является одной из важных задач теории дискретных управляющих систем. При анализе энергопотребления, обычно, выделяют статическое энергопотребление, которое связано с рассеянием тепла и поддержанием заданного потенциала в узлах схемы, подключенных к источнику питания, и динамическое энергопотребление, возникающее при изменении потенциалов в узлах схемы. При этом в современных интегральных схемах, построенных по КМОП-технологиям, динамическое энергопотребление играет ключевую роль.

Результаты изложенные в данной работе связаны с понятием динамической активности, формализующим и оценивающим динамическое энергоптребление современных интегральных схем. Данная проблема не является новой, но стала более актуальной в связи с тем, что портативные вычислительные устройства становятся широко используемыми и доступными, а одной из главных их характеристик является время автономной работы.

Основные результаты, связанные с теоретической оценкой статического энергопотребления в модели схем из функциональных элементов (СФЭ) были получены в работах М. Н. Вайнцвайга [1] и работах О. М. Касим-Заде [2, 3]. В свою очередь, исследование динамического энергопотребления началось с разработки подходов и построения алгоритмов оценки энергопотребления заданной интегральной схемы. Один из первых алгоритмов оценки динамического энергопотребления интегральных схем описан в работе [4], а обзор основных результатов в этом направлении представлен в работе [5]. Первые теоретические результаты в области исследования динамической активности были получены в работе [6].

Данная статья посвящена получению оценок динамической активности мультиплексорной функции, которая используется во многих ключевых компонентах современных интегральных схем и, в частности, в блоках выбора из памяти.

Основные определения

Пусть Σ — СФЭ в базисе $\mathfrak{B}$, имеющая n входов $x_1, \ldots, x_n$ и k функциональных элементов (ФЭ). Занумеруем произвольным образом все ФЭ СФЭ Σ и

через φ_i, $i = 1, \ldots, k$, обозначим ФАЛ от булевых переменных (БП) $x_1, \ldots, x_n$, которая реализуется на выходе i-го ФЭ СФЭ Σ. Пусть B^n — множество всех булевых наборов длины n и наборы $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\widetilde{\beta} = (\beta_1, \ldots, \beta_n)$ из B^n — наборы значений БП $x_1, \ldots, x_n$, приписанных входам СФЭ Σ. Тогда величина

$$S(\Sigma, (\widetilde{\alpha}, \widetilde{\beta})) = \sum_{i=1}^{k} (\varphi_i((\widetilde{\alpha}) \oplus \varphi_i(\widetilde{\beta})))$$

называется *динамической активностью СФЭ Σ на (упорядоченной) паре наборов* $(\widetilde{\alpha}, \widetilde{\beta})$. В свою очередь, *динамическая активность* $S(\Sigma)$ СФЭ Σ — максимальное значение величины $S(\Sigma, (\widetilde{\alpha}, \widetilde{\beta}))$ взятое по всем парам наборов $(\widetilde{\alpha}, \widetilde{\beta})$ из $B^n \times B^n$. Для произвольной ФАЛ f её динамической активностью $S_{\mathfrak{B}}(f)$ называется минимальная динамическая активность СФЭ в базисе $\mathfrak{B}$, реализующих указанную ФАЛ. Сложность $L(\Sigma)$ СФЭ Σ — число ФЭ в ней.

Пусть $\widetilde{x} = (x_1, \ldots, x_n)$ и $\widetilde{y} = (y_1, \ldots, y_{2^n})$. *Мультплексорной функцией порядка* n называется ФАЛ $\mu_n = \mu_n(\widetilde{x}, \widetilde{y})$, зависящая от n адресных БП $\widetilde{x}$ и 2^n информационных БП $\widetilde{y}$, для которой верно следующее представление:

$$\mu_n(\widetilde{x}, \widetilde{y}) = \bigvee_{\sigma \in B^n} K_\sigma(\widetilde{x}) y_{\nu(\sigma)},$$

где $\sigma = (\sigma_1, \ldots, \sigma_n) \in B^n$ — произвольный набор значений переменных x, $K_\sigma(\widetilde{x})$ — элементарная конъюнкция $x_1^{\sigma_1} x_2^{\sigma_2} \cdot \ldots \cdot x_n^{\sigma_n}$, а число $\nu(\sigma) = \sum_{i=1}^{n} \sigma_i 2^{n-i}$ — номер набора σ при лексикографическом упорядочивании наборов куба B^n.

Основные результаты

В данной работе изучается динамическая активность $S_{\mathfrak{B}_0}(\mu_n)$ мультиплексорной ФАЛ μ_n в стандартном базисе $\mathfrak{B}_0 = \{\&, \vee, \neg\}$. Основные полученные в ней результаты содержатся в следующих двух теоремах.

Теорема 1. *Если ФАЛ f существенно зависит от n переменных, то* $S_{\mathfrak{B}_0}(f) \geqslant \lceil \log_2 n \rceil$.

Так как мультиплексорная ФАЛ μ_n существенно зависит от всех своих $2^n + n$ переменных, то из теоремы 1, в частности, следует, что $S_{\mathfrak{B}_0}(\mu_n) \geqslant n + 1$.

Теорема 2. *Существует неотрицательная и стремящееся к нулю последовательность действительных чисел $\epsilon(1), \epsilon(2), \ldots$ такая, что для любого n, $n = 1, 2, \ldots$, мультиплексорная ФАЛ μ_n может быть реализована некоторой СФЭ Σ_n над базисом $\mathfrak{B}_0$, удовлетворяющей неравенствам*

$$L(\Sigma_n) \leqslant (1 + \epsilon(n)) \cdot 2^{n+1}, \; S(\Sigma_n) \leqslant (1 + \epsilon(n)) \cdot 4n.$$

С учетом теоремы 1 и результатов [7] теорема 2 устанавливает возможность построения такой реализующей ФАЛ μ_n СФЭ Σ_n, которая является асимптотически оптимальной по сложности и имеет оптимальную по порядку роста динамическую активность. Кроме того, из теорем 1 и 2 следует, что указанная ФАЛ имеет линейный относительно числа адресных переменных порядок роста динамической активности.

Работа выполнена при поддержке РФФИ (проект № 15-01-07474-а).

Список литературы

[1] Вайнцвайг М. Н. О мощности схем из функциональных элементов // Докл. АН СССР. — 1961. — Т. 139, № 2. — С. 320–323.

[2] Касим-Заде О. М. Об одновременной минимизации сложности и мощности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1978. — Вып. 33. — С. 215–220.

[3] Касим-Заде О. М. Об одной мере сложности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1981. — Вып. 38. — С. 117–179.

[4] Devadas S., Keutzer K., White J. Estimation of power dissipation in CMOS combinational circuits // Proc. Custom Integrated Circuits Conf. — 1990. — P. 19.7.1–19.7.6.

[5] Najm F. A survey of power estimation techniques in VLSI circuits (Invited paper) // IEEE Trans VLSI Syst. — 1994. — V. 2, N 4. — P. 446–455.

[6] Ложкин С. А., Шуплецов М. С. О динамической активности схем из функциональных элементов и построении асимптотически оптимальных по сложности схем с оптимальной по порядку динамической активностью // Учён. зап. Казан. ун-та. Сер. Физ.-матем. науки. — Т. 156, кн. 3. — 2014. — С. 84–97.

[7] Коровин В. В. О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — Т. 7, вып. 2. — 1995. — С. 95–102.

Независимые множества в деревьях с заданными степенными последовательностями

Курносов Артем Дмитриевич, Дайняк Александр Борисович

Московский физико-технический институт, e-mail: kurnosov@phystech.edu, dainiak@phystech.edu

Будем называть n-последовательностью набор из n натуральных чисел, упорядоченных по неубыванию. Последовательность $\tilde{a} = (a_1, a_2, \ldots, a_n)$ называется *графической*, если существует простой граф на множестве вершин $\{v_i\}_{i=1}^n$, такой, что $\deg v_i = a_i$ для каждого $i \in \{1, \ldots, n\}$. Сам граф называется *реализацией* n-последовательности $\tilde{a}$. Если существует реализация последовательности, являющаяся деревом, то соответствующую последовательность будем называть *древесной*.

Широко известен следующий критерий древесности n-последовательностей (см., например, [1, теорема 47.2]): последовательность положительных целых чисел $a_1, a_2, \ldots, a_n$ может быть реализована деревом тогда и только тогда, когда выполнено равенство $\sum_{i=1}^n a_i = 2(n-1)$. Следующим естественным шагом после проверки реализуемости последовательности деревом является получение оценок на различные инварианты дерева, исходя из свойств степенной последовательности [2]. В частности, актуальность имеют оценки количества

независимых множеств и сопутствующих инвариантов у деревьев и близких к ним графов [3].

Пусть $\tilde{a}$ — последовательность натуральных чисел $a_1 \leq a_2 \leq \ldots \leq a_n$, где $a_1 \geq 2$. Введём обозначение

$$l(\tilde{a}) := \sum_{i=1}^{n} a_i - 2(n-1).$$

Обозначим через $\mathcal{T}_{\tilde{a}}$ множество всех деревьев, реализующих последовательность $1, 1, \ldots, 1, a_1, a_2, \ldots, a_n$, в которой ровно $l(\tilde{a})$ единиц. Нетрудно доказать, что у такой $(n + l(\tilde{a}))$-последовательности всегда существуют реализации-деревья.

Наш основной результат сформулирован в следующей теореме.

Теорема 1. *Пусть n-последовательность $\tilde{a} = (a_1, a_2, \ldots, a_n)$ такова, что $a_1 \geq 2$. Пусть $r(\tilde{a})$ — наибольшее натуральное число такое, что $\sum_{i=1}^{r(\tilde{a})} a_i \leq n - 1$. Пусть T — произвольное дерево из класса $\mathcal{T}_{\tilde{a}}$. Справедливы оценки*

$$\max\left\{l(\tilde{a}), \left\lceil \frac{n + l(\tilde{a})}{2} \right\rceil\right\} \leqslant \alpha(T) \leqslant l(\tilde{a}) + r(\tilde{a}).$$

Указанные оценки достижимы. Более того, любое промежуточное значение также достижимо на некотором дереве из $\mathcal{T}_{\tilde{a}}$.

В ходе дальнейшей работы планируется получить оценки на количество независимых множеств в деревьях с заданной степенной последовательностью.

Список литературы

[1] Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. — М.: Наука, 1990. — 392 с.

[2] Schmuck N. S., Wagner S. G., Wang H. Greedy Trees, Caterpillars, and Wiener–type Graph Invariants // MATCH. Communications in Mathematical and in Computer Chemistry. — 2012. — V. 68, N 1. — P. 273–292.

[3] Wagner S., Gutman I. Maxima and Minima of the Hosoya Index and the Merrifield-Simmons Index // Acta Applicandae Mathematicae. — 2010. — V. 112, N 3. — P. 323–346.

Все гранево 2-раскрашиваемые d-ангуляции раскрашиваемы по Грюнбауму

Лавренченко Сергей Александрович[1], **Магомедов Абдулкарим Магомедович**[2]

[1] Российский государственный университет туризма и сервиса, e-mail: lawrencenko@hotmail.com

[2] Дагестанский государственный университет, e-mail: magomedtagir1@yandex.ru

В работе рассматриваются укладки простых графов на замкнутые поверхности. Под *d-ангуляцией P* поверхности подразумевается *d-угольная укладка* 3-

связного графа $G = G(P)$ на эту поверхность, т. е. такая укладка, каждая грань которой ограничена простым циклом фиксированной длины d ($d \geqslant 3$). С комбинаторной точки зрения P определяется тройкой множеств $V(P), E(P)$ и $F(P)$ вершин, ребер и граней соответственно. *Двойственный граф* $G^*(P)$ определяется как граф, множество вершин которого соответствует $F(P)$ и в котором две вершины смежны тогда и только тогда, когда смежны соответствующие грани P. Заметим, что $G^*(P)$ является регулярным графом степени d.

Рассматриваются только d-ангуляции P, двойственные графы которых суть простые графы. Из этих соображений предполагается 3-связность $G(P)$; последнее в следующих двух важных случаях обеспечивает, что граф $G^*(P)$ является простым: 1) $d = 3$; 2) поверхностью-носителем служит сфера. Во втором случае по теореме Штайница каждый 3-связный планарный граф G является 1-мерным остовом некоторого выпуклого политопа (в 3-мерном пространстве) с граничным комплексом P, и тогда двойственный граф $G^*(P)$ оказывается 1-мерным остовом двойственного политопа с граничным комплексом P^*.

Вершинная (соответственно *реберная* или *граневая*) k*-раскраска* d-ангуляции P определяется как такая сюръекция множества $V(P)$ ($E(P)$ или $F(P)$) на множество из k цветов, что образы смежных вершин (ребер или граней) различны. *Раскраской по Тейту* называется всякая реберная 3-раскраска 3-регулярного графа. *Вершинным*, *реберным* и *граневым хроматическими числами* d-ангуляции P называются наименьшие значения k, для которых существуют соответствующие k-раскраски P; эти числа обозначаются $\chi(P)$, $\chi'(P)$ и $\chi''(P)$ соответственно. Числа $\chi(P)$ и $\chi'(P)$ также называются вершинным и реберным хроматическими числами самого графа $G(P)$ и обозначаются $\chi(G(P))$ и $\chi'(G(P))$ соответственно.

Очевидно, всякая граневая k-раскраска произвольной d-ангуляции P соответствует некоторой вершинной k-раскраске двойственного графа $G^*(P)$ и обратно, а значит, $\chi''(P) = \chi(G^*(P))$. Интересно отметить, что из d-регулярности графа $G^*(P)$ следуют два включения: а) $\chi(G^*(P)) \in \{2, 3, \ldots, d, d+1\}$; б) $\chi'(G^*(P)) \in \{3, \ldots, d, d+1\}$, причем второе получается по теореме Визинга [1].

Раскраска по Грюнбауму определяется как такая раскраска ребер d-ангуляции P в d цветов, что для каждой грани P в множестве инцидентных ей ребер представлены все d цветов. До недавнего времени понятие раскраски по Грюнбауму относилось лишь к триангуляциям (т. е. к случаю $d = 3$), но в [4, 5] это понятие обобщено на произвольные d-ангуляции, $d \geqslant 3$.

Если T — триангуляция, то $\chi'(G^*(T)) \in \{3, 4\}$ по теореме Визинга. Равенство $\chi'(G^*(T)) = 3$ означает, что граф $G^*(T)$ раскрашивается по Тейту, а T — двойственным образом по Грюнбауму.

Гипотеза 1 (Грюнбаум [2], 1969 г.). *Каждая триангуляция T ориентируемой поверхности раскрашивается по Грюнбауму, т. е.* $\chi'(G^*(T)) = 3$.

Сорок лет эта гипотеза оставалась открытой. Лишь в 2009 году Кохол [3] построил бесконечные серии контрпримеров к гипотезе 1 на ориентируемых поверхностях рода g для всех $g \geqslant 5$. Здесь мы выдвигаем новую гипотезу о

триангуляциях путем усиления вакуумного ограничения $\chi''(T) \leqslant 4$ (которое, очевидно, выполняется для любой T) до ограничения $\chi''(T) \leqslant 3$:

Гипотеза 2. *Каждая триангуляция T ориентируемой поверхности с $\chi''(T) \leqslant 3$ раскрашивается по Грюнбауму.*

В случае неориентируемой поверхности гипотеза 2 неверна. Например, нетрудно убедиться, что минимальная триангуляция проективной плоскости с полным графом K_6 гранево 3-раскрашиваема, но она не раскрашивается по Грюнбауму, потому что ее двойственный граф является графом Петерсена, который, как хорошо известно, не является суммой трех 1-факторов и по лемме 1 имеет реберное хроматическое число не менее 4 (еще сам Петерсен показал, что оно равно 4).

Пусть $P - d$-ангуляция ориентируемой или неориентирумой поверхности (с простым двойственным графом). Поскольку двойственный граф $G^*(P)$ d-регулярен, следующая лемма очевидна.

Лемма 1. *Для выполнения равенства $\chi'(G^*(P)) = d$ необходимо и достаточно, чтобы граф $G^*(P)$ был 1-факторизуем, т. е. был суммой d 1-факторов.*

Классическая теорема Кёнига утверждает, что каждый двудольный d-регулярный граф раскладывается в сумму d 1-факторов. Поскольку граф двудолен тогда и только тогда, когда он вершинно 2-раскрашиваем, приходим к следующей переформулировке теоремы Кёнига:

Теорема 1 (Кёниг). *Если $\chi(G^*(P)) = 2$, то граф $G^*(P)$ 1-факторизуем.*

Комбинируя теорему 1 с леммой 1, приходим к теореме, которая фактически утверждает, что каждая гранево 2-раскрашиваемая d-ангуляция ориентируемой или неориентируемой поверхности раскрашивается по Грюнбауму:

Теорема 2. *Если $\chi(G^*(P)) = 2$, то $\chi'(G^*(P)) = d$.* Двойственная формулировка: *если $\chi''(P) = 2$, то P раскрашивается по Грюнбауму.*

В качестве частного случая теоремы 2, при $d = 3$ можно утверждать, что гипотеза 1 заведомо верна для всех гранево 2-раскрашиваемых триангуляций ориентируемых и неориентируемых поверхностей. Заметим, что в теореме 2 ограничение по хроматичности лишь минимально усилено по сравнению с соответствующим ограничением в гипотезе 2.

В работах [4, 5] в качестве следствий теоремы 2 установлено существование раскрашиваемых по Грюнбауму триангуляций ориентируемых и неориентируемых поверхностей с полными графами K_n по меньшей мере для половины классов вычетов в спектре возможных значений n:

Следствие 1. *Для каждого $n \equiv 3$ или $7 \pmod{12}$ (при $n \neq 3$) существует раскрашиваемая по Грюнбауму триангуляция ориентируемой поверхности с полным графом K_n.*

Следствие 2. *Для каждого $n \equiv 1$ или $3 \pmod 6$ (при $n \geqslant 9$) существует раскрашиваемая по Грюнбауму триангуляция неориентируемой поверхности с полным графом K_n.*

Список литературы

[1] Визинг В. Г. Об оценке хроматического класса p-графа // Дискретный анализ. — Т. 3. — Новосибирск: Ин-т мат. СО АН СССР, 1964. — С. 25–30.

[2] Grünbaum B. Conjecture 6 // Recent progress in combinatorics (ed. Tutte W. T.). — New York: Academic press, 1969. — P. 343.

[3] Kochol M. Polyhedral embeddings of snarks in orientable surfaces // Proc. amer. math. soc. — 2009. — V. 137. — P. 1613–1619.

[4] Лавренченко С. А., Магомедов А. М. К гипотезе Грюнбаума о раскраске ребер графа // Вестн. Даг. гос. ун-та. Естеств. науки. — 2014. — Вып. 6. — С. 27–31.

[5] Lawrencenko S., Magomedov A. M. All face 2-colorable d-angulations are Grünbaum colorable // Электрон. архив б-ки Корнел. ун-та. Деп. 06.01.2015. URL: http://arxiv.org/pdf/1501.01261v1.pdf (дата обращения: 08.02.2015).

О сложности и глубине реализации булевых функций схемами, вложенными в единичный куб

Ложкин Сергей Андреевич, Садовников Олег Александрович

Московский государственный университет имени М. В. Ломоносова, e-mail: lozhkin@cs.msu.ru, oleg.a.sadovnikov@gmail.com

Введение

Рассматривается класс схем из функциональных элементов в стандартном базисе из элементов конъюнкции, дизъюнкции и отрицания. Для каждой схемы Σ из данного класса наряду с глубиной $D(\Sigma)$ определим ее размерность $R(\Sigma)$, равную минимальной размерности единичного (булева) куба, допускающего изоморфное вложение Σ. Установлено, что для произвольной функции алгебры логики f от n булевых переменных существует реализующая ее схема Σ такая, что $D(\Sigma) \leqslant 3n + o(n)$ и $R(\Sigma) \leqslant n - \log\log n + O(1)$. Также показано, что для любой схемы Σ, удовлетворяющей указанному ограничению на размерность, справедлива нижняя оценка $D(\Sigma) \geqslant n + o(n)$. Тем самым доказано, что для $n = 1, 2, \ldots$ почти все функции от n переменных допускают реализацию их схемами рассматриваемого вида, размерность и глубина которых отличаются от минимальных (по всем эквивалентным им схемам) значений указанных параметров не более чем на константу и асимптотически не более, чем в 3 раза соответственно.

Основные определения

Данная работа посвящена исследованию ряда вопросов геометрической реализации схем из функциональных элементов[¶] над стандартным базисом $Б_0 = \{\&, \vee, \neg\}$ в единичном (булевом) кубе B^n, где $B = \{0, 1\}$.

Напомним [4], что граф $\hat{G}$ называется *подразбиением* графа G, если $\hat{G}$ можно получить из G заменой некоторых его ребер на простые цепи, и что два графа считаются *гомеоморфными*, если они имеют изоморфные подразбиения.

Будем говорить, что граф G допускает изоморфное (соответственно, гомеоморфное) вложение в граф H, если в графе H, существует подграф $\hat{G}$, изоморфный графу G (являющийся, соответственно, подразбиением G).

При этом будем считать, что указанное вложение φ графа G в граф H задается изоморфным (соответственно, гомеоморфным) отображением вершин и ребер графа G в вершины и ребра (соответственно, простые цепи) графа H.

Под изоморфным вложением СФЭ Σ в граф H будем понимать изоморфное вложение в граф H ее графа G, то есть графа, полученного из Σ в результате снятия ориентации с ее ребер и удаления пометок с ее вершин, а также отождествления (удаления) параллельных ребер.

Будем рассматривать куб B^n как граф с 2^n вершинами и $n \cdot 2^{n-1}$ ребрами, соединяющими всевозможные пары соседних вершин, то есть вершин, соответствующих наборам куба, отличающимся ровно в одном разряде. Обозначим через $R(\Sigma)$ минимальную размерность единичного куба, допускающего изоморфное вложение (далее — просто “вложение”) СФЭ Σ, а через $D(\Sigma)$ — ее глубину.

Заметим, что элементы $\&$ и $\vee$ с отождествленными входами (то есть, с параллельными входными дугами) можно рассматривать как одновходовые коммутационные элементы, реализующие тождественные ФАЛ. С помощью эквивалентных преобразований СФЭ Σ, связанных с добавлением и удалением коммутационных элементов, можно изменять структуру ее коммутационных подсхем, соединяющих входы Σ и выходы ее функциональных элементов с выходами Σ и входами функциональных элементов. Таким образом можно изменять геометрическую структуру схемы Σ, и, в частности, уменьшить степень ее вершин. При этом, в общем случае, глубина СФЭ Σ может возрасти.

Обычным образом определим размерность $R(f)$ (глубину $D(f)$) ФАЛ f как минимальную размерность (соответственно, глубину) СФЭ, реализующей ФАЛ f, а затем введем связанные с ними функции Шеннона:

$$R(n) = \max_{f \in P_2(n)} R(f), \; D(n) = \max_{f \in P_2(n)} D(f),$$

где $P_2(n)$ — множество всех ФАЛ от n переменных.

В работе [3] исследовалось поведение функции Шеннона $R(n)$ и было доказано, что

$$n - \log\log n + c_1 \leqslant R(n) \leqslant n - \log\log n + c_2,$$

[¶]Понятия, которые здесь используются, но не раскрываются, см., например, в [2, 4]

где c_1 и c_2 — некоторые константы. При этом типичное значение глубины схем, построенных при получении верхней оценки для ФАЛ от n булевских переменных (БП) имело при $n = 1, 2, \ldots$ экспоненциальный относительно n порядок роста, хотя известно [1,2], что

$$n - \log\log n + c_3 \leqslant D(n) \leqslant n - \log\log n + c_4,$$

где c_3 и c_4 — некоторые константы.

В настоящей работе доказывается, что для любой ФАЛ f от n переменных существует такая реализующая ее схема Σ в базисе Б_0, что

$$R(\Sigma) \leqslant n - \log\log n + c_5,\ D(\Sigma) \leqslant 3n + \bar{o}(n),$$

где c_5 — некоторая константа. Кроме того, доказывается, что для любой СФЭ Σ, реализующей произвольную ФАЛ f от n переменных, справедлива следующая нижняя оценка ее глубины:

$$D(\Sigma) \geqslant n + \frac{n}{\log\log n} + c_6,$$

где c_6 — некоторая константа. Тем самым доказывается, что для произвольной ФАЛ от n переменных существует реализующая ее СФЭ, размерность которой отличается от функции Шеннона $R(n)$ не более, чем на константу, а глубина асимптотически не больше, чем $3D(n)$.

В основе геометрической реализации СФЭ Σ лежит специальное гомеоморфное отображение полного двоичного n-ярусного дерева D_n в поддерево глубины $2n$ куба B^{n+2}, обладающее свойством регулярности: любые два параллельных (соседних) поддерева D_n переводятся в параллельные (соседние) подкубы куба B^{n+2}. Указанное отображение позволяет улучшить верхнюю оценку глубины вложения СФЭ Σ в методе из работы [3].

Работа выполнена при поддержке РФФИ (проект № 12-01-00964-а).

Список литературы

[1] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. — Вып. 6. — М.: Наука, Физматлит, 1996. — С. 189–214.

[2] Ложкин С. А. Лекции по основам кибернетики (учебное пособие). — М.: Изд. отдел ф-та ВМК МГУ, 2004. — 256 с.

[3] Седелев О. Б. Реализация функций алгебры логики схемами из функциональных элементов, вложенными в единичный куб // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2008. — № 1. — С. 44–50.

[4] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

О связи между глубиной и динамической активностью схем из функциональных элементов в унимодальных базисах

Ложкин Сергей Андреевич, Шуплецов Михаил Сергеевич

Московский государственный университет имени М. В. Ломоносова, e-mail: lozhkin@cs.msu.ru, mikle.shupletsov@gmail.com

Введение

Оценка энергопотребления интегральных схем является одной из важных задач проектирования СБИС. В современных интегральных схемах, построенных на основе КМОП технологий, выделяют как статическое энергопотребление, связанное с рассеянием тепла и поддержанием заданного потенциала в узлах схемы, подключенных к источнику питания, так и динамическое энергопотребление, возникающее при изменении потенциалов в узлах схемы.

Первые подходы к анализу статического энергопотребления для модели схем из функциональных элементов (СФЭ) были предложены в работе [1]. Основные теоретические результаты в этом направлении были получены О. М. Касим-Заде в работах [2, 3]. В указанных работах исследовался функционал сложности СФЭ, характеризующий статическое энергопотребление, — так называемая мощность СФЭ. При этом был установлен порядок роста соответствующей функции Шеннона в произвольном конечном полном базисе. Оказалось, в частности, что существуют базисы как с линейным‖, так и с экспоненциальным поведением указанной функции Шеннона. Кроме того, была показана возможность построения для “типичной” функции алгебры логики (ФАЛ) такой реализующей ее СФЭ, сложность которой асимптотически оптимальна, а мощность оптимальна по порядку роста.

В свою очередь, различные подходы к оценке динамического энергопотребления схем на основе модели СФЭ были предложены в работе [4]. В работе [5] была изложена вероятностная модель для оценки среднего энергопотребления СФЭ, а в работе [6] приводится обзор основных подходов к построению алгоритмов расчета динамического энергопотребления конкретных схем. В работе [7] был введен функционал динамической активности СФЭ, который моделирует их динамическое энергопотребление. В ней был установлен не более чем линейный порядок роста функции Шеннона для динамической активности СФЭ в произвольном полном конечном базисе. Доказано также, что для произвольной ФАЛ от n переменных можно построить такую реализующую ее СФЭ в стандартном базисе, сложность которой асимптотически не больше, чем $\frac{2^n}{n}$, а ее динамическая активность и мощность асимптотически не превосходят $5n$ и $3n$ соответственно. Заметим, что последняя оценка улучшает оценки мощности из работы [2].

‖Авторы считают, что сформулированная в [1] и использованная в [3] линейная нижняя оценка функции Шеннона для статической активности СФЭ в произвольном конечном полном базисе на самом деле в [1] не доказана.

В настоящей работе доказывается, что динамическая активность любой ФАЛ в произвольном унимодальном базисе не меньше, чем её глубина в том же базисе. Из данного неравенства вытекает аналогичное неравенство для соответствующих функций Шеннона, которое в силу [8] даёт линейную нижнюю оценку функции Шеннона для динамической активности СФЭ в унимодальном базисе.

Основные определения и результаты.

Пусть Σ — произвольная СФЭ в базисе $\mathfrak{B}$, имеющая n входов, которым сопоставлены булевские переменные (БП) набора $(x_1, \ldots, x_n) = x$ и k функциональных элементов(ФЭ), причем на выходе ФЭ с номером i в Σ реализуется ФАЛ $\varphi_i(x)$, $i = 1, \ldots, k$. Пусть B^n — единичный n-мерный куб. Тогда для произвольных наборов $\widetilde{\alpha}$ и $\widetilde{\beta}$ из B^n — наборов значений переменных x, приписанных входам СФЭ Σ, — величина

$$S(\Sigma, \widetilde{\alpha}, \widetilde{\beta}) = \sum_{i=1}^{k} (\varphi_i(\alpha) \oplus \varphi_i(\beta))$$

называется *динамической (переключательной) активностью СФЭ Σ на паре наборов* $(\widetilde{\alpha}, \widetilde{\beta})$. Заметим, что введенная величина характеризует число ФЭ СФЭ Σ, на выходах которых происходит изменение значения при смене набора значений на входах СФЭ с набора $\widetilde{\alpha}$ на набор $\widetilde{\beta}$ или обратно. При этом *динамической активностью* $S(\Sigma)$ СФЭ Σ называется максимальное значение величины $S(\Sigma, \widetilde{\alpha}, \widetilde{\beta})$ взятое по всем парам наборов $(\widetilde{\alpha}, \widetilde{\beta})$ из $B^n \times B^n$. Глубиной $D(\Sigma)$ СФЭ Σ назовем максимальное число ФЭ схемы, лежащих на какой-либо цепи, соединяющих один из входов СФЭ Σ с её выходом. Для произвольной ФАЛ f ее динамическую активность $S_{\mathfrak{B}}(f)$ и глубину $D_{\mathfrak{B}}(f)$ определим как минимальную динамическую активность и, соответственно, глубину СФЭ в базисе $\mathfrak{B}$, реализующих ФАЛ f, а затем обычным образом введем соответствующие функции Шеннона

$$S_{\mathfrak{B}}(n) = \max_{f \in P_2(n)} S_{\mathfrak{B}}(f) \quad \text{и} \quad D_{\mathfrak{B}}(n) = \max_{f \in P_2(n)} D_{\mathfrak{B}}(f).$$

Произвольную ФАЛ f монотонную или антимонотонную по каждой своей переменной будем называть *унимодальной*. Базис $\mathfrak{B}$ называется *унимодальным*, если состоит только из унимодальных ФАЛ.

Теорема 1. *Если $\mathfrak{B}$ — произвольный конечный полный унимодальный базис, то для любой ФАЛ f выполняется неравенство $D_{\mathfrak{B}}(f) \leqslant S_{\mathfrak{B}}(f)$.*

Следствие. $D_{\mathfrak{B}}(n) \leqslant S_{\mathfrak{B}}(n)$.

Из следствия теоремы 1 и работы [8] вытекает следующее неравенство:

$$S_{\mathfrak{B}}(n) \geqslant (\log k_{\mathfrak{B}})^{-1} \cdot (n - \log\log n - o(1)),$$

где $k_{\mathfrak{B}}$ — максимальное число входов у элементов базиса $\mathfrak{B}$.

Работа выполнена при поддержке РФФИ (проект № 15-01-007474-а).

Список литературы

[1] Вайнцвайг М. Н. О мощности схем из функциональных элементов // Докл. АН СССР. — 1961. — Т. 139, № 2. — С. 320–323.

[2] Касим-Заде О. М. Об одновременной минимизации сложности и мощности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1978. — Вып. 33. — С. 215–220.

[3] Касим-Заде О. М. Об одной мере сложности схем из функциональных элементов // Проблемы кибернетики. — М.: Наука, 1981. — Вып. 38. — С. 117–179.

[4] Devadas S., Keutzer K., White J. Estimation of power dissipation in CMOS combinational circuits // Proc. Custom Integrated Circuits Conf. — 1990. — P. 19.7.1–19.7.6.

[5] Ghosh A, Devadas S., Keutzer K., White J. Estimation of average switching activity in combinational and sequential circuits // Proc. 29th Design Automation Conf. — 1992. — P. 253–259.

[6] Najm F. A survey of power estimation techniques in VLSI circuits (Invited paper) // IEEE Trans VLSI Syst. — 1994. — V. 2, N 4. — P. 446–455.

[7] Ложкин С. А., Шуплецов М. С. О динамической активности схем из функциональных элементов и построении асимптотически оптимальных по сложности схем с оптимальной по порядку динамической активностью // Учён. зап. Казан. ун-та. Сер. Физ.-матем. науки. — Т. 156, кн. 3. — 2014. — С. 84–97.

[8] Ложкин С. А. О глубине функций алгебры логики в произвольном полном базисе // Вестник Московского университета. Серия 1. Математика и механика. — 1996. — № 2. — С. 80–82.

Последовательное разбиение ребер двудольного графа на паросочетания

Магомедов Абдулкарим Магомедович[1], **Магомедов Тагир Абдулкаримович**[2]

[1] Дагестанский государственный университет, e-mail: magomedtagir1@yandex.ru
[2] Дагестанский государственный университет, e-mail: tagir.magomedov@gmail.com

В работе приняты обозначения и определения монографии [1].

Пусть $G = (X, Y, E)$ — связный двудольный граф. Под *последовательным разбиением* множества ребер E на паросочетания будем понимать такое разбиение E на Δ паросочетаний множества X с множеством Y:

$$E[0], \ldots, E[\Delta - 1], \tag{1}$$

что для каждой вершины $x \in X$ степени k $(1 \leq k \leq \Delta)$ в каждом из паросочетаний $E[0], \ldots, E[k-1]$ найдется ребро, инцидентное вершине x.

Последовательные разбиения востребованы в расписаниях обслуживания в системе «приборов» X объектов множества Y с условиями одновременного включения «приборов» и их беспростойной работы. Задача о существовании последовательного разбиения NP-полна.

Легко видеть, что $E[0]$ является полным паросочетанием множества X с множеством Y. Условия существования полного паросочетания в двудольном графе $G = (X, Y, E)$ даются классической теоремой Холла, см., например, [1, с. 164]. Там же на с. 165 показано, что в G существует полное паросочетание X с Y, если

$$\min_{x \in X}\{d(x)\} \geq \max_{y \in Y}\{d(y)\}. \qquad (2)$$

Условие (2) можно ослабить: в G существует полное паросочетание X с Y, если $d(x) \geq d(y)$ для каждого ребра $(x, y) \in E$.

Основным результатом работы является следующая теорема.

Теорема 1. *Последовательное разбиение* (1) *существует, если*

$$d_G x_1 + d_G x_2 \geq d_G y_1 + d_G y_2$$

для каждой пары различных ребер (x_1, y_1) *и* (x_2, y_2) *из* E.

Работа выполнена при поддержке ДНЦ РАН и задания № 2014/33 на выполнение государственных работ в сфере научной деятельности в рамках базовой части государственного задания Минобрнауки России.

Список литературы

[1] Свами М., Тхуласираман К. Графы, сети и алгоритмы. — М.: Мир, 1984. — 455 с.

Агрегирование аналитического пространства задержек передачи информации

Майсурадзе Арчил Иериевич

Московский государственный университет имени М. В. Ломоносова, e-mail: maysuradze@cs.msu.ru

Рассматриваются предметные области, в которых для пересылки материальных объектов или информации из точки в точку требуются определённые затраты. Эти затраты зависят от источника и приёмника, от параметров пересылаемого объекта, а также от текущего состояния изменяющейся транспортной среды. При этом при транспортировке имеются специфические особенности — транспортируемый объект может быть разрезан на части, размеры которых принадлежат некоторому дискретному множеству значений.

В частности, в задачах анализа коммуникационной среды вычислительного кластера под затратами понимается задержка, возникающая при передаче сообщения между узлами. Существенным параметром каждого сообщения является его длина, измеряемая в байтах. Длинное сообщение может быть разрезано на части по длине, несколько коротких — объединены в один пакет. Современные

системы тестирования коммуникационной среды (benchmarks) многократно измеряют задержки передачи информации от каждого узла к каждому при различных параметрах сообщения и различных режимах функционирования коммуникационной среды. Примером служит система [1], которая использовалась для сбора исходной информации в данном исследовании. Каждая отдельная задержка — это неотрицательное число (миллисекунды). Под рассматриваемые условия также подходят некоторые задачи развозки нефтепродуктов, некоторых видов спиртов (в частности, бутилового спирта) и сжиженных газов: условия обусловлены соображениями безопасности транспортировки.

Исходно система тестирования собирает огромное число индивидуальных задержек. Данное исследование посвящено агрегированию этой информации в целях её анализа и дальнейшего использования в задачах автоматического динамического планирования расписания выполнения заданий на узлах вычислительного кластера.

Исходное аналитическое пространство задержек

Рассмотрим аналитическое пространство исходных задержек, измерениями которого являются параметры сообщения и коммуникационной среды: процесс-отправитель, процесс-получатель, длина сообщения, режим функционирования коммуникационной среды. Для фиксированной вычислительной системы и фиксированных параметров сообщения программное обеспечение Network Test из пакета Parus [1] позволяет многократно измерить задержки. Таким образом, в каждой ячейке многомерного массива мы получаем некоторое множество задержек.

Такое аналитическое пространство отдельных задержек имеет большой размер. Каждая коммуникационная матрица (одна задержка из среза пространства в двух измерениях) для типичного суперкомпьютера занимает примерно 1 ГБ. Следовательно, это пространство требуется агрегировать для последующего анализа коммуникационной среды. Агрегирование предлагается проводить поэтапно. Вначале нашей задачей является построение оптимального описания набора задержек независимо в каждой ячейке массива данных, то есть при фиксированных отправителе, получателе, длине и режиме. Затем предлагается ввести функции сходства между отдельными элементами пространства, между парами источник-приёмник, между отдельными процессами. На основе указанных функций сходства проводится дальнейшее агрегирование.

Расширенные метрические свойства задержек

Основным требованием к коммуникационной среде, как к любой технической сети передачи информации, является гарантированная доставка неискажённого сообщения от процесса-источника к процессу-приёмнику. Если это требование не выполнено, то сеть считается неработоспособной. Для работающей коммуникационной среды разумно ставить дополнительные требования, которые расширяют стандартные аксиомы метрики в направлении дополнительных измерений: не выгодно явно пересылать сообщение через процессы-

посредники (аксиомы метрики); не выгодно явно разбивать сообщение на части (расширение на длину).

Отметим, что формализация данных требований не столь очевидна, поскольку элементами пространства являются выборки. Соответственно, описание набора задержек независимо в каждой ячейке массива данных следует строить таким образом, чтобы эти требования удалось формализовать и проверить их выполнение.

Статистическое описание

Рассмотрим задержку в каждой отдельной ячейке массива данных как случайную величину с некоторым распределением. Даже для такого традиционного описания в нашем исследовании пришлось преодолеть ряд проблем. Во-первых, по какому принципу упорядочить случайные величины и их суммы. Во-вторых, есть ли разумные предположения о семействе распределений. В-третьих, каких числовых характеристик распределений хватило бы для такого описания распределений задержек, которое позволит проверить требования.

Естественно, для многих классов транспортных систем уже предпринимались попытки разработать модели задержек. Большинство исследователей сходятся в том, что задержки передачи информации предпочтительно описывать трёхпараметрическим логнормальным или трёхпараметрическим гамма-распределением. В данном исследовании установлено, что в вычислительных кластерах преобладают смеси указанных распределений. Существенная трудность заключается в том, что даже для одного трёхпараметрического логнормального или гамма-распределения при попытке оценить параметры классическим методом максимума правдоподобия возникают проблемы (возникают несходящиеся оптимизирующие последовательности). Для настройки параметров смеси указанных распределений пришлось использовать функционал расстояния между распределениями и разработать специальную процедуру оптимизации.

Заключение

Требуется повышенное внимание при выборе метода агрегирования набора задержек независимо в каждой ячейке массива данных.

Для анализа результатов тестирования коммуникационной среды вычислительных кластеров с большим числом узлов наиболее перспективным алгоритмом кластеризации на текущий момент видится применение приближённых алгоритмов дивизивной кластеризации. Данный класс алгоритмов при небольших потерях в точности по сравнению с точными агломеративными методами имеет большую скорость вычисления на экспериментальных данных, решает проблему хранения/вычисления большого объёма расстояний. Также данный алгоритм предоставляет возможность параллельной реализации, что может быть существенно при больших размерах тестов.

Функции расстояния на связях позволяют использовать все длины сообщений одновременно и однородно, а не последовательно.

Автор выражает свою благодарность студенту МГУ имени М. В. Ломоносова А. А. Горелову за сбор исходных данных и проведённые расчёты.

Исследование выполнено при финансовой поддержке РФФИ (проекты № 13-01-00751, № 15-07-09214).

СПИСОК ЛИТЕРАТУРЫ

[1] Salnikov A. N. Parus: A parallel programming framework for heterogeneous multiprocessor systems // Recent Advances in Parallel Virtual Machine and Message Passing Interface. — Springer, 2006. — P. 408–409.

О некоторых решётках замкнутых классов в функциональной системе линейных полиномов с целыми коэффициентами

Мамонтов Андрей Игоревич

Московский энергетический институт, e-mail: MamontovAI@mpei.ru

В настоящей работе исследуется функциональная система $L(\mathbb{Z})$ линейных полиномов над кольцом $\mathbb{Z}$ с операциями суперпозиции. В $L(\mathbb{Z})$ изучаются решётки по включению замкнутых классов, изоморфные решётке натуральных чисел по отношению делимости. Следует отметить, что замкнутые классы полиномов над бесконечными полями изучаются рядом авторов (см. например, [1], [2]). В настоящей работе внимание также уделяется алгоритмическим вопросам, связанным с полнотой в $L(\mathbb{Z})$. Отметим, что эффективные алгоритмы распознавания свойств дискретных функций, в частности, представленных полиномами, заслужили внимание многих авторов (см., например, [3]).

Итак, основными объектами нашего рассмотрения являются функции $f : \mathbb{Z}^n \to \mathbb{Z}$, задаваемые полиномами

$$f(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \ldots + a_n x_n, \quad a_0, a_1, \ldots, a_n \in \mathbb{Z}. \tag{1}$$

Каждый такой полином полностью определяется вектором коэффициентов $(a_0, a_1, \ldots, a_n)$ и представляет ровно одну функцию. Мы отождествляем функцию f, реализующий ее полином вида (1) и все конгруэнтные и равные f функции (т. е. получаемые из f переименованием переменных, а также введением и изъятием фиктивных переменных). Множество всех таких функций мы обозначаем как $L(\mathbb{Z})$. Такое же обозначение применяем и для функциональной системы (алгебры) $L(\mathbb{Z})$ с операциями суперпозиции. Буквами p, q, возможно с индексами, обозначаем простые числа, *НОД*$(c_1, \ldots, c_k)$ — наибольший общий делитель целых $c_1, \ldots, c_k$.

Пусть далее $F = \{f_1, \ldots, f_m\}$ — конечная система функций из $L(\mathbb{Z})$. Требуется определить, полна ли система F в $L(\mathbb{Z})$ (выдать ответ «Да» или «Нет»). Каждую из функций системы F считаем зависящей от одного множества переменных $\{x_1, \ldots, x_n\}$ и представляем в виде

$$f_i(\tilde{x}) = a_{i0} + a_{i1} x_1 + \ldots + a_{in} x_n,$$

$i = 1, \ldots, m$, при этом некоторые из коэффициентов a_{ij}, $j = 0, \ldots, n$, могут быть нулевыми.

В [4] получен алгоритм A распознавания полноты в $L(\mathbb{Z})$ и

Теорема 1. *Если все коэффициенты функций системы F ограничены по абсолютной величине константой t и максимальное количество переменных функций есть n, то размером задачи является $N = mnt$ и алгоритм имеет при реализации машиной с произвольным доступом к памяти временну́ю сложность $O(N^2 \log^2 N)$ (двоичных операций) и емкостную сложность $O(N \log N)$ (битов).*

Для функции f вида (1) рассмотрим сумму коэффициентов

$$SC(f) = a_1 + \ldots + a_n.$$

Для каждого $k \in \mathbb{N}$ определим $S(k)$ как класс функций, удовлетворяющих условию $SC(f) \equiv 1 \pmod{k}$. Для каждого $k \in \mathbb{N}$ и $b \in 0 \cup \mathbb{N}$ обозначим через $U(b, k)$ класс всех функций, сохраняющих множество

$$\mathbf{Z}(b_1, k) = \{c \in \mathbf{Z} : c \equiv b_1 \pmod{k}\},$$

где b_1 — наименьший неотрицательный вычет числа b по модулю k.

Для всех $k \in \mathbb{N}$ определим также $S^0(k)$ — класс всех функций из $S(k)$, у которых свободный член равен 0.

Следует отметить, что если для каждого $k \in \mathbb{N}$ и $b \in 0 \cup \mathbb{N}$ обозначить через $U^0(b, k)$ класс всех функций из $U(b, k)$, у которых свободный член равен 0, то $S^0(k) = U^0(b, k)$.

Введём на множестве $\mathbb{N}$ частичный порядок ρ такой, что

$$\alpha \rho \beta \Leftrightarrow \alpha | \beta. \tag{2}$$

Утверждение 1. 1. *Системы $\{1 + x, x + ky, x + y - z\}$ и $\{b, x + k, x + y - z\}$ являются базисами классов $S(k)$ и $U(b, k)$ соответственно.*

2. *Условие $k_1 | k_2$ равносильно включениям*

$$S(k_2) \subseteq S(k_1), U(b, k_2) \subseteq U(b, k_1).$$

3. *Если $[k_1, k_2] = k_3$, то $S(k_1) \cap S(k_2) = S(k_3)$ и $U(b, k_1) \cap U(b, k_2) = U(b, k_3)$.*

4. *Если $k_0 = (k_1, k_2)$, то*

$$[S(k_1) \cup S(k_2)] = S(k_0) \text{ и } [U(b, k_1) \cup U(b, k_2)] = U(b, k_0).$$

5. *Класс $S(k_2)$ является предполным в $S(k_1)$ в том и только том случае, когда $k_2 = k_1 p$. Аналогичное утверждение верно и для классов $U(b, k)$.*

6. *Классы $S(k)$ и $U(b, k)$ образуют решётку по включению, изоморфную решётке $(\mathbf{N}, \rho)$ с частичным порядком (2).*

Утверждение 2. *Система $\{x + ky, x + y - z\}$ является базисом класса $S^0(k)$. Для классов $S^0(k)$ верны утверждения, аналогичные утверждениям из пунктов 2–6 утверждения 1.*

Исследовалось распознавание относительной полноты.

Проблема *полноты относительно* заданного *класса* K (не обязательно замкнутого) состоит в выяснении полноты системы, содержащей класс K. Рассмотрим эту проблему для классов $K = S(k), U(b,k), S^0(k)$.

Утверждение 3. *Если $S(k) \subset F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов $S(p)$.*

Проверка полноты конечной системы размера N относительно класса $S(k)$ имеет временную сложность $O(N \log^2 N)$ и емкостную сложность $O(N \log N)$.

Если $U(b,k) \subset F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов $U(b,p)$.

Проверка полноты конечной системы размера N относительно класса $U(b,k)$ имеет временную сложность $O(N^2 \log^2 N)$ и емкостную сложность $O(N \log N)$.

Если $S^0(k) \subset F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов $U(b,p)$ и S(p).

Проверка полноты конечной системы размера N относительно класса $S^0(k)$ имеет временную сложность $O(N^2 \log^2 N)$ и емкостную сложность $O(N \log N)$.

Работа выполнена при поддержке РФФИ (проект № 13-01-00684-а).

Список литературы

[1] Семигродских А. П. О клонах полиномов над бесконечными полями // Изв. вузов. Матем. — 2000. — № 7. — С. 53–58.

[2] Алексиадис Н. Ф. Функциональная система полиномов с натуральными коэффициентами // Вестник МЭИ. — 2013. — № 6. — С. 125–140.

[3] Селезнева С. Н. Полиномиальный алгоритм для распознавания принадлежности функций k-значной логики, представленных полиномами, к предполным классам линейных функций // Вестник МГУ. Сер. 15. Выч. матем. и кибернетика. — 2001. — № 3. — С. 40–43.

[4] Мамонтов А. И., Мещанинов Д. Г. Алгоритм распознавания полноты в функциональной системе L(Z) // Дискрет. матем. — 2014. — Т. 26 — № 1. — С. 85–95.

Векторные пространства над решетками: базисы и размерность

Маренич Евгений Евгеньевич[1], **Маренич Валентина Евгеньевна**[2]

[1] Московский педагогический государственный университет, e-mail: marenich1@yandex.ru

[2] Российский государственный социальный университет, e-mail: vmarenich@yandex.ru

Пусть P — дистрибутивная решетка с нулем $\widetilde{0}$ и единицей $\widetilde{1}$, $(V, \vee, \leq)$ — верхняя полурешетка. В дальнейшем операцию объединения $\vee$ в полурешетке $(V, \vee, \leq)$ мы будем обозначать значком $+$.

1. Решеточные векторные пространства

Векторным пространством над решеткой P (пространством) называется непустое множество V, с бинарной операцией сложения $+$ и операцией умножения на элементы решетки P, обладающее свойствами:

1) $(V, +, \leq)$ — верхняя полурешетка с нулем 0;
2) $\lambda(u + v) = \lambda u + \lambda v$ для любых $\lambda \in P$, $u, v \in V$;
3) $(\lambda \vee \mu)u = \lambda u + \mu u$ для любых $\lambda, \mu \in P$, $u \in V$;
4) $(\lambda \wedge \mu)u = \lambda(\mu u)$ для любых $\lambda, \mu \in P$, $u \in V$;
5) $\widetilde{1}u = u$ для любых $u \in V$;
6) $\widetilde{0}u = 0$ для любых $u \in V$.

2. Базисы векторных пространств

На множестве V определен частичный порядок $\preceq$: $u \preceq v$ тогда и только тогда, когда $u = \lambda v$ для некоторого элемента $\lambda \in P$. Линейной оболочкой мультимножества $U = \{u_1, u_2, \ldots, u_n\}$ векторов пространства V называется $Lin(U) = Lin(u_1, u_2, \ldots, u_n)$ — множество всех линейных комбинаций векторов $u_1, u_2, \ldots, u_n$.

Определим множества: $join(V)$ — множество всех $\vee$-неразложимых векторов пространства V; $J(V) = join(V) - \{0\}$; $MJ(V) = \max\{J(V), \preceq\}$; $M(V) = \max\{V, \preceq\}$. Для векторов $v \in V$, обозначим $[v)_{\preceq} = \{z \mid z \in V, v \preceq z\}$ — полуинтервалы ЧУМ $(V, \preceq)$.

Базисом ненулевого пространства V называется минимальное конечное множество W такое, что $V = Lin(W)$. Базисы пространства могут содержать различное число векторов. Разложение вектора по базису не обязательно единственно.

3. Свойства базисов

Теорема 3.1. *Пусть $MJ(V)$ — базис пространства V. Конечное множество U, $U \subseteq V$, порождает пространство V тогда и только тогда, когда $U \cap [w)_{\preceq} \neq \emptyset$ для любого вектора $w \in MJ(V)$.*

Следствие 3.1. *Пусть $MJ(V)$ — базис пространства V. Конечное множество U является базисом пространства V тогда и только тогда, когда U — минимальное множество такое, что $U \cap [w)_{\preceq} \neq \emptyset$ для любого вектора $w \in MJ(V)$.*

Теорема 3.3. *Пусть $MJ(V)$ — базис пространства V. Тогда для любого базиса U пространства V справедливо неравенство $|MJ(V)| \geq |U|$.*

Теорема 3.4. *Пусть $MJ(V)$ — базис пространства V, $n = |MJ(V)|$. Каждый базис пространства V содержит n векторов тогда и только тогда, когда полуинтервалы $[w)_{\preceq}$, где $w \in MJ(V)$, попарно не пересекаются.*

4. Стандартные базисы

Пусть $U = \{u_1, u_2 \ldots, u_k\}$ — базис пространства V. Последовательность $(u_1, u_2, \ldots, u_k)$ будем называть упорядоченным базисом пространства V.

Базис U называется стандартным, если для любого вектора $u_i \in U$ из любого его разложения по базису U, $u_i = \sum\limits_r \lambda_{ir} u_r$, следует, что $u_i = \lambda_{ii} u_i$. Понятие стандартного базиса введено в работах [1], [3].

Теорема 4.1. *Если $MJ(V)$ — базис пространства V, то $MJ(V)$ — стандартный базис.*

Обозначим $base(V)$ — множество всех упорядоченных базисов пространства V. На множестве $base(V)$ определен ЧП $\preceq$: неравенство $(w_1, w_2, ..., w_k) \preceq (w'_1, w'_2, ..., w'_k)$ равносильно неравенствам $w_i \preceq w'_i$ для всех i.

Теорема 4.2. *Множество всех минимальных элементов ЧУМ $(base(V), \preceq)$ совпадает с множеством всех упорядоченных стандартных базисов пространства V.*

Следствие 4.1. *Пусть все $\preceq$-цепи ЧУМ $(base(V), \preceq)$ конечны. Справедливы утверждения.*

i) Если $U = \{u_1, u_2, \ldots, u_k\}$ — базис пространства V, то $\{\mu_1 u_1, \mu_2 u_2, \ldots, \mu_k u_k\}$ — стандартный базис пространства V для некоторых $\mu_1, \mu_2, \ldots, \mu_k \in P$.

ii) Пространство V имеет базис, содержащий k векторов, тогда и только тогда, когда V имеет стандартный базис, содержащий k векторов.

iii) Если пространство V имеет единственный стандартный базис, то все базисы пространства V содержат одинаковое число векторов.

5. Размерность векторного пространства

Размерностью ненулевого конечнопорожденного пространства V называется число $\dim(V)$, равное наименьшему числу векторов в базисах пространства.

Теорема 5.1. *Пусть $MJ(V)$ — базис пространства V. Тогда множество U, содержащее наименьшей число векторов и такое, что $U \cap [w)_{\preceq} \neq \emptyset$ для любого вектора $w \in MJ(V)$, является базисом пространства V*

Теорема 5.2. *Пусть $MJ(V)$ — базис пространства V, $\max[w)_{\preceq} \neq \emptyset$ для каждого вектора $w \in MJ(V)$. Тогда множество B, $B \subseteq M(V)$, содержащее наименьшее число векторов и пересекающее каждое из множеств $\max[w)_{\preceq}$, является базисом пространства V и $\dim(V) = |B|$.*

Теорема 5.2 позволяет вычислять размерность известными алгоритмами [6].

6. Векторные пространства над цепями

Теорема 6.1. *Пусть V — ненулевое конечнопорожденное подпространство. Справедливы утверждения.*

i) Пространство V имеет единственный стандартный базис.

ii) Стандартный базис пространства V совпадает с базисом $MJ(V)$.

Следствие 6.1. Если V — ненулевое конечнопорожденное пространство, то все базисы пространства V содержат одинаковое число векторов, равное $|MJ(V)|$.

Список литературы

[1] Kim K. H., Roush F. F. Generalized fuzzy matrices // Fuzzy Sets and Systems. — 1980 — N 4. — P. 293–315.

[2] Kim K. H., Roush F. F. Idempotent fuzzy matrices. Seminar report. — Alabama State Univ., Montgomery, Al. — 1981.

[3] Kim Ki Hang. Boolean matrix theory and applications. — Marcel Dekker, Inc.— 1982.

[4] Giveon J. Lattice matrices // Information and control. — 1964. — N 7. — P. 477–484.

[5] Скорняков Л. А. Обратимые матрицы над дистрибутивными структурами // Сибирский математический журнал. — Т. XXVII, № 2. — 1986. — С. 182–185.

[6] Lin L., Jiang Y. The computation of hitting sets: review and new algorithms // Inf. Process. Lett. — May 2003. — V. 86. — P. 177–184.

О числе нетерминалов в деревьях вывода разложимой стохастической КС-грамматики

Мартынов Игорь Михайлович

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: murbidodrus@gmail.com

В работе исследуются вероятностные свойства деревьев вывода высоты t, порождаемых разложимой стохастической КС-грамматикой, при $t \to \infty$. Предполагается, что грамматика согласованная, т. е. перронов корень матрицы A первых моментов грамматики не превосходит 1.

Стохастической КС-грамматикой называется система $G = \langle V_T, V_N, R, s\rangle$, где V_T и V_N — конечные алфавиты терминальных и нетерминальных символов соответственно, $s \in V_N$ — аксиома, $R = \cup_{i=1}^{k} R_i$, где k — мощность алфавита V_N и R_i — множество правил вывода вида

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij},\ j = 1, 2, \ldots, n_i,$$

где $A_i \in V_N$, $\beta_{ij} \in (V_T \cup V_N)^*$ и p_{ij} — вероятность применения правила r_{ij}, причём $0 < p_{ij} \leq 1$ и $\sum_{j=1}^{n_i} p_{ij} = 1$.

Применение правила грамматики к слову состоит в замене вхождения нетерминала из левой части правила на слово, стоящее в его правой части.

Каждому слову α КС-языка соответствует последовательность $\omega(\alpha) = (r_1, \ldots, r_s)$ правил грамматики (вывод), с помощью которой α выводится из аксиомы s. Выводу слова соответствует дерево вывода [1] d, вероятность $p(d)$ которого определяется как произведение вероятностей правил, образующих вывод: $p(d) = \prod_{k=1}^{s} p(r_k)$.

Грамматика называется *согласованной*, если сумма вероятностей всех конечных деревьев вывода равна 1. Согласованная стохастическая грамматика G задаёт распределение вероятностей на множестве слов порождаемого ею языка $L(G)$. В дальнейшем всюду будем предполагать, что грамматика солгасованна.

По стохастической КС-грамматике строится матрица A первых моментов. Её элемент a_j^i определяется как $\sum_{l=1}^{n_i} p_{il} s_{il}^j$, где величина s_{il}^j равна числу нетерминальных символов A_j в правой части правила r_{il}. Перронов корень [2] матрицы A обозначим через r. Известно, что согласованная грамматика имеет перронов корень $r \leq 1$.

Введём некоторые отношения на множестве нетерминальных символов. Будем говорить, что нетерминал A_j непосредственно следует за нетерминалом A_i (и обозначать $A_i \to A_j$), если в грамматике существует правило вида $A_i \xrightarrow{p_{il}} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_T \cup V_N)^*$. Рефлексивное транзитивное замыкание отношения $\to$ обозначим $\to_*$.

Классом нетерминалов назовём максимальное по включению подмножество $K \subseteq V_N$ такое, что $A_i \to_* A_j$ для любых $A_i, A_j \in K$. Для различных классов нетерминалов K_1 и K_2 будем говорить, что класс K_2 непосредственно следует за классом K_1 (и обозначать $K_1 \prec K_2$), если существуют $A_1 \in K_1$ и $A_2 \in K_2$, такие, что $A_1 \to A_2$. Рефлексивное транзитивное замыкание отношения $\prec$ обозначим через $\prec_*$. Классы грамматики, за которыми непосредственно не следует ни один класс, будем называть завершающими. Грамматика называется *разложимой*, если она содержит более одного класса, и *неразложимой* в противном случае.

Случай $r < 1$ рассматривался Л. П. Жильцовой (в [3] и других работах). А. Е. Борисов обобщил [4] полученные результаты на случай $r \leq 1$ для грамматики из двух классов.

Пусть $\mathcal{K} = \{K_1, K_2, \ldots, K_m\}$ — множество классов нетерминалов грамматики, $m \geq 2$. Будем полагать, что классы нетерминалов перенумерованы таким образом, что $i \leq j$ для любых $K_i \prec_* K_j$. Заметим, что при этом класс K_1 содержит аксиому s грамматики. Матрица первых моментов A грамматики имеет следующий вид:

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1,n-1} & A_{1,n} \\ 0 & A_{22} & A_{23} & \cdots & A_{2,n-1} & A_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_{n-1,n-1} & A_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & A_{n,n} \end{pmatrix}.$$

Подматрица A_{ij} является нулевой, если $K_i \not\prec K_j$. Блоки, расположенные ниже главной диагонали, нулевые в силу упорядоченности классов.

Для каждого класса K_i матрица A_{ii} неразложима. Без ограничения общности будем считать, что она строго положительна и непериодична. Обозначим через r_i перронов корень матрицы A_{ii}. Для неразложимой матрицы перронов корень является вещественным и простым [2]. Очевидно, $r = \max_i\{r_i\}$. Классы K_i, перроновы корни r_i которых равны 1, будем называть критическими. Остальные классы грамматики будем называть докритическими.

Для каждого класса K_i рассмотрим всевозможные цепочки классов $K_i \prec K_{j_1} \prec K_{j_2} \prec \ldots \prec K_{j_s}$, где класс K_{j_s} — завершающий. Максимум числа критических классов среди $K_i, K_{j_1}, \ldots, K_{j_s}$ по всем таким цепочкам обозначим q_i, а сами такие цепочки будем называть *насыщенными*.

Через $P_i(t)$ обозначим вероятность множества деревьев вывода высоты t, корень которых помечен нетерминалом A_i. Верна следующая теорема.

Теорема 1. *Пусть матрица первых моментов A разложимой КС-грамматики G имеет перронов корень, равный* 1. *Тогда вероятность $P_i(t)$ деревьев высоты*

t с корнем в A_i имеет вид:

$$P_i(t) \sim \tilde{c}_i \cdot t^{-1-\left(\frac{1}{2}\right)^{q_l-1}},$$

где $c_i, \tilde{c}_i$ — некоторые константы, $A_i \in K_l$, и $q_l \geq 1$ — максимальное число критических классов в цепочке от K_l до завершающего класса.

Для каждого класса K_i рассмотрим также всевозможные цепочки классов $K_1 \prec K_{j_1} \prec K_{j_2} \prec \ldots \prec K_i$ из начального класса K_1 грамматики в класс K_i. Максимальное число критических классов в такой цепочке обозначим q_i^-. Верна следующая теорема.

Теорема 2. *Пусть матрица первых моментов A разложимой КС-грамматики G имеет перронов корень, не превосходящий 1. Тогда математическое число применений правила r_{ij} в случайном дереве вывода высоты t имеет следующий вид:*

$$M_{ij}(t) \sim d_i \cdot p_{ij} \cdot t^{\left(\frac{1}{2}\right)^{\tilde{q}_l-1}},$$

где p_{ij} — вероятность правила r_{ij}, d_i — некоторая константа, $A_i \in K_l$, и

$$\tilde{q}_l = q_1 - q_l^- .$$

Таким образом, наибольшую асимптотику имеют $M_{ij}(t)$, для которых A_i расположен в последнем критическом классе K_l какой-либо насыщенной цепочки из K_1 в завершающий класс, либо в докритических классах, следующих за K_l. Величина $q_1 - q_l^-$ для таких правил обращается в 0, и $M_{ij}(t)$ имеет асимптотику t^2.

Список литературы

[1] Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. — М.: Мир, 1978.

[2] Гантмахер Ф. Р. Теория матриц. — М.: ФИЗМАТЛИТ, 2010.

[3] Жильцова Л. П. Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. — Вып. 9. — М.: Наука, 2000. — С. 101–126.

[4] Борисов А. Е. Закономерности в словах стохастических контекстно-свободных языков, порождённых грамматиками с двумя классами нетерминальных символов. Вопросы экономного кодирования : дис. . . . канд. физ.-мат. наук : 01.01.09. — Нижний Новгород: ННГУ им. Н. И. Лобачевского, 2006. — 103 с.

О замкнутых классах полиномов над кольцом $\mathbb{Z}_k$

Мещанинов Дмитрий Германович

НИУ Московский энергетический институт, e-mail: MeshchaninovDG@mpei.ru

Рассматривается функциональная система P_k функций k-значной логики с операциями суперпозиции, замкнутый класс $\mathcal{P}(k)$ функций, представимых

полиномами над кольцом $\mathbb{Z}_k$ вычетов по составному модулю k, и его подкласс $\mathcal{L}(k)$, состоящий из линейных по модулю k функций, т. е. представимых полиномами только первой (и нулевой) степени. В [1] описана решетка $[\mathcal{L};\mathcal{P}]$ всех классов, находящихся между $\mathcal{L}(k)$ и $\mathcal{P}(k)$, она полностью построена для $k=4$ (4 — наименьшее составное число). Решетка оказалась счетно-бесконечной, в ней две бесконечно возрастающие неуплотняемые цепи классов. В данной работе эти результаты обобщаются на случай $k=p^2$ и частично на $k=p^\alpha$, $\alpha\geq 3$ (здесь и далее буквой p обозначается простое число).

При составном k полином над $\mathbb{Z}_k$, представляющий функцию из $\mathcal{P}(k)$, не является единственным. Если $k=p^\alpha$, то для любой функции из $\mathcal{P}(k)$ существует реализующий ее полином над $\mathbb{Z}_k$, в котором каждая переменная имеет степень не выше $p\alpha-1$ [2]. Такой полином назовем *приведенным*. Он также не является единственным, например, приведенные полиномы px^p и px реализуют одну функцию из $\mathcal{P}(p^\alpha)$.

При $k=p^2$ рассмотрим следующие замкнутые классы.

1. Положим $K_1=\mathcal{L}(p^2)$. Если $m\geq 2$, то $K_m=[\{1,x+y,px_1\cdots x_m\}]$ — класс функций, представимых полиномами, в которых каждый нелинейный моном имеет степень не выше m и кратен p.

2. Если $m\geq p$, то $\Lambda_m=[K_m\cup\{x^p\}]$ — класс функций, представимых полиномами, в которых каждый нелинейный моном принадлежит K_m или имеет вид ay^p, где $(a,p)=1$.

3. Определим также классы

$$K_\infty=\bigcup_{m=1}^{\infty}K_m,\quad \Lambda_\infty=\bigcup_{m=p}^{\infty}\Lambda_m.$$

Эти классы не имеют базисов.

Теорема 1. *Решетка $[\mathcal{L};\mathcal{P}]$ содержит следующие неуплотняемые цепи классов*:

$$K_1\subset\ K_2\subset\cdots\subset K_m\subset K_{m+1}\subset\cdots\subset K_\infty,$$

$$\Lambda_p\subset\Lambda_{p+1}\subset\cdots\subset\Lambda_m\subset\Lambda_{m+1}\subset\cdots\subset\Lambda_\infty.$$

При $m=p,p+1,\ldots,\infty$ каждый класс K_m является также предполным в классе Λ_m.

4. Введем также $\Lambda^2=[\{1,x+y,x^py^p\}]$ — класс функций, реализуемых приведенными полиномами, в которых каждый нелинейный моном принадлежит Λ_∞ или имеет вид $ay_1^p\cdots y_N^p$, где $N\geq 2$, $(a,p)=1$.

Теорема 2. *Класс Λ_∞ является предполным в классе Λ^2.*

5. В [3] для произвольных k и их делителей d определены классы $R(d)$ и $L(d)$ функций, сохраняющих и абсолютно сохраняющих d-разности.

Теорема 3 [3,4]. *Если $d\neq 1$ и $d\neq k$, то $L(d)\subset R(d)$. Если $k=pd$, то класс $L(d)$ является предполным в классе $R(d)$. Если $k=p^2$, то $\mathcal{P}(k)=R(p)$.*

Теорема 4. *Справедливо включение $\Lambda^2\subseteq L(p)$. Равенство выполняется только при $p=2$.*

6. Рассмотрим класс $S(p)$ функций $f(x_1,\dots,x_n)$, реализуемых приведенными полиномами с нелинейной частью вида

$$\sum_{\tilde{\mu}\in\{0,1,\dots,p-1\}^n}\ \sum_{j=1}^{n} a_j(\tilde{\mu})\chi_{p,j}(\tilde{x}-\tilde{\mu}),$$

где

$$a_j(\tilde{\mu})\in\{0,1,\dots,p^2-1\},\quad \chi_{p,j}(\tilde{x})=\begin{cases} x_j, & \tilde{x}\equiv\tilde{0} \pmod p,\\ 0, & \tilde{x}\not\equiv\tilde{0} \pmod p.\end{cases}$$

Теорема 5. *Система* $\{1, x+y, x^{2p-1}\}$ *является базисом класса* $S(p)$.

Теорема 6. *Предполными в* $\mathcal{P}(p^2)$ *являются только классы* $S(p)$ *и* $L(p)$.

Теорема 7. *Выполняется включение* $\Lambda_\infty\subset S(p)$, *а при* $p=2$ *класс* Λ_∞ *является предполным в классе* $S(p)$.

Таким образом, описан обширный фрагмент решетки $[\mathcal{L};\mathcal{P}]$ при $k=p^2$. Если $p=2$, то этот фрагмент совпадает со всей решеткой (она построена в [1]). Две бесконечно возрастающие цепи сохраняются при обобщении случая $k=2^2$ на $k=p^2$. При других значениях k свойства решетки описывает

Теорема 8. *Если* $k=p_1\cdots p_N$, *где* $p_1,\dots,p_N$ *— различные простые числа, то решетка* $[\mathcal{L};\mathcal{P}]$ *конечна и изоморфна* N*-мерному кубу* [4]. *Если* $k=p^\alpha$, *где* $\alpha\geq 3$, *то решетка* $[\mathcal{L};\mathcal{P}]$ *имеет бесконечную ширину.*

Работа выполнена при поддержке РФФИ (проект № 13-01-00684-а).

Список литературы

[1] Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика. — 1997. — Т. 9, № 2. — С. 24–39.

[2] Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k // Многоустойчивые элементы и их применение. — М.: Сов. радио, 1971. — С. 84–88.

[3] Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Матем. вопросы кибернетики. — 1998. — Вып. 7. — С. 265–280.

[4] Мещанинов Д. Г. О замкнутых классах k-значных функций, сохраняющих первые d-разности // Матем. вопросы кибернетики. — 1999. — Вып. 8. С. 219–230.

Критерий базируемости для одного типа семейств замкнутых классов функций многозначной логики

Михайлович Анна Витальевна

Национальный исследовательский университет «Высшая школа экономики», e-mail: anna@mikhaylovich.com

Известно, что все замкнутые классы булевых функций имеют конечный базис. В [1] приведены примеры, показывающие, что при всех $k\geq 3$ в P_k су-

ществуют как замкнутые классы со счётным базисом, так и замкнутые классы без базиса. Функции из этих примеров являются симметрическими и принимают значения только из множества $\{0,1\}$, причем равны нулю на наборах, содержащих хотя бы одну нулевую компоненту. Кроме того, замыкание любого подмножества таких функций совпадает с объединением их замыканий. В [2] несколько таких семейств достаточно общего вида исследованы на конечную порожденность и базируемость. Данная работа является обобщением [3] (а также некоторых результатов из [2]), в ней приводится критерий базируемости для множеств фукнций описанного выше вида, к которым добавляется конечное множество произвольных функций. Все недостающие определения можно найти в [2, 3].

Пусть $A \subset P_k$, $B \subset P_k$. Положим $[A]_B = [A \cup B]$. Для $f, g \in A$ введем обозначение $f \preceq_B g$, если $f \in [\{g\}]_B$. Будем говорить, что функции f и g эквивалентны относительно множества B (обозначение $f \sim_B g$), если $f \preceq_B g$ и $g \preceq_B f$. Будем использовать обозначение $f \prec_B g$, если $f \preceq_B g$ и $f \not\sim_B g$.

Множество всех функций, символы которых содержатся в некоторой формуле Φ над A, обозначим через $\Theta(\Phi)$. Для f, $g \in A$, введем обозначение $f \trianglelefteq_A g$, если существует такая формула Φ над A, реализующая функцию f, что $g \in \Theta(\Phi)$. Тогда если $B \subset A$ и $f \preceq_B g$, то $f \trianglelefteq_A g$.

Пусть B — конечное множество. Будем говорить, что множество A обладает свойством $(*)_B$, если для любого $G \subset A$ выполняется равенство $(\cup[\{g\}]_B) \cap A = [\cup\{g\}]_B \cap A$, где объединения берутся по всем функциям $g \in G$. Пусть $A \subset P_k$, $B \subset A$. Будем говорить, что множество A обладает свойством $(**)_B$, если для любых $f, g \in A$, таких, что $f \trianglelefteq_A g$ и $g \trianglelefteq_A f$, выполняется соотношение $f \sim_B g$ и для любых функций $f, g, h \in A$, таких, что $f \trianglelefteq_A g$, $g \trianglelefteq_A h$, $f \preceq_B h$, выполняется по крайней мере одно из следующих соотношений: $f \preceq_B g$, $g \preceq_B h$.

Теорема. *Пусть $A \subset P_k$, $B \subset A$, $G \subset A$, $F = [G \cup B]$, множество B конечно, множество A обладает свойствами $(*)_B$ и $(**)_B$, все функции из G попарно неэквивалентны относительно множества B. При этих условиях класс F имеет базис тогда и только тогда, когда $G \subset [B]$ или каждая функция из G содержится в некоторой ограниченной максимальной цепи множества G относительно $\preceq_B$.*

Доказательство. Множество всех функций из G, являющихся верхними гранями ограниченных максимальных цепей множества G, обозначим $\mathfrak{B}$.

Необходимость. Пусть $\mathfrak{A}$ — базис класса F. Если $G \subset [B]$, то необходимость доказана. Пусть $G \not\subset [B]$. Для каждой функции $f \in \mathfrak{A}$ зафиксируем некоторую формулу Υ_f над $G \cup B$, реализующую функцию f. Пусть Φ — произвольная формула над $\mathfrak{A}$. Заменим в формуле Φ каждую из функций базиса $\mathfrak{A}$ на соответствующую ей формулу над $G \cup B$. Полученную формулу над $G \cup B$ обозначим через $\pi(\Phi)$.

Пусть $f \in \mathfrak{A}$. Положим $G_f = [\mathfrak{A}\backslash\{f\}]_B$. Обозначим через $\mathfrak{A}_B$ множество функций f из $\mathfrak{A}$, для которых выполняется соотношение $B \subset [\mathfrak{A}\backslash\{f\}]$. Пусть $f \in \mathfrak{A}_B$. Поскольку множество $\mathfrak{A}$ является базисом, то выполняется соотно-

шение $f \notin G_f$. Легко видеть, что существует функция $g \in \Theta(\Upsilon_f)$, такая, что $g \notin G_f$. Пусть $g \in G$, $g \notin G_f$, Ψ — произвольная формула над $\mathfrak{A}$, реализующая функцию g. Очевидно, что $f \in \Theta(\Psi)$. Положим $G_0 = \cup\Theta(\Upsilon_f)$, где объединение берется по всем функциям f из множества $\mathfrak{A}\backslash\mathfrak{A}_B$. Нетрудно показать, что множества $\mathfrak{A}\backslash\mathfrak{A}_B$ и G_0 конечны.

Рассмотрим функцию $f \in \mathfrak{A}_B$ и формулу Υ_f над $G \cup B$. Используя свойство $(**)_B$ можно показать, что если $g_1 \in \Theta(\Upsilon_f)\backslash\mathfrak{B}$, то функция g_1 принадлежит множеству G_f. Отсюда следует, что существует функция $g \in \mathfrak{B} \cap \Theta(\Upsilon_f)$, такая, что $g \notin G_f$.

Покажем, что любая функция h из G лежит в некоторой ограниченной максимальной цепи множества G. Если $h \in [G_0] \cap G$ и для любой фукнции $h_1 \in G$, такой, что $h \preceq_B h_1$ выполняется соотношение $h_1 \in [G_0] \cap G$, то нетрудно видеть, что функция h содержится в некоторой ограниченной максимальной цепи множества G.

Пусть теперь $h \in G\backslash[G_0]$ (в случае если $h \in [G_0] \cap G$ и существует функция $h_1 \in G\backslash[G_0]$, такая, что $h \preceq h_1$, рассуждения аналогичны с заменой функции h_1 на h). Рассмотрим произвольную формулу Ψ над $\mathfrak{A}$, реализующую функцию h. Используя свойство $(*)_B$, можно показать, что существуют функции $f \in \mathfrak{A}_B$, $h_1 \in G$, такие, что $h \preceq_B h_1$, $f \in \Theta(\Psi)$, $h_1 \in \Theta(\Upsilon_f)$.

Поскольку $f \in [\mathfrak{A}]_B$, то как показано выше, для функции f существует функция $g \in \mathfrak{B}$, такая, что $g \notin G_f$ и $g \in \Theta(\Upsilon_f)$. Пусть Φ — некоторая формула над $\mathfrak{A}$, реализующая функцию g. Так как $g \notin G_f$, то выполняется соотношение $f \in \Theta(\Phi)$. Поскольку $f \in \Theta(\Psi)$, $g \in \Theta(\Upsilon_f)$, то $g \in \Theta(\pi(\Psi))$, а значит, $h \trianglelefteq_A g$. Кроме того, поскольку $f \in \Theta(\Phi)$ и $h_1 \in \Theta(\Upsilon_f)$, то $h_1 \in \Theta(\pi(\Phi))$, и следовательно, $g \trianglelefteq_A h_1$. В силу свойства $(**)_B$ и соотношения $h \preceq_B h_1$ получаем, что выполняется по крайней мере одно из неравенств: $h \preceq_B g$, $g \preceq_B h_1$. Если $h \preceq_B g$, то функция h содержится в некоторой ограниченной максимальной цепи множества G. Если же $g \preceq_B h_1$, то в силу того, что $g \in \mathfrak{B}$, получаем соотношение $h_1 \sim_B g$. Следовательно, функция h содержится в некоторой ограниченной максимальной цепи.

Достаточность. Обозначим через $\widehat{B}$ множество функций из B, таких, что $[B] \subset [\widehat{B} \cup \mathfrak{B}]$, а для любого $C \subset \widehat{B}$, $C \neq \widehat{B}$, аналогичное вложение не выполняется: $[B] \not\subset [C \cup \mathfrak{B}]$. Поскольку $\mathfrak{B} \cup \widehat{B} \subset G$, то $[\mathfrak{B} \cup \widehat{B}] \subset [G]$. Так как каждая функция из G содержится в некоторой ограниченной максимальной цепи множества G, то $G \subset [\mathfrak{B}]_{\widehat{B}} = [\mathfrak{B} \cup \widehat{B}]$. Следовательно, $F = [\mathfrak{B} \cup \widehat{B}]$.

Покажем, что для любой функции $g \in \mathfrak{B} \cup \widehat{B}$ выполняется соотношение $g \notin [(\mathfrak{B} \cup \widehat{B})\backslash\{g\}]$. Из определения множества $\widehat{B}$ следует, что для любой функции $g \in \widehat{B}$ выполняется соотношение $g \notin [(\mathfrak{B} \cup \widehat{B})\backslash\{g\}]$. Пусть $g \in [(\mathfrak{B} \cup \widehat{B})\backslash\{g\}]$ для некоторой $g \in \mathfrak{B}$. Тогда $g \in [\mathfrak{B}\backslash\{g\}]_B$. Поскольку $\mathfrak{B} \subset A$ и множество A обладает свойством $(*)_B$, то существует функция $f \in \mathfrak{B}\backslash\{g\}$, такая, что $g \in [\{f\}]_B$, то есть $g \preceq_B f$. В силу того, что множество G состоит из попарно неэквивалентных относительно множества B функций, выполняется соотношение $g \not\sim_B f$. Поэтому $g \prec_B f$. Полученное соотношение

противоречит тому, что g является верхней гранью ограниченной максимальной цепи множества G. Поэтому $g \notin [\mathfrak{B} \cup \widehat{B} \backslash \{g\}]$. Таким образом, множество $\mathfrak{B} \cup \widehat{B}$ является базисом класса F. **Теорема доказана.**

Данное научное исследование (проект № 14-01-0144) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014/2015 гг.

Список литературы

[1] Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

[2] Михайлович А. В. О замкнутых классах функций многозначной логики, порожденных симметрическими функциями // Математические вопросы кибернетики. Выпуск 18. — М.: Физматлит, 2013. — С. 123–212.

[3] Михайлович А. В. О замкнутых классах трехзначной логики, порожденных системами, содержащими симметрические функции // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2012. — № 1. — С. 58–62.

О равенстве чисел P_4-упаковки и P_4-покрытия в графах

Мокеев Дмитрий Борисович

Нижегородский Государственный Университет им. Н. И. Лобачевского; НИУ Высшая Школа Экономики в Нижнем Новгороде, e-mail: MokeevDB@gmail.com

Введение

Пусть $\mathcal{F}$ — множество графов. Максимальное число попарно непересекающихся порожденных подграфов графа G, принадлежащих $\mathcal{F}$, называется *числом $\mathcal{F}$-упаковки* графа G. Минимальное число вершин графа G, покрывающее все порожденные подграфы из $\mathcal{F}$ называется его *числом $\mathcal{F}$-покрытия*. *Кёниговым графом относительно $\mathcal{F}$* называется граф, каждый порожденный подграф которого обладает свойством: число $\mathcal{F}$-упаковки равно числу $\mathcal{F}$-покрытия. Класс всех кёниговых графов относительно множества $\mathcal{F}$ обозначаем через $\mathcal{K}(\mathcal{F})$. Если $\mathcal{F}$ состоит из единственного графа H, то будем говорить об H-упаковках и т. п.

Задаче об упаковке графа посвящено немало работ, особенно её алгоритмическим аспектам (см., например, [1, 2]). Известно, что задача поиска числа H-упаковки NP-полна для любого графа H, имеющего компоненту связности с тремя или более вершинами. Будучи сформулированы как задачи ЦЛП, задачи об $\mathcal{F}$-упаковке и $\mathcal{F}$-покрытии образуют пару двойственных задач. Кёниговы графы, таким образом, суть графы, у которых для любого порождённого подграфа отсутствует разрыв двойственности, что способствует эффективному решению этих задач для таких графов.

Класс $\mathcal{K}(\mathcal{F})$ при любом $\mathcal{F}$ является наследственным и, следовательно, может быть описан множеством запрещенных графов (минимальных по отношению

«быть порожденным подграфом» графов, не принадлежащих $\mathcal{F}$). Для P_2 такую характеризацию даёт теорема Кёнига вместе с известным критерием двудольности. Кроме этой классической теоремы автору известны следующие результаты такого рода для обыкновенных графов: в [3] эта задача решена для класса $\mathcal{K}(P_3)$; в [4] — для класса $\mathcal{K}(\mathcal{C})$, где $\mathcal{C}$ — множество всех простых циклов.

Цель настоящей работы — охарактеризовать класс графов $\mathcal{K}(P_4)$. Применяется два подхода к описанию этого класса. Один из них — конструктивный: показано, как можно построить графы данного класса с помощью процедуры расширенного подразбиения. Второй подход — стандартное описание наследственного класса запрещёнными подграфами.

Далее под кёниговым графом подразумеваем кёнигов граф относительно P_4. Рассматривая цикл C_n, предполагаем, что его вершины пронумерованы вдоль цикла числами $0, 1, \ldots, n-1$. Каждый класс вычетов номеров вершин по модулю 4 называем 4-классом.

Расширенные подразбиения двудольных графов

Будем называть связный граф G P_4-*связным*, если его дополнение связно и через каждую его вершину проходит хотя бы один порождённый 4-путь.

Лемма 1. *Граф является кёниговым тогда и только тогда, когда каждый его максимальный по включению P_4-связный подграф кёнигов.*

Операция замены кографом вершины x состоит в следующем: эта вершина удаляется из графа; к графу добавляются несколько новых вершин, и каждая из них соединяется ребром с каждой вершиной, смежной x в исходном графе; новые вершины соединены между собой так, что образуют кограф.

Назовём путь графа *висячим*, если степень одной из его вершин 1, а остальных — не более 2. Смежной вершиной висячего пути назовём вершину графа, смежную одной из вершин пути, но ему не принадлежащую (если такая имеется, то она единственная).

Операция замены кографом висячего пути из 3 вершин, смежного вершине y состоит следующем: вершины этого пути удаляются из графа; к графу добавляется несколько новых вершин, соединённых между собой так, что образуют кограф; новые вершины соединены с вершиной y так, чтобы максимальный путь, содержащий y и добавленные вершины имел длину 3.

Операция замены кографом висячего пути из 2 вершин смежного вершине y состоит в следующем: вершины этого пути удаляются из графа; к графу добавляются вершины $k_1, k_2, \ldots, k_p$, которые соединены попарно между собой и соединены с y; к графу добавляются вершины $l_1, l_2, \ldots, l_{p-1}$ и, быть может, l_p, причём $N(l_i) = \{k_1, k_2, \ldots, k_i\}$; каждую вершину из множества $\{y, k_1, \ldots, k_p, l_1, \ldots, l_p\}$ можно заменить кографом произвольной структуры.

Пусть H — двудольный граф. Каждое ребро этого графа, принадлежащее какому-нибудь циклу, подразобьём одной вершиной. Заменим произвольными кографами некоторые вершины степени 1 и 2, при этом если в цикле графа H есть вершина v, смежная с 3 и более вершинами степени больше 1, то вершины 4-класса, содержащего v, не могут быть заменены кографами, а так

же если в цикле графа H есть вершина v степени 3 и более, то вершина 4-класса, содержащего v и вершина 4-класса, содержащего вершину, отстоящую на расстоянии 2 от v, не могут быть заменены кографами одновременно. Последним шагом заменим кографами некоторые висячие пути из 2 и 3 вершин. Полученный таким образом граф будем называть *расширенным подразбиением* исходного двудольного графа.

Запрещённые графы

Обозначим $\mathcal{A}$ множество графов и дополнений графов, полученных из цикла длины кратной 4 добавлением двух вершин, не смежных между собой, каждая из которых соединяется ребром с одной вершиной цикла, причём расстояние между добавленными вершинами нечётно.

Обозначим $\mathcal{B}$ множество графов и дополнений графов, полученных из цикла длины кратной 4 добавлением висячего пути длины 2, смежного с вершиной с номером 0 и заменой кографом из двух вершин вершины цикла с номером $4k, k \in \mathbb{N}$, а так же полученных из цикла длины кратной 4 добавлением вершины, смежной с вершиной с номером 0 и заменой кографами из двух вершин вершин цикла с номерами $4k, k \in \mathbb{N}$ и $4l + 2, l \in \mathbb{N} \cup \{0\}$.

Обозначим $\mathcal{C}$ множество циклов и их дополнений с числом вершин не менее 5 и не кратным 4.

Обозначим $\mathcal{D}$ множество графов и дополнений графов, полученных из цикла длины $k_1 + k_2 + k_3 + k_4$ заменой кографами из двух вершин вершин с номерами $0, k_1, k_1 + k_2, k_1 + k_2 + k_3$, причём $k_1 \equiv k_2 \equiv k_3 \equiv k_4 \equiv 1 \pmod 4$, $k_i \geq 5$, $i = 2, 3, 4$ или $k_1 \equiv 1 \pmod 4$, $k_1 \geq 5$, $k_2 \equiv k_4 \equiv 2 \pmod 4$, $k_3 \equiv 3 \pmod 4$.

Обозначим $\mathcal{E}$ множество минимальных запрещённых графов из 6 и 7 вершин, не входящих в $\mathcal{A} \cup \mathcal{C}$. Таких графов ровно 64.

Теорема 1. *P_4-связный граф является кёниговым тогда и только тогда, когда может быть получен расширенным подразбиением двудольного графа и не содержит порождённых подграфов из множества $\mathcal{D}$.*

Теорема 2. *Графы множества $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C} \cup \mathcal{D} \cup \mathcal{E}$ составляют множество минимальных запрещённых графов для класса $\mathcal{K}(P_4)$.*

Работа выполнена при финансовой поддержке лаборатории ЛАТАС, НИУ ВШЭ (грант правительства ag. 11.G34.31.0057); РФФИ, проект № 14-01-00515-а).

Список литературы

[1] Hell P. Graph packing // Electronic Notes in Discrete Mathematics. — 2000. — V. 5. — P. 170–173.

[2] Yuster R. Combinatorial and computational aspects of graph packing and graph decomposition // Computer Science Review. — 2007. — V. 1. — P. 12–26.

[3] Алексеев В. Е., Мокеев Д. Б. Кёниговы графы относительно 3-пути // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 4. — С. 3–14.

[4] Ding G., Xu Z., Zang W. Packing cycles in graphs, II // J. Comb. Theory. B. — 2003. — V. 87. — P. 244–253.

О пересечениях предполных классов монотонных функций в четырехзначной логике

Нагорный Александр Степанович

Московский государственный университет имени М. В. Ломоносова, e-mail: anagorny@list.ru

Введение

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$ и пусть P_k есть множество всех конечноместных функций на E_k. Элементы множества P_k будем называть функциями k-значной логики. Определения используемых ниже операции суперпозиции, понятий замыкания и замкнутого класса можно найти в [1]. Замкнутый (относительно суперпозиции) класс H функций k-значной логики назовем *предполным* в P_k, если $H \neq P_k$, но для любой функции k-значной логики f, не принадлежащей классу H, замыкание множества $H \cup \{f\}$ совпадает с P_k.

Известно, что при любом $k \geqslant 2$ все классы функций k-значной логики, монотонных относительно некоторого частичного порядка на E_k с наименьшим и наибольшим элементами (т. н. *ограниченный частичный порядок*), являются замкнутыми и предполными в P_k [2]. Обозначим семейство всех таких классов через **M(k)**. Очевидно, имеется ровно 1, 3 и 18 классов в семействе **M(k)** при k, равном 2, 3 и 4, соответственно.

Рассмотрим всевозможные пересечения классов из **M(k)**. Ясно, что при каждом k такие (попарно различные как классы функций) пересечения образуют нижнюю полурешетку (по вложению), т. н. *решетку пересечений* M^k, максимальными элементами которой являются сами предполные классы из **M(k)**, а в роли наименьшего элемента выступает пересечение всех классов из **M(k)** (оно содержит только константы и селекторные функции).

Легко видеть, что решетка M^2 тривиальна и имеет глубину 0, а элементами решетки M^3 являются все 7 возможных пересечений, и она имеет глубину 2 (это следует, например, из результатов, опубликованных автором в [3]). Однако, уже при $k = 4$ решетку M^k построить существенно сложнее, поскольку многие из пересечений классов из **M(4)** равны как множества функций. Отметим также, что из диссертационного исследования [4] (утверждения 1.30, 1.36) вытекает, что глубина M^4 не больше 9. Целью данной работы как раз является построение решетки M^4 пересечений классов из **M(4)** и, в частности, нахождение точного значения глубины этой решетки.

Обозначим через M_{abcd} и $M_{a\{bc\}d}$ классы функций четырехзначной логики, монотонных относительно линейного порядка $a < b < c < d$ и относительно частичного порядка $a < b < d, a < c < d$ (элементы b и c несравнимы), соответственно. Учитывая, что инверсные ограниченные порядки задают один и тот же предполный класс, а не инверсные — различные классы [2], имеем 12 классов первого типа и 6 классов второго типа. Других классов семейство **M(4)**, очевидно, не содержит.

Пусть класс K является пересечением n предполных в P_4 классов из семейства **M(4)**, где $1 \leq n \leq 18$. *Каноническим видом* класса K (относительно

семейства **M(4)**) назовем множество $\chi(K)$ тех и только тех предполных классов из **M(4)**, в которых K содержится целиком. Ясно, что задача построения решетки M^4 эквивалентна задаче нахождения всех возможных канонических видов пересечений классов из **M(4)**.

Основные результаты

Пусть π — произвольная перестановка на E_4, f — функция четырехзначной логики, зависящая от n переменных.

Функцию $f^*(x_1, x_2, \ldots, x_n) = \pi^{-1}(f(\pi(x_1), \pi(x_2), \ldots, \pi(x_n)))$ назовем *двойственной к функции* f относительно перестановки π.

Классы функций K_1 и K_2 ($K_1, K_2 \subseteq P_4$) назовем *двойственными* (друг другу), если существует перестановка π на множестве E_4 такая, что класс K_2 состоит из всех функций, двойственных функциям из K_1 относительно π, и только из них.

Следующая теорема является основным результатом работы.

Теорема 1. *Решетка пересечений* M^4 *содержит в точности* 399 *узлов и* 1258 *дуг и имеет глубину* 6. *Из них ровно* 31 *узлов соответствуют попарно недвойственным классам — пересечениям* K*, их канонические виды* $\chi(K)$ *и кратности (числа двойственных классов)* $n(K)$ *перечислены ниже. Полный список всех возможных канонических видов можно размещен в [5].*

	$\chi(K)$	$n(K)$		$\chi(K)$	$n(K)$
1	M_{0123}	12	2	$M_{0\{12\}3}$	6
3	$M_{0123}M_{1230}$	12	4	$M_{0123}M_{2130}$	24
5	$M_{0123}M_{3201}$	12	6	$M_{0123}M_{0\{12\}3}$	12
7	$M_{0123}M_{2\{13\}0}$	24	8	$M_{0\{12\}3}M_{2\{13\}0}$	12
9	$M_{0\{12\}3}M_{2\{30\}1}$	3	10	$M_{0123}M_{1230}M_{0\{12\}3}$	24
11	$M_{0123}M_{1230}M_{2\{13\}0}$	12	12	$M_{0123}M_{2130}M_{2\{13\}0}$	24
13	$M_{0123}M_{3201}M_{0\{12\}3}$	24	14	$M_{0123}M_{0213}M_{0\{12\}3}$	6
15	$M_{0123}M_{0\{12\}3}M_{2\{13\}0}$	24	16	$M_{0\{12\}3}M_{2\{13\}0}M_{2\{01\}3}$	4
17	$M_{0123}M_{1230}M_{0\{12\}3}M_{1\{32\}0}$	12	18	$M_{0123}M_{2130}M_{0132}M_{2\{13\}0}$	24
19	$M_{0123}M_{3201}M_{2301}M_{0132}$	3	20	$M_{0123}M_{3201}M_{0\{12\}3}M_{3\{02\}1}$	12

	$\chi(K)$	$n(K)$
21	$M_{0123}M_{1230}M_{2130}M_{0213}M_{0\{12\}3}$	12
22	$M_{0123}M_{1230}M_{0\{12\}3}M_{1\{32\}0}M_{3\{02\}1}$	12
23	$M_{0123}M_{3201}M_{2301}M_{0132}M_{0\{12\}3}$	12
24	$M_{0123}M_{1230}M_{2130}M_{0213}M_{0\{12\}3}M_{2\{13\}0}$	24
25	$M_{0123}M_{3201}M_{2301}M_{0132}M_{0\{12\}3}M_{2\{13\}0}$	12
26	$M_{0123}M_{3201}M_{2301}M_{0132}M_{0\{12\}3}M_{2\{30\}1}$	6
27	$M_{0123}M_{1230}M_{2130}M_{3012}M_{3021}M_{0213}M_{0\{12\}3}$	6
28	$M_{0123}M_{3201}M_{2301}M_{0132}M_{0\{12\}3}M_{2\{13\}0}M_{2\{30\}1}$	12
29	$M_{0123}M_{1230}M_{2130}M_{1320}M_{0213}M_{0132}M_{0\{12\}3}M_{2\{13\}0}M_{1\{32\}0}$	4
30	$M_{0123}M_{1230}M_{2130}M_{3012}M_{3021}M_{0213}M_{0\{12\}3}M_{2\{13\}0}M_{2\{01\}3}$	12
31	$M_{0123}M_{1230}\ldots M_{2\{01\}3}$ (все 18 классов из M(4))	1

Как видим, среди всех $2^{18} - 1 = 262\ 143$ пересечений 18 классов из **M(4)** всего лишь 399 классов являются попарно различными, что составляет менее двух десятых процента от общего числа классов.

Работа выполнена при поддержке РФФИ (проект № 13-01-00958-а).

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986. — 384 с.

[2] Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. — 1960. — № 3. — С. 49–60.

[3] Нагорный А. С. О распределении трехзначных функций по предполным классам // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — № 3. — С. 45–52.

[4] Нагорный А. С. О пересечениях и объединениях предполных классов многозначной логики : дис. на соискание ученой степени канд. физ.-мат. наук : 01.01.09 : защищена 07.06.13 : утв. 21.10.13 / Нагорный Александр Степанович. — Москва, 2013. — 162 с. — Библиогр. : с. 158–162.

[5] Нагорный А. С. Пересечения предполных классов монотонных функций в четырехзначной логике // (http://goo.gl/OINsfj), 2015. [Электронный ресурс].

Оптимизация решения задачи об изоморфизме графов

Назаров Максим Николаевич

Московский институт электронной техники, e-mail: Nazarov-Maximilian@yandex.ru

Напомним, что в своей классической постановке задача о проверке на изоморфизм двух графов относится к классу NP. Таким образом, полиномиальные алгоритмы для решения данной задачи либо являются вероятностными, либо известны только для достаточно узких классов графов (например для деревьев). На практике задача об изоморфизме в классической постановке почти никогда не решается, а гораздо большее распространение получили различные способы обхода проблемы за счёт специального представления графов в памяти. Примером реализации данной идеи является переход от графа G к его канонической форме $\mathrm{Canon}(G)$ (см. примеры в [1]). Главное преимущество канонических форм заключается в том, что два графа изоморфны $G_1 \cong G_2$ тогда и только тогда, когда совпадают их канонические формы $\mathrm{Canon}(G_1) = \mathrm{Canon}(G_2)$. В результате, если в памяти хранятся не сами графы, а их канонические формы, то проверка на изоморфизм для них становится полиномиальной задачей.

В рамках работы [2] был разработан ещё один вариант для описания классов изоморфных графов — линейная нотация $I[G]$, и позиционирован как альтернатива канонической форме $\mathrm{Canon}(G)$ для хранения графов. Построение линейной нотации $I[G]$ в статье [2] проводится с помощью алгоритма для

однозначной натуральной индексации классов автоморфизма вершин $I(\overline{v})$ и рёбер $I(\overline{u,v})$ произвольного графа G на основе его макси-кода (см. рис. 1).

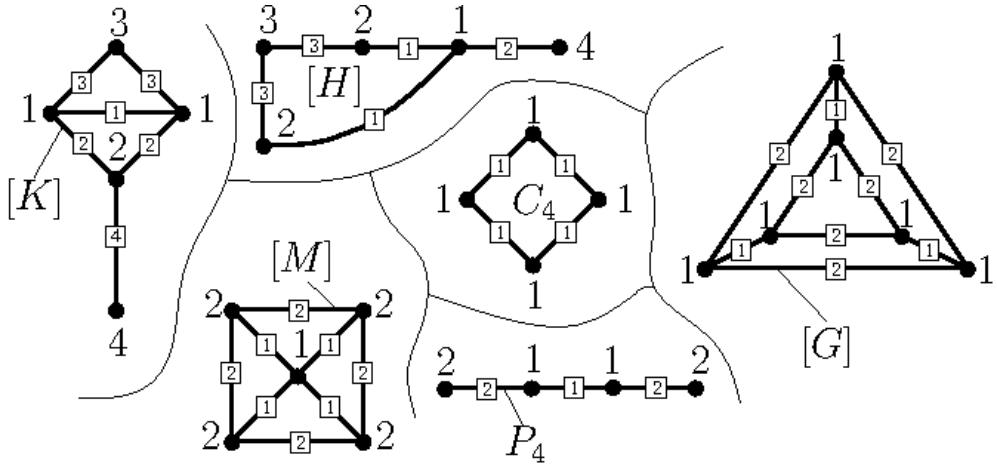

Рис. 1. Пример графов с метками вершин $I(\overline{v})$ и рёбер $I(\overline{u,v})$.

Определение 1. *Симметрическая линейная нотация* $\mathfrak{L}(G)$ для графа G — это строка символов, которая определяется на основе четырёх правил:

Правило 1. Строка $\mathfrak{L}(G)$ начинается с вершины v первого индекса $I(v) = 1$.

Правило 2. Для всех вершин $u \in V(G)$ в нотацию $\mathfrak{L}(G)$ вместе с вершиной u обязательно вводится её окружение в виде записи: $u[\overset{i_1}{\rightarrow} \ldots ; \overset{i_2}{\rightarrow} \ldots ; \overset{i_k}{\rightarrow} \ldots]$, где $i_1, i_2, \ldots, i_k$ — это индексы классов симметрии рёбер. При этом, в пределах скобок $u[\overset{i_1}{\rightarrow} \ldots ; \overset{i_2}{\rightarrow} \ldots ; \overset{i_k}{\rightarrow} \ldots]$ *ровно один раз* должны быть учтены все вершины из окружения u и все рёбра $\overset{i}{\rightarrow}$, которые их связывают.

Правило 3. При повторном появлении на последующих уровнях вложенных скобок $[\ldots[\ldots]\ldots]$ уже встречавшихся вершин u вместо них будут использоваться специальные символы $\#1, \#2, \#3, \ldots, \#m$. Обозначение $\#1$ будет задавать вершину v перед первой скобкой [в нотации $\mathfrak{L}(G)$, а запись $\#2$ будет означать вершину перед второй скобкой, и так далее до вершины $\#m$.

Правило 4. Для каждой вершины u при выборе в какой последовательности записывать в скобках $u[\ldots;\ldots;\ldots]$ вершины $\overset{i_1}{\rightarrow} v_1\ldots$, $\overset{i_2}{\rightarrow} v_2\ldots$ и специальные символы $\overset{i}{\rightarrow} \#m$ из окружения вершины u действуют приоритеты:

1. Наиболее приоритетным является код $\#1$, затем код $\#2$, и так далее до последнего уровня вложенности $\#m$.
2. После кодов $\#m$ по приоритетам идут вершины с наименьшими индексами классов симметрии $I(\overline{v^*})$.
3. Если у двух вершин совпадают индексы $I(\overline{v_1}) = I(\overline{v_2})$, то более приоритетной будет избрана такая вершина v_1, у которой будет меньше индекс симметрии ребра, соединяющего её с u, то есть $I(\overline{u,v_1}) < I(\overline{u,v_2})$.

4. При совпадении индексов вершин и рёбер предпочтение будет отдано вершине, которая ближе** на графе G к вершине кода $\#1$. Если эти расстояния совпадают — то ближе к вершине кода $\#2$, и так далее.

Определение 2. *Линейной нотацией абстрактного графа* $[G]$ назовём такую строку $I[G]$, которая получается из любой произвольной симметрической линейной нотации $\mathfrak{L}(G)$ путём замены всех вершин v на индексы классов симметрии $I(\overline{v})$.

Для примеров классов изоморфных графов, которые изображены на рис. 1, мы можем составить следующие линейные нотации.

$$I[K] = 1\left[\xrightarrow{1} 1\left[\xrightarrow{2} 2\left[\xrightarrow{2} \#1;\ \xrightarrow{4} 4[\,]\right];\ \xrightarrow{3} 3\left[\xrightarrow{3} \#1\right]\right]\right],$$

$$I[H] = 1\left[\xrightarrow{1} 2\left[\xrightarrow{3} 3\left[\xrightarrow{3} 2\left[\xrightarrow{1} \#1\right]\right]\right];\ \xrightarrow{2} 4[\,]\right],$$

$$I[M] = 1\left[\xrightarrow{1} 2\left[\xrightarrow{2} 2\left[\xrightarrow{1} \#1;\ \xrightarrow{2} 2\left[\xrightarrow{1} \#1;\ \xrightarrow{2} 2\left[\xrightarrow{1} \#1;\ \xrightarrow{2} \#2\right]\right]\right]\right]\right],$$

$$I[C_4] = 1\left[\xrightarrow{1} 1\left[\xrightarrow{1} 1\left[\xrightarrow{1} 1\left[\xrightarrow{1} \#1\right]\right]\right]\right], \quad I[P_4] = 1\left[\xrightarrow{1} 1\left[\xrightarrow{2} 2\,[\,]\right];\ \xrightarrow{2} 2[\,]\right],$$

$$I[G] = 1\left[\xrightarrow{1} 1\left[\xrightarrow{2} 1\left[\xrightarrow{1} 1\left[\xrightarrow{2} \#1;\ \xrightarrow{2} 1\left[\xrightarrow{2} \#1;\ \xrightarrow{1} 1\left[\xrightarrow{2} \#2;\ \xrightarrow{2} \#3\right]\right]\right]\right]\right]\right].$$

Основной идей при построении линейной нотации $I[G]$ в рамках статьи [2] было получение универсального описания для классов изоморфных графов, которое давало бы одновременно простое и наглядное представление всех вершинных и рёберных автоморфизмов графа. Побочной задачей было упрощение визуализации графа с изображением максимального количества автоморфизмов в виде симметричного расположения вершин и рёбер графа. Фактически данные задачи были успешно решены, и в рамках работы [2] было доказано, что $I[G]$ будет полным инвариантом графа.

Список литературы

[1] Katebi H., Sakallah K., Markov I. L. Graph Symmetry Detection and Canonical Labeling: Differences and Synergies // Proc. Turing-100, EPIC. — 2012. — V. 10. — P. 181–195.

[2] Назаров М. Н. Альтернативные подходы к описанию классов изоморфных графов // Прикладная дискретная математика. — 2014. — № 3. — С. 86–97.

Логико-термальная эквивалентность схем программ с динамической памятью

Новикова Татьяна Анатольевна[1], **Захаров Владимир Анатольевич**[2]

[1] Казахстанский филиал МГУ имени М. В. Ломоносова, e-mail: tanian.cmc@gmail.com

[2] Московский государственный университет имени М. В. Ломоносова, e-mail: zakh@cs.msu.su

Одной из важных задач статического анализа программного кода является проверка эквивалентности фрагментов программ. Эта задача часто используется для рефакторинга программ (см. [1]), при построении суперкомпиляторов и

**Близость понимается в смысле существования пути с минимальным количеством вершин, который соединяет эти две вершины.

в других областях программирования. Логико-термальная эквивалентность (л-т эквивалентность) программ — это разрешимое неинтерпретационное отношение программ, которое при этом является корректным, т. е. из л-т эквивалентности программ следует их функциональная эквивалентность. Логико-термальная эквивалентность была впервые введена в работе [2]. Ранее в статье [3] нами был предложен полиномиальный алгоритм ее проверки, использующий операции композиции и антиунификации термов.

В данной работе мы рассмотрим возможность использования методов, предложенных в работе [3] для проверки л-т эквивалентности программ с динамической памятью.

Рассмотрим конечный алфавит, состоящий из множества функциональных символов $F = \{f_1^{(n_1)}, \ldots, f_m^{(n_m)}\}$, множества предикатных символов $P = \{P_1^{(k_1)}, \ldots, P_\ell^{(k_\ell)}\}$ и множества Var переменных. Над этими множествами стандартным образом вводятся множество термов $Term(Var, F)$ и множество подстановок $Subst(Var, F, Var)$.

Расширим эти понятия таким образом, чтобы мы могли иметь дело с переменными, имеющими указательный тип. Для этого необходимо ввести дополнительные операторы: оператор *выделения памяти* : `x = malloc`; оператор *высвобождения памяти*: `x = free`; оператор *взятия адреса переменной*: `&x`; оператор *разыменования указателя*: `*x`.

Выражениями разыменования или разыменованиями будем называть всевозможные выражения, построенные из переменных и оператора разыменования. Множество всех разыменований над множеством переменных Var обозначим $DE(Var)$. Адресными выражениями будем называть множество $AE(Var)$ выражений вида `&x`, где $x \in DE(Var)$.

Тогда, по аналогии с понятием множества термов,введем расширенное множество термов $ETerm(Var, F)$ — наименьшее множество, удовлетворяющее трем условиям: 1) $Var \subseteq ETerm(Var, F)$; 2) $DE(Var) \subseteq ETerm(Var, F)$; 3) если $f^{(n)} \in F$ и $t_1, \ldots, t_n \in ETerm(Var, F)$, то $f^{(n)}(t_1, \ldots, t_n) \in ETerm(Var, F)$.

Выражение вида $e = t$, где $e \in DE(Var)$, $t \in AE(Var) \cup ETerm(Var)$, будем называть расширенным присваиванием.

Работа с динамической памятью в последовательных императивных программах подразумевает наличие особого типа переменных — указателей. Условимся считать, что память для этого класса переменных выделяется в «куче» и будем в дальнейшем называть такие переменные динамическими или переменными в динамической памяти.

Рассмотрим бесконечное множество $Heap = \{m_1, m_2, \ldots, m_i, \ldots\}$ переменных в динамической памяти. Будем считать, что кроме них в динамической памяти присутствуют специальная константа $NULL$ и константа $\perp$ (неопределенное значение). Тогда расширенной подстановкой мы назовем отображение $\Theta : Var \cup Heap \to Term(Var) \cup AE(Var \cup Heap) \cup \{NULL, \perp\}$. При этом будем считать, что у всех переменных из кучи начальное значение равно

$NULL$, оно может быть изменено в результате присваивания этой переменной какого-либо другого значения.

Множество всех расширенных подстановок над множеством переменных Var, множеством динамических переменных $Heap$ и функциональных символов F обозначим $ESubst(Var, Heap, F)$.

Для каждого расширенного присваивания вида $e = t$ и подстановки $\Theta \in FESubst(Var, Heap, F)$ введем операцию применения присваивания к подстановке $update(\Theta, e, t)$. Эта операция состоит из трех шагов.

На первом шаге осуществляется упрощение левой части присваивания, выражения-разыменования e, в контексте подстановки Θ. Иными словами, для таким образом введенных указателей, справедливы соотношения: $*(\&e) = e$, $\&(*e) = e$, тогда упрощение выражения сводится к последовательному применению этих соотношений. Если в результате упрощения получено адресное выражение или разыменование некой переменной, значение которой не является адресом, то процедура упрощения завершается с ошибкой $ERROR$. Если упрощение прошло успешно, то в результате получено выражение e'.

Следующий шаг процедуры $update(\Theta, e, t)$ заключается в последовательном упрощении всех выражений-разыменований, входящих в состав терма t. Так же, как и на предыдущем шаге, будем считать, что упрощение закончилось с ошибкой, если в результате получился терм, содержащий адреса или разыменования неадресных переменных. Полученное в результате этого шага выражение назовем t'.

На последнем шаге происходит применение связки $\{e'/t'\}$ к подстановке Θ.

Аналогичные процедуры описываются также для операций вида `x = malloc`, `x = free`.

Заметим, что процедура $update(\Theta, e, t)$ выполняется за время, линейное относительно размеров подстановки Θ.

Кроме того, над множеством расширенных подстановок вводится операция антиунификации $\Theta_1 \downarrow \Theta_2$. Отметим, что эта операция легко применима к расширенным подстановкам, представленным в виде ациклических ориентированных графов.

Для введенных над расширенными подстановками операций антиунификации $\Theta_1 \downarrow \Theta_2$ и $update(\Theta, e, t)$ справедливо следующее утверждение:

Теорема 1. $update(\Theta_1, e, t) \downarrow update(\Theta_2, e, t) = update(\Theta_1 \downarrow \Theta_2, e, t)$.

Указанное свойство расширенных подстановок позволяет использовать их в качестве альтернативы для операций композиции и антиунификации простых подстановок в алгоритме, предложенном в статье [3]. С учетом этого, справедлива следующая теорема:

Теорема 2. *Существует алгоритм проверки логико-термальной эквивалентности программ с динамической памятью, работающий за полиномиальное время.*

Список литературы

[1] Фаулер М. Рефакторинг. Улучшение существующего кода. — М.: Символ-Плюс, 2008. — 432 с.

[2] Иткин В. Э. Логико-термальная эквивалентность схем программ // Кибернетика. — 1972. — № 1. — С. 5–27.

[3] Новикова Т. А., Захаров В. А. Полиномиальный по времени алгоритм проверки логико-термальной эквивалентности программ // Труды института системного программирования РАН. — 2012. — Т. 22 — С. 435–455.

[4] Костылев Е. В., Захаров В. А. О сложности задачи антиунификации // Дискретная математика. — 2008. — Т. 20, № 5. — С. 131–144.

Оценки периода полиномиальной рекуррентной последовательности

Парватов Николай Георгиевич[1], **Алексеева Дарья Владимировна**[2]

[1] Томский государственный университет, e-mail: parvatov@mail.tsu.ru
[2] Томский государственный университет, e-mail: alekseevad@gmail.com

Рассматриваются полиномиальные рекуррентные последовательности над конечными алгебраическими структурами. Приводятся верхние оценки периода для полиномиальных рекуррентных последовательностей над примарным кольцом классов вычетов.

Рекуррентные последовательности

Пусть m — целое положительное число, p — простое и $f_1, \ldots, f_n$ — целочисленные многочлены от n переменных. Обозначим через $s(f, m, x)$ рекуррентную последовательность

$$f^0(x) + p^m Z^n, f^1(x) + p^m Z^n, f^2(x) + p^m Z^n, \ldots,$$

где Z — кольцо целых чисел, $x \in Z^n$, $f(x) = (f_1(x), \ldots, f_n(x))$, $f^0(x) = x$ и $f^k(x) = f(f^{k-1}(x))$ для $k > 0$.

Пусть $d > 0$. Последовательность называется *периодической с периодом* d, если выполняется равенство $f^0(x) = f^d(x)$; обозначим $\tau(f, m, x)$ наименьший период в этом случае. Функцию f назовём *периодической по модулю* p^m, если указанная последовательность периодична при любом выборе x (и тогда функция f определяет подстановку по модулю p^m).

Полиномиальные подстановки рассматривались в ряде работ [1,2,3]. В том числе в [1] установлены условия периодичности. В [1,2] описаны транзитивные (одноцикловые) полиномиальные подстановки, существующие только при $n = 1$. В [3] найдены возможные длины периодов полиномов одной переменной над кольцом Галуа. Этот результат обобщается далее для полиномиальных вектор-функций от n переменных над примарным кольцом классов вычетов.

Именно, устанавливается верхняя оценка длины периода $\tau(f, m, x)$ при условии, что последовательность $s(f, m, y)$ периодична для любого набора y из смежного класса $x + pZ^n$.

Условия периодичности и оценка периода

Обозначим через M_n кольцо целочисленных квадратных матриц размера n с единичной матрицей E, через $det(A)$ — определитель матрицы A и через $ord_p(A)$ — порядок обратимой матрицы по модулю p, то есть наименьшее положительное k, при котором $A^k \equiv E \mod pM_n$, существующее, если $det(A) \not\equiv 0 \mod pZ$. Положим

$$D_f(x) = \begin{pmatrix} \frac{d f_1}{dx_1}(x) & \cdots & \frac{d f_n}{dx_1}(x) \\ \vdots & & \vdots \\ \frac{d f_1}{dx_n}(x) & \cdots & \frac{d f_n}{dx_n}(x) \end{pmatrix}$$

и $D_f^\tau(x) = D_f(f^0(x)) \cdots D_f(f^{\tau-1}(x))$ для любого положительного τ. Матрица $D_f(x)$ называется *матрицей Якоби* функции f в точке x.

Следующая теорема даёт условия периодичности и верхние оценки для периода полиномиальной рекуррентной последовательности.

Теорема. *Пусть последовательность $s(f, 1, x)$ периодична с наименьшим периодом $\tau_1 = \tau(f, 1, x)$ и $m > 1$.*

Имеют место следующие свойства.

1. *Последовательность $s(f, m, y)$ периодична для любого набора y из смежного класса $x + pZ^n$ тогда и только тогда, когда $det_p(D_f^{\tau_1}(x)) \mod pZ \neq 0$.*
2. *Пусть $det_p(D_f^{\tau_1}(x)) \mod pZ \neq 0$. Тогда для любого набора y из $x + pZ^n$ имеет место следующее соотношение для периода:*

$$\tau(f, m, y) | \tau_1 \cdot p^{m-1} \cdot ord_p(D_f^{\tau_1}(x)).$$

3. *Если ещё и $det_p(D_f^{\tau_1}(x) - E) \mod pZ \neq 0$, то для любого y из $x + pZ^n$ выполняется соотношение:*

$$\tau(f, m, y) | \tau_1 \cdot p^{m-2} \cdot ord_p(D_f^{\tau_1}(x)).$$

Свойства, сформулированные выше для последовательностей над кольцом классов вычетов по приматрному модулю, допускают обобщение на случай произвольного конечного коммутативного кольца с единицей.

Список литературы

[1] Анашин В. С. Равномерно распределенные последовательности целых p-адических чисел. Дискретная математика. — 2002. — Т. 14, № 4. — С. 3–64.

[2] Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов. Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 20–32.

[3] Ермилов Д. М., Козлитин О. А., Цикловая структура полиномиального генератора над кольцом Галуа. Математические вопросы криптографии. — 2013 — Т. 4, № 1. — С. 27–57.

Многокритериальная оптимизация на гиперграфах с нечеткими весами в управлении земельными ресурсами сельскохозяйственного предприятия

Перепелица Виталий Афанасьевич, Заховалко Татьяна Викторовна, Максишко Наталия Константиновна

Запорожский национальный университет, e-mail: perepel2@yandex.ru, tvz_99@mail.ru, maxishko@ukr.net

Предприятие в рыночной экономике выступает агентом как на рынке готовой продукции, так и на рынке производственных ресурсов. В условиях обострения кризисных явлений в экономике проблематика эффективного использования экономических ресурсов (природных, людских и произведенных человеком), которые используются сельскохозяйственным предприятием, становится все более актуальной. Для управления такими предприятиями разрабатываются и внедряются в практику хозяйствования современные информационные системы и технологии (в частности, [1]). Их функционирование, с одной стороны, создает возможности для практического применения богатого инструментария математического моделирования, с другой стороны — в результате сотрудничества с фирмами, входящими в сеть “1С:Франчайзинг”, является источником постановки новых задач, решение которых позволяет получать экономический эффект.

Исследованию одной из задач, возникающих при обосновании оптимального плана производства продукции растениеводства с учетом использования земельных ресурсов и технологических способов внесения минеральных удобрений, посвящена данная работа.

Для адекватного отображения в системном единстве сложной организации внутренних взаимосвязей моделируемой системы будем использовать аппарат гиперграфов, который наряду с классическими теоретико-графовыми подходами является мощным средством моделирования задач управления дискретными процессами и системами [2–4].

Для построения модели рассмотрим 3-дольный гиперграф $G = (V_1, V_2, V_3, E)$, где $V_1 = \{v_1^1, v_2^1, ...v_k^1, ..., v_m^1\}$, $V_2 = \{v_1^2, v_2^2, ...v_i^2, ..., v_n^2\}$, $V_3 = \{v_1^3, v_2^3, ...v_j^3, ..., v_{n_3}^3\}$. Содержательно данная модель описывает задачу землепользования, в которой вершины первой доли V_1 соответствуют номерам сельскохозяйственных культур, которые выращиваются в хозяйстве. Вершины второй доли V_2 соответствуют возделываемым полям, а вершины третьей доли V_3 — порциям удобрений.

Множество $E = \{e\}$ состоит из ребер $e = (v_k^1, v_i^2, v_j^3)$, где $v_k^1 \in V_1$, $v_i^2 \in V_2$, $v_j^3 \in V_3$. Наличие ребра $e = (v_k^1, v_i^2, v_j^3)$ означает, что поле i может быть отведено под культуру k и при этом для пары i, k по технологии необходимо внести порцию удобрения j. Из содержательной постановки очевидно, что для мощностей долей гиперграфа G выполняются условия: $m \leq n$, $n_3 \leq n$. Без

потери общности будем считать, что доли V_2 и V_3 являются равномощными ($|V_2| = |V_3| = n$), так как этого можно добиться введением дополнительных (фиктивных) вершин в соответствующую долю. Следовательно, можно считать, что гиперграф $G = (V_1, V_2, V_3, E)$ является 3-однородным.

Звездой гиперграфа $G = (V_1, V_2, V_3, E)$ будем называть его связную часть $z = (V_z, E_z)$, в которой любая пара ребер $e_1, e_2 \in E_z$ пересекается в одной и той же вершине $v_0 \in V_z$ и не пересекается ни в одной другой вершине $v \neq v_0$. При этом вершину v_0 будем называть центром звезды z, а число ребер $|E_z|$ — её степенью.

Пусть задано множество типовых звезд $T = \{z_k, k = \overline{1,m}\}$, причем каждая звезда z_k имеет степень $q_k, k = \overline{1,m}$.

Для заданных натуральных чисел $q_k, k = \overline{1,m}$, таких, что $\sum\limits_{k=1}^{m} q_k = n$, допустимым решением (покрытием трехдольного 3-однородного гиперграфа $G = (V_1, V_2, V_3, E)$ звездами) $z_k \in T, k = \overline{1,m}$, является любой его остовный подгиперграф $x = (V_1, V_2, V_3, E_x)$, который состоит из m компонент связности, каждая из которых является звездой с центром в одной из вершин первой доли V_1, при этом звезда с центром $V_k^1 \in V_1$ имеет степень, равную $q_k, 1 \leq k \leq m$.

Множество всех допустимых решений (МДР) обозначим через $X = X(G) = \{x\}$.

Заметим, что рассматриваемая модель является модификацией известной задачи землепользования [5], которая учитывает как неопределенность результатов хозяйствования (данных), так и неоднозначность целей. Неопределенность данных в модели учитывается посредством введения нечеткой меры для задания значений показателей, характеризующих результат процесса земледелия. Неоднозначность цели приводит к многокритериальной постановке задачи и необходимости использования методов многокритериальной оптимизации на гиперграфе.

В данной модели каждому ребру $e \in E$ гиперграфа $G = (V_1, V_2, V_3, E)$ поставим в соответствие пару нечетких чисел $(R-L)$-типа [6]

$$w_l(e) = \{(w_l, \mu(w_l)\}; \;\; \mu(w_l) = \begin{cases} L(\frac{a_l - w_l}{\alpha_{el}}) \\ R(\frac{w_l - a_{el}}{\beta_{el}}) \end{cases}; \; l = 1, 2,$$

где w_l — возможное значение показателя, который является оценкой экономического, экологического и др. результата. Например, значение урожайности культуры, уровень загрязнения почвы, изменение ее плодородности и т. п, которые ожидаются в случае размещения культуры k, на поле i при условии внесения в грунт j-й порции удобрения; $\mu(w_l)$ — функция принадлежности значения w_l (урожайности, плодородности) нечеткому числу $w_l(e)$; a_e — мода нечеткого числа $w(e)$; α_e, β_e — коэффициенты его нечеткости. Функции R-типа и L-типа определяются на основании результатов прогнозирования экономической эффективности и экологического эффекта в условиях неопределенности и неустойчивости условий хозяйствования на основе ретроспективных данных. Вес ребра гиперграфа как нечеткое число обозначим $w(e) = (a_{el}, \alpha_{el}, \beta_{el})$.

Для учета неоднозначности целей на МДР $X = X(G) = \{x\}$ определим векторную целевую функцию (ВЦФ) $F(z) = (F_1(x), F_2(x))$, которая содержит критерии типа MAXSUM и MINMAX:

$$F_1(x) = w_1(x) \to max,\ F_2(x) = maxw_2(x) \to min$$

где $w_1(x)$ — вес допустимого решения $x = (V_1, V_2, V_3, E_x)$, который определяет экономический эффект и равен сумме весов всех входящих в него ребер. На основании определения операции сложения нечетких чисел $(R-L)$-типа вес допустимого решения является также нечетким числом $(R-L)$-типа:

$$w_l(x) = \sum_{e \in E_x} w_l(e) = (a_{lx}, \alpha_{lx}, \beta_{lx}),\ a_{1x} = \sum_{e \in E_x} a_{e1},\ \alpha_{lx} = \sum_{e \in E_x} \alpha_{e1},\ \beta_{lx} = \sum_{e \in E_x} \beta_{e1};$$

$maxw_2(x)$ — наихудшее значение, например, экологического показателя (уровня загрязнения почвы, ухудшения ее плодородности), который отражает хозяйственные риски. Построенная экономико-математическая модель управления ресурсами сельскохозяйственного предприятия позволяет учитывать неопределенность условий и направлена на повышение эффективности хозяйствования. Построение метода выбора эффективного (парето-оптимального) решения базируется на методах многокритериального анализа, а также процедуре сравнения нечетких чисел, основанной на использовании индекса ранжирования.

Список литературы

[1] 1С:Управление сельскохозяйственным предприятием. — Официальный сайт компании “1С” ABBYY. [Электронный ресурс]. — Режим доступа: http://1c.abbyy.ua/solutions/agroholding/

[2] Gross J. L., Yellen J. Graph Theory and Its Applications — К.: CRC Press, 2006. — 800 с.

[3] Voloshin V. Introduction to Graph and Hypergraph Theory. — Nova Science Publishers, Inc., 2009.

[4] Омельченко Г. Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности : дис. канд. физ.-мат. наук. — Черкесск, 2004. — 161 с.

[5] Максишко Н. К., Заховалко Т. В. Моделі та методи розв’язання прикладних задач покриття на графах та гіперграфах : монографія / Наук. ред. проф. В. О. Перепелиця. — Запоріжжя: Поліграф, 2009. — 244 с.

[6] Павлов А. Н. Принятие решений в условиях нечеткой информации — СПб.: ГУАП, 2006. — 72 с.

Fuzzy transform as a universal tool for image processing

Perfilieva Irina

University of Ostrava, Centre of Excellence IT4Innovations, e-mail: irina.perfilieva@osu.cz

1. Introduction

Fuzzy modeling is still regarded as a modern technique with a non-classical background. The goal of this contribution is to bridge standard mathematical methods and methods for construction of fuzzy approximation models. We discuss the theory of the *fuzzy transform* (the *F-transform*), which was introduced with the purpose of encompassing both classical (usually, integral) transforms and approximation models based on fuzzy IF-THEN rules (*fuzzy approximation models*). We start with an informal characterization of integral transforms, and from this discussion, we examine the similarities and differences among integral transforms, the F-transform and fuzzy approximation models.

An integral transform is performed using some kernel. The kernel can be characterized as a "collection of local factors" or closeness areas around elements of an original space. The F-transform is associated with a kernel that consists of a collection of fuzzy subsets (local factors or closeness areas around chosen "nodes") of an original space. We say that this collection establishes a "fuzzy partition" of the space. Similar to integral transforms, the F-transform assigns an average value of a transforming object to each fuzzy subset from the fuzzy partition of the space.

Similar to conventional integral transforms (e. g., the Fourier and Laplace transforms), the F-transform performs a transformation of an original universe of functions into a universe of their "skeleton models" (sequences of F-transform components) for which further computations are easier. In this respect, the F-transform can be as useful in applications as traditional transforms (see applications to image compression, image fusion, image reconstruction, and time series processing, for example). Moreover, sometimes the F-transform can be more efficient than its counterparts; see the details below.

2. Fuzzy Transform

The F-transform establishes a correspondence between a set of square integrable functions on a real interval $[a, b]$ (i. e. $L_2(a, b)$) and the set of finite/infinite dimensional (real) vectors. Interval $[a, b]$ is a space with fuzzy equivalence, determined by generating function $a\colon [-1, 1] \to [0, 1]$, such that a is even, bell-shaped and vanishing at boundaries. Generating function determines a kernel function, the latter determines a fuzzy partition of $[a, b]$.

If a fuzzy partition of $[a, b]$ is fixed, then the F-transform of $f \in L_2[a, b]$ is a sequence of components, each one is an orthogonal projection on a finite dimensional Hilbert space, spanned by orthogonal polynomials. The orthogonality is considered with respect to a weighted inner product, where the weight given by a certain element of the fuzzy partition.

The main theorem about reconstruction from a sequence of F-transform components is below.

Theorem. *Let signal $x \in L_2(\mathbb{R})$ be continuous and band-limited, i.e. $\widehat{x}(\omega) = 0$ for $|\omega| > \Omega$ where Ω is some constant. Let $h = \frac{\pi}{\Omega}$, $a\colon \mathbb{R} \to [0,1]$ be a generating function, and $H > h/2$ a scale factor. Let the set of translations $\{a_{H,k},\, k \in \mathbb{Z}\}$, where $a_{H,k}(s) = a_H(t_k - s)$, establish a (h,H)-*uniform fuzzy partition *of $\mathbb{R}$ with nodes $t_k = k \cdot h$, $k \in \mathbb{Z}$, so that the sequence $\{X_k,\, k \in \mathbb{Z}\}$ consists of the corresponding F-transform components of x. Let finally $\widehat{a}_H(\omega) \neq 0$, for all $\omega \in [-\Omega, \Omega]$.*

Then x can be determined by its F-transform components so that

$$x(t) = \frac{H\pi}{\Omega} \sum_{k=-\infty}^{\infty} X_k \cdot b_H(t - t_k),$$

where

$$X_k = X(t_k) = \frac{1}{H} \int_{-\infty}^{\infty} a_{H,k}(s) \cdot x(s)\, ds,$$

and $b_H \in L_2(\mathbb{R})$ is the function whose Fourier transform is equal to

$$\widehat{b}_H(\omega) = \frac{\mathbf{1}_{[-\Omega,\Omega]}}{\widehat{a}_H(\omega)}.$$

3. Applications

In this Section, we consider applications of the F-transform to image processing.

3.1. Image Compression and Reconstruction

The F-transform of 2D images is a natural lossy compression technique. We combine the F-transform with the quadtree technique and obtain the efficient compression method that is comparable and in many cases, is more advantageous than the JPEG compression.

3.2. Image Fusion

Image fusion aims to integrate complementary distorted multisensor, multitemporal and/or multiview scenes into one new image that contains the “best” parts of each scene. Thus, the primary problem in image fusion is to find the least distorted scene for every pixel.

The idea of the F-transform approach to image fusion consists in a combination of (at least) two fusion operators. The first operator is applied to the F-transform components of a scene, while the second one is applied to the residuals with respect to the inverse F-transform. Although this approach is not explicitly based on focus measures, it uses the fusion operator, which is able to choose an undistorted scene among the available blurred ones.

3.3. F-transform based edge detector

Edge detection is inevitable in image processing. In particular, it is a first step in feature extraction and image segmentation. For gray scale images, an edge is used

to be described as a part of an image with a *sharp change* in intensity. This is not a definition, but a vague characterization of a certain area around every pixel.

We focus on the Canny edge detector, which is widely used in computer vision. It was developed to ensure three basic criteria, good detection, good localization, and minimal response. We propose to apply the F-transform with linear components in order to simplify the first two steps of the Canny algorithm.

The reason is that the F-transform with linear components filters out noise when computing approximate values of the first partial derivatives.

Acknowledgment

This work is supported by the European Regional Development Fund in the IT4Innovations Centre of Excellence project (CZ.1.05/1.1.00/02.0070).

References

[1] Perfilieva I. Fuzzy transforms: Theory and applications // Fuzzy Sets and Systems. — 2006. — 157. — P. 993–1023.

[2] Perfilieva I., Daňková M., Bede B. Towards a higher degree F-transform // Fuzzy Sets and Systems. — 2011. — 180. — P. 3–19.

[3] Di Martino F., Loia V., Perfilieva I., Sessa S. An image coding/decoding method based on direct and inverse fuzzy transforms // International Journal of Appr. reasoning. — 2008. — 48. — P. 110–131.

[4] Perfilieva I., Hodáková P., Hurtík P. Differentiation by the F-transform and Application to Edge Detection // Fuzzy Sets and Systems. — To appear.

Шефферовы операции в алгебрах унарных мультиопераций

Перязев Николай Алексеевич

Санкт-Петербургский государственный электротехнический университет, e-mail: nikolai.baikal@gmail.com

Отображение из A в множество всех подмножеств A называется унарной мультиоперацией на A. Для множества всех унарных мультиопераций на A используем обозначение M_A^1.

Мультиоперации $f \in M_A^1$ на множестве $A = \{a_0, ..., a_{k-1}\}$ можно представлять как отображения

$$f : \{2^0, 2^1, ..., 2^{k-1}\} \to \{0, 1, ..., 2^k - 1\},$$

получаемые из f при кодировании

$$a_i \to 2^i; \quad \varnothing \to 0; \quad \{a_{i_1}, ..., a_{i_s}\} \to 2^{i_1} + ... + 2^{i_s}.$$

При этом унарную мультиоперацию f задаем векторной формой $(\alpha_0, ..., \alpha_{k-1})$, где $f(a_i) = \alpha_i$.

Пусть $S \subseteq M_A^1$. Алгебра $\mathfrak{F} =< S; *, \cap, \mu, \varepsilon, \theta, \pi >$ типа $\langle 2, 2, 1, 0, 0, 0\rangle$ с ниже определенными операциями подстановки $(f * g)$, пересечения $(f \cap g)$, обратимости (μf) и нульместными операциями ε, θ, π называется *алгеброй унарных мультиопераций* над A:

$(f * g)(a) = \{b \mid$ существует $c \in g(a)$ такой, что $b \in f(c)\}$;
$(f \cap g)(a) = f(a) \cap g(a)$;
$(\mu f)(a) = \{b \mid a \in f(b)\}$;
$\varepsilon(a) = \{a\}$;
$\theta(a) = \varnothing$;
$\pi(a) = A$.

Мощность множества A называется рангом алгебры.

Алгебры унарных мультиопераций введены в [1], где приведены результаты для алгебр рангов 2 и 3.

Мультиоперация в алгебре называется шефферовой, если она порождает всю алгебру. В наибольшей алгебре унарных мультиопераций ранга 2 шефферовых мультиопераций нет, а ранга 3 таких мультиопераций 12: (243), (251), (253), (413), (452), (453), (612), (613), (641), (643), (651), (652).

Для произвольных рангов получен следующий результат.

Теорема 1. *Наибольшая алгебра унарных мультиопераций любого ранга не менее 3 содержит шефферовы мультиоперации.*

Доказательство. Пусть ранг алгебры унарных мультиопераций равен k ($k \geq 3$). Покажем, что $g = (2^{k-2} + 2^{k-1}, 1, 2, ..., 2^{k-2})$ является шефферовой в наибольшей алгебре унарных мультиопераций.

Проведем следующие вычисления.

$(\mu g) = (2, 4, ..., 2^{k-2}, 1 + 2^{k-1}, 1)$;

$(2, 4, ..., 1 + 2^{k-1}, 1)^{k-1} = (1 + 2^{k-1}, 1 + 2, 2 + 4, ..., 2^{k-3} + 2^{k-2}, 2^{k-2})$;

$(2, 4, ..., 1 + 2^{k-1}, 1)^{2(k-1)} =$

$= (1 + 2^{k-2} + 2^{k-1}, 1 + 2 + 2^{k-1}, 1 + 2 + 4, ..., 2^{k-4} + 2^{k-3} + 2^{k-2}, 2^{k-3} + 2^{k-2})$;

$(2, 4, ..., 1 + 2^{k-1}, 1)^{(k-1)^2} =$

$= (1 + 2 + ... + 2^{k-1}, 1 + 2 + ... + 2^{k-1}, ..., 1 + 2 + ...2^{k-1}, 1 + 2 + ... + 2^{k-2})$.

Так как для любого s выполняется $1 + 2 + ... + 2^{s-1} = 2^s - 1$, то получаем:

$(2, 4, ..., 1 + 2^{k-1}, 1)^{(k-1)^2} = (2^k - 1, 2^k - 1, ..., 2^k - 1, 2^{k-1} - 1)$.

Отметим, что $g \cap (\mu g)^{k-1} = (2^{k-1}, 1, 2, ..., 2^{k-2})$.

Введем обозначения:

$p = (2^{k-1}, 1, 2, ..., 2^{k-2})$;

$d_{i,\alpha} = (\alpha_0, ..., \alpha_{k-1})$, где $\alpha_i = \alpha, \alpha_j = 2^k - 1, i \neq j$.

Подстановкой вычисленных мультиопераций $d_{k-1,2^{k-1}-1}$ и p можно получить все $d_{i,2^{k-1}-1}$, где $i = 0, ..., k-1$. А учитывая, что $(\mu d_{i,2^k-1-2^j}) = d_{j,2^k-1-2^i}$, то можно получить и все $d_{i,2^k-1-2^j}$, где $i, j = 0, ..., k-1$.

Теперь любую мультиоперацию можно представить как пересечение некоторого числа мультиопераций $d_{i,2^k-1-2^j}$. Этим доказали, что мультиоперация $g = (2^{k-2} + 2^{k-1}, 1, 2, ..., 2^{k-2})$ шефферова. Заметим, что мы так же показали шефферовость мультиоперации $(\mu g) = (2, 4, ..., 2^{k-2}, 1 + 2^{k-1}, 1)$.

Теорема 1 доказана.

Так как все операции алгебры унарных мультиопераций выразимы в суперклонах и множество всех унарных мультиопераций в супеклоне порождает наибольший суперклон [2], то верно следующее утверждение.

Следствие. *Наибольший суперклон любого ранга не менее 3 содержит шефферовы унарные мультиоперации.*

Список литературы

[1] Казимиров А. С., Перязев Н. А. Алгебры унарных мультиопераций // Тезисы докладов международной конференции Мальцевские чтения, Новосибирский государственный университет, 2013. — С. 156.

[2] Перязев Н. А. Стандартные формы мультиопераций в суперклонах // Известия Иркутского государственного ун-та. Серия: Математика. — 2010.— Т. 3, № 4. — С. 88–95.

Свойства графов-обструкций для тора

Петренюк Владимир Ильич[1], **Петренюк Анатолий Яковлевич**[2], **Донец Георгий Афанасьевич**[3]

[1] Кировоградский национальный технический университет, e-mail: petrenjukvi@rambler.ru
[2] Кировоградский национальный технический университет, e-mail: ptrnklp@mail.ru
[3] Институт кибернетики Национальной академии наук Украины, e-mail: g_donets@mail.ru

Задача состоит в следующем: 1) установление структурных свойств 8-ми или 9-ти вершинных графов-обструкций для тора, пригодных для построения n-вершинных, $n > 9$, графов-обструкций для тора; 2) проверка гипотезы о том, что графы-обструкции для тора на 8-ми или 9-ти вершинах, у которых каждое ребро существенно относительно рода при операции удаления ребра, являются результатом отождествления некоторых подмножеств множества точек двух графов G_i, гомеоморфных либо K_5, либо $K_{3,3}$, либо этим графам без одного ребра, а граф G_2 — суперзвезда $St_{n,m}(G)$ с n висячими рёбрами-лучами и m лучами-треугольниками, исходящими из вершин центра звезды графа G. Известно, что 8-ми вершинных неизоморфных графов-обструкций рода 2 известно три графа [1], [2], а 9-ти вершинных — 63, из которых 51 граф приведён в [3]. Согласно [4], построение графов-обструкций может осуществляться на основе двух указанных графов G_i с множествами M_i точек, т. е. либо вершин, либо внутренних точек рёбер, соединённых рёбрами (v_1, v_2) с концевыми вершинами в M_i, $i = 1, 2$, которые подлежат сжатию. По меньшей мере два ребра (v_1, v_2) стянуты в точку. В качестве числовой оценки свойств этих множеств M_i из указанных выше графов G_i используются числа достижимости $t_{G_i}(M_i)$, являющиеся наименьшими числами клеток тора, на границах которых расположены все элементы множества M_i, при всевозможных различных вложениях графов G_i в тор, $i = 1, 2$. Обозначим через $krt_G(M_i)$, где $i = 1, 2$, наибольшее число звёзд $St(v_j)$ с центром в вершине v_j графа G и $|M_i|$ висячими рёбрами-лучами, присоединенными к элементам множества точек M_i графа G, и вложенных 2-клеточно в различные клетки графа G, вложенного

минимально в тор. Под двусторонним доступом понимаем число $ms_G(M_i)$, $i = 1, 2$, как наибольшее число звёзд $St(v_j)$ с центром в вершине v_j графа G и $|M_i|$ висячими рёбрами-лучами, присоединенными к элементам множества точек M_i графа G, и вложенных 2-клеточно в одну клетку графа G, вложенного минимально в тор.

Лемма. *Пусть граф G является φ-образом графов-обструкций G_i, $i = 1, 2$, при φ-преобразовании, определённом следующим образом: $\varphi(G_1 + G_2, \sum\limits_{i=1}^{2}(e_1 \underset{\bullet}{+} e_2)) \to (G, e)$, где $e = (a, b)$, $e \in G^1$, $e_i = (a_i, b_i)$ — либо ребро, либо часть ребра графа G_i, $i = 1, 2$. Имеют место следующие утверждения:* 1) *Если по меньшей мере одна концевая вершина ребра $e_i = (a_i, b_i)$ не имеет двустороннего доступа, то граф G является графом-обструкцией рода $\gamma(G) = \gamma(G_1) + \gamma(G_2)$.* 2) *Если каждая концевая вершина ребра $e_i = (a_i, b_i)$, $i = 1, 2$, имеет двусторонний доступ, то граф G не является графом-обструкцией, и выполняется равенство $\gamma(G) = \gamma(G_1) + \gamma(G_2) - 1$.*

Для иллюстрации к лемме приведём следующее: 1) граф, полученный из двух копий графа K_5 при отождествлении пары рёбер имеет род 1; 2) граф, полученный из двух копий графа K_5 при отождествлении пары, состоящей из ребра и части ребра, имеет род 2.

Структура 8-ми вершинных графов-обструкций для тора

Под квазизвездою $St_{n_1,n_2,n_3}(G_1)$ с центром-графом G_1 будем понимать объединение графа G_1, $G_1 = (\{v_i\}_{i=1}^3)$, с тремя звёздами $St_{n_i}(v_i)$ и висячими вершинами $\{g_{ij}\}_{j=1}^{n_i}$ и висячими рёбрами в количестве n_i, без общих рёбер, с центральными вершинами v_i, порождающими подграф G_1 графа G. Будем называть треугольным лучом квазизвезды граф K_3, образованный из одного ребра графа G_1 и двух смежных ему рёбер $St_{n_1,n_2,n_3}(G_1)\backslash G_1$ с общей вершиной степени 2.

Теорема 1. *Неизоморфных графов-обструкций для тора известно три подграфа графа K_8: B_i, $i = 1, 2, 3$.*

Доказательство приведено в [1], [2] и в полном варианте этой статьи.

Следствие. *Для каждого B_i имеют место следующие φ-преобразования:* 1) $\varphi(K_5 + \sum\limits_{j=1}^{3} St_5(j), \sum\limits_{j=1}^{3}\sum\limits_{i=1}^{5} a_i \underset{\bullet}{+} g_{ji}) \to (B_1, \{\{a_i^*\}_1^5\})$, $M_1 = \{a_i\}_1^5$, $t_{K_5}(M_1) = 1$, $M_2 = \{\{g_{ji}\}_1^5\}_1^3$, *где* $krt_{K_5}(\{a_i\}_1^5) = 3$, $\sum\limits_{j=1}^{3} St_5(j)$ — *квазизвезда с центром из трёх несмежных между собой вершин j, каждая из которых имеет по пять висячих ребер $\{\{g_{ji}\}_1^5\}_1^3$, отождествляющихся с a_i, $i = \overline{1,5}$;* 2) $\varphi(K_5 + St_{1,4}(K_5 - e), \sum\limits_{i=1}^{5} a_5 \underset{\bullet}{+} g_5) \to (B_2, \{\{a_i^*\}_1^5\})$, $M_1 = \{a_i\}_1^5$ — *множество вершин графа K_5,* $t_{K_5-e}(M_1) = 1$, $M_2 = \{\{g_i\}_1^5\}$, *где* $ms_{K_5}(\{a_i\}_1^5) = 4$, $St_{1,4}(K_5 - e)$ — *квазизвезда с центром $K_5 - e$;* 3) $\varphi(K_5 + St_3(K_5), \sum\limits_{i=1}^{5} a_5 \underset{\bullet}{+} g_5) \to (B_3, \{\{a_i^*\}_1^5\})$, $M_1 = \{a_i\}_1^5$ — *множество вер-*

шин графа K_5, $t_{K_5}(M_1) = 1$, $M_2 = \{\{g_i\}_1^5\}$, *где* $ms_{K_5}(\{a_i\}_1^3) = 2$, $St_3(K_5)$ — *квазизвезда с центром* K_5.

Вывод. В зависимости от значений характеристик $ms_{K_5}(M_1)$, $krt_{K_5}(M_1)$ множества M_1 вершин графа K_5, граф-обструкция порядка 8 является φ-образом графа K_5 и графа H, где H является одним из следующих графов: 1) объединение трёх одинаковых звёзд с несмежными центрами и пятью лучами, 2) квазизвезда с центром-графом K_3 и тремя треугольными лучами с двумя висячими лучами, подлежащими сжатию в точку, 3) квазизвезда с центром-графом K_3 и пятью лучами, два из которых подлежат сжатию в точку.

Структура 9-ти вершинных графов-обструкций для тора

Изучим структурные свойства 9-ти вершинных графов-обструкций для тора с целью установления свойств, пригодных для построения n-вершинных, $n > 9$, графов-обструкций для тора. Граф называется t-минимальным рода g, если число достижимости множества вершин этого графа равно t, а, при удалении или сжатии в точку произвольного ребра число достижимости множества вершин полученного графа меньше t либо род полученного графа меньше g. Например, граф $K_6 \backslash K_3^1$ — 2-минимальный рода 1, т. е. или это $K_{3,3}$ с дополнительными тремя рёбрами на вершинах одной из долей, или это граф $K_5 \backslash e$ с дополнительной вершиной степени 3, соединённой рёбрами с тремя вершинами графа $K_5 \backslash e$, образовывающими множество с числом достижимости 2.

Теорема 2. *Для* D_4, D_5, D_6, D_7 — 9*-вершинных графов-обструкций для тора — имеют место следующие* φ*-преобразования:* 1) $K_{4,5} \backslash u = D_4$, *причём* D_4 *изоморфен либо графу* E_{18}, *либо графу* $\varphi(K_{3,3} + K, \sum\limits_{i=1}^{6} (i^{'} \underset{\bullet}{+} i^{''})) \to (D_4, \{i\}_1^6)$, *где* $K = (\{i''\}_{i=1}^6 \cup \{a, b, c\}, K_{2,3}^1 \cup \{(a, 2''), \{(b, j'')\}_{j=4}^6\})$. 2) $K_{3,3}^0 = \{i'\}_{i=1}^6$, $St_{3(2)}(K_{2,3}) \cup St_3(9) = \{i''\}_{i=1}^6 \cup \{7, 8\}$, *где* $St_3^0(9) = \{i''\}_{i=1}^3$, *причём* D_5 *содержит подграфы, изоморфные либо графу* E_3, *либо графу* E_{18}, *приведенным в списке графов-обструкций для проективной плоскости* [5]. 3) $(K_5 + St_{1(4)}(K_4), \sum\limits_{i=1}^{4} (i^{'} \underset{\bullet}{+} i^{''})) \to (D_6, \{\{i\}_{i=1}^4)$, *где* $St_{1(4)}^0(K_4) = \{i''\}_{i=1}^4 \cup K_4^0$. 4) $\varphi(K_5 + St_{1,1,1(2)}(K_4), \sum\limits_{i=1}^{3} (i^{'} \underset{\bullet}{+} i^{''})) \to (D_7, \{i\}_{i=1}^3)$, $K_5^0 = \{i'\}_{i=1}^5$, *где* $St_{1,1,1(2)}^0(K_4) = \{i''\}_{i=1}^3 \cup K_4^0$.

Доказательство носит конструктивный характер и приведено в полном варианте этой статьи.

Теорема 3. D_{26} — 9*-вершинная граф-обструкция для тора — не является* φ*-образом двух графов* G_i, *гомеоморфных либо* K_5, *либо* $K_{3,3}$, *либо этим графам без одного ребра, выполненного путём отождествления некоторых подмножеств множества их точек.*

Доказательство. Граф D_{26} имеет подграфы K_5 и K_4 с одной общей вершиной v, являющейся внутренней точкой ребра графа K_5, у которого имеется треугольник K_3, каждая вершина v_i которого соединена парой рёбер $(v_i, u_{i_1}), (v_i, u_{i_2})$ с одной из различных пар вершин u_{i_j}, $j = 1, 2$, $i = 1, 2, 3$ из графа $K_4 - v$. Под-

граф H, $H = K_4 \bigcup K_3$, графа D_{26} вместе с тремя парами рёбер $(v_i, u_{i_1}), (v_i, u_{i_2})$, $i = 1, 2, 3$, негомеоморфен ни одному из упомянутых в условии графам. Отметим наличие части графа H, гомеоморфной $K_5 - e$. **Теорема 3 доказана.**

Вывод. Несмотря на то, что большинство 9-вершинных графов допускает подобное представление, подтверждающее упомянутую выше гипотезу, имеются некоторые графы, например D_{26}, для которых гипотеза неверна.

Список литературы

[1] Duke R. A., Haggard G.The genus subgraphs K_8 // Israel J. Math. —1972. — V. 11. — P. 452–455.

[2] Brown T., Duke R. An irreducible graph consisting a single block // Journal Math. and Mech. — 1966. — V. 15, N 1. — P. 129–135.

[3] Suhjin Hur. B. The Kuratowski covering conjecture for graphs of order less than 10 // Ohio State University PhD dissertation : online, 2008. — P. 1–346.

[4] Петренюк В. И. Построение графов-обструкций ограниченного ориентируемого рода // Сборник трудов XVI Международной конференции «Проблемы теоретической кибернетики». 20–25 июня 2011 г. — Нижний Новгород, 2011. — С. 452–455.

[5] Archdeacon D. A. A Kuratowski theorem for the projective plane // Journal of Graph Theory —1981. — V. 5. — P. 243–246.

Полнота динамики значений свойств данных в СУБД DIM

Петров Алексей Николаевич[1], **Рублев Вадим Сергеевич**[2]

[1] Ярославский государственный университет им. П. Г. Демидова, e-mail: axel_petroff@mail.ru

[2] Ярославский государственный университет им. П. Г. Демидова, e-mail: roublev@mail.ru

Объектная СУБД DIM

В связи с тем, что имеющиеся технологии СУБД несовершенны, это позволило поставить задачу разработки нового объектного подхода к созданию СУБД, который предполагает не только изменение данных объектов, но и возможность изменения типов объектов, т. е. схемы базы данных. В этом подходе мы выделили 6 базовых отношений объектов: *наследования*, *включения*, *внутреннего наследования*, *внутреннего включения*, *истории* и *взаимодействия* и назвали эту СУБД *динамической информационной моделью* (DIM), а также разработали объектный язык запросов ODQL и другие языки для описания динамики данных. Введение новой технологии СУБД требует обоснования полноты описания данных и полноты динамики данных этой модели. Последнее связано с точным описанием предметной области, вернее с созданием ее математической модели, которую мы назвали OD-моделью.

Работа [1] посвящена обоснованию полноты статического описания данных в СУБД DIM. При этом OD-модель не уточнялась для описания алгоритмических процедур, связанных с динамикой данных. Такого описания предметной

области было вполне достаточно, чтобы для любого статического среза данных произвольной OD-модели построить отображение в данные СУБД DIM, адекватно отражающие свойства и связи объектов OD-модели. Данная работа является продолжением работы [1] и ее цель состоит в обосновании полноты динамики данных СУБД DIM. Поэтому необходимо, во-первых, уточнить описание OD-модели в части алгоритмических процедур изменения данных этой модели. Во-вторых, необходимо описать отношения взаимодействия и истории, которые являются аналогами средств изменения данных в СУБД DIM и темпоральных связей таких данных. И, в-третьих, построить отображение произвольной алгоритмической процедуры OD-модели во взаимодействие DIM, при котором сохраняются все свойства отображений двух статических срезов данных: перед выполнением алгоритмической процедуры и после ее выполнения.

Объектно-динамическая модель

В [1] под OD-моделью понималась одиннадцатка

$$(O, A, \overline{A}(o), V(o), L_p, L_o, L_f, \overline{A}_{L_f}(o_l^j), V_{L_f}(o_l^j), F, T), \tag{1}$$

однако, такая форма описывает только статичное состояние объектов модели в опеределённый момент времени. Расширим модель, дополнив ее динамически детерминированными законами взаимодействия объектов.

Обозначим через $F^{'}$ конечное множество алгоритмических процедур, определяющих динамику изменения свойств-атрибутов объектов модели. При выполнении любой $f \in F^{'}$ из которых в некоторый момент времени $t \in T$ по множеству кортежей значений всех существующих в этот момент объектов, существенных для выполнения процедуры взаимодействия, и множеству связей этих объектов определяются значения этих кортежей в следующий момент времени.

Помимо множества $F^{'}$ введем конечное множество алгоритмических процедур $F^{''}$ таких, что при выполнении процедуры $g \in F^{''}$ в момент времени t некоторые из существующих в этот момент объектов прекращают свое существование, а некоторые начинают свое существование («рождаются»).

Процедуры $F^{''}$ определяют динамику изменения OD-модели, а объединение $F = F^{'} \cup F^{''}$ определяет динамику модели.

С этим уточнением под OD-моделью мы будем понимать двенадцатку:

$$(O, A, \overline{A}(o), V(o), L_p, L_o, L_f, \overline{A}_{L_f}(o_l^j), V_{L_f}(o_l^j), F^{'}, F^{''}, T). \tag{2}$$

Дополнение описания Динамической информационной модели

Ранее в работе [1] было доказано, что произвольная OD-модель может быть статически описана с помощью некоторой схемы классов DIM, однако для реализации динамики изменений в Динамической информационной модели необходимо ввести дополнительные элементы.

Для введения отношения взаимодействия определим специальный класс c_h *взаимодействий*, описывающий методы взаимодействия объектов классов *Откуда*, *Куда* и *Что* на множестве B четверок этих классов и и объекта класса c_h взаимодействий *Как* (o_h — *how*), а также вводится отношение истории, отражающее характер баз данных в данной технологии.

Для описания динамики изменения классов, свойств и взаимодействий вводятся аналогичные конструкции.

Динамическая полнота DIM

В [1] было построено отображение G произвольной OD-модели в *схему классов* DIM, с помощью которого доказывалась теорема *о полноте статического представления* данных DIM. Наша задача продолжить это отображение на алгоритмы множества F OD-модели во взаимодействия DIM таким образом, чтобы оно осталось согласованным с объектами обоих моделей, их свойствами и значениями свойств перед непосредственным выполнением каждого алгоритма $f \in F$ (соответствующего взаимодействия $G(f) \in B$) и сразу после его выполнения. Чтобы отображение $G(f)$ возможно меньше зависело от конструкций описаний f и $G(f)$, мы прибегнем к универсальному описанию алгоритма в виде *машины Тьюринга* (МТ) и для этого опишем OD-модель МТ (OD.МТ) и DIM-модель МТ (DIM.МТ).

По построенной МТ для OD-модели строится отображение $G(OD.MT) = DIM.MT$, которое строит МТ DIM путем преобразования функциональной таблицы OD.МТ в DIM.МТ, а также структуры входных и выходных состояний ленты обеих МТ.

С вызовом в некоторый момент $t \in T$ произвольного алгоритма $f \in F'$ произвольной OD-модели связаны 2 ее статических описания при помощи схем классов DIM: S_0 в момент t непосредственно перед вызовом f и S_1 в момент $t+1$ завершения выполнения f. Будем говорить, что *некоторое взаимодействие DIM $b \in B$ описывает динамику значений свойств объектов, вызываемую алгоритмом f, если оно преобразует схему классов DIM S_0 в схему классов S_1*. *Взаимодействие* является реализацией алгоритма изменения данных модели в DIM, его составляющие определяют алгоритм следующим образом: *Откуда* — объект или группа объектов в момент t, у которых изменяются значения свойств; *Куда* — объект или группа объектов, получающая в момент $t + 1$ новые значения свойств; *Что* — свойство или группа свойств-объектов, у которых изменяются значения этих свойств; *Как* — процедура изменения свойств (процедура вызова в цикле МТ, которая это делает).

Теорема о полноте динамики значений свойств объектов. *Для произвольного алгоритма $f \in F'$ произвольной OD-модели существует взаимодействие DIM $b \in B$, описывающее динамику значений свойств объектов, вызываемую алгоритмом f в произвольный момент $t \in T$.*

Список литературы

[1] Рублев В. С. Теорема о статической полноте СУБД DIM // Проблемы теоретической кибернетики. Материалы XVII международной конференции. — Казань: Отечество, 2014. — С. 242–245.

Обзор последних результатов в теории алгебраических моделей программ с процедурами

Подловченко Римма Ивановна

Московский государственный университет имени М. В. Ломоносова, e-mail: podlovchenko.rimma@gmail.com

В статье дается обзор последних результатов решения проблем эквивалентности и эквивалентных преобразований для алгебраических моделей программ с рекурсивными процедурами.

Схемы программ строятся над базисом B четырех конечных алфавитов Y, C, R, P; элементы первых трех называются символами операторов, вызовов и возвратов, P — множество логических переменных. Слова из множества $H = (Y \cup C \cup R)^*$ будем называть *цепочками*.

Схема программ над B — это конечный размеченный ориентированный граф, состоящий из связанных между собой подграфов; один из них называется *главным*, а остальные — *процедурами*. Главный граф содержит две обязательные вершины, именуемые входом и выходом; остальные вершины называются *преобразователями*, *вызовами* и *возвратами*; они помечены символами из Y, C, R соответственно. Каждый вызов входит в подграф вместе с соответствующим ему *парным* возвратом. Процедурный подграф отличается от главного тем, что в нем вход заменяется вершиной, называемой *инициальной*, а выход — вершиной, именуемой *финальной*. Каждая вершина вызова соединена дугой с инициальной вершиной процедуры, а из финальной вершины этой процедуры исходит дуга в парный вызову возврат. Из вершин типа вход, инициальная, преобразователь, возврат исходит $2^{|P|}$ дуг, помеченных *наборами* из множества $X = \{x \mid x : P \to \{0, 1\}\}$.

Выполнение схемы программ проводится на входных функциях, называемых *функциями разметки* вида $\mu : H \to X$, представляет собой процесс обхода графа, сопровождающийся построением цепочки из H, который подробно описан в статье [1].

Алгебраическая модель программ определяется двумя параметрами — отношением эквивалентности ν на множестве цепочек H и множеством функций разметки L. Если L включает в себя все ν-согласованные функции разметки, то модель называется *однопараметрической*. Две схемы эквивалентны в заданной модели, если для любой функции разметки μ из L всякий раз, как на ней останавливается одна из схем с результатом h', также останавливается и другая с результатом h'', и при этом $h' \nu h''$.

Если алфавиты C и R пусты, то модель и принадлежащие ей схемы называются *простыми*. Модель $\mathcal{M}$ называется *перегородчатой*, если ее параметры ν и L определяются параметрами τ и ℓ простой модели $\mathcal{M}_0$ следующим образом. Цепочки h' и h'' являются ν-эквивалентными, если совпадают их проекции $b_1 b_2 \dots b_k$ на множество $C \cup R$, и при этом $h' = h'_0 b_1 h'_1 b_2 \dots b_k h'_k$, $h'' = h''_0 b_1 h''_1 b_2 \dots b_k h''_k$, а каждая пара h'_i, h''_i, $0 \le i \le k$, состоит из τ-эквивалентных подцепочек. Выполнение схемы на функциях разметки из L таково: всякий раз, когда встречается вершина типа вход, вызов, возврат выбирается какая-либо функция разметки из ℓ, и до встречи с очередной вершиной типа вызов, возврат, выход схема выполняется на ней. Будем говорить, что перегородчатая модель $\mathcal{M}$ *индуцируется* простой моделью $\mathcal{M}_0$.

Пусть $\mathcal{M}$ — перегородчатая модель с параметрами ν, L, индуцированная простой моделью $\mathcal{M}_0$ с параметрами τ, ℓ.

Утверждение 1. *Если простая модель $\mathcal{M}_0$ удовлетворяет достаточным требованиям ее аппроксимируемости, сформулированным в статье* [1]*, то индуцируемая ею модель $\mathcal{M}$ является аппроксимирующей.*

Требования, предъявляемые к параметрам τ и ℓ, таковы. Отношение эквивалентности τ на множестве цепочек над Y должно быть *полугрупповым*, т. е. соотношение $(h_1 \tau h_2) \& (h_3 \tau h_4) \Rightarrow h_1 h_3 \tau h_2 h_4$ должно выполняться для любых цепочек h_1, h_2, h_3, h_4. Кроме того, множество ℓ должно состоять из τ-согласованных функций разметки над Y, P и быть замкнутым относительно операции сдвига. При этом *τ-согласованной* называется функция, принимающая равные значения на τ-эквивалентных цепочках. *Сдвигом функции μ* на цепочку h называется функция μ_h, значение которой на каждой цепочке h' равно $\mu(hh')$. Множество ℓ *замкнуто по операции сдвига*, если для любой функции μ из ℓ и любой цепочки h функция μ_h принадлежит ℓ. При изучении перегородчатых моделей программ важную роль играет

Утверждение 2. *Схемы из $\mathcal{M}$ эквивалентны тогда и только тогда, когда, каким бы ни был реализуемый маршрут через одну из них, всякий сочетаемый с ним маршрут в другой схеме ведет в ее выход, и при этом цепочки, несомые обоими маршрутами, ν-эквивалентны.*

Маршрутом в схеме называется ориентированный путь в схеме из ее входа; он называется *маршрутом через схему*, если завершается в ее выходе. *Реализуемым* называется маршрут, который прокладывается при выполнении схемы на некоторой функции разметки из L. *Несомой маршрутом цепочкой* называется цепочка, составленная из символов, приписанных вершинам, через которые проходит маршрут.

Теорема 1 [2]. *Проблема эквивалентности схем в перегородчатой модели $\mathcal{M}$ разрешима, если в индуцирующей её модели $\mathcal{M}_0$ разрешимы проблема эквивалентности и проблема непустоты пересечения.*

Проблема непустоты пересечения состоит в поиске алгоритма, который, получив на свой вход две схемы из $\mathcal{M}_0$, определяет, имеются ли в этих схемах

сочетаемые маршруты. *Сочетаемыми* называются маршруты, прокладываемые общей функцией разметки.

В статье [2] получена оценка сложности алгоритма, разрешающего эквивалентность схем в модели $\mathcal{M}$; она полиномиальна в случае полиномиальной сложности двух проблем, упомянутых в Теореме 1. Однако эта оценка сложности достаточно высока. В связи с этим рассмотрен частный случай, когда сложность существенно ниже.

Теорема 2. *В классе примитивных схем, принадлежащих однопараметрической перегородчатой модели программ $\mathcal{M}$, проблема эквивалентности разрешима, если она разрешима в простой модели, индуцирующей $\mathcal{M}$.*

Примитивной называется схема, в которой преемники любой опорной вершины не имеют одинаковых меток. *Опорной* называется вершина схемы из $\mathcal{M}$ типа вход, выход, вызов и возврат. Для всякой опорной вершины определяются ее преемники — тоже опорные вершины.

Теорема 3 [3]. *Пусть перегородчатая модель программ индуцируется уравновешенной полугрупповой моделью программ с левым сокращением. Тогда в классе примитивных схем, принадлежащих этой модели, и в которых каждая опорная вершина имеет в точности одного преемника, разрешима проблема построения полной системы эквивалентных преобразований схем.*

Список литературы

[1] Подловченко Р. И. Рекурсивные схемы и иерархия их моделей // Программирование. — 1991. — № 5. — С. 44–61.

[2] Молчанов А. Э. Разрешимость эквивалентности в двухпараметрических перегородчатых моделях программ // Моделирование и анализ информационных систем. — 2014. — Т. 21, № 4. — С. 104–115.

[3] Подловченко Р. И. Исследование примитивных схем программ с процедурами // Моделирование и анализ информационных систем. — 2014. — Т. 21, № 4. — С. 116–131.

О единичных тестах для функциональных элементов

Попков Кирилл Андреевич

Московский государственный университет имени М. В. Ломоносова, e-mail: kirill-formulist@mail.ru

Введение

Рассматриваются задачи проверки исправности и распознавания состояний функциональных элементов с использованием экспериментов, заключающихся в составлении произвольных схем из заданных функциональных элементов с последующим «прозваниванием» этих схем, т. е. нахождением булевых функций, реализуемых составляемыми схемами. Суть общепринятой математической модели схемы из функциональных элементов и тех элементов, из которых

строятся эти схемы, с исчерпывающей полнотой и ясностью представлена в [1]; именно такая математическая модель является объектом исследования и рассматривается ниже.

Представим, что имеются N функциональных элементов $E_1, \ldots, E_N$ ($N \geqslant 1$). Каждый элемент, рассматриваемый как простейшая схема из функциональных элементов, имеет $n \geqslant 1$ входов и один выход и в исправном состоянии реализует на выходе заданную булеву функцию $f(x_1, \ldots, x_n)$, где $x_1, \ldots, x_n$ — переменные, подаваемые на его входы (считаем, что функция $f(x_1, \ldots, x_n)$ существенно зависит от всех своих переменных и, как следствие, отлична от константы). В неисправном состоянии каждый элемент реализует одну из констант 0 или 1. Неисправность элемента E_i, при которой он реализует константу 0 (или 1), будем называть неисправностью E_i типа 0 (соответственно 1). Будем предполагать, что среди заданных N функциональных элементов может оказаться не более одного неисправного. Допускается составлять любые схемы с одним выходом из данных функциональных элементов и наблюдать выдаваемые схемами значения на любых наборах значений переменных.

Задача заключается в том, чтобы протестировать функциональные элементы, т. е. для каждого из них определить, исправен данный элемент или неисправен (задача проверки), и, в дополнение к этому, при наличии неисправного элемента определить тип его неисправности (задача диагностики), используя при тестировании по возможности меньшее число схем.

Основные определения и вспомогательные утверждения

Единичным проверяющим тестом назовём такой набор схем $S_1, \ldots, S_l$, составленных из заданных функциональных элементов, что по набору функций, реализуемых этими схемами, можно однозначно определить исправность или неисправность каждого из N элементов. Число l назовём *длиной* этого теста. (Здесь используется терминология, общепринятая для диагностики управляющих систем: см., например, [2].)

Единичным диагностическим тестом назовём такой набор схем $S_1, \ldots, S_l$, составленных из заданных функциональных элементов, что по набору функций, реализуемых этими схемами, можно однозначно определить состояние каждого из N элементов. Число l назовём *длиной* этого теста.

Отметим, что единичный проверяющий тест, в отличие от диагностического, не обязан определять тип неисправности (0 или 1) неисправного элемента, если такой элемент существует.

Введём функции $L_c(f, N)$ и $L_d(f, N)$, равные длинам самого короткого соответственно проверяющего и диагностического тестов для N функциональных элементов, среди которых не более одного элемента неисправно (в исправном состоянии каждый элемент реализует булеву функцию f). Основной задачей в дальнейшем будет нахождение величин $L_c(f, N)$ и $L_d(f, N)$ при различных f и N.

Утверждение 1. *Множества единичных проверяющих и единичных диагностических тестов для N функциональных элементов, каждый из которых реализует в исправном состоянии булеву функцию f, совпадают.*

Следствие. *Справедливо равенство* $L_c(f, N) = L_d(f, N)$.

Замечание 1. В силу следствия из утверждения 1 для нахождения величины $L_d(f, N)$ достаточно знать только $L_c(f, N)$. Поэтому после введения обозначения $L(f, N) = L_c(f, N)$ можно формулировать основные результаты в терминах величины $L(f, N)$.

Формулировка основного результата

Выделим два возможных представления функции f:

$$f(x_1, \ldots, x_n) = x_1^{\sigma_1} \& \ldots \& x_n^{\sigma_n}, \tag{1}$$

$$f(x_1, \ldots, x_n) = x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n}, \tag{2}$$

где $\sigma_1, \ldots, \sigma_n \in \{0, 1\}$.

Основным результатом данной работы является следующая

Теорема 1. *Справедливо равенство*

$$L(f, N) = \begin{cases} 1, \text{ если функция } f \text{ не представима ни в одном из видов (1), (2);} \\ \min(2; N), \text{ если функция } f \text{ представима в виде (1) или (2),} \\ \quad \text{причём } n \geqslant 2 \text{ и хотя бы одно из чисел } \sigma_1, \ldots, \sigma_n \text{ равно нулю;} \\ \lceil \log_2(N+1) \rceil, \text{ если } f(x_1, \ldots, x_n) \in \{x_1 \& \ldots \& x_n,\ x_1 \vee \ldots \vee x_n\}; \\ \lceil \log_3(2N+1) \rceil, \text{ если } n = 1 \text{ и } f(x_1) = \overline{x_1}. \end{cases}$$

Замечание 2. Легко видеть, что четыре случая, указанные в формулировке основной теоремы, охватывают все возможные случаи. Таким образом, теорема 1 полностью решает поставленную задачу.

Автор выражает глубокую благодарность своему научному руководителю профессору Н. П. Редькину за постановку задачи и внимание к работе.

Работа выполнена при поддержке РФФИ (проект № 14-01-00598).

Список литературы

[1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М. : Изд-во МГУ, 1984. — 137 с.

[2] Редькин Н. П. Надёжность и диагностика схем. — М. : Изд-во МГУ, 1992. — 192 с.

Программные управления для одного класса стохастических производственных систем

Прилуцкий Михаил Хаимович

Нижегородский государственный университет им. Н. И.Лобачевского, e-mail: pril@iani.unn.ru

Будем рассматривать производственные системы, функционирующие по следующей схеме ([1]). Под воздействием технологических режимов произ-

водятся полуфабрикаты, из которых изготавливаются продукты производства. Применение технологического режима не определяет продукт, который будет изготовлен, а задает вероятности получения того или иного полуфабриката. Каждому полуфабрикату соответствует набор продуктов, которые могут быть из него изготовлены. Известны как затраты на использование технологических режимов, так и доходы от выпуска запланированных продуктов. Задачи программного управления ([2]) решаются до начала планируемого периода. Цель их решения состоит в определении ресурсов, необходимых для обеспечения технологических режимов, которые будут использоваться в планируемом периоде. В задачах программного управления требуется определить, какие технологические режимы, и в каком количестве необходимо использовать с целью «наилучшего» выполнения заданного плана по продуктам производства, где под «наилучшим» выполнением плана понимается применение таких управлений, при которых математическое ожидание полного суммарного дохода от функционирования системы в планируемом периоде будет максимально. В качестве примеров таких систем в работе рассматриваются производственные системы по переработке газового конденсата в нефтепродукты, изготовления печатных схем и мартеновского производства стали.

Пусть I — множество технологических режимов, J — множество полуфабрикатов, K — множество выпускаемых продуктов, $T = \{0, 1, \ldots, T_0\}$ — множество тактов функционирования системы. Через $P = ||p_{ij}||$ — обозначим матрицу вероятностей, где p_{ij} — вероятность того, что применив технологический режим i, будет получен полуфабрикат j, $\sum_{j \in J} p_{ij} = 1$, $i \in I$, $p_{ij} \geq 0$, $i \in I$, $j \in J$. Пусть $K(j)$ — множество продуктов, любой из которых (но только один) может быть изготовлен из полуфабриката j, $K(j) \subseteq K$, $j \in J$. Обозначим через $\vec{\pi}$ -– план производства продуктов в планируемом периоде, где π_k — количество k-ых продуктов, которые должны быть выпущены в планируемом периоде, $k \in K$. Пусть c_i — затраты производственной системы, связанные с использованием i-го технологического режима, $i \in I$; g_k — доход, который получит система от производства единицы запланированного k-го продукта, $k \in K$.

Рассмотрим целочисленную случайную величину $\sigma_k = \sigma_k(\vec{x}, Y)$, принимающую значения из множества $\{0, 1, \ldots, T_0\}$ — сколько продуктов k будет выпущено, если будут применяться технологические режимы из набора $\vec{x}$, а в случае получения полуфабриката j, с вероятностью y_{jk} будет выпускаться продукт $k, j \in J, k \in K$.

Обозначим через $F(\vec{\pi}, T_0, \vec{x}, Y)$ — математическое ожидание полного дохода, который получит система, если известен план производства продуктов $\vec{\pi}$, количество тактов функционирования системы T_0, и к системе будут применяться управления, определяемые набором $\vec{x}$ и матрицей $Y = ||y_{jk}||$, задающей распределение вероятностей изготовления тех или иных продуктов. Тогда $F(\vec{\pi}, T_0, \vec{x}, Y) = \sum_{k \in K} g_k E \min(\pi_k, \sigma_k) - \sum_{i \in I} c_i x_i$, где $E \min(\pi_k, \sigma_k)$ — математическое ожидание целочисленной случайной величины $\min(\pi_k, \sigma_k)$, и задача поиска оптимального программного управления ставится как следующая задача

математического программирования:

$$F(\vec{\pi}, T_0, \vec{x}, Y) = \max\{\sum_{k\in K} g_k E\min(\pi_k, \sigma_k) - \sum_{i\in I} c_i x_i | \sum_{k\in K} y_{jk} = 1; y_{jk} = 0,$$
$$\text{если } k \notin K(j); x_i \in Z^+, y_{jk} \geq 0, j \in J, k \in K\}.$$

Существенная сложность функционала $F(\vec{\pi}, T_0, \vec{x}, Y)$ не позволяет решить поставленную задачу известными методами. Рассмотрим следующую задачу 1 с функционалом $H(\vec{\pi}, T_0, \vec{x}, Y) = \sum_{k\in K} g_k \min(\pi_k, E\sigma_k) - \sum_{i\in I} c_i x_i \to \max$, и ограничениями исходной задачи. Задачу 1 путем преобразований удается свести к задаче частично-целочисленного линейного программирования, решение которой можно осуществлять известными методами и программными средствами.

Теорема. *Пусть* $(\vec{x}^0, Y^0)$ *— оптимальное решение исходной задачи, а* $(\vec{x}^*, Y^*)$ *— оптимальное решение задачи 1, тогда* $\lim\limits_{T_0\to\infty} = \frac{F(\vec{\pi},T_0,\vec{x}^0,Y^0)-F(\vec{\pi},T_0,\vec{x}^*,Y^*)}{F(\vec{\pi},T_0,\vec{x}^0,Y^0)} = 0.$

Доказательство теоремы основано на следующей лемме.

Лемма. *Для произвольной целочисленной случайной величины* σ, $\sigma \in \{0, 1, \ldots, n\}$, *и произвольного целого числа* π, $\min(\pi, E\sigma) - E\min(\pi, \sigma) = \frac{1}{2}(E|\pi - \sigma| - |E\pi - \sigma|)$.

Из теоремы следует, что при замене оптимального программного управления $(\vec{x}^0, Y^0)$, получающегося при решении исходной задачи, на программное управление $(\vec{x}^*, Y^*)$, получающееся при решении задачи 1, математическое ожидание полного дохода уменьшится, однако с ростом T_0 эти потери по отношению к математическому ожиданию полного дохода при оптимальном программном управлении будут стремиться к нулю. Тем самым решение задачи 1 определяет псевдооптимальное решение исходной задачи.

Список литературы

[1] Прилуцкий М. Х. Оптимальное планирование двухстадийных стохастических производственных систем // Автоматика и телемеханика. — 2014. — № 8. — С. 37–47.

[2] Моисеев Н. Н. Математические задачи системного анализа. — М.: Наука, Главная редакция физико-математической литературы, 1981. — 488 с.

Подход Ляпунова–Яблонского как метод исследования приоритетной управляющей системы обслуживания

Пройдакова Екатерина Вадимовна

Нижегородский государственный университет, e-mail: pev_1@mail.ru

В работе изучается система управления независимыми и конфликтными транспортными потоками Π_1, Π_2, …, Π_m. Конфликтность потоков означает,

что их обслуживание должно происходить в непересекающиеся промежутки времени. Поступающие потоки делятся на три типа: Π_1 — малоинтенсивный поток; Π_2, …, Π_{m-1} — потоки средней интенсивности и Π_m — интенсивный поток. Только поток Π_1 обладает приоритетом. Это означает, что любая заявка по Π_1 должна быть обслужена как можно быстрее, но не прерывая обслуживания других требований. У каждого потока есть основной этап обслуживания и переналадка. Для Π_m введен дополнительный промежуток времени, в котором продолжается его обслуживание. Обслуживающее устройство имеет $2m+1$ состояние $\Gamma^{(1)}$, $\Gamma^{(2)}$, …, $\Gamma^{(2m)}$, $\Gamma^{(2m+1)}$, где $\Gamma^{(2j-1)}$ — состояние, при котором пропускается только поток Π_j с интенсивностью $\mu_j > 0$; $\Gamma^{(2j)}$ — состояние, при котором пропускается только Π_j и ${\mu'}_j > \mu_j$; $\Gamma^{(2m+1)}$ — состояние, при котором пропускается только Π_m и ${\mu''}_m > \mu_m$. Здесь при $j = \overline{1,m}$ интенсивности μ_j, μ'_j и μ''_m определяют среднее число заявок, обслуживающихся в единицу времени в состояниях $\Gamma^{(2j-1)}$, $\Gamma^{(2j)}$ и $\Gamma^{(2m+1)}$ соответственно. Длительности T_1, T_2, …, T_{2m+1} состояний $\Gamma^{(1)}$, $\Gamma^{(2)}$, …, $\Gamma^{(2m+1)}$ являются управляющими параметрами. Входные потоки Π_1, Π_2, …, Π_m считаем пуассоновскими с интенсивностями λ_1, λ_2, …, λ_m, где $\lambda_1 \ll \lambda_m$. По всем потокам разрешены неограниченные очереди. На обслуживание заявки поступают группами и стратегии механизма обслуживания полагаем экстремальными [1]. Потоки насыщения, определяющие выходные потоки системы при ее максимальной загрузке и эффективном функционировании, считаем независимыми.

При построении математической модели изучаемой управляющей системы использовался кибернетический подход, методологически разработанный А. А. Ляпуновым и С. В. Яблонским [2]. В основе кибернетического подхода лежат три положения: 1) дискретность актов функционирования системы во времени; 2) нелокальность в описании строения системы; 3) совместное рассмотрение блочного строения системы и ее функционирования во времени. Эти положения позволяют выделить схему, информацию, координаты и функцию управляющей системы. В свою очередь, схема изучаемой системы состоит из следующих блоков: 1) входные потоки — первый тип входных полюсов; 2) потоки насыщения — второй тип входных полюсов; 3) очереди — внешняя память; 4) стратегии механизма обслуживания — блок по переработке информации внешней памяти; 5) обслуживающее устройство с $2m+1$ состояниями — внутренняя память; 6) приоритетный алгоритм смены состояний обслуживающего устройства — блок по переработке информации внутренней памяти; 7) потоки реально обслуженных требований — выходные полюса. Набор состояний очередей, состояний обслуживающего устройства, входных потоков, потоков насыщения и потоков обслуженных требований определяют информацию системы. Номера входных и выходных потоков, потоков насыщения, очередей и состояний обслуживающего устройства задают координаты системы. Функция изучаемой системы — это управление и непосредственное обслуживание потоков неоднородных требований.

Согласно положениям кибернетического подхода система наблюдалась в дискретные моменты времени τ_i, $i = 0, 1, \ldots$ переключений фаз обслуживаю-

щего устройства или на промежутке $[\tau_i, \tau_{i+1})$. Точечный случайный процесс $\{\tau_i; i \geqslant 0\}$ задает шкалу тактов времени работы управляющей системы. Рассмотрим при $j = \overline{1,m}$ и $i = 0, 1, \ldots$ случайные элементы: 1) $\eta_{j,i}$ — число заявок потока Π_j, пришедших за $[\tau_i, \tau_{i+1})$, $\eta_{j,i} \in X = \{0, 1, \ldots\}$; 2) $\xi_{j,i}$ — максимально возможное число заявок, которое может обслужиться за время $[\tau_i, \tau_{i+1})$ по потоку Π_j, $\xi_{j,i} \in \{0, l'_j, l_j\}$ при $j = \overline{1,m-1}$, а $\xi_{m,i} \in \{0, l''_m, l'_m, l_m\}$. Здесь l_j определяет максимальное число требований потока Π_j, которое может обслужиться за $\Gamma^{(2j-1)}$, причем $l_j = [\mu_j T_{2j-1}]$, $l'_j = [\mu'_j T_{2j}]$ и $l''_m = [\mu''_m T_{2m+1}]$, $l_j \geqslant l'_j$ и $l_m \geqslant l''_m$; 3) Γ_i — состояние обслуживающего устройства на промежутке $[\tau_i, \tau_{i+1})$, $\Gamma_i \in \Gamma = \{\Gamma^{(1)}, \Gamma^{(2)}, \ldots, \Gamma^{(2m)}\}$; 4) $\varkappa_{j,i}$ — длина очереди по потоку Π_j в момент τ_i, $\varkappa_{j,i} \in X$; 5) $\bar{\xi}_{j,i}$ — число реально обслуженных заявок потока Π_j за промежуток $[\tau_i, \tau_{i+1})$, $\bar{\xi}_{j,i} \in Y_j = \{0, 1, \ldots, l_j\}$; 6) $\bar{\xi}_{j,-1}$ — число реально обслуженных заявок потока Π_j за $[0, \tau_0)$, $\bar{\xi}_{j,-1} \in Y_j$.

Для описания приоритетного алгоритма смены состояний обслуживающего устройства определим при $w_1, u_1 \in X$, $\Gamma^{(r)} \in \Gamma$, функцию $U(\Gamma^{(r)}, w_1, u_1)$:

$$U(\Gamma^{(r)}, w_1, u_1) = \begin{cases} \Gamma^{(1)} & \text{при } r = 2m; \\ \Gamma^{(r+1)} & \text{при } r = \overline{1, 2m-2}; \\ \Gamma^{(2m)} & \text{при } r \in \{2m-1, 2m+1\},\ w_1 = 0,\ u_1 > 0; \\ \Gamma^{(2m)} & \text{при } r \in \{2m-1, 2m+1\},\ w_1 > 0; \\ \Gamma^{(2m+1)} & \text{при } r \in \{2m-1, 2m+1\},\ w_1 = u_1 = 0. \end{cases}$$

Тогда $\Gamma_{i+1} = U(\Gamma_i, \varkappa_{1,i}, \eta_{1,i})$. Стратегии механизма обслуживания определяются соотношением: $\bar{\xi}_{j,i} = \min\{\varkappa_{j,i} + \eta_{j,i}; \xi_{j,i}\}$. Для входных потоков справедливо: $P(\eta_{j,i} = u_j | \Gamma_i = \Gamma^{(r)}) = (\lambda_j T_r)^{u_j} (u_j!)^{-1} \exp\{-\lambda_j T_r\} = \varphi_j(u_j, T_r)$, $u_j \in X$, $r = \overline{1, 2m+1}$. В силу независимости входных потоков и потоков насыщения, изучалась только случайная пятимерная векторная последовательность $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}, \bar{\xi}_{1,i-1}, \bar{\xi}_{m,i-1}); i \geqslant 0\}$, определяющая поведение системы по приоритетному Π_1 и интенсивному Π_m потокам. Данная последовательность задает и нелокальное описание выходных потоков по этим направлениям, причем за выходной поток отвечают компоненты $\bar{\xi}_{1,i}$ и $\bar{\xi}_{m,i}$, а $\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}$ играют роль меток. Считаем, что в момент времени τ_0 задано распределение начального вектора $(\Gamma_0, \varkappa_{1,0}, \varkappa_{m,0}, \bar{\xi}_{1,-1}, \bar{\xi}_{m,-1})$, то есть известны вероятности $P(\Gamma_0 = \Gamma^{(s)}, \varkappa_{1,0} = x_1, \varkappa_{m,0} = x_m, \bar{\xi}_{1,-1} = y_1, \bar{\xi}_{m,-1} = y_m)$, где $\Gamma^{(s)} \in \Gamma$, $x_1 \in X$, $x_m \in X$, $y_1 \in Y_1$, $y_m \in Y_m$. Для $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}, \bar{\xi}_{1,i-1}, \bar{\xi}_{m,i-1}); i \geqslant 0\}$ выполняется: $(\Gamma_{i+1}, \varkappa_{1,i+1}, \varkappa_{m,i+1}, \bar{\xi}_{1,i}, \bar{\xi}_{m,i}) = (U(\Gamma_i, \varkappa_{1,i}, \eta_{1,i}), \max\{0, \varkappa_{1,i} + \eta_{1,i} - \xi_{1,i}\}, \max\{0, \varkappa_{m,i} + \eta_{m,i} - \xi_{m,i}\}, \min\{\varkappa_{1,i} + \eta_{1,i}, \xi_{1,i}\}, \min\{\varkappa_{m,i} + \eta_{m,i}, \xi_{m,i}\})$. Также для данной последовательности были доказаны [1] некоторые утверждения.

Теорема 1. *Последовательность* $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}, \bar{\xi}_{1,i-1}, \bar{\xi}_{m,i-1}); i \geq 0\}$ *является однородной марковской цепью со счетным числом состояний, при известном распределении начального вектора* $(\Gamma_0, \varkappa_{1,0}, \varkappa_{m,0}, \bar{\xi}_{1,-1}, \bar{\xi}_{m,-1})$.

Теорема 2. *Пространство всех возможных состояний однородной марковской цепи* $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}, \bar{\xi}_{1,i-1}, \bar{\xi}_{m,i-1}); i \geq 0\}$ *распадается на незамкнутое множе-*

ство несущественных состояний и на минимальное замкнутое множество существенных сообщающихся апериодических состояний.

Теорема 3. *Для существования стационарного распределения однородной марковской цепи* $\{(\Gamma_i, \varkappa_{1,i}, \varkappa_{m,i}, \bar{\xi}_{1,i-1}, \bar{\xi}_{m,i-1}); i \geq 0\}$ *достаточно выполнения двух неравенств:* $\lambda_1 T - l_1 - l'_1 < 0$, $\lambda_m T - l_m - l'_m < 0$.

Работа выполнена в рамках госбюджетной темы № 01201456585 «Математическое моделирование и анализ стохастических эволюционных систем и процессов принятия решений» и государственной программы «Поддержка ведущих университетов РФ в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров».

Список литературы

[1] Пройдакова Е. В. Исследование вероятностных свойств выходных потоков в системе управления с приоритетным направлением // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2012. — № 5 (2). — С. 190–196.

[2] Ляпунов А. А., Яблонский С. В. Теоретические проблемы кибернетики // Проблемы кибернетики. — Вып. 9. — М.: Физматгиз, 1963. — С. 5–22.

Численное исследование и синтез дискретных управляющих систем обслуживания

Рачинская Мария Анатольевна, Федоткин Михаил Андреевич

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: rachinskaya.maria@gmail.com, fma5@rambler.ru

Постановка задачи

Рассматривается перекресток, на который поступает $m \geq 2$ потоков $\Pi_j, j \in J = \{1, 2, \ldots, m\}$ машин (заявок). Эти потоки с целью безопасности движения пропускаются через перекресток только в непересекающиеся промежутки времени. Адекватной моделью каждого потока Π_j считается неординарный пуассоновский поток с параметрами: λ_j — интенсивность поступления пачек, p_j, q_j и $s_j = 1 - p_j - q_j$ — вероятности поступления пачек из одной, двух и трех машин соответственно. Машины любого потока, подъехавшие к перекрестку, ожидают возможности переезда (обслуживания) в очереди по соответствующему направлению. Перекресток регулируется автоматом-светофором, реализующим циклический алгоритм управления потоками: $2m$ состояний $\Gamma^{(1)}, \Gamma^{(2)}, \ldots, \Gamma^{(2m)}$ с длительностями $T_1, T_2, \ldots, T_{2m}$ соответственно сменяются в циклическом ритме $\Gamma^{(1)} \to \Gamma^{(2)} \to \ldots \to \Gamma^{(2m)} \to \Gamma^{(1)} \to \ldots$. В каждом из состояний $\Gamma^{(2j-1)}, j \in J$, зеленый свет горит для потока Π_j (машины этого потока пропускаются через перекресток), для остальных — красный свет. Каждое последующее состояние $\Gamma^{(2j)}, j \in J$, служит для переналадки светофора: желтый свет для потока Π_j (машины, начавшие переезд в предыдущем состоянии, заканчивают его), для остальных потоков — красный свет. Длительность

полного цикла $T = \sum_{k=1}^{2m} T_k$. Машины пропускаются через перекресток согласно экстремальной стратегии, означающей в данном случае, что в состоянии $\Gamma^{(2j-1)}$, $j \in J$, пропускается как можно большее число имеющихся в очереди машин потока Π_j, но не превышающее числа $l_j = [\mu_j T_{2j-1}]$. Здесь μ_j — параметр, характеризующий пропускную способность перекрестка по потоку Π_j. За системой наблюдаем в дискретные случайные моменты $\tau_0, \tau_1, \ldots$ переключения состояния светофора.

Цели исследования: представить способ определения момента завершения переходных процессов и достижения системой стационарного режима и алгоритм определения значений длительностей фаз светофора, при которых достигается минимальное значение оценки $\widetilde{\mathbf{M}}\gamma$ среднего времени $\mathbf{M}\gamma$ ожидания начала обслуживания произвольной машины в стационарном режиме. Исследование будем проводить средствами имитационного моделирования, при этом полагая, что в момент τ_0 включается фаза $\Gamma^{(1)}$ светофора.

Способы численного исследования

В работе [1] с использованием кибернетического подхода показано, что критерий существования в системе стационарного режима заключается в выполнении системы неравенств $\lambda_j T(2s_j + q_j + 1) < l_j$, $j \in J$. Для определения момента наступления стационарного режима системы по потоку Π_j будем имитировать функционирование перекрестка при отсутствии машин, а также при наличии некоторого количества $[\lambda_j T]$ машин в очереди по потоку Π_j в момент τ_0. Пусть величины $\gamma_{j,v}$ и $\gamma^+_{j,v}$ обозначают случайные времена ожидания начала обслуживания машины с номером v потока Π_j в системе при отсутствии и наличии машин в очереди в начальный момент соответственно. При $i = 1, 2, \ldots$ обозначим через $\pi(\tau_{2mi})$ случайное число машин потока Π_j, обслуженных к моменту τ_{2mi} в системе с начальной очередью размера $[\lambda_j T]$. Будем считать средние арифметические значения $\widehat{\gamma}_{j,\pi(\tau_{2mi})} = \frac{1}{\pi(\tau_{2mi})} \sum_{v=0}^{\pi(\tau_{2mi})} \gamma_{j,v}$ и $\widehat{\gamma}^+_{j,\pi(\tau_{2mi})} = \frac{1}{\pi(\tau_{2mi})} \sum_{v=0}^{\pi(\tau_{2mi})} \gamma^+_{j,v}$. Случайная величина θ определяет номер i цикла, по окончании которого произойдет d-кратное выполнение неравенств $|\widehat{\gamma}^+_{j,\pi(\tau_{2m\theta})} - \widehat{\gamma}_{j,\pi(\tau_{2m\theta})}| < \delta \widehat{\gamma}_{j,\pi(\tau_{2m\theta})}$, где d — заданное натуральное число и $0 < \delta < 1$. Указанное неравенство гарантирует сближение траекторий процессов обслуживания машин в системе при отсутствии и наличии машин в момент τ_0. Эту процедуру повторим N раз с независимыми реализациями потока Π_j, сгенерированными при различных начальных значениях датчика псевдослучайных чисел. Среди значений i^*_n, $1 \le n \le N$, величины θ, полученных по N реализациям, выберем максимальное значение $i^*_{max} = \max_{1 \le n \le N} i^*_n$, и пусть максимум достигается на реализации с номером n^*. Длительность переходного процесса равна $i^*_{max} T$ и по истечении этого времени стационарный режим по потоку Π_j достигнут во всех N реализациях.

Обозначим через w_j номер заявки, которая оказалось первой обслуженной заявкой реализации с номером n^* потока Π_j в стационарном режиме. Мы имеем выборку x^n_{j,w_j}, $1 \le n \le N$, для случайной величины γ_{j,w_j}. Найдем оценку $\widetilde{\mathbf{M}}\gamma_{j,w_j} = \frac{1}{N} \sum_{n=1}^{N} x^n_{j,w_j}$ математического ожидания времени ожидания

начала обслуживания заявки с номером w_j потока Π_j. Поскольку система находится в стационарном режиме, ожидаем, что величины $\gamma_{j,w_j}, \gamma_{j,w_j+1}, \ldots$ будут одинаково распределены. Эта гипотеза может быть проверена методами математической статистики. Если гипотеза будет принята, считаем, что выражение $\widetilde{\mathbf{M}}\gamma = \frac{\sum_{j=1}^{m} \lambda_j(2s_j+q_j+1)\widetilde{\mathbf{M}}\gamma_{j,w_j}}{\sum_{j=1}^{m} \lambda_j(2s_j+q_j+1)}$ дает оценку для среднего взвешенного времени ожидания начала обслуживания произвольной заявки в системе, находящейся в стационарном режиме. Данная оценка при объеме выборки N и заданной доверительной вероятности дает точность, определяемую стандартными методами через распределение Стьюдента. Если получаемая точность не достаточна, число реализаций увеличивается. Аналогичным образом могут быть получены оценки для математического ожидания и дисперсии длин очередей перед зеленым светом и числа обслуженных за зеленый свет машин для каждого потока. Данные оценки служат показателями качества функционирования системы.

Пусть $m = 2$. Необходимо найти оптимальные значения $\widehat{T}_1, \widehat{T}_3$ длительностей T_1, T_3 зеленых фаз для первого и второго потока соответственно, при которых среднее взвешенное время ожидания начала обслуживания произвольной заявки системы будет минимальным. Значения длительностей T_2, T_4 фиксированы заранее и равны T_0. Область оптимизации определяется областью существования стационарного режима и границами $\underline{T}, \overline{T}$ безопасного интервала для длительности полного цикла: $\{(T_1, T_3) : \lambda_1(T_1+T_3+2T_0)(2s_1+q_1+1) < [\mu_1 T_1]$, $\lambda_2(T_1 + T_3 + 2T_0)(2s_2 + q_2 + 1) < [\mu_2 T_3]$, $\underline{T} \le T_1 + T_3 + 2T_0 \le \overline{T}\}$. Определим соотношением $\frac{\lambda_1(2s_1+q_1+1)}{[\mu_1 T_1]} = \frac{\lambda_2(2s_2+q_2+1)}{[\mu_2 T_3]}$ ломаную, на которой оценки загрузки системы по обоим потокам совпадают (кривая равных квазизагрузок). Зафиксируем натуральные числа h_1 и h_2. По алгоритмам, описанным выше, будем имитировать работу системы в точках области оптимизации, лежащих на кривой равных квазизагрузок с шагом h_1 для длительности T_1, и определим среди них точку (T_1^*, T_3^*), для которой значение $\widetilde{\mathbf{M}}\gamma$ минимально. Далее имитируем работу системы в точках области оптимизации, лежащих на прямой $T_1 + T_3 = T_1^* + T_3^*$ с шагом h_2 для T_1. Определим среди них точку $(\widehat{T}_1, \widehat{T}_3)$, для которой значение $\widetilde{\mathbf{M}}\gamma$ минимально. Эту точку называем оптимальной.

Работа выполнена в ННГУ при финансовой поддержке госбюджетной темы № 01201456585 «Математическое моделирование и анализ стохастических эволюционных и процессов принятия решений» и государственной программы «Поддержка ведущих университетов РФ в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров».

Список литературы

[1] Федоткин М. А., Рачинская М. А. Подход Ляпунова–Яблонского при построении и исследовании модели управляющих систем обслуживания конфликтных потоков // Проблемы теоретической кибернетики. Материалы XVII международной конференции. — Казань: Отечество, 2014. — С. 280–282.

Оптимизация на булевых решетках

Ревякин Александр Михайлович

Национальный исследовательский университет “МИЭТ”, e-mail: arevyakin@mail.ru

Многие проблемы комбинаторики можно рассматривать как задачи минимизации субмодулярных функций на булевых решетках. Так, например, можно сформулировать задачи объединения и пересечения матроидов, где в роли субмодулярных функций выступают ранговые функции [1–4].

Пусть K — дистрибутивная решетка с 0 (нулем) и 1 (единицей). Например, таковой является семейство всех подмножеств конечного множества S с операциями объединения и пересечения, в которой 0 является пустым множеством, а 1 — множеством S. Действительная функция μ, определенная на K, называется субмодулярной, если для всех x, y из K выполняется неравенство: $\mu(x)+\mu(y) \geq \mu(x \vee y)+\mu(x \wedge y)$. Если для всех x, y из K справедливо равенство: $\mu(x) + \mu(y) = \mu(x \vee y) + \mu(x \wedge y)$, то функция mu называется модулярной.

Подрешетка L дистрибутивной решетки K называется μ-остовом, если субмодулярная функция μ, определенная на дистрибутивной решетке K, будет модулярной на L.

Пусть $\mu(x) = \sum\limits_{i=1}^{n} c_i \mu_i(x)$, где $\mu_i(x)$ — субмодулярные функции на дистрибутивной решетке K, c_i — положительные действительные коэффициенты и $i = 1, 2, \ldots, n$. Очевидно, $\mu(x)$ также является субмодулярной функцией на K. Рассмотрим задачу минимизации субмодулярной функции $\mu(x)$ на K.

Теорема 1. *Семейство L всех элементов дистрибутивной решетки K, на которых субмодулярная функция μ достигает своего минимума, образует μ-остов решетки K. Более того, подрешетка L является также и μ_i-остовом решетки K для всех $i, i = 1, 2, \ldots, n$.*

Полученный остов L зависит не только от субмодулярных функций μ_i, но и от коэффициентов c_i. Обозначим остов L через $L(c_1, c_2, \ldots, c_n)$, подчеркивая его зависимость от коэффициентов $c_1, c_2, \ldots, c_n$. Поскольку для всех $\lambda > 0$ $L(\lambda \cdot c_1, \ldots, \lambda \cdot c_n) = L(c_1, \ldots, c_n)$, остов L можно рассматривать как функцию на $(n-1)$-мерном симплексе S^{n-1} со значениями в семействе подрешеток дистрибутивной решетки K. Причем симплекс S^{n-1} снабжен структурой многогранного комплекса. В случае когда μ_i являются монотонными, можно детальнее охарактеризовать структуру этого комплекса.

Теорема 2. *Пусть $\mu_1, \ldots, \mu_p$ — неубывающие, $\mu_{p+1}, \ldots, \mu_q$ — невозрастающие субмодулярные функции, а $c_i \geq c_i'$ для $i = 1, 2, \ldots, p$, $c_i \leq c_i'$ для $i = p+1, p+2, \ldots, q$ и $c_i = c_i'$ для $i = q+1, q+2, \ldots, n$. Тогда если $y \in L(c_1, \ldots, c_n)$ и $y' \in L(c_1', \ldots, c_n')$, то $y \wedge y' \in L(c_1, \ldots, c_n)$, $y \vee y' \in L(c_1', \ldots, c_n')$ для всех $i, i = 1, 2, \ldots, n$, имеет место равенство $\mu_i(y) + \mu_i(y') = \mu_i(y \vee y') + \mu_i(y \wedge y')$.*

Два интервала $[x, y]$ и $[x', y']$ решетки L называются транспонированными, если $[x, y] = [b, a \vee b]$ и $[x', y'] = [a \wedge b, a]$ для некоторых a и $b \in L$.

Транспонированные интервалы модулярной решетки изоморфны. Скажем, что интервалы $[x, y]$ и $[x', y']$ являются проективными (обозначение: $[x, y] \sim [x', y']$), если найдется конечная последовательность инвервалов $[x, y], [x_1, y_1], \ldots, [x_N, y_N], [x', y']$, в которой любые два соседних интервала — транспонированы.

Теорема 3. *Любые максимальные цепи, соединяющие наименьший и наибольший элементы конечной модулярной решетки, имеют одинаковую длину. Если $a_0, a_1, \ldots, a_n$ и $b_0 = a_0, b_1, \ldots, b_n = a_n$ — пара таких максимальных цепей, то существует перестановка σ индексов $1, 2, \ldots, n$ такая, что $[a_{i-1}, a_i] \sim [b_{\sigma(i)-1}, b_{\sigma(i)}]$ для $i = 1, 2, \ldots, n$. Кроме того, если рассматриваемая решетка является дистрибутивной, то перестановка σ однозначно определена.*

Таким образом, $\mathcal{F} = \{[a_{i-1}, a_i], i = 1, 2, \ldots, n\}$ — семейство интервалов максимальной цепи $a_0, a_1, \ldots, a_n$ конечной дистрибутивной решетки — одназначно определено с точностью до проективности. На $\mathcal{F}$ можно ввести отношение порядка $\leq$: $[x, y] \leq [z, w]$, если для каждой максимальной цепи $a_0, a_1, \ldots, a_n$ найдутся p и q такие, что $p \leq q, [a_p, a_{p+1}] \sim [x, y]$ и $[a_q, a_{q+1}] \sim [z, w]$.

Пусть μ — субмодулярная функция на дистрибутивной решетке K с 0 и 1, L — подрешетка решетки K с наименьшим элементом a и наибольшим — b, а $\mathcal{F} = \{[a_i, a_{i+1}], i = 1, 2, \ldots, n-1\}$, где $a = a_1, a_2, \ldots, a_n = b$ — произвольная максимальная цепь из a в b в подрешетке L. На каждом интервале $\mathcal{F}$ зададим функцию ϕ_i, где $i = 1, 2, \ldots, n-1$, положив $\phi_i(x) = \mu(x) - \mu(a_i)$ для всех $x \in [a_i, a_{i+1}]$. Если $[0, a]$ и $[b, 1]$ в K не пусты, то положим $\phi_0(x) = \mu(x)$ для всех $x \in [0, a]$ и $\phi_n(x) = \mu(x) - \mu(b)$ для всех $x \in [b, 1]$. Аналогично определим функцию $\phi_i{}'(x) = \mu(x) - \mu(a_i{}')$ для другой максимальной цепи $a = a_1{}', a_2{}', \ldots, a_n{}' = b$ из a в b. Очевидно, что так определенные функции ϕ_i и $\phi_i{}'$ являются субмодулярными.

В силу теоремы 3 найдется определенная перестановка σ индексов $1, 2, \ldots, n-1$ такая, что $[a_i, a_{i+1}] \sim [a'_{\sigma(i)}, a'_{\sigma(i+1)}]$ для всех $i, i = 1, 2, \ldots, n-1$. Пусть $\pi_i : [a_i, a_{i+1}] \to [a'_{\sigma(i)}, a'_{\sigma(i+1)}]$ — естественный изоморфизм, обусловленный проективностью интервалов максимальных цепей. Скажем, что определение «новой» субмодулярной функции ϕ_i не зависит от выбора максимальной цепи из a в b в подрешетке L дистрибутивной решетки K (или выполняется условие $(*)$) , если

$$\phi_i(x) = \mu(x) - \mu(a_i) = \mu(\pi_i(x)) - \mu(a'_{\sigma(i)}) = \phi'_{\sigma(i)}(\pi_i(x))$$

для всех $x \in [a_i, a_{i+1}]$, где $i = 1, 2, \ldots, n-1$.

Теорема 4. *Пусть L — подрешетка конечной дистрибутивной решетки K , μ — субмодулярная функция на K. Тогда для μ — имеет место условие (*) в том и только в том случае, когда L является μ-остовом решетки K.*

Булевы интерпретации полученных теорем типа Жордана – Гельдера (теоремы 3 и 4) полезны при наличии эффективных алгоритмов решения задач комбинаторной оптимизации [2, 4].

Список литературы

[1] Ревякин А. М. Полумодулярные функции и полиматроиды // Комбинатор. анализ. — М.: МГУ, 1983. — Вып. 6. — С. 99.

[2] White N. Theory of matroids // L.: Cambridge University Press. — 2008. — P. 317.

[3] Nakamura M. Boolean sublattices connected with minimization problem on matroids // Math. Program. — 1982. — V. 22, N 1. — P. 117–120.

[4] Nakamura M., Iri M. Fine structures om matroid intersections and their applications // Int. Symp. Circuits and Syst. Proc., Tokyo, 1979. — New York, N. Y., s. a., 1979. — P. 996–999.

Единичные проверяющие тесты для схем переключательного типа

Романов Дмитрий Сергеевич[1], **Романова Елена Юрьевна**[2]

[1] Московский государственный университет имени М. В. Ломоносова, e-mail: romanov@cs.msu.ru

[2] Российский государственный социальный университет, e-mail: RomanovaEJu@rgsu.net

Все не введенные в работе определения — в частности, связанные с графами, контактными схемами (КС) и их обобщениями и тестами — можно найти в книгах [1, 2]. По аналогии с итеративной контактной схемой [2; стр. 143–144] определяется понятие обобщенной итеративной контактной схемы (ОИКС), отличающееся лишь тем, что контакты итеративных переменных могут быть и размыкающими (могут содержать отрицания).

Пусть $f(\tilde{x}^n)$ — произвольная булева функция, отличная от константы и зависящая от переменных $x_1, x_2, \ldots, x_n$ ($f \in P_2^n$), S — двухполюсная КС или двухполюсная ОИКС (с одним входным и одним выходным полюсом; количество внутренних итеративных полюсов в ОИКС может быть произвольным), реализующая функцию f (т.е. функция проводимости между входным и выходным полюсами в схеме S равна функции f). Пусть на схему S действует источник неисправностей U, способный вызывать размыкания и замыкания контактов в схеме. Схема S называется *тестопригодной (относительно обнаружения неисправностей для источника неисправностей U)* тогда и только тогда, когда при любой неисправности схемы S, вызванной действием на нее источника U, полученная вследствие этой неисправности схема S' реализует функцию $f'(\tilde{x}^n)$, не равную f. Будем говорить, что двухполюсная схема (КС или ОИКС), реализующая функцию $g(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+d+r})$, *моделирует функцию* $f(x_1, \ldots, x_n)$, если существует такой набор булевых констант $(\alpha_1, \ldots, \alpha_r)$, что $g(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+d}), \alpha_1, \ldots, \alpha_r) = f(x_1, \ldots, x_n)$. Минимально возможная величина r при этом называется *входной избыточностью моделирования функции f схемой S*. Обозначим через $D_U(S)$ длину минимального проверяющего теста относительно источника неисправностей U в схеме S, через $D_U(f(\tilde{x}^n))$ (через $\hat{D}_U(f(\tilde{x}^n))$) — минимум величины $D_U(S)$ по всем тестопри-

годным относительно обнаружения неисправностей для источника неисправностей U реализующим (соответственно, моделирующим) функцию $f(\tilde{x}^n)$ схемам S. Пусть $\hat{P}_2^n$ — множество всех булевых функций, существенно зависящих от всех своих переменных $x_1, x_2, \ldots, x_n$ (в частности, $\hat{P}_2^0 = \{0,\ 1\}$). Всюду в дальнейшем будем, не ограничивая общности, считать, что любая не равная тождественно константе функция $f(\tilde{x}^n)$ существенно зависит от всех своих переменных. Через $D_U(n)$ (через $\hat{D}_U(n)$) обозначим *функцию Шеннона (соответственно, слабую функцию Шеннона) длины проверяющего теста относительно источника неисправностей* U, т. е. функцию $D_U(n) = \max\limits_{f(\tilde{x}^n)\in\hat{P}_2(n)} D_U(f(\tilde{x}^n))$ (соответственно, функцию $\hat{D}_U(n) = \max\limits_{f(\tilde{x}^n)\in\hat{P}_2(n)} \hat{D}_U(f(\tilde{x}^n))$). Аналогично вводится функция Шеннона длины диагностического теста относительно источника неисправностей U. Верхний индекс (КС или ОИКС) в обозначении слабой или обычной функции Шеннона длины теста будет указывать на класс схем.

В настоящей работе предлагаются новые верхние оценки обычной и слабой функций Шеннона длины единичного проверяющего теста для ОИКС, демонстрирующие легкотестируемость ОИКС в рамках задачи обнаружения одиночных неисправностей (замыканий или размыканий контактов).

Теорема 1. *Пусть $f(\tilde{x}^n)$ — произвольная булева функция, отличная от константы. Тогда функцию $f(\tilde{x}^n)$ можно реализовать тестопригодной двухполюсной ОИКС, допускающей*

а) единичный проверяющий тест размыкания, имеющий длину, не превосходящую 7,

б) единичный проверяющий тест замыкания, имеющий длину, не превосходящую 4.

Следствие. *Пусть $U^{\mathrm{cl},1}$ — источник одиночных замыканий контактов, а $U^{\mathrm{br},1}$ — источник одиночных размыканий контактов. Тогда при любом натуральном n справедливы оценки:*

$$D^{\text{ОИКС}}_{U^{\mathrm{cl},1}}(n) \le 4, \qquad D^{\text{ОИКС}}_{U^{\mathrm{br},1}}(n) \le 7.$$

Теорема 2. *Пусть $f(\tilde{x}^n)$ — произвольная булева функция, отличная от константы. Тогда функцию $f(\tilde{x}^n)$ можно реализовать тестопригодной ОИКС, допускающей единичный проверяющий тест длины, не превосходящей* 30.

Следствие. *Пусть U^1 — источник одиночных неисправностей контактов (замыканий или размыканий). Тогда при любом натуральном n справедлива оценка: $D^{\text{ОИКС}}_{U^1}(n) \le 30$.*

Теорема 3. *Пусть $f(\tilde{x}^n)$ — произвольная булева функция. Тогда функцию $f(\tilde{x}^n)$ можно смоделировать тестопригодной двухполюсной ОИКС $\hat{\Sigma}_f$, допускающей единичный проверяющий тест, имеющий длину, не превосходящую* 11, *и при этом входная избыточность моделирования функции f этой схемой не превосходит* 5.

Следствие. *Пусть U^1 — источник одиночных неисправностей контактов (замыканий или размыканий). Тогда при любом целом неотрицательном n справедлива оценка: $\hat{D}^{\text{оикс}}_{U^1}(n) \leq 11$.*

Теорема 4. *Пусть $f(\tilde{x}^n)$ — произвольная булева функция. Тогда функцию $f(\tilde{x}^n)$ можно смоделировать тестопригодной двухполюсной КС $\hat{\Sigma}^*_f$, допускающей единичный проверяющий тест, имеющий длину, не превосходящую 35, и при этом входная избыточность моделирования функции f этой схемой не превосходит 5.*

Следствие. *Пусть U^1 — источник одиночных неисправностей контактов (замыканий или размыканий). Тогда при любом целом неотрицательном n справедлива оценка: $\hat{D}^{\text{кс}}_{U^1}(n) \leq 35$.*

Авторы выражают благодарность профессору С. А. Ложкину за обсуждение работы и ценные замечания.

Финансирование работы осуществлялось в рамках проектов РФФИ № 15-01-07474-а и № 13-01-00958-а и Государственного задания № 2014/601 от 06.02.2014.

Список литературы

[1] Редькин Н. П. Надежность и диагностика схем. — М: Изд-во МГУ, 1992. — 192 с.

[2] Ложкин С. А. Лекции по основам кибернетики. — М: МАКС Пресс, 2004. — 256 с.

О вычислительной сложности языков, распознаваемых автоматами со словарём (Set Automata)

Рубцов Александр Александрович

МФТИ/НИУ ВШЭ, e-mail: rubtsov99@gmail.com

Назовём автоматом со словарём односторонний конечный автомат с рабочей лентой и дополнительной структурой — словарём, который фактически является множеством. Автомат в процессе работы пишет на рабочую ленту запрос, после чего выполняет одну из операций: **in** — операция добавления слова на ленте в словарь, **out** — операция удаления слова из словаря, если оно там есть, и **test** — запрос на принадлежность слова с рабочей ленты словарю. После каждой операции со словарём рабочая лента опустошается. Будем обозначать детерминированный автомат со словарём как DSA, а недетерминированный как NSA (от Set Automata), следуя работам [1], [2], в которых впервые вводится это понятие. Автоматы со словарём интересны тем, что подобно МП-автоматам увеличивают вычислительную силу конечных автоматов, однако сохраняют такие важные свойства как разрешимость проблемы пустоты языка, а также распознаваемые ими языки замкнуты относительно объединения и пересечения с регулярными языками. Кроме того, языки, распознаваемые DSA, находятся в

общем положении с детерминированными КС-языками. В этой работе мы показали, что языки, распознаваемые DSA и NSA, лежат в $\mathbf{P}$ и $\mathbf{NP}$ соответственно, более того среди них есть полные языки.

Автомат со словарём M задан набором

$$M = \langle S, \Sigma, \Gamma, \lhd, \delta, s_0, F\rangle, \text{где}$$

- S — множество состояний;
- Σ — алфавит входной ленты;
- Γ — алфавит рабочей ленты;
- $\lhd \notin \Sigma$ — маркер правого конца слова;
- $s_0 \in S$ — начальное состояние;
- $F \subseteq S$ — множество принимающих состояний;
- δ — отношение переходов

$$\delta : S \times (\Sigma \cup \{\varepsilon, \lhd\}) \times [S \times (\Gamma^* \cup \{\textbf{in}, \textbf{out}\}) \cup S \times \{\textbf{test}\} \times S] .$$

Под конфигурацией будем понимать набор $S \times (\Sigma \cup \{\lhd\})^* \times \Gamma^* \times \mathbb{S}$, где $\mathbb{S}$ — множество, содержащее элементы словаря. Для наглядности определим δ через отношение на конфигурациях.

$$\begin{aligned}
&(s, xv, z, \mathbb{S}) \vdash (s', v, zz', \mathbb{S}), && \text{при } \delta(s, x) = (s', z');\\
&(s, xv, z, \mathbb{S}) \vdash (s', v, \varepsilon, \mathbb{S} \cup \{z\}), && \text{при } \delta(s, x) = (s', \textbf{in});\\
&(s, xv, z, \mathbb{S}) \vdash (s', v, \varepsilon, \mathbb{S} \setminus \{z\}), && \text{при } \delta(s, x) = (s', \textbf{out});\\
&(s, xv, z, \mathbb{S}) \vdash (s_+, v, \varepsilon, \mathbb{S}), && \text{при } \delta(s, x) = (s_+, \textbf{test}, s_-), z \in \mathbb{S};\\
&(s, xv, z, \mathbb{S}) \vdash (s_-, v, \varepsilon, \mathbb{S}), && \text{при } \delta(s, x) = (s_+, \textbf{test}, s_-), z \notin \mathbb{S}.
\end{aligned}$$

Конфигурация является принимающей, если состояние автомата принадлежит F и слово прочитано, то есть конфигурация имеет вид $(s_f, \varepsilon, z, \mathbb{S})$, причём слово z может быть пустым. Автомат со словарём принимает слово w, если существует ход из начальной конфигурации $(q_0, w\lhd, \varepsilon, \varnothing)$ в принимающую.

Лемма 1. *DSA распознаёт* $\mathbf{P}$*-трудный язык.*

Доказательство. Возьмём $\mathbf{P}$-полный язык CVP вычисления булевых схем и сведём его к языку L, распознаваемому DSA. Построим язык L, описав поведение автомата со словарём на входе. Будем предполагать, что автомат получает на вход последовательность присваиваний, каждое из которых записано в обратном порядке, т.е. $P_j \operatorname{op} P_k =: P_i$, кроме того, в отличие от CVP переприсваивания допустимы и последовательность присваиваний не обязана быть корректной — в случае, если P_j или P_k не определены, полагаем, что они имеют значение ноль. Индексы присваиваний закодированы двоичными словами. Такие условия на вход задаются регулярными ограничениямя. В случае их невыполнения автомат считывает слово до конца и отвергает его.

В случае присваивания $1 =: P_i$, автомат помещает P_i в словарь, в случае присваивания нуля автомат просто считывает описание P_i без работы со словарём. В случае остальных присваиваний автомат проверяет, находятся ли операнды в словаре; отсутствие интерпретирует как равенство нулю, а вхождение как равенство единице. Автомат кладёт в словарь P_i, в случае равенства левой части присваивания единице. Автомат принимает слово, если последнее вычисленное значение перед маркером конца строки было равно единице.

Легко видеть, что такой автомат правильно вычисляет значение булевой схемы, присваивания которой записаны в обратном порядке. Указанная сводимость реализуется на логарифмической памяти.

Лемма 2. *Любой язык, распознаваемый* DSA*, лежит в классе* $\mathbf{P}$.

Доказательство. DSA легко эмулировать трёхленточной машиной Тьюринга, первая лента которая служит входной лентой, вторая рабочей лентой, а третья лента хранит содержимое словаря. Слово, записанное на рабочей ленте при обработке подслова u, ограничено по длине $c|u|$, где c — некоторая константа. Таким образом, сумма длин всех слов в словаре на входе w ограничена $c|w|$. Следовательно, операции работы со словарём осуществляются за полиномиальное время, а их число также ограничено линейной функцией.

Теорема 1. *Задача проверки принадлежности слова языку, распознаваемому* DSA*, является* $\mathbf{P}$*-полной.*

Язык SA-SAT состоит из слов вида $x_1\#x_2\#\ldots\#x_n\#\#\varphi(x_1,\ldots,x_n)$, где слова $x_i \in \{0,1\}^*$ кодируют переменные, а $\varphi(x_1,\ldots,x_n)$ кодирует 3-КНФ C, причём выполнима КНФ C', которая получается из C удалением дизъюнктов, содержащих литералы по перменным, которые встречаются в списке $x_1\#x_2\#\ldots\#x_n\#\#$.

Лемма 3. *Существует* NSA*, распознающий язык* SA-SAT. *Язык* SA-SAT *является* $\mathbf{NP}$*-полным.*

Доказательство. Сначала автомат обрабатывает префикс, содержащий описание переменных до двух решёток. На префиксе, содержащем описание переменных, автомат недетерминировано угадывает значение $a \in \{0,1\}$ переменной x_i и кладёт в словарь пару (x_i, a), причём если существует повторяющаяся пара $x_i = x_j$, то в одном случае автомат добавляет в словарь пару $(x_i, 0)$, а в другом $(x_i, 1)$. При обработке КНФ C автомат недетерминировано выбирает литерал, который делает дизъюнкт истинным, и проверяет вхождение соответствующей пары (x_i, a) в словарь. Таким образом, все тесты истинны тогда и только тогда, когда 3-КНФ C' выполнима.

Язык SA-SAT очевидно является $\mathbf{NP}$-трудным, а значит и $\mathbf{NP}$-полным.

Основным результатом является следующая теорема, доказательство которой технически трудное.

Теорема 2. *Пусть L язык, распознаваемый NSA, тогда $L \in \mathbf{NP}$.*

Работа выполнена при поддержке РФФИ (проект № 14–01–00641).

Список литературы

[1] M. Kutrib, A. Malcher, M. Wendlandt. Deterministic Set Automata // In A. M. Shur, M. V. Volkov (eds.): Developments in Language Theory (DLT 2014). LNCS 8633. — Springer, 2014. — P. 303–314.

[2] M. Kutrib, A. Malcher, M. Wendlandt. Regularity and Size of Set Automata // In H. Jürgensen, J. Karhumäki, A. Okhotin (eds.): Descriptional Complexity of Formal Systems (DCFS 2014), LNCS 8614. — Springer, 2014. — P. 281–293.

Об одной оценке сложности клеточных схем из ненадежных элементов

Рыбаков Андрей Валентинович

Пензенский государственный университет, e-mail: anajrov@gmail.com

Впервые задачу синтеза надежных схем из ненадежных функциональных элементов (ФЭ) рассматривал Дж. фон Нейман. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε, $\varepsilon \in (0; 1/2)$ подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию ϕ, а в неисправном — функцию $\overline{\phi}$. С помощью итерационного метода Дж. фон Нейман установил [1], что в произвольном полном базисе при $\varepsilon \in (0; 1/6]$ любую булеву функцию можно реализовать схемой, вероятность ошибки, на выходе которой при любом входном наборе значений переменных не превосходит $c\varepsilon$ (c — некоторая положительная константа, зависящая от базиса).

В этой статье рассматривается реализация булевых функций клеточными схемами (КС) (еще их называют плоскими схемами), содержащими как надежные, так и ненадежные элементы, и оценивается их ненадежность и сложность. Впервые класс клеточных схем рассматривается в работе С. С. Кравцова [2]. Для них определен базис, состоящий из двух типов элементов: функциональных (рис. 1 (а, б, в)) и коммутационных (рис. 1 (г, д, е)).

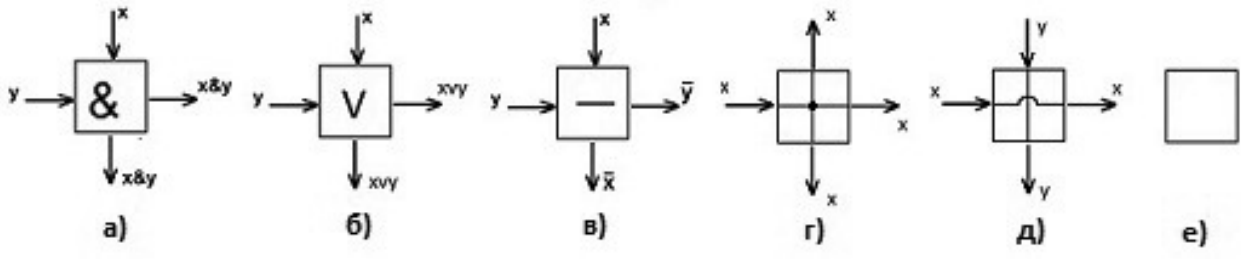

Рис. 1.

Каждый из элементов может быть повернут на плоскости на угол $\frac{k\pi}{2}$, ($k = 0, 1, 2, 3$). Предполагается, что коммутационные элементы абсолютно надежны, а на любом из двух выходов каждого из функциональных элементов

с вероятностью ε, $\varepsilon \in (0; 1/2)$ независимым образом появляются инверсные неисправности.

Считаем, что КС, содержащая ненадежные элементы, реализует булеву функцию $f(\widetilde{x}^n)$, ($\widetilde{x}^n = (x_1, ..., x_n)$), если она реализует $f(\widetilde{x}^n)$ при отсутствии неисправностей.

Пусть КС S реализует функцию $f(\widetilde{x}^n)$. Обозначим через $P_{\overline{f(\widetilde{a}^n)}}(S, \widetilde{a}^n)$ вероятность появления ошибки на входном наборе $\widetilde{a}^n$ схемы S. Ненадежность $P(S)$ схемы S определяется как максимальная вероятность ошибки на выходе схемы при всевозможных входных наборах. Надежность схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf\limits_S P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, ..., x_n)$. Схема A из ненадежных элементов, реализующая функцию f, называется асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Сложность КС, которая, напомним, имеет вид прямоугольника, определяется как площадь этого прямоугольника. Определим две функции Шеннона для площади схем этой модели. Обозначим высоту клеточной схемы S через $h(S)$, длину через $l(S)$ и будем считать, что $h(S) \leq l(S)$.

Пусть f — произвольная булева функция. Обозначим через $L(f)$ наименьшую из площадей $L(S) = l(S)h(S)$, где минимум берется по всем КС S, реализующим функцию f, а через $L(n)$ — функцию Шеннона, которая равна $L(n) = \max(L(f))$, где максимум берется по всем функциям f от n переменных.

Аналогично определяется функция Шеннона $L^h(n)$ для случая, когда высота h клеточных схем фиксирована. Для клеточных схем из абсолютно надежных элементов в работе [3] получена асимптотика функции Шеннона (в произвольном базисе при $h \geq 4$, а в рассматриваемом базисе при $h \geq 3$), которая имеет вид $L^h(n) \sim \frac{h2^n}{\log n}$

В работе [4] описан метод построения асимптотически оптимальных по надежности клеточных схем, доказаны верхняя и нижняя оценки ненадежности, а так же получена оценка сложности. Позже оценку сложности [5] удалось улучшить. Сформулируем этот результат.

Теорема 1 [5]. *Любую булеву функцию $f(x_1, x_2, ..., x_n)$ можно реализовать такой клеточной схемой S, что $P(S) \leq 3\varepsilon + 48\varepsilon^2$, $L(S) \lesssim 36 \cdot 4^n$ при всех $\varepsilon \in (0, 1/1000]$.*

Приведенную в теореме 1 оценку сложности асимптотически оптимальных по надежности клеточных схем можно улучшить (см. теорему 2).

Теорема 2. *Любую булеву функцию $f(x_1, x_2, ..., x_n)$ можно реализовать такой клеточной схемой S, что $P(S) \leq 3\varepsilon + 1185\varepsilon^2$, $L(S) \lesssim \frac{192 \cdot 4^n}{n^2}$ при всех $\varepsilon \in (0, 1/2000]$.*

Работа выполнена при поддержке РФФИ (проект № 14-01-31360).

Список литературы

[1] von Neuman J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata studies / Edited by Shannon C., McCarthy J.

— Princeton University Press, 1956. — P. 43–98. (Русский перевод: Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. — М.: ИЛ, 1956. — С. 68–139.)

[2] Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. — Вып. 19. — М.: Наука, 1967. — С. 273–285.

[3] Улесова А. Ю. Сложность реализации булевых функци в некоторых моделях клеточных схем // Дипломная работа. — Москва: МГУ имени М. В. Ломоносова, факультет ВМК, кафедра математической кибернетики. — 2010. — 25 с.

[4] Алехина М. А., Рыбаков А. В. Синтез и сложность асимптотически оптимальных по надежности клеточных схем // Известия высших учебных заведений. Физико-математические науки. — 2014. — № 4. — С. 3–12.

[5] Рыбаков А. В. Улучшение оценки сложности асимптотически оптимальных по надежности клеточных схем // Труды XI Международной научно-практической конференции «Новые информационные технологии и системы», 25–27 ноября 2014 г. — Пенза: Издательство ПГУ, 2014. — С. 42–45.

Распределение признаков по классам в дискретной трехдольной модели данных

Сабурова Мария Ивановна[1], **Майсурадзе Арчил Иериевич**[2]

[1] Московский государственный университет имени М. В. Ломоносова, e-mail: masha-saburova@ya.ru
[2] Московский государственный университет имени М. В. Ломоносова, e-mail: maysuradze@cs.msu.ru

Задача распределения признаков по классам

Дана конечная обучающая выборка, в которой каждый объект имеет признаковое описание и метку класса из конечного набора предопределенных классов. Требуется каждый признак однозначно отнести либо к одному из предопределенных классов, либо к специальному дополнительному классу. Интерпретация дополнительного класса зависит от предметной области; общая идея состоит в том, что изменение значений признаков, отнесенных к дополнительному классу, не является специфическим ни для какого предопределенного класса.

Нас интересуют такие ситуации, когда значения признака интерпретируются как наличие или отсутствие у объекта некоторого (соответствующего признаку) свойства, причём за распознавание класса отвечает именно наличие свойства, а не его отсутствие. Предельным случаем проявления этого требования является ситуация, когда признаки — это предикаты наличия свойства у объекта. В указанной ситуации принято говорить о маркерах или индикаторах свойств. Тогда рассматриваемая задача интерпретируется как задача распределения маркеров по классам, её можно также воспринимать как задачу однозначной классификации маркеров. Результат решения задачи распределения маркеров

по классам интерпретируется как ядра классов. Таким образом, в данной постановке результат распределения признаков по классам имеет собственную интерпретацию и ценность.

В предметной области рубрикации текстов [1] и контент-анализа рассматриваемая задача может интерпретироваться как задача выделения лексического (семантического) ядра рубрики. При этом объектами являются фрагменты текста, классами являются рубрики текстовой коллекции, а признаки текстов показывают присутствие лексических маркеров (например, отдельных слов, словосочетаний, специфических терминов). В данной предметной области дополнительный класс иногда называют классом общей лексики.

В предметной области анализа экспрессии генов [2] рассматриваемая задача может интерпретироваться как задача поиска комплекса генов, ответственных за специфические состояния или процессы в организме. При этом объектами являются организмы, классам соответствуют специфические состояния, а признаки показывают уровень экспрессии каждого из изучаемых генов. В данной предметной области нет устоявшегося названия для дополнительного класса.

Трёхдольная модель данных

Пусть признаки — это маркеры, то есть предикаты наличия свойства у объекта. Тогда данные могут быть естественным образом представлены в рамках реляционной модели набором бинарных отношений.

Определение. *Трёхдольная модель данных* — это реляционная модель, в которой три единицы анализа: объекты, маркеры и классы — и три бинарных гетерогенных отношения между этими единицами анализа.

Для задачи распределения маркеров по классам формализация в рамках трёхдольной модели получает следующее уточнение — отношение между маркерами и классами является функциональным, то есть это частичное отображение маркеров в исходные классы. Такую трёхдольную модель данных, в которой часть бинарных отношений должна быть частичными отображениями, будем называть *трёхдольной полужесткой*.

Функция как параметр классификатора

В исследуемой постановке разметка дана для объектов, а не признаков. Сведём задачу классификации признаков к задаче классификации объектов. Для этого введём линейную информационную модель с неотрицательными весами признаков, в которую частичная функция из признаков в классы входит явным образом как параметр, т. е. в классификаторе явно происходит приписывание признака к классу. Пусть T — число признаков, t — номер признака от 1 до T, I — число размеченных объектов, i — номер объекта от 1 до I, J — число классов, j — номер класса от 1 до J, a_t — номер класса, к которому приписан признак t (искомая функция), f_{it} — значение признака t для объекта i (в частности, 0 или 1 для бинарного отношения объект-признак), c_i — истинная метка объекта i. Модель действует по формуле $\Gamma_k = \sum_{t=1}^{T} w_t f_t[a_t = k]$. Предлагаемый метод обучения модели напоминает многоклассовый SVM [3], и в упрощенном виде

в случае линейно разделимой выборки задача обучения выглядит следующим образом:

$$\begin{cases} \dfrac{1}{2}||w||^2 \to \min \\ \displaystyle\sum_t w_t f_{it}([a_t = c_i] - [a_t = j]) \geq 1,\ \forall i,\ \forall j \neq c_i, \\ w_i \geq 0,\ \forall t. \end{cases}$$

Эксперименты на модельных и реальных данных

Семейство модельных данных — 3 класса, 60 объектов (по 20 на класс), 600 признаков (по 200 на класс). От 10 до 100 шумовых признаков, уровень шума от 30% до 70%. Сравнение полученной разметки признаков с заранее заданными ответами показало точность от 86% на самой сильной зашумленности до 99% на данных с наименьшим шумом. Шум менее 30% на 3 классах просто не может существенно исказить признак.

Реальные данные — ответы на вопросы интервью, 20 респондентов, 6 тем. В соответствии с темами каждый документ был разбит на 6 разделов, итого 120 объектов. Каждая тема интервью представляет собой один класс. После нормализации текстов, удаления имен собственных в корпусе осталось 3657 разных лемм. Точность на уровне 20 слов при сравнении с экспертной разметкой составила от 70% до 90% в зависимости от темы.

Заключение

Предложена дискретная трехдольная модель данных, применимая в разных предметных областях, например в социологии, наукометрии, обработке текстов. Данная модель удобна для формализации и решения разных аналитических задач, например классификация объектов, определение класса нового объекта и многие другие, включая рассматриваемую задачу распределения маркеров по классам. Предложена информационная модель и метод её обучения, которые даже в упрощенном варианте показывают результаты, сравнимые с экспертным мнением.

Исследование выполнено при финансовой поддержке РФФИ (проекты № 13-01-00751, № 15-07-09214).

Список литературы

[1] Sebastiani F. Machine learning in automated text categorization // ACM computing surveys (CSUR). — 2002. — V. 34. — N 1. — P. 1–47.

[2] Velculescu V. E. et al. Serial analysis of gene expression // Science. — 1995. — V. 270. — N 5235. — P. 484–487.

[3] Duan K. B., Keerthi S. S. Which is the best multiclass SVM method? An empirical study // Multiple Classifier Systems. — Springer Berlin Heidelberg, 2005. — P. 278–285.

О представлении помеченных графов множествами слов в алфавите меток

Сапунов Сергей Валерьевич

Институт прикладной математики и механики НАН Украины, e-mail: sapunov_sv@yahoo.com

Помеченные графы широко применяются в информатике для описания и моделирования разнообразных вычислительных процессов. В этом контексте наиболее изучены конечные орграфы с помеченными дугами (LTS [1], взвешенные автоматы [2], конечные автоматы). Тем не менее, существует множество вычислительных процессов, естественным образом представляемых графами с помеченными вершинами (в программировании, робототехнике [3], верификации моделей [4]). В данном докладе рассматривается модель информационной системы как системы взаимодействующих объектов: агента и его операционной среды [5]. Операционная среда представляется в виде топологической модели, т. е. графа с помеченными вершинами.

Одной из центральных задач анализа операционной среды является построение ее карты, т. е. восстановление графа среды [3]. Причем построенная карта должна быть пригодной для дальнейшей навигации агентов (под навигацией понимается перемещение агента из текущей области его операционной среды в заданную ее область). В [6] предложено решение задачи восстановления связного неорграфа мобильным агентом путем так называемой детерминированной разметки его вершин. При решении этой задачи удобным оказалось использование представления помеченного графа парой конечных множеств слов в алфавите меток вершин. Эти слова порождаются траекториями перемещений агента по вершинам графа и могут также служить для описания таких траекторий. В докладе рассматривается задача отыскания критериев, которым должна удовлетворять пара множеств слов для того, чтобы однозначно выделять данный граф из класса всех помеченных графов.

Помеченным графом называется простой конечный связный неориентированный граф с помеченными вершинами $G = (V, E, M, \mu)$, где V — множество вершин, $|V| = n$, E — множество ребер (т. е. неупорядоченных пар вершин), M — множество меток, $|M| = m$, $\mu : V \to M$ — сюръективная функция разметки. Путем в графе G будем называть последовательность вершин $p = v_1 \dots v_k$ такую, что $(v_i, v_{i+1}) \in E$, $i = 1, \dots, k-1$. Меткой $\mu(p)$ пути p назовем слово $w = \mu(v_1) \dots \mu(v_k)$ в алфавите меток M. Будем говорить, что слово w определяется вершиной v_1. Множество L_v всех слов $w \in M^+$, определяемых вершиной $v \in V$, будем называть языком, определяемым этой вершины. Граф G будем называть приведенным, если для любых вершин $v, s \in V$ из $v \neq s$ следует $L_v \neq L_s$. Языком L_G графа G назовем объединение $\bigcup_{v \in V} L_v$ языков всех его вершин. Если в графе G зафиксирована начальная вершина $v_0 \in V$, то положим $L_G = L_{v_0}$. Введем операцию $\star : V \times M^+ \to 2^V$ соотношением: для любой вершины $v \in V$ и любого слова $w \in M^+$ через $v \star w$ обозначим множество всех вершин $s \in V$ таких, что существует путь p из v в s, и $\mu(p) = w$.

Ясно, что если слово $w \in L_v$, то $|v \star w| > 0$ и $|v \star w| = 0$ в противном случае. Инверсией слова $w = \mu(v_1) \dots \mu(v_k)$ назовем слово $w^{-1} = \mu(v_k) \dots \mu(v_1)$.

Под окрестностью Γ_v вершины $v \in V$ будем понимать множество всех смежных с ней вершин. Функцию разметки $\mu : V \to M$ будем называть детерминированной или Д-разметкой, если для любой вершины $v \in V$ и любых вершин $s, t \in \Gamma_v$ из $s \neq t$ следует $\mu(s) \neq \mu(t)$. Помеченный граф с детерминированной функцией разметки будем называть детерминированным или Д-графом. Показано, что для любой вершины v Д-графа путь с меткой $w \in L_v$ определен однозначно.

В [6] обосновано использование Д-разметки для восстановления графов мобильным агентом, поле зрения которого ограничено окрестностью текущей вершины. В этой работе в качестве имени вершины использовалась метка простого пути в нее из начальной вершины по дереву обхода в ширину. Обозначим множество таких имен всех вершин графа G через A_G. Ясно, что A_G определяет некоторое остовное дерево этого графа. Обозначим через C_G множество всех слов вида $w_i w_j^{-1}$, где $w_i, w_j \in A_G$, вершины с именами w_i и w_j смежны в графе G, но не смежны в рассматриваемом дереве. Ясно, что множество C_G описывает базис циклов, определяемый данным остовным деревом.

Теорема 1. *Пара конечных множеств слов (A_G, C_G) позволяет однозначно восстановить граф G.*

Разработан алгоритм отыскания кратчайших путей между вершинами помеченного графа, заданного такой парой. Этот алгоритм может служить составной частью алгоритмов восстановления графа среды и самостоятельного определения агентом своего местоположения в среде.

Обозначим через $\mathbf{A}_G$ множество всех слов $wx \in M^+$ таких, что $x \in M$, $w \in L_G$ и $wx \notin L_G$. Обозначим через $\mathbf{C}_G$ множество всех слов $w \in L_G$ таких, что $v_0 \star w = v_0$. Показано, что ни множество $\mathbf{C}_G$, ни любое конечное подмножество множества $\mathbf{A}_G$ по отдельности не выделяют граф G из класса K всех помеченных графов. Пару $\{A, C\}$ конечных множеств слов назовем определяющей парой помеченного графа G, если одновременно выполняются условия: 1) $A \subseteq \mathbf{A}_G$ и $C \subseteq \mathbf{C}_G$; 2) для любого графа $H \in K$ из $A \subseteq \mathbf{A}_H$ и $C \subseteq \mathbf{C}_H$ следует изоморфизм графов H и G.

Обозначим через $\tilde{A}_G$ множество слов $A_G X \cap \mathbb{A}_G$, где $A_G X$ состоит из всех слов вида wx таких, что $w \in A_G$ и $x \in M$. Доказана справедливость следующего утверждения.

Теорема 2. *Пара $\left(\tilde{A}_G, C_G\right)$ является определяющей парой графа G.*

Предложенная определяющая пара аналогична системе определяющих соотношений для конечного автомата. Разработан метод проверки изоморфизма данного графа и произвольного представителя класса всех помеченных графов основанный на представлении графа определяющей парой.

Список литературы

[1] Letichevsky A. Algebra of behavior transformation and its application // Structural Theory of Automata, Semigroups and Universal Algebra. — Springer, 2005. — P. 241–272.

[2] Droste M., Kuich W., Vogler H. Handbook of Weighted Automata. — Springer, 2009. — 608 p.

[3] Dudek G., Jenkin M. Computational Principles of Mobile Robotics. — Cambridge : Cambridge University Press, 2010. — 406 p.

[4] Baier C., Katoen J.-P. Principle of Model Checking. — MIT Press, 2008. — 984 p.

[5] Капитонова Ю. В., Летичевский А. А. Математическая теория проектирования вычислительных систем. — М.: Наука, 1988. — 298 с.

[6] Грунский И. С., Сапунов С. В. Восстановление графа операционной среды мобильного робота путем разметки вершин, пригодной для дальнейшей навигации // Искусственный интеллект. — 2012. — № 4. — С. 420–428.

Сложность систем функций алгебры логики и функций трехзначной логики в классах поляризованных полиномиальных форм

Селезнева Светлана Николаевна

Московский государственный университет имени М. В. Ломоносова, e-mail: selezn@cs.msu.su

Поляризованная полиномиальная форма (ППФ) — это сумма по модулю k произведений переменных или их отрицаний. Количество отрицаний над каждой переменной определяется вектором поляризации этой ППФ. Длина ППФ — это число ее слагаемых, длина функции k-значной логики в классе ППФ — это минимальная длина среди всех ППФ, которые реализуют эту функцию. В [1] доказано, что для каждой функции алгебры логики $f(x_1, \ldots, x_n)$ найдется ППФ, реализующая функцию f, с длиной, не превосходящей $2^{n+1}/3$, и построена такая последовательность функций алгебры логики $f_n(x_1, \ldots, x_n)$, что длина каждой из функций f_n в классе ППФ равна $\lfloor 2^{n+1}/3 \rfloor$, где $\lfloor a \rfloor$ обозначает максимальное целое число, не превосходящее число a. В отличие от двузначного случая к настоящему моменту не получено значение максимальной длины функций трехзначной логики в классе ППФ. В [2] доказано, что для каждой функции трехзначной логики $f(x_1, \ldots, x_n)$ найдется ППФ, реализующая функцию f, с длиной, не превосходящей $6 \cdot 3^n/7$. В [3] построена такая последовательность функций трехзначной логики $f_n(x_1, \ldots, x_n)$, что длина каждой из функций f_n в классе ППФ не меньше $\lfloor 3^{n+1}/4 \rfloor$. Отметим, что ППФ является логической основой для программируемых логических матриц (ПЛМ) [4], и длина ППФ соответствует сложности ПЛМ. Однако, при помощи ПЛМ реализуются не только отдельные функции, но и системы функций. В

настоящей работе исследуется сложность систем функций k-значной логики в классе ППФ.

Пусть $k \geq 2$ — натуральное число, $E_k = \{0, 1, \ldots, k-1\}$. Весом набора $\alpha = (a_1, \ldots, a_n) \in E_k^n$ назовем число $|\alpha| = \sum\limits_{i=1}^{n} a_i$ (здесь рассматривается сумма целых чисел). Функцией k-значной логики называется отображение $f(x_1, \ldots, x_n) : E_k^n \to E_k$, $n = 0, 1, \ldots$. Множество всех функций k-значной логики обозначим как P_k, множество всех функций k-значной логики, зависящих от переменных $x_1, \ldots, x_n$ обозначим как P_k^n.

Поляризованной переменной x_i с поляризацией d, $d \in E_k$, назовем выражение вида $(x_i + d)$. Поляризованным мономом по вектору поляризации δ, $\delta = (d_1, \ldots, d_n) \in E_k^n$, назовем произведение вида $(x_{i_1} + d_{i_1})^{m_1} \cdot \cdots \cdot (x_{i_r} + d_{i_r})^{m_r}$, где $1 \leq i_1 < \cdots < i_r \leq n$, и $1 \leq m_1, \ldots, m_r \leq k-1$. Выражение вида $\sum\limits_{i=1}^{l} c_i \cdot K_i$, где $c_i \in E_k \setminus \{0\}$ — коэффициенты, K_i — попарно различные мономы, поляризованные по вектору $\delta \in E_k^n$, $i = 1, \ldots, l$, назовем *поляризованной полиномиальной нормальной формой* (ППФ) *по вектору поляризации* δ. Будем полагать константу 0 ППФ по произвольному вектору поляризации. При простых k для каждого вектора поляризации δ каждую функцию k-значной логики можно представить однозначной ППФ по этому вектору поляризации. Эту ППФ будем обозначать как $P^\delta(f)$.

Длиной $l(p)$ ППФ p назовем число попарно различных слагаемых в этой ППФ. Положим, что $l(0) = 0$. При простых k *длиной* функции k-значной логики в классе ППФ называется величина $l_k^{\text{ППФ}}(f) = \min\limits_{\delta \in E_k^n} l(P^\delta(f))$.

Сложностью системы ППФ, имеющих один и тот же вектор поляризации, называется число попарно различных слагаемых, встречающихся во всех этих ППФ. При простых k *сложностью* $L_k^{\text{ППФ}}(F)$ системы функций k-значной логики $F = \{f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\}$ в классе ППФ называется минимальная сложность среди всех таких систем ППФ $\{p_1, \ldots, p_m\}$, что все ППФ $p_1, \ldots, p_m$ имеют один и тот же вектор поляризации, и ППФ p_j реализует функцию f_j, $j = 1, \ldots, m$. При простых k для произвольной системы функций k-значной логики $F = \{f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\}$ верно, что $L_k^{\text{ППФ}}(F) \leq k^n$.

Пусть k — простое число, и $A_k \subseteq P_k$, а $A_k^n = A_k \cap P_k^n$. Введем функцию Шеннона $L_{A_k}^{\text{ППФ}}(m, n)$ сложности систем функций k-значной логики, принадлежащих множеству A в классее ППФ:

$$L_{A_k}^{\text{ППФ}}(m, n) = \max_{B \subseteq A_k^n, |B| = m} L_k^{\text{ППФ}}(B).$$

Если $A_k = P_k$, то функцию Шеннона будем обозначать как $L_k^{\text{ППФ}}(m, n)$.

Функция k-значной логики $f(x_1, \ldots, x_n)$ называется симметрической, если $f(\pi(x_1), \ldots, \pi(x_n)) = f(x_1, \ldots, x_n)$ для произвольной перестановки π на

множестве переменных $\{x_1, \ldots, x_n\}$. Множество всех симметрических функций k-значной логики обозначим как S_k. Через $f^{(n)}_{(\tau_0\tau_1\ldots\tau_{T-1})}$ будем обозначать такую симметрическую функцию из P_k, что $f(\alpha) = \tau_j$ при $|\alpha| = j(\mathrm{mod}\ T)$ для каждого набора $\alpha \in E_k^n$.

В работе доказаны следующие теоремы.

Теорема 1. *Для каждой из систем симметрических функций алгебры логики* $F_1 = \{f_n, g_n\}$, $F_2 = \{f_n, h_n\}$, $F_3 = \{g_n, h_n\}$, *где* $f_n = f^{(n)}_{(110)}$, $g_n = f^{(n)}_{(101)}$, $h_n = f^{(n)}_{(011)}$ *верно, что* $L_2^{\text{ППФ}}(F_j) = 2^n$, $n \geq 1$, $j = 1, 2, 3$.

Теорема 2. *Для всех* $m \geq 2$, $n = 1, 2, \ldots$ *верны равенства*

$$L_2^{\text{ППФ}}(m, n) = L_{S_2}^{\text{ППФ}}(m, n) = 2^n.$$

Теорема 3. *При* $n \geq 1$ *для симметрических функций трехзначной логики* $f_n = f^n_{(1122)}$ *и* $g_n = f^n_{(1221)}$ *верны следующие равенства:*

$$l_k^{\text{ППФ}}(f_n) = l_k^{\text{ППФ}}(g_n) = (3^{n+1} - 1)/4, \text{ если } n \text{ – нечетное число},$$
$$l_k^{\text{ППФ}}(f_n) = l_k^{\text{ППФ}}(g_n) = (3^{n+1} - 3)/4 + 1, \text{ если } n \text{ – четное число}.$$

Теорема 4. *Для каждой из систем симметрических функций трехзначной логики* $F_1 = \{f_n, g_n\}$, $F_2 = \{h_n, t_n\}$, *где* $f_n = f^{(n)}_{(1122)}$, $g_n = f^{(n)}_{(1221)}$, $h_n = f_n + g_n$, $t_n = 2f_n + g_n$, *верно, что* $L_3^{\text{ППФ}}(F_j) = 3^n$, $n \geq 1$, $j = 1, 2$.

Теорема 5. *Для всех* $m \geq 2$, $n = 1, 2, \ldots$ *верны равенства*

$$L_3^{\text{ППФ}}(m, n) = L_{S_3}^{\text{ППФ}}(m, n) = 3^n.$$

Работа поддержана РФФИ, гранты 13–01–00684-а, 13–01–00958-а.

Список литературы

[1] Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, № 3. — С. 323–326.

[2] Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, № 2. — С. 48–53.

[3] Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — № 3. — С. 40–45.

[4] Угрюмов Е. П. Цифровая схемотехника. — СПб.: БХВ-Петербург, 2004.

Распознавание отдельных предложений с использованием быстрого непрерывного вейвлет-преобразования

Семенов Владимир Ильич, Сорокин Геннадий Михайлович, Шурбин Александр Кондратьевич, Христофоров Олег Владимирович

Чувашский государственный университет им. И. Н. Ульянова, e-mail: syundyukovo@yandex.ru, shurti@mail.ru, kafobph@rambler.ru, gensorokmich@mail.ru

В отличие от печатного текста или искусственных сигналов естественная речь не допускает простого и однозначного членения на элементы (фонемы, слова, фразы), поскольку эти элементы не имеют явных физических границ. Они вычленяются в сознании слушателя — носителя данного языка — в результате сложного многоуровневого процесса распознавания и понимания речи [1].

Для сегментации речи в работе используется МНАТ-вейвлет, длительность речевого сигнала составляет четыре секунды, частота дискретизации речевого сигнала — 8000 Гц, разрешение — 16 бит, режим записи — моно.

Для вычисления вейвлет-спектра речевого сигнала используется формула непрерывного вейвлет-преобразования.

$$W(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} S(t)\Psi(\frac{t-b}{a})dt.$$

Вычисление вейвлет-спектра производится в частотной области с применением быстрого преобразования Фурье (БПФ) [2, 3].

Для определения границ между гласными и согласными буквами слова в работе вычисляется энергия сегментов функций $W(1,b)$, $W(2,b)$, $W(20,b)$ и исследуемого слова $S(t)$. В каждом сегменте вычисляются коэффициенты Фурье $d(i)$, $e(i)$ функций $W(2,b)$ и $W(20,b)$ с помощью БПФ. Таким образом, математической моделью речевого сигнала в сегменте является:

$$d(n) = \frac{1}{M} \sum_{k=0}^{M-1} W(a,k) \cos \frac{2\pi nk}{M}, \tag{1}$$

$$e(n) = \frac{1}{M} \sum_{k=0}^{M-1} W(a,k) \sin \frac{2\pi nk}{M}. \tag{2}$$

По формуле

$$F(i) = d^2(i) + e^2(i) \tag{3}$$

вычисляется Фурье-спектр функций $W(1,b)$, $W(2,b)$, $W(20,b)$ и $S(t)$. Энергия сегментов вычисляются по формуле

$$E = \sum_{i=1}^{n} F(i). \tag{4}$$

Обозначим энергию сегментов вейвлет-преобразования (ВП) $W(1,b)$, $W(2,b)$ и исследуемого слова $S(t)$ функциями $E1(n)$, $E2(n)$ и $E3(n)$ соответственно, где n меняется от 1 до 256. Результаты анализа показывают, что энергия сегментов гласных букв в $W(1,b)$, $W(2,b)$ выделяется в виде максимальных пиков, а энергия согласных букв всегда ниже, чем энергия гласных. Энергия сегментов шипящих букв в $E1(n)$ выделяется в виде максимальных пиков, в $E2(n)$ и $E3(n)$ — в виде минимумов. Чтобы определить местоположение фонем в слове, вычисляется ВП функцией $E1(n)$, $E2(n)$ и $E3(n)$ с масштабным коэффициентом $a = 4$. Математической моделью речевого сигнала при нахождении границ между гласными и согласными звуками речи является вейвлет-спектр энергии сегментов вейвлет-спектра речевого сигнала. Коэффициент a может меняться от 3 до 8. Обозначим их функциями $W1(4,b)$, $W2(4,b)$ и $W3(4,b)$ соответственно, где b меняется от 1 до 256. На рис. 1 представлен результат ВП функции $E2(n)$ предложения «Бегите быстро». На рис. 1 положительным значениям функции $W2(4,b)$ соответствуют гласные звуки, а отрицательным значениям — согласные.

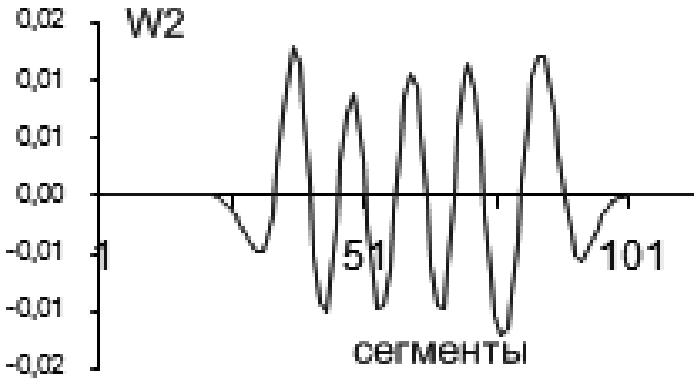

Рис. 1. Вейвлет-спектр $W2(4,b)$ функции $E2(n)$ предложения «Бегите быстро».

По результатам ВП установлено, что гласные буквы всегда имеют положительное значение в $W1(4,b)$, $W2(4,b)$ и $W3(4,b)$. Шипящие согласные имеют отрицательное значение в функции $W2(4,b)$ и $W3(4,b)$. Некоторые шипящие буквы имеют положительное значение в $W1(4,b)$. Поэтому для нахождения местоположения гласных букв нормируются энергии $E2(n)$, $E3(n)$, находится их сумма и выполняется ВП $W4(4,b)$. Вейвлет-анализ речевого сигнала показывает, что гласные фонемы и фонемы ‘н’, ‘м’, ‘л’ имеют максимальные энергии при средних значениях a. Энергия фонем ‘н’, ‘м’, ‘л’ много меньше энергии гласных звуков речи, но значительно выше энергии шума. Шипящие и свистящие фонемы при малых значениях масштабного коэффициента a имеют энергию $W(a,b)$, сравнимую с энергией гласных фонем. При средних значениях a они имеют энергию на уровне шума.

Работа выполнена при поддержке РФФИ, проект № 14-07-00143-а.

Список литературы

[1] Потапова Р. К. Речь: коммуникация, информация, кибернетика. — М.: Эдиториал УРСС, 2001. — 568 с.

[2] Аграновский А. В., Леднов Д. А. Математическая модель распознавания речи с использованием протяженных контекстов // Информационные технологии. — 2013. — № 7. — С. 33–36.

[3] Семенов В. И. Свидетельство об официальной регистрации программы для ЭВМ № 2007615024. Непрерывное быстрое вейвлет-преобразование / Зарег. в Реестре программ для ЭВМ 4 декабря 2007 г.

О задаче существования грациозной разметки одноциклических графов

Семенюта Марина Фроловна

Кировоградская летная академия НАУ, e-mail: marina_semenyuta@mail.ru

В 1984 году Трасжинский [1] предположил, что все одноциклические графы, кроме C_n с $n \equiv 1 \pmod 4$ и $n \equiv 2 \pmod 4$, являются грациозными. В связи с огромным разнообразием одноциклических графов возникает сложность в доказательстве этой гипотезы или ее опровержении. Более детально изучены циклы, у которых ко всем или к нескольким вершинам прикреплены висячие ребра. Фрахт [2] доказал грациозность короны $C_n \bigodot K_1$. Его результаты обобщили независимо авторы работ [3] и [4] на графы $C_n \bigodot mK_1$. C_n^t представляет класс графов, образованных присоединением по одному висячему ребру к t вершинам цикла C_n, где $1 \leq t \leq n$. В 1989 году Руп и Гальян предположили, что все представители этого класса — грациозные графы. Эта гипотеза доказана в [5]. В данной работе продолжено изучение грациозности одноциклических графов. Предметом исследования является задача существования грациозной разметки у некоторых представителей класса одноциклических графов. Для ее решения применяем два подхода: конструктивный и аналитический. Первый заключается в нахождении грациозной разметки непосредственно построением или с помощью формул, второй — получение грациозного графа из некоторого класса графов с известными разметками, наложением дополнительных условий. Будем рассматривать конечные неориентированные графы без петель и кратных ребер. Под порядком графа понимаем число его вершин, а под размером — число ребер. Для некоторых графов используем стандартные обозначения: P_n — цепь порядка n, C_n — цикл порядка n. Инъективную функцию $f : V \to \{0, 1, 2, ..., q\}$ называют грациозной разметкой графа $G = (V, E)$ размера q, если она индуцирует такую реберную разметку $f^* : E \to \{1, 2, ..., q\}$, что f^* — биекция и $f^*(uv) = |f(u) - f(v)|$ для любых смежных вершин $u, v \in V(G)$. Граф G — грациозный, если он допускает грациозную разметку f.

Теорема 1. *Пусть граф G получен отождествлением произвольной вершины u_i, где $i = 1, 2, ..., n$, цепи $P_n = (u_1, u_2, ..., u_n)$ с вершиной цикла C_4. Тогда G является грациозным для любого $n \geq 8$.*

Доказательство. Пусть $V(C_4) = \{v_1, v_2, v_3, v_4\}$ и вершина $v_1 = u_i$, $i = 1, 2, ..., n$, — общая для цепи $P_n = (u_1, u_2, ..., u_n)$ и цикла C_4. Порядок и размер графа G совпадают и равны числу $n+3$. Для любой вершины u_i цепи $P_n = (u_1, u_2, ..., u_n)$ при $n \geq 8$ существует грациозная разметка ϕ с $\phi(u_i) = 1$. Для цепи функция ϕ будет биекцией из множества вершин на множество $\{0, 1, ..., n-1\}$. Зададим вершинную разметку f графа G. Будем назначать вершинам $u_1, u_2, \ldots, u_n$ метки из множества $\{1, 2, ..., n\}$ таким образом, что $f(u_1) = \phi(u_1) + 1$, $f(u_2) = \phi(u_2) + 1$, $\ldots$, $f(u_n) = \phi(u_n) + 1$. Для ребер цепи P_n, рассматриваемой в качестве подграфа графа G, разметка f индуцирует метки $1, 2, ..., n-1$. Так как $u_i = v_1$, то $f(v_1) = f(u_i) = \phi(u_i) + 1 = 2$. Далее зададим $f(v_2) = n+3$, $f(v_3) = 0$, $f(v_4) = n+2$. По определению грациозной разметки имеем: $f^*(v_1v_2) = n+1$, $f^*(v_1v_4) = n$, $f^*(v_2v_3) = n+3$, $f^*(v_3v_4) = n+2$. Таким образом, f представляет собой инъективную функцию из множества вершин графа G в множество $\{0, 1, 2, ..., n+2, n+3\}$, порождающую биективную функцию из множества ребер графа G на множество $\{1, 2, ..., n-1, n, n+1, n+2, n+3\}$. По определению, разметка f для графа G является грациозной. **Теорема 1 доказана.**

Следствие. *Пусть граф G получен отождествлением вершины u_i, где $i = 1, 2, ..., n$ цепи $P_n = (u_1, u_2, \ldots, u_n)$ с вершиной цикла C_4. Существует такая вершина u_i, что G является грациозным для любого $n \geq 1$.*

Доказательство следует непосредственно из теоремы 1, если учесть, что цепь P_n имеет грациозную разметку для любого $n \geq 1$.

Инструментом в доказательстве теоремы 2 послужило условие грациозности дерева, рассматриваемого в качестве подграфа некоторых представителей класса одноциклических графов.

Теорема 2. *Пусть T — грациозное дерево порядка n с не смежными вершинами u и w, помеченными метками 0 и 1. Граф G, полученный отождествлением концов цепи P_3 с вершинами u и w, является грациозным для любого $n \geq 2$.*

Доказательство. Если $n = 2$, то граф $G = C_3$ — грациозный, если $n = 3$, то $G = C_4$ также будет грациозным графом. Пусть $n \geq 4$ и для дерева T существует грациозная разметка ϕ с $\phi(u) = 0$, $\phi(w) = 1$, где u и w — не смежные вершины T. Тогда, вершины u, w являются концами цепи $P_3 = (u, v, w)$ в графе G. Зададим разметку f графа G следующим образом: $f(x) = \phi(x)$ для любой вершины $x \in V(G) - \{v\}$ и $f(v) = n+1$. Тогда функция f представляет собой инъекцию из множества вершин графа G в множество чисел $\{0, 1, ..., n-1, n, n+1\}$. Отметим, что число n не будет использовано при указанной вершинной разметке f. Все индуцированные f, метки ребер различные и образуют множество $\{1, 2, ..., n-1, n, n+1\}$. Следовательно G — грациозный граф. **Теорема 2 доказана.**

Список литературы

[1] Truszczynski M. Graceful unicyclic graphs // Demonstatio Mathematica. — 1984. — V. 17. — P. 377–387.

[2] Frucht R. W. Graceful numbering of wheels and related graphs // Ann. NY Acad. Sci. — 1979. — V. 319. — P. 219–229.

[3] Barrientos C. Graceful labeling of chain and corona graphs // Bull. inst. combin. appl. — 2002. — V. 34. — P. 17–26.

[4] Bu C., Zhang D., He B. k-Gracefulness of C_n^m // J. Harbin Shipbuilding Eng. Inst. — 1994. — V. 15. — P. 95–99.

[5] Kang Q. D., Liang Z.-H., Gao Y.-Z, Yang G.-H. On the labeling of some graphs // J. Combin. Math. Combin. Comput. — 1996. — V. 22. — P. 193–210.

Сохранение ключей операциями табличных алгебр

Сенченко Алексей Сергеевич

Киевский национальный университет имени Тараса Шевченко, e-mail: senchenko@pisem.net

Введение

В настоящее время информационные системы широко используются практически во всех областях деятельности человека. Базы данных являются ядром для подавляющего большинства информационных систем. Наиболее распространенными остаются реляционные базы данных, математическая модель которых была впервые предложена Э. Коддом в 1970 году [1]. Табличные алгебры, введённые В. Н. Редько и Д. Б. Буем [2], построены на основе реляционных алгебр Кодда, существенно их развивают и составляют теоретический фундамент языков запросов современных табличных баз данных.

В реляционных базах данных важную роль играют ключи таблицы — один или несколько ее атрибутов, на значениях которых записи таблицы однозначно идентифицируются. С помощью ключей (первичных и внешних) устанавливаются бинарные связи типа «один-ко-многим». Эти связи служат для поддержания целостности баз данных. Как правило, ключи определяются таким образом, чтобы они были инвариантными к любым изменениям записей в базе данных. В настоящей работе рассматривается вопрос сохранения ключей таблиц, полученных в результате применения к ним сигнатурных операций табличных алгебр. Полученные результаты представляют интерес для выбора оптимальных ключей при проектировании реляционных баз данных [3].

Основные результаты

Зафиксируем некоторое непустое множество атрибутов $A = \{A_1, \ldots, A_n\}$. Произвольное конечное подмножество множества A назовем схемой, причем схема может быть пустым множеством. Строкой s схемы R называется множество пар $s = \{(A'_1, d_1), \ldots, (A'_k, d_k)\}$, проекция которого по первой компоненте равна R, причем атрибуты $A'_1, \ldots, A'_k$ попарно различны, т. е. строка является функциональным бинарным отношением. Таблицей схемы R называется конечное множество строк схемы R, количество строк в таблице T обозначаем

$|T|$. Активным доменом атрибута A относительно таблицы T называется множество $D_{A,T} = \{d \mid \exists s \in T \wedge (A, d) \in s\}$, состоящее, говоря содержательно, из всевозможных значений атрибута A в таблице T.

На множестве таблиц введены [4, 5] операции объединения ($\bigcup\limits_{R}$), пересечения ($\bigcap\limits_{R}$), разности ($\underset{R}{-}$), активного дополнения ($\tilde{T}$), проекции ($\pi_X(T)$), селекции ($\sigma_P(T)$), соединения ($\otimes$), деления ($T_1 \overset{R_1}{\underset{R_2}{\div}} T_2$) и переименования атрибутов ($R\,T_\xi$). Табличной алгеброй называют частичную алгебру с носителем — множеством всех таблиц произвольной схемы — и приведёнными выше девятью операциями. В табличной алгебре выделяют две особые таблицы: таблицу $T_\varepsilon = \{\varepsilon\}$, где ε — пустая строка, при этом схема таблицы T_ε является пустым множеством, и таблицу $T_\emptyset = \emptyset$ — пустое множество строк произвольной (в том числе и непустой) схемы. Таблица T, не являющаяся особой, называется ненасыщенной, если выполняется неравенство $\tilde{T} \neq T_\emptyset$.

Множество атрибутов $K \subseteq R$ называется ключом таблицы T, если для любых строк $s_1, s_2 \in T$ выполняется импликация $s_1 \mid K = s_2 \mid K \to s_1 = s_2$; другими словами, ограничения по атрибутам ключа всех строк таблицы T попарно различны. Несложно заметить, что схема таблицы будет являться ее ключом, поэтому наибольший интерес представляют так называемые нетривиальные ключи, которые являются собственным подмножеством схемы таблицы. На практике в реальных базах данных особые таблицы используются чрезвычайно редко, поэтому для удобства изложения результатов в работе рассматриваются исключительно таблицы, не являющиеся особыми, при этом большинство результатов справедливо и для таблицы $T_\emptyset$.

Доказано, что пересечение, разность и селекция сохраняют ключи.

Предложение 1. *Пусть T_1, T_2 — таблицы схемы R и K — ключ таблиц T_1 и (или) T_2. Тогда K является ключом таблиц $T_1 \bigcup\limits_{R} T_2$, $T_1 \underset{R}{-} T_2$, $\sigma_P(T_1)$.*

Найдены необходимые и достаточные условия, при которых нетривиальные ключи для ненасыщенных таблиц T и $\tilde{T}$ совпадают.

Теорема 1. *Пусть R — схема ненасыщенной таблицы T и $K = \{K_1, \ldots, K_q\}$ — нетривиальный ключ для T. K является ключом таблицы $\tilde{T}$ тогда и только тогда, когда одновременно выполняются два условия:*

а) множество $R - K$ содержит точно один такой атрибут B, что $\mid D_{B,T} \mid > 1$, причем $\mid D_{B,T} \mid = 2$;

б) для всех значений $d_1 \in D_{K_1,T}, \ldots, d_q \in D_{K_q,T}$ строка $s' = \{(K_1, d_1), \ldots, (K_q, d_q)\} \in \pi_K(T)$, причем существует только одна такая строка $s \in T$, что $s' = s \mid \{K_1, \ldots, K_q\}$.

Пусть K — ключ таблицы T и $X \subset R$. После рассмотрения всех возможных случаев относительно включения множеств X и K получили, что в случае $K \subseteq X$ операция проекции сохраняет ключи.

Теорема 2. *Пусть K — ключ таблицы T и $K \subseteq X$. Тогда K — ключ $\pi_X(T)$.*

Для исследования сохранения ключей операцией соединения были рассмотрены случаи, при которых таблицы, к которым применяется операция соединения, могут иметь как одинаковый, так и разные ключи.

Теорема 3. *Пусть K_1 — ключ таблицы T_1 и K_2 — ключ таблицы T_2. Тогда $K_1 \bigcup K_2$ является ключом таблицы $T_1 \otimes T_2$. Если K — ключ таблиц T_1 и T_2, то K является ключом таблицы $T_1 \otimes T_2$.*

Будем рассматривать сохранение ключей операцией деления таблиц только в том случае, когда значение $T_1 \overset{R_1}{\underset{R_2}{\div}} T_2$ не пусто. Были рассмотрены ситуации взаимного включения ключа таблицы T_1 и схемы R_2, при которых ключ таблицы T_1 либо не пересекается со схемой таблицы T_2, либо пересекается со схемой таблицы T_2, но при этом этот ключ полностью не входит в нее.

Теорема 4. *Пусть R_1, R_2 — схемы таблиц T_1 и T_2, $T_1 \overset{R_1}{\underset{R_2}{\div}} T_2 \neq T_\emptyset$, K — ключ таблицы T_1. Если $K \bigcap R_2 = \emptyset$, то K — ключ таблицы $T_1 \overset{R_1}{\underset{R_2}{\div}} T_2$. Если же $K \bigcap R_2 \neq \emptyset$ и $K' = K - (K \bigcap R_2) \neq \emptyset$, то K' — ключ таблицы $T_1 \overset{R_1}{\underset{R_2}{\div}} T_2$.*

Доказано, что операция переименования атрибутов сохраняет ключи.

Предложение 2. *Пусть $K = \{K_1, \ldots, K_q\}$ — ключ таблицы T и пусть $\xi[K] = \{\xi(K_1), \ldots, \xi(K_q)\}$. Тогда $\xi[K]$ является ключом таблицы $R\,T_\xi$.*

Выводы

В работе исследовано сохранение ключей операциями табличных алгебр. Результаты работы могут быть использованы для выбора оптимальных ключей при проектировании реляционных баз данных.

Список литературы

[1] Codd E. F. A Relational Model of Data for Large Shared Data Banks // Communications of the ACM. — 1970. — Vol. 13, No 6. — P. 377–387.

[2] Редько В. Н., Буй Д. Б. К основаниям теории реляционных моделей баз данных // Кибернетика и системный анализ. — 1996. — № 4. — С. 3–12.

[3] Дейт К. Дж. Введение в системы баз данных, 8-е издание.: Пер. с англ. — М.: ИД «Вильямс», 2005. — 1328 с.

[4] Мейер Д. Теория реляционных баз данных. — М.: Мир, 1987. — 608 с.

[5] Редько В. Н., Брона Ю. Й., Буй Д. Б., Поляков С. А. Реляційні бази даних: табличні алгебри та SQL-подібні мови. — К.: Академперіодика, 2001. — 198 с.

О мощностных характеристиках базисов Гребнера торических идеалов

Сидоров Сергей Владимирович, Костров Сергей Александрович

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: sesidorov@yandex.ru, a.big.thick.dictionary@gmail.com

На сегодняшний день существует масса подходов для решения задач целочисленного линейного программирования (ЦЛП), большинство из которых основано на геометрических или комбинаторных свойствах многогранника задачи. В [1] представлен метод, оперирующий чисто алгебраическими объектами — базисами Гребнера полиномиальных идеалов специального вида.

Пусть k — поле, тогда из теоремы Гильберта о базисе следует, что всякий идеал $I \subset k[x_1, \dots, x_n]$ является конечно порожденным, т. е. представим в виде:

$$I = \langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}.$$

Обозначим через $LT(f)$ старший член многочлена f по некоторому мономиальному упорядочению. Аналогично для множества многочленов $F = \{f_1, \dots, f_s\}$ обозначим $LT(F) = \{LT(f_1), \dots, LT(f_s)\}$. *Базисом Гребнера* идеала $I \subset k[x_1, \dots, x_n]$ называется такое порождающее множество $G = \{g_1, \dots, g_s\}$ этого идеала, что $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Базис Гребнера любого полиномиального идеала может быть построен за конечное число шагов с использованием алгоритма Бухбергера, время работы которого зачастую сильно зависит от количества переменных, степеней многочленов и их количества в начальном порождающем множестве.

Полиномиальные идеалы, встречающиеся при решении задач ЦЛП, имеют специальный вид и называются *торическими*. Рассмотрим матрицу $A \in \mathbb{Z}^{m \times n}$, $\operatorname{rank} A = m$. Введем следующее обозначение:

$$\ker A = \{u \in \mathbb{Z}^n \mid Au = 0\}.$$

Для каждого $u \in \ker A$ определим вектора $u_+ \in \mathbb{N}^n$ и $u_- \in \mathbb{N}^n$ следующим образом:

$$u_+ = \sum_{u_i > 0} u_i e_i \quad \text{и} \quad u_- = -\sum_{u_i < 0} u_i e_i,$$

где e_i — вектор, i-ая координата которого равна единице, а остальные нулевые. Нетрудно видеть, что $u = u_+ - u_-$ и множества ненулевых координат векторов u_+ и u_- не пересекаются. Торическим идеалом матрицы A будем называть идеал вида:

$$I_A = \langle \{x^{u_+} - x^{u_-} \mid u \in \ker A\} \rangle.$$

С вычислительной точки зрения нахождение даже какого-либо конечного порождающего множества идеала I_A является нетривиальной задачей, однако для решения данной проблемы было приложено немало усилий. В частности,

подходы, рассмотренные в [2, 3, 4, 5], подразумевают работу с многочленами только от n переменных (в отличие от [1], оперирующем в кольце многочленов от $m+n+1$ переменной). Все они используют следующую лемму.

Лемма. [6] Пусть $A \in \mathbb{Z}^{m\times n}, I_A \subset k[x_1,\dots,x_n]$ — торический идеал и $L=\left\{l^1,\dots,l^r\right\}$ — базис $\ker A$. Пусть также $I_L=\left\langle\left\{x^{l^i_+}-x^{l^i_-} \mid i=\overline{1,r}\right\}\right\rangle$. Тогда $I_A = I_L : (x_1\cdot\ldots\cdot x_n)^\infty$, где

$$I_L : (x_1\cdot\ldots\cdot x_n)^\infty = \{f\in k[x_1,\dots,x_n] \mid \exists m\in\mathbb{Z}, m\geqslant 1, (x_1\cdot\ldots\cdot x_n)^m f\in I_L\}$$

называется *насыщением* идеала I_L по многочлену $x_1\cdot\ldots\cdot x_n$.

На сегодняшний день вопрос о рамках практического применения данного подхода для решения задач ЦЛП является открытым. Авторам настоящего доклада неизвестны классы торических идеалов, для которых задача построения порождающего множества или базиса Гребнера решалась бы эффективно. В общем случае неизвестна и оценка в терминах матрицы A (или базиса L) на мощность базиса Гребнера идеала I_A при фиксированном мономиальном упорядочении.

Тем не менее известна верхняя оценка на степени элементов *универсального базиса Гребнера* идеала I_A. Согласно [4] полная степень многочленов в универсальном базисе Гребнера идеала I_A не превосходит $(m+1)(n-m)\Delta(A)$, где $\Delta(A)$ — максимальное значение рангового минора матрицы A. Данный результат побудил авторов провести серию вычислительных экспериментов с вполне бимодулярными матрицами специального вида.

Рассмотрим множество матриц из класса $\{0,1\}^{m\times n}$, удовлетворяющих следующим двум свойствам: 1) каждый столбец матрицы содержит ровно две единицы, 2) все миноры матрицы по модулю ограничены 2 и существует ранговый минор, равный 2. Обозначим через $U(m,n)$ и $D(m,n)$ соответственно максимальную и минимальную мощность базисов Гребнера торических идеалов, соответствующих матрицам из описанного класса. Были проведены вычислительные эксперименты для значений $m\in\{4,5,6,7\}$ и $m+2\leqslant n\leqslant 50$. Для каждой пары значений m,n генерировалась выборка по 100 псевдослучайных матриц и в каждой выборке вычислялась максимальная и минимальная мощность базиса Гребнера по градуированному лексикографическому упорядочению. По результатам проведенных экспериментов была сформулирована следующая гипотеза.

Гипотеза.

$U(m,n)=a(m)\cdot n+b(m)$, $D(m,n)=c(m)\cdot n+d(m)$, где $a(m)$, $b(m)$, $c(m)$, $d(m)$ — некоторые функции, зависящие только от m, причем $U(4,n)=D(4,n)=n-4$, $U(5,n)=n+1$, $D(5,n)=n-5$.

Таким образом, при фиксированном m величины $U(m,n)$ и $D(m,n)$ являются линейными функциями от n.

Список литературы

[1] Conti P., Traverso C. Buchberger Algorithm and Integer Programming // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-9. — 1991. — P. 130–139.

[2] Pottier L. Gröbner Bases of Toric Ideals // Research Report 2224, INRIA, Sophia Antipolis. — 1994.

[3] Di Biase F., Urbanke R. An Algorithm to Calculate the Kernel of Certain Polynomial Ring Homomorphisms // Experimental Mathematics. — V. 4, Iss. 5 — 1995. — P. 227–234.

[4] Sturmfels B. Gröbner Bases and Convex Polytopes, AMS University Lecture Series. — V. 8. — AMS, Providence, RI, 1996.

[5] Bigatti A., La Scala R., Robbiano L. Computing Toric Ideals // Journal of Symbolic Computation. — V. 27, Iss. 4 — 1999. — P. 351–365.

[6] Miller E., Sturmfels B. Combinatorial Commutative Algebra — Graduate Texts in Math. — V. 227. — Springer-Verlag, New York, 2005.

Некоторые полиномиальные подклассы задачи о наибольшем кратном потоке в делимой сети

Смирнов Александр Валерьевич

Ярославский государственный университет им. П. Г. Демидова, e-mail: alexander_sm@mail.ru

Кратные сети произвольной натуральной кратности k, а также делимые сети (частный случай кратной сети) рассматривались в работе [1]. Кратные сети целочисленного сбалансирования кратности 2 использовались в работах [2, 3] для поиска решения задачи целочисленного сбалансирования с ограничениями первого и второго рода.

Напомним несколько определений (подробнее см. в [1]).

Сначала введем натуральное $k > 1$ (*кратность потока*). В качестве сети рассматривается ориентированный мультиграф $G(X, U)$, между вершинами которого могут быть дуги одного из 3 видов: *обычная дуга* u^o с пропускной способностью $c(u^o)$, поток по которой не связан с потоком по другим дугам; множество обычных дуг обозначим через U^o; *кратная дуга* u^k между двумя вершинами, которая состоит из k дуг одной ориентации с одинаковой пропускной способностью $c(u^k)$ и одинаковым потоком по каждой из них; множество кратных дуг обозначим через U^k; *связанная дуга* u между двумя вершинами, которая связана с еще $k - 1$ дугой, имеющей одинаковый один из концов; множество связанных дуг, выходящих из одной вершины или входящих в одну вершину, будем называть *мультидугой* u^m; пропускная способность всех связанных дуг одной мультидуги одинакова; поток по каждой связанной дуге одной мультидуги одинаков; множество мультидуг обозначим через U^m.

Множество выходящих из вершины дуг может быть либо только кратными дугами, либо только одной мультидугой (k связанных дуг), либо только обыч-

ными дугами. Из источника x_0 сети выходят только кратные дуги, а в сток z сети входит только одна мультидуга. Если из вершины выходят связанные дуги мультидуги, то в нее обязательно входит кратная дуга. Если в вершину входит мультидуга, то из нее может выходить только кратная дуга. Определенный таким образом мультиграф $G(X, U)$ с целочисленными пропускными способностями дуг назовем *кратной (транспортной) сетью*.

Кратным потоком по сети называется целочисленная функция, определенная на множестве дуг $U = U^o \cup U^k \cup U^m$, для которой выполнены условия неотрицательности, ограниченности (пропускными способностями дуг) и неразрывности потока (в каждой вершине). *Величиной кратного потока* называется сумма φ_z входящего потока для стока z, равная сумме выходящего из источника потока. В силу того, что поток по каждой обычной дуге и по каждой связанной дуге каждой кратной и мультидуги должен быть целочислен, величина φ_z должна быть кратна k. Отметим, что при $k = 1$ кратная сеть превращается в обычную транспортную сеть, а кратный поток превращается в обычный поток по этой сети. *Задача о наибольшем кратном потоке* для кратной сети является обобщением задачи о наибольшем потоке для обычной транспортной сети.

Пусть имеется кратная сеть произвольной кратности k. Пусть при удалении всех мультидуг сеть распадается на $k + 2$ слабо связных компоненты, при этом одна компонента состоит только из вершины z, компонента, содержащая вершину x_0, содержит только кратные дуги, а остальные k компонент содержат только обычные дуги. Если при этом каждая мультидуга имеет ровно один конец в каждой из k компонент, содержащих обычные дуги, то такую сеть мы будем называть *делимой*. Пример делимой сети — кратная сеть целочисленного сбалансирования трехмерной матрицы, подробно рассмотренная в [2, 3].

Обозначим через P_0 компоненту делимой сети, содержащую кратные дуги, через $P_1, \ldots, P_k$ обозначим компоненты, содержащие обычные дуги. Тогда *частью* G_i делимой сети ($i \in \overline{1,k}$) назовем объединение соответствующей компоненты P_i с инцидентными ей связанными дугами всех мультидуг кроме мультидуги с концом в z, а также с i-ой связанной дугой каждой кратной дуги компоненты P_0. Заметим, что возможность выделения частей G_i является особенностью делимых сетей, в общем случае это не всегда возможно.

Обозначим начальные вершины мультидуги с концом в z через $z_1, \ldots, z_k$. Вершины, являющиеся началом остальных мультидуг, обозначим через y_j.

Если в делимой сети существует поток величины kT (T — натуральное число), то в ней всегда существует поток любой другой величины kS ($1 \le S < T$, S — натуральное число). Для произвольной кратной сети это условие выполнено не всегда. На данном свойстве основан алгоритм нахождения максимального потока в делимой сети, рассмотренный в работе [1]. При этом задача нахождения максимального потока в кратной сети является NP-полной (обоснование см. в [1]). Поэтому важным является вопрос поиска подклассов полиномиально разрешимых задач о максимальном кратном потоке.

Теорема 1. *Пусть $G(X, U)$ — делимая сеть кратности k. Пусть в каждой компоненте P_i ($i \in \overline{1, k-1}$) существует только одна вершина y_0^i, являющаяся*

концом мультидуги, а в компоненте P_k таких вершин может быть несколько. Тогда задача нахождения максимального кратного потока разрешима за полиномиальное время.

Следствие. *Пусть $G(X,U)$ — делимая сеть кратности k, в которой в каждой компоненте P_i ($i \in \overline{1,s}$, $1 < s < k$) существует только одна вершина y_0^i, являющаяся концом мультидуги, а в компонентах P_i ($i \in \overline{s+1,k}$) таких вершин несколько. Для такой сети возможно понизить размерность задачи о максимальном кратном потоке до $k-s$.*

Пусть теперь делимая сеть $G(X,U)$ устроена таким образом, что для любой пары вершин y_j, y_t ($j \neq t$) произвольный путь из x_0 в y_j и произвольный путь из x_0 в y_t не имеют общих вершин кроме x_0. В этом случае будем говорить, что сеть $G(X,U)$ имеет *параллельную структуру*.

Пусть для определенности $j \in \overline{1,m}$. Компоненту P_0 сети $G(X,U)$ можно разделить на субкомпоненты P_0^j, каждая из которых состоит из всех возможных путей из x_0 в y_j. Очевидно, что

$$P_0^1 \cup P_0^2 \cup \ldots \cup P_0^m = P_0; \quad P_0^j \cap P_0^t = \{x_0\}, \quad j \neq t,$$

а каждая субкомпонента P_0^j — это обычная транспортная сеть с источником x_0 и стоком y_j, содержащая только кратные дуги. Следовательно, в каждой такой субкомпоненте можно применить (с учетом кратности дуг) полиномиальный алгоритм Форда – Фалкерсона для нахождения максимального потока.

Теорема 2. *Задача о наибольшем кратном потоке в делимой сети $G(X,U)$ параллельной структуры разрешима за полиномиальное время при кратности сети $k = 2$.*

Теорема 3. *Задача о наибольшем кратном потоке в делимой сети $G(X,U)$ параллельной структуры NP-полна при кратности сети $k \geq 3$.*

Доказательство теоремы 3 основано на полиномиальном сведении классической NP-полной задачи о 3-сочетаниях (см. [4]) к данной задаче.

Работа выполнена при поддержке РФФИ (проект № 15-07-03038 А).

Список литературы

[1] Рублев В. С., Смирнов А. В. Потоки в кратных сетях // Ярославский педагогический вестник. — 2011. — Т. 3, № 2. — С. 60–68.

[2] Рублев В. С., Смирнов А. В. Задача целочисленного сбалансирования трехмерной матрицы и алгоритмы ее решения // Моделирование и анализ информационных систем. — 2010. — Т. 17, № 2. — С. 72–98.

[3] Смирнов А. В. Некоторые классы разрешимости задачи целочисленного сбалансирования трехмерной матрицы с ограничениями второго рода // Моделирование и анализ информационных систем. — 2013. — Т. 20, № 2. — С. 54–69.

[4] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982. — 416 с.

Сравнение базисов многозначной логики

Стеценко Владимир Алексеевич
Московский педагогический государственный университет, e-mail: stetsenko.vladimir@yandex.ru

Б. А. Субботовская [1] показала, что сложность реализации последовательности линейных функций $x_1 \oplus \cdots \oplus x_n$ формулами в базисе $\{\&, \vee, \neg\}$ по порядку не меньше, чем $n^{3/2}$. С другой стороны, сложность реализации этой же последовательности формулами в базисе $\{\&, \vee, \neg, \oplus\}$ равна n. В связи с этим результатом О. Б. Лупанов предложил ввести следующее отношение предшествования на множестве базисов, характеризующее сложность отдельных последовательностей функций: базис B_1 предшествует базису B_2, если существуют такие действительные положительные константы c и d, что для любой булевой функции f выполнено неравенство $L_{B_1}(f) \leq cL_{B_2}(f) + d$, где $L_B(f)$ — сложность реализации булевой функции f формулами в базисе B. Отношение предшествования естественно порождает отношения эквивалентности, строгого предшествования, несравнимости и непосредственного предшествования на множестве базисов. О. Б. Лупанов показал, что если функции базиса B_2 бесповторно выразимы в базисе B_1 то базис B_1 предшествует базису B_2. С помощью этого признака О. Б. Лупанов показал, что любой базис предшествует базису $B_0 = \{\&, \vee, \neg\}$, т. е. базис B_0 является максимальным или «самым плохим». Далее исследование отношения предшествования было продолжено Б. А. Субботовской. Используя результат работы [1] она показала, что базис $\{\&, \vee, \neg, \oplus\}$ строго предшествует базису B_0. Затем Б. А. Субботовская дала критерий эквивалентности произвольного базиса B базису B_0. Она показала, что базис B эквивалентен базису B_0 тогда и только тогда, когда все функции из базиса B бесповторно выразимы в базисе B_0 [2]. Тем самым Б. А. Субботовская описала класс базисов, строго предшествующих базису B_0. После этого Б. А. Субботовская (Мучник) показала, что сложность реализации последовательности линейных функций $x_1 \oplus \cdots \oplus x_n$ формулами в произвольном «нелинейном» базисе по порядку не меньше, чем n^{1+c} где c — действительная положительная константа, зависящая только от базиса [3]. Тем самым было показано, что если B — произвольный «нелинейный» базис, а B' — произвольный «линейный» базис, то базис B' не предшествует базису B, а базис B строго предшествует базису $B \cup B'$. Примером «нелинейного» базиса является базис $B_0 \cup \{xy \vee xz \vee yz\}$, а примером «линейного» базиса — базис $B_0 \cup \{\oplus\}$. В силу результатов работы [2], базис $B_0 \cup \{\oplus, xy \vee xz \vee yz\}$ строго предшествует базису $B_0 \cup \{xy \vee xz \vee yz\}$. Последний базис, в силу результатов работы [3], строго предшествует базису B_0. Таким образом, используя результаты Б. А. Субботовской, можно построить последовательность из трех базисов, каждый следующий из которых строго предшествует предыдущему.

В работе [1] Б. А. Субботовской был описан метод получения нелинейных нижних оценок при реализации индивидуальных последовательностей булевых функций формулами. В дальнейшем этот метод, в настоящее время известный как метод «забивания переменных», подвергся различным усовершенствовани-

ям. В частности, используя некоторое обобщение этого метода Д. Ю. Черухин показал, что существует бесконечная последовательность базисов, каждый следующий член которой строго предшествует предыдущему. Примером такой последовательности является последовательность $P_2(2), P_2(3), \ldots$, где $P_2(n)$ — множество всех n-местных булевых функций [4]. Из данного результата следует, что не существует минимального базиса, т. е. такого базиса, который предшествует любому базису. Д. Ю. Черухиным также была доказана гипотеза О. Б. Лупанова, согласно которой базис B_1 предшествует базису B_2 тогда и только тогда, когда функции, принадлежащие базису B_1 бесповторно выразимы формулами в базисе B_2 [5]. Используя этот результат Д. Ю. Черухин показал, что каждый базис предшествует лишь конечному числу классов эквивалентности базисов. Таким образом, не существует бесконечной последовательности базисов, каждый член которой строго предшествует следующему. Далее, для каждого базиса существует бесконечное число попарно не эквивалентных базисов, непосредственно ему предшествующих. Наконец, если рассмотреть две произвольные цепи базисов, у которых совпадают начала и концы, и в которых каждый следующий член строго предшествует предыдущему, то длины этих цепей совпадут. Последний факт позволяет все базисы распределить по ярусам [6].

Естественно после изучения свойств отношения предшествования на множестве булевых базисов встал вопрос об изучении такого же отношения предшествования на множестве базисов, состоящих из функций многозначной логики. Автору настоящего доклада удалось метод забивания переменных обобщить для функций многозначной логики. Это позволило доказать гипотезу О. Б. Лупанова для функций многозначной логики. Оказалось, что «самым плохим» базисом является базис $\{0, 1, \ldots, k-1, J_0, \ldots, J_{k-1}, \max, \min\}$. Были также получены результаты аналогичные результатам Д. Ю. Черухина, о которых говорилось выше.

Список литературы

[1] Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, \neg$ // Докл. АН СССР. — 1961. — Т. 136, № 3. — С. 553–555.

[2] Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. — 1963. — Т. 149, № 4. — С. 784–787.

[3] Мучник Б. А. Оценка сложности реализации линейной функции формулами в некоторых базисах // Кибернетика. — 1970. — № 4. — С. 29–38.

[4] Черухин Д. Ю. Об одной бесконечной последовательности улучшающихся булевых базисов // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 4. — С. 79–95.

[5] Черухин Д. Ю. Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. — Вып. 8. — М.: Наука, 1999. — С. 77–122.

[6] Черухин Д. Ю. О предплохих булевых базисах // Дискретная математика. — 1999. — Т. 11, вып. 2. — С. 118–160.

Распознавание неориентированных графов с помощью коллектива агентов

Стёпкин Андрей Викторович

Донбасский государственный педагогический университет, e-mail: stepkin.andrey@rambler.ru

В настоящее время в мире существуют многочисленные среды, требующие изучения [1] (к примеру, исследование организма человека при помощи наноботов или исследование поверхностей планет с помощью планетоходов). Это является одной из причин активного развития такого направления математической кибернетики как теория дискретных динамических систем [2]. Одной из эффективных моделей описания и изучения сред явилась модель, предложенная В. М. Глушковым, — модель взаимодействия управляющей и управляемой систем (управляющего автомата и операционной среды). Взаимодействие этих систем часто представляется как процесс перемещения управляющего автомата по графу управляемой системы. Такое представление привело к обширному и интенсивно развивающемуся исследованию поведения автоматов в лабиринтах, заданных в виде графов [3].

Исследованию графа при помощи одного агента посвящено много работ, при этом остается малоисследованным распознавание графа при помощи нескольких блуждающих по нему агентов. Что делает актуальной задачу проведения систематического исследования экспериментов по распознаванию графа несколькими агентами. При таком распознавании основной проблемой является проблема эффективности их взаимодействия с целью уменьшения затрат времени и памяти на распознавание. Требуется разработать такой алгоритм движения, при котором блуждающие агенты не мешают друг другу, не дублируют работу друг друга и ищут новые подграфы для распознавания после распознавания своего подграфа.

В данной работе рассматривается коллектив из трех агентов: два агента-исследователя блуждают по графу, перекрашивают его элементы, записывают номера в вершины графа и передают полученную информацию агенту-экспериментатору. Агенты-исследователи A и B имеют конечную на каждом шаге, но растущую память. Взаимодействие агентов-исследователей осуществляется за счет окраски элементов графа, нумерации вершин графа и обмена информацией через агента-экспериментатора. Алгоритм распознавания основан на методе обхода графа в глубину. Разработана процедура, позволяющая агентам после завершения распознавания своего подграфа искать новые подграфы для распознавания. Это решило проблему простоя агента, в случае, когда начальное расположение агентов не позволило распознавать граф в равных частях и одному из агентов приходилось стоять, пока второй агент продолжал работу над распознаванием оставшегося подграфа, который мог в разы пре-

вышать подграф, распознанный простаивающим агентом. Поэтому начальное расположение агентов сильно влияло на время выполнения алгоритма, а в некоторых случаях приводило к тому, что весь граф (кроме вершины, в которой находился второй агент) распознавался одним агентом.

В начале работы все элементы графа окрашены в белый цвет, агенты A и B помещаются в произвольные несовпадающие вершины графа G, нумеруют их и передают номера агенту-экспериментатору, который помещает их во множество вершин V_H. Агенты-исследователи передвигаются по графу из вершины v в вершину u по ребру (v,u), могут изменять окраску вершин v, u, ребер (v,u), инцидентов $((v,u),v)$, $((v,u),u)$, а так же записывают в вершины номера. Находясь в вершине v, агент-исследователь воспринимает метки всех элементов окрестности $Q(v)$ и номера смежных с ней вершин, на основании этой информации определяет, по какому ребру будет дальше перемещаться, и как будет окрашивать элементы графа. Агент-экспериментатор может передавать сообщения агентам-исследователям, а также принимать и идентифицировать сообщения от агентов-исследователей, обладает конечной, неограниченно растущей внутренней памятью, в которой фиксируется результат функционирования агентов-исследователей на каждом шаге и, кроме того, строится представление графа G, вначале неизвестного агентам, списками ребер и вершин.

Выполняя обход графа, агенты A и B создают красный и желтый пути соответственно. Рассмотрим принцип построения агентами пути «своего» цвета. При движении в белую вершину красный (желтый) путь удлиняется, при движении назад по своему пути — укорачивается. Если агент-исследователь вернулся в вершину, из которой начал обход графа, а в её окрестности не оказалось белых вершин, то он окрашивает эту вершину в черный цвет. Алгоритм заканчивает работу, когда красный и желтый пути становятся пустыми, а все вершины черными. Выполняя обход графа G, агенты создают нумерацию посещенных вершин. Первый раз посетив вершину агент A окрашивает её в красный цвет (агент B — в желтый цвет), записывает в память вершины соответствующий номер (полученный от агента-экспериментатора). Распознавание графа G происходит на основе созданной агентами-исследователями нумерации, путем построения графа H изоморфного G.

Предложен новый метод и процедура реализации этого метода, в котором агент, закончивший распознавание своего подграфа, переходит на чужой подграф и там начинает движение в поисках еще не распознаных подграфов, как можно ближе к своему расположению. Поиск начинается с той части чужого подграфа, где наименее вероятно появление в нужной вершине другого агента раньше рассматриваемого агента. Такой метод не требует дополнительных сложных вычислений и лишних шагов для поиска вершин, подобранных по какому-либо фиксированному критерию, так же не требует дополнительной информации о нахождении другого агента вблизи выбранной вершины. В случае, если вершина все же будет занята другим агентом, рассматриваемый агент либо остановится до появления других вершин (если вершины, удо-

влетворяющие необходимым условиям отсутствуют), либо сразу определит следующую ближайшую подходящую вершину и начнет движение в ее направлении. Сложность же предложенного метода обусловлена сложностью поиска пути перехода в новый подграф для распознавания.

Теорема 1. *Три агента, выполнив алгоритм распознавания на графе G, распознают рассматриваемый граф с точностью до изоморфизма.*

Теорема 2. *Временная сложность алгоритма распознавания равна $O(n)$, емкостная — $O(n^2)$, а коммуникационная — $O(n^2 \cdot \log(n))$. При этом в алгоритме используется три краски.*

Основным результатом данного алгоритма является решение проблемы простоя агента в случае, когда начальное расположение агентов не позволило распознавать граф в равных частях и одному из агентов приходилось стоять, пока второй агент продолжал работу над распознаванием оставшегося подграфа, который мог в разы превышать подграф, распознанный простаивающим агентом. Это, в общем случае, дает значительное преимущество при использовании двух агентов-исследователей по сравнению с алгоритмами, использующими одного агента. Предложенный алгоритм является дальнейшим развитием результатов работы [3].

Автор выражает благодарность своему научному руководителю Грунскому И. С. за постановку задачи.

Список литературы

[1] Albers S., Henzinger M. R. Exploring unknown environments // SIAM Journal on Computing. — 2000. — V. 29, N 4. — P. 1164–1188.

[2] Кудрявцев В. Б., Ушчумлич Щ., Килибарда Г. О поведении автоматов в лабиринтах // Дискретная математика. — 1992. — Т. 4, № 3. — С. 3–28.

[3] Стёпкин А. В. Использование коллектива агентов для распознавания графов // Компьютерные исследования и моделирование. — 2013. — Т. 5, № 4. — С. 525–532.

Расширение модели линейной комбинации метрик на конечной размеченной выборке

Суворов Михаил Андреевич, Майсурадзе Арчил Иериевич

Московский государственный университет имени М. В. Ломоносова, e-mail: suvorov_m90@mail.ru, maysuradze@cs.msu.su

Для задач компьютерного зрения, биологии, социологии становятся характерными ситуации, когда сходство одних и тех же объектов распознавания можно измерить различными способами. В первую очередь, это связано со сложной природой самих объектов, для которых возможны различные представления. Одним из способов формализовать понятие сходства является метрика. Сложность природы объектов, а также недетерминированность формализации, приводит к различным метрикам. В этом случае можно сказать, что объекты распознавания являются элементами мультиметрического пространства.

Наличие в задачах интеллектуального анализа данных, в первую очередь в задачах обучения с учителем, метрических данных делает естественным использование метрических классификаторов, таких как методы ближайших соседей и парзеновского окна, методы потенциальных функций. Однако эти классические методы формулируются, получают теоретическое обоснование и исследуются для ситуаций с одной метрикой. Во многих случаях, когда задано несколько метрик, из их набора выбирается «наилучшая» метрика. При этом «наилучшесть» оценивается по значениям расстояний на объектах обучающей выборки. Тем не менее, возможно, и мы предлагаем идти этим путем, решать задачу агрегирования первичной метрической информации, т. е. по набору метрик строить новую. Кроме того, при решении прикладных задач в случае наличия нескольких метрик можно ожидать, что агрегированная метрика позволит улучшить качество разделения объектов на классы в сравнение с отдельными метриками. Заметим, что в интеллектуальном анализе данных авторы обычно допускают равенство расстояния нулю на несовпадающих объектах и формально правильно было бы везде говорить о полуметриках.

В случаях, когда разбиение объектов выборки на классы неизвестно, можно строить метрические аналоги методов разделения сигналов (blind signal separation), как это сделано в метрическом методе главных компонент или в метрической неотрицательной матричной факторизации [1, 2, 3].

В данной работе рассматривается задача построения метрики *на всей генеральной совокупности*, которая агрегирует информацию, поступающую в виде значений попарных расстояний между объектами конечной размеченной выборки по каждой из исходных метрик. Новая метрика должна наилучшим образом соответствовать разбиению прецедентов на классы.

Ранее было замечено [4], что данная задача схожа с задачей обучения метрик (metric learning) [5] с тем различием, что новая метрика строится по исходным метрикам, но не по исходным признакам. На основе идей Large-Margin Nearest Neighbor (LMNN) [5] была предложена задача линейного программирования, решением которой является метрика r, являющаяся линейной неотрицательной комбинацией, $r(x, y) = w_1\rho_1(x, y) + \ldots + w_N\rho_N(x, y)$, исходных $\rho_1, \ldots, \rho_N$ и минимизирующая сумму внутриклассовых расстояний между объектами $x_1, \ldots, x_M$ обучающей выборки. В качестве «сдерживающих» ограничений требуется, чтобы межклассовые расстояний были не менее 1. Выбор линейной функции в качестве агрегирующей обусловлен удобством теоретических исследований и вычислительной эффективностью [6, 7]. Неотрицательность весов гарантирует выполнение аксиом полуметрики. Кроме того, при отсутствии в выборке противоречивых пар объектов, в указанной задаче линейного программирования всегда существует допустимый план [4].

Недостаток описанной модели заключается в ее «чувствительности» к шумам и ошибкам в обучающей выборке. Примером шумовых данных могут быть объекты-выбросы, то есть те объекты, которые лежат ближе к объектам не своего класса. В этих случаях, излишне «жесткие» ограничения на межклассовые

расстояния приводят к тому, что модель настраивается именно на незначащие объекты и теряет в своей обобщающей способности.

Так же, как это сделано в LMNN, мы предлагаем избавиться от «жесткости» ограничений, вводя переменные натяжения ξ. Эти неотрицательные переменные позволяют нарушать межклассовым расстояниям порог 1. При этом, конечно, их сумма добавляется к минимизируемой линейной функции. Тогда справедлива следующая теорема.

Теорема 1. *В указанной задаче линейного программирования с переменными натяжениями всегда существует допустимый план.*

Чтобы проиллюстрировать влияние предлагаемой модификации на устойчивость модели, рассмотрим, как и в [4], задачу классификации из области компьютерного зрения, в которой задано 8 исходных метрик. Для сравнения исходных и новых метрик используется простой метод 1NN. В таблице ниже представлены проценты ошибок для каждой из исходных метрик, для метрики r, полученной методом без переменных натяжения, и для метрики q, полученной предлагаемым методом. Качество классификации оценивается на контроле, все обучение является эталонами.

ρ_1	84.2	ρ_2	89.7	ρ_3	86.2	ρ_4	89.5	ρ_5	86.6
ρ_6	84.8	ρ_7	88.7	ρ_8	85.0	r	23.0	q	20.4

Введение переменных натяжения позволило уменьшить влияние шумовых объектов в обучении, что, в свою очередь, увеличило обобщающую способность модели, и качество на контроле повысилось. Однако новые переменные существенно меняют размерность задачи, увеличивая время оптимизации в несколько раз в сравнение с моделью без переменных натяжения.

Исследование выполнено при финансовой поддержке РФФИ (проекты № 13-01-00751, № 15-07-09214).

Список литературы

[1] Суворов М. А., Майсурадзе А. И. Методы агрегирования метрических описаний // ММРО: 16-я Всероссийская конференция, г. Казань, 6–12 сентября 2013 г.: Тезисы докладов. — М.: Торус Пресс, 2013. — С. 11.

[2] Майсурадзе А. И. Метрический метод главных компонент для генеральной совокупности // Интеллектуализация обработки информации: 9-я международная конференция. Черногория, гор. Будва, 2012 г.: Сборник докладов. — М.: Торус Пресс, 2012. — С. 168–170.

[3] Суворов М. А. Методы агрегации метрических описаний на основе оптимальной матричной факторизации // Ломоносов-2012: XIX Международная конференция студентов, аспирантов и молодых ученых; секция Вычислительная математика и кибернетика: Москва, МГУ имени М. В. Ломоносова, 9–13 апреля 2012 г.: Сб. тезисов. — М.: Издательский отдел факультета ВМиК МГУ; МАКС Пресс, 2012. — С. 109–110.

[4] Майсурадзе А. И., Суворов М. А. Обучение линейной комбинации метрик на конечной выборке // Проблемы теоретической кибернетики. Материалы

XVII международной конференции (Казань, 16–20 июня 2014г.) — Казань: Отечество, 2014. — С. 186–189.

[5] Weinberger K. Q., Saul L. K. Distance metric learning for large margin nearest neighbor classification // Journal of Machine Learning Research. — 2009. — V. 10. — P. 207–244.

[6] Maysuradze A. I. On optimal decompositions of finite metric configurations in pattern recognition problems // J. Comput. Math. Math. Phys. — 2004. — V. 44, N 9. — P. 1615–1624.

[7] Maysuradze A. I. Homogeneous and rank bases in spaces of metric configurations // J. Comput. Math. Math. Phys. — 2004. — V. 46, N 2. — P. 330–344.

Максимальное число булевых функций, порождаемых инициальным автоматом с двумя константными состояниями

Сысоева Любовь Николаевна

Московский государственный университет имени М. В. Ломоносова, e-mail: s-luba@mail.ru

Рассматривается задача о порождении булевых функций инициальными константными автоматами с двумя состояниями и n входами, то есть такими автоматами с двумя состояниями, что в любом из них функция выхода совпадает с одной из булевых функций $0(x_1, x_2, \ldots, x_n)$ или $1(x_1, x_2, \ldots, x_n)$, $n \geq 1$. Найдена максимальная возможная мощность множества булевых функций, реализуемых константным автоматом с двумя состояниями и n входами, где $n > 1$.

Введем необходимые определения. Через $P_2(n)$ обозначается множество всех булевых функций, зависящих только от переменных $x_1, x_2, \ldots, x_n$, $n \geq 1$. Под булевым автоматом будем понимать автомат $V = (A, B, Q, F, G)$ с произвольным числом входов, входным алфавитом $A = \{0, 1\}$, выходным алфавитом $B = \{0, 1\}$, алфавитом состояний Q, функцией перехода G и функцией выхода F. Определения автомата и инициального автомата можно найти в [1, 2]. Пусть n — число входов автомата V. Без ограничения общности будем полагать, что входы автомата V занумерованы от 1 до n, и на i-ый вход автомата V подается значение булевой переменной x_i. Тем самым можно считать, что в каждый момент времени на вход автомата V подается некоторый двоичный набор значений переменных $x_1, x_2, \ldots, x_n$, и для любого состояния $q \in Q$ функция выхода $F(q, x_1, x_2, \ldots, x_n)$ является булевой функцией от переменных $x_1, x_2, \ldots, x_n$. Булев автомат V будем называть константным, если для любого $q \in Q$ функция $F(q, x_1, x_2, \ldots, x_n)$ является константной булевой функцией $0(x_1, x_2, \ldots, x_n)$ или $1(x_1, x_2, \ldots, x_n)$.

Пусть $V_{q_1} = (\{0, 1\}, \{0, 1\}, Q, F, G, q_1)$ — инициальный булев автомат с начальным состоянием q_1 и n входами, входным алфавитом $A = \{0, 1\}$, выходным алфавитом $B = \{0, 1\}$, алфавитом состояний Q, функцией перехода G и

функцией выхода F. И пусть $C = (\widetilde{\beta}_1, \widetilde{\beta}_2, \ldots, \widetilde{\beta}_{2^n})$ — упорядоченная последовательность всех двоичных наборов длины n, $n \geq 1$. Будем говорить, что автомат V_{q_1} с последовательностью C реализует булеву функцию f, если при последовательной подаче на вход V_{q_1} наборов из C в первые 2^n моментов времени, в каждый момент $t = 1, 2, \ldots, 2^n$ на входе V_{q_1} выдается значение $f(\widetilde{\beta}_t)$. Будем также говорить, что V_{q_1} реализует функцию f, если для некотой последовательности наборов C автомат V_{q_1} с последовательностью C раелизует f. Обозначим через $P(V_{q_1})$ множество всех булевых функций, реализуемых автоматом V_{q_1}.

Пусть $\mathfrak{A} \subseteq P_2(n)$. Автомат V_{q_1} называется универсальным для множества $\mathfrak{A}$, если выполнено равенство $P(V_{q_1}) = \mathfrak{A}$. В данной работе рассматриваются вопросы, связанные с универсальностью константных автоматов. Аналогичные вопросы, касающиеся универсальности формул над автоматными функциями, рассматривались в работах [3, 4].

Заметим, что если $F(q_1, x_1, x_2, \ldots, x_n)$ является константной булевой функцией $c(x_1, x_2, \ldots, x_n)$, то функция $\overline{c}(x_1, x_2, \ldots, x_n)$ не может быть реализована автоматом V_{q_1}. Поэтому верно следующее утверждение.

Утверждение 1. *Не существует инициального константного автомата универсального для множества $P_2(n)$, для любого $n \geq 1$.*

Далее рассматривается задача построения константных инициальных автоматов с двумя состояниями, универсальных для множеств булевых функций максимальной возможной мощности. Множество всех константных инициальных автоматов с двумя состояниями и n входами обозначим через $\mathfrak{V}_2(n)$. Пусть V_{q_1} — константный инициальный автомат с двумя состояниями q_1 и q_2. Без ограничения общности будем считать, что верны следующие равенства $F(q_1, x_1, x_2, \ldots, x_n) = 0(x_1, x_2, \ldots, x_n)$ и $F(q_2, x_1, x_2, \ldots, x_n) = 1(x_1, x_2, \ldots, x_n)$. Заметим, что такой автомат однозначно определяется множествами $M \subseteq \{0, 1\}$ и $N \subseteq \{0, 1\}$, такими, что набор $\widetilde{\beta}$ принадлежит множеству M тогда и только тогда, когда верно равенство $G(q_1, \widetilde{\beta}) = q_2$, и набор $\widetilde{\beta}$ принадлежит множеству N тогда и только тогда, когда верно равенство $G(q_2, \widetilde{\beta}) = q_1$. Верно следующее утверждение.

Утверждение 2. *Существует два автомата V^1 и V^2 из множества $\mathfrak{V}_2(n)$, таких, что верно равенство $P(V^1) \cup P(V^2) = P_2(n)$, для любого $n \geq 1$.*

Для доказательства этого утверждения достаточно для некоторого фиксированного двоичного набора $\widetilde{\alpha}$ длины n рассмотреть автомат $V^1_{q_1}$, определяемый соотношениями $M = \{\widetilde{\alpha}\}$ и $N = \emptyset$, и автомат $V^2_{q_2}$, определяемый соотношениями $M = \emptyset$ и $N = \{\widetilde{\alpha}\}$.

Основным результатом данной работы является следующая теорема.

Теорема 1. *Для любого автомата V из множества $\mathfrak{V}_2(n)$ мощность множества $P(V)$ не превосходит $\frac{5}{8} \cdot |P_2(n)|$, для любого $n \geq 1$.*

Доказательство этой теоремы разбивается на три случая. Сформулируем их ниже в виде независимых утверждений.

В первом случае рассматриваются автоматы, для которых выполнено соотношение $M \cap N = \emptyset$.

Утверждение 3. *Если автомат V_{q_1} из множества $\mathfrak{V}_2(n)$ таков, что верно соотношение $M \cap N = \emptyset$, то верно следующее неравенство $|P(V_{q_1})| \leq \frac{5}{8} \cdot 2^{2^n}$, при $n \geq 1$.*

Во втором случае рассматриваются автоматы, для которых выполнено одно из включений $M \subseteq N$ или $N \subseteq M$.

Утверждение 4. *Если автомат V_{q_1} из множества $\mathfrak{V}_2(n)$ таков, что верно одно из включений $M \subseteq N$ или $N \subseteq M$, то верно следующее неравенство $|P(V_{q_1})| \leq \frac{1}{2} \cdot 2^{2^n}$, при $n \geq 1$.*

В третьем случае рассматриваются автоматы, для которых выполнены соотношения $M \cap N \neq \emptyset$, $M \backslash N \neq \emptyset$ и $N \backslash M \neq \emptyset$.

Утверждение 5. *Если автомат V_{q_1} из множества $\mathfrak{V}_2(n)$ таков, что верны соотношения $M \cap N \neq \emptyset$, $M \backslash N \neq \emptyset$ и $N \backslash M \neq \emptyset$, то верно следующее неравенство $|P(V_{q_1})| \leq \frac{1}{2} \cdot 2^{2^n}$, при $n \geq 1$.*

Кроме того, верна следующая теорема.

Теорема 2. *Существует ровно один вид автоматов V_{q_1} из множества $\mathfrak{V}_2(n)$, таких, что верно равенство $|P(V_{q_1})| = \frac{5}{8} \cdot 2^{2^n}$, а именно автомат, определяемый множествами M и N, такими, что $M \cap N = \emptyset$ и выполнены равенства $|M| = 2$ и $|N| = 1$, где $n \geq 2$.*

Следствие 1. *Максимальная мощность множества $P(V_{q_1})$ для автомата V_{q_1} из множества $\mathfrak{V}_2(n)$ равна $\frac{5}{8} \cdot |P_2(n)|$, где $n \geq 2$.*

В заключение автор выражает искреннюю признательность Р. М. Колпакову за постановку задачи.

Работа выполнена при поддержке РФФИ (проект № 15-01-12345-а).

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006. — 384 с.

[2] Конспект лекций О. Б. Лупанова по курсу “Введение в математическую логику” // Отв. ред. А. Б. Угольников. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2007. — 191 с.

[3] Сысоева Л. Н. О некоторых свойствах обобщенных α-формул // Вестник Московского университета. Серия 1. Математика. Механика. — 2013. — № 4. — С. 51–55.

[4] Сысоева Л. Н. О реализации булевых функций обобщенными α-формулами // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. — 2014. — Т. 156, № 3. — С. 116–122.

Управление обслуживанием мультипотока объектов мобильным процессором

Трухина Мария Александровна, Федосенко Юрий Семенович, Шеянов Анатолий Владимирович

Волжский государственный университет водного транспорта, e-mail: fds@vgavt-nn.ru

Исследуется проблема оптимизации однофазного обслуживания мобильным процессором конечного детерминированного мультипотока объектов. Динамические модели такого типа адекватно описывают, в частности, локальные логистические процессы, в которых для грузовой обработки поступающих транспортных единиц используется перемещаемый перегрузочный комплекс. В качестве примера укажем рассредоточенную систему причалов порта, на которых грузовая обработка поступающих судов осуществляется плавучим краном, перемещаемым между причалами буксирным судном в соответствии с оперативным планом реализации транспортно-технологических работ.

Рассматривается n-элементный, состоящий из m подпотоков $O_1, O_2, \ldots, O_m$ мультипоток O^n независимых объектов $o_1, o_2, \ldots, o_n$, подлежащих однофазному обслуживанию, $1 < m \leq n$. Каноническая модель, соответствующая случаю $m = 1$, и возникающие задачи оптимизации управления обслуживанием исследованы в работе [1].

Каждый объект o_i мультипотока O^n характеризуется целочисленными параметрами: t_i — момент времени поступления в очередь для обслуживания; τ_i — норма длительности обслуживания; a_i — величина штрафа за единицу времени пребывания в системе обслуживания; g_i — признак принадлежности объекта к подпотоку O_{g_i}, $i = \overline{1,n}$, $g_i = \overline{1,m}$.

Обслуживание объектов осуществляется процессором P, который характеризуется начальным моментом временем T готовности к обслуживанию, начальной настройкой g_0 и квадратной матрицей $H(h_{\alpha\beta})$ продолжительностей переналадки от режима обслуживания объектов подпотока O_α к режиму обслуживания объектов подпотока O_β; $h_{\alpha\beta} > 0$ при $\alpha \neq \beta$ и $h_{\alpha\beta} = 0$ при $\alpha = \beta$, $\alpha, \beta = \overline{1,m}$.

Обслуживание каждого объекта реализуется без прерываний; в каждый момент времени процессор P может обслуживать только один объект; по завершению обслуживания объект немедленно освобождает процессор; немотивированные простои процессора и объектов запрещены. Не ограничивая общности, полагаем объекты упорядоченными соответственно моментам их готовности к обслуживанию, т. е. $0 \leq t_1 \leq t_2 \leq \ldots \leq t_n$.

Под расписанием обслуживания понимаем однозначно установленный порядок выполнения подлежащих диспетчеризации технологических операций, например, путем указания моментов времени начала каждой операции.

В силу принятых выше условий реализации процесса обслуживания мультипотока O^n расписание ρ является компактным и, следовательно, однозначно отображается перестановкой номеров объектов $(i_1, i_2, \ldots, i_n)$ в порядке их

взаимодействия с процессором P. Множество всех возможных перестановок является конечным мощности $n!$.

Из компактности расписания ρ следуют соотношения, связывающие моменты начала $t^{\text{н}}_{i_k}$ и завершения $t^{\text{к}}_{i_k}$ обслуживания объекта $o_{o_k}, k = \overline{1,n}$

$$\begin{array}{ll} t^{\text{н}}_{i_1} = max[t_{i_1}, T + h(g_0, g_{i_1})]; & \\ t^{\text{н}}_{i_k} = max[t_{i_k}, t^{\text{к}}_{i_k-1} + h(g_{i_k-1}, g_{i_k})], & k = \overline{2,n}; \\ t^{\text{к}}_{i_k} = t^{\text{н}}_{i_k} + \tau_{i_k}, & k = \overline{1,n}. \end{array}$$

Для каждого объекта o_{i_k} расписание ρ однозначно определяет продолжительность $\Delta_{i_k} = t^{\text{к}}_{i_k} - t_{i_k}$ пребывания его в системе обслуживания и величину штрафа $\varphi(\Delta_{i_k}) = a_{i_k} \cdot \Delta_{i_k}$ за этот промежуток времени. Соответственно, по всем объектам мультипотока O^n величина штрафа вычисляется как сумма $K(\rho) = \sum\limits_{k=1}^{n} \varphi(\Delta_{i_k})$. Задача оптимизации состоит в нахождении расписания ρ^*, минимизирующего значение критерия $K(\rho)$.

Введем следующие обозначения:

$\Upsilon_t = S_t.g \cup \{f_w\} \cup \Phi$ — объекты из текущего подпотока, ожидающие обслуживания;

$F(\nu) = \{o_i \mid t_i = \nu\}$ — объекты, поступающие на обслуживание в момент времени ν;

$D(t, t_+) = \bigcup\limits_{\nu=t+1}^{t_+} F(\nu)$ — объекты, поступающие на интервале $[t+1, t_+]$;

$G(\alpha)$ — величина суммарного штрафа за обслуживание на временном отрезке $[t^{\text{н}}, t^{\text{к}}]$ (здесь $t^{\text{н}} = t$) обслуживания объекта α объектов из Υ_t и объектов, поступающих в систему в моменты времени $t+1, t+2, \ldots, t^{\text{к}} - 1$:

$$G(\alpha) = \sum_{\beta \in \Upsilon_t} a_\beta \cdot (t^{\text{к}}_\alpha - t) + \sum_{\nu=t+1}^{t^{\text{к}}_\alpha - 1} \sum_{\gamma \in F(\nu)} a_\gamma \cdot (t^{\text{к}}_\alpha - \nu);$$

$\Psi(t, g, S_t)$ — минимальная величина суммарного штрафа за временной отрезок от момента t до момента завершения обслуживания в ситуации, определяемой тройкой (t, g, S_t) при оптимальном управлении.

В принятых обозначениях рекуррентное соотношение динамического программирования [2] запишется в виде

$$\Psi(t, g, S_t) = \min_{\alpha \in \Upsilon_t} \left\{ \begin{array}{l} G(\alpha) + \Psi(t^{\text{к}}_\alpha, g, (S_t \backslash \{\alpha\}) \cup D(t, t^{\text{к}}_\alpha)) \mid \alpha \in S_t.g, \\ G(\alpha) + \Psi(t^{\text{к}}_\alpha, j, S_t \cup D(t, t^{\text{к}}_\alpha)) \mid \alpha = f_j, f_j \in \Phi, j \neq q, \\ G(\alpha) + \Psi(t^{\text{к}}_\alpha, g, S_t \cup D(t, t^{\text{к}}_\alpha)) \mid \alpha = f_w, \end{array} \right\}.$$

Реализация полученных решающих соотношений предполагает расчет суммарного штрафа $\Psi(t, g, S_t)$ для всех возможных наборов (t, g, S_t). $\Psi(t_n, g, S_t) = \Psi(t_n + \Delta, g, S_t)$ для любого $\Delta > 0$. С учетом данного обстоятельства расчет начинается в ситуации $(t_n, g, \varnothing)$ для всех возможных подпотоков g,

далее t последовательно принимает натуральные значения на отрезке от t_n до T. Процесс завершается вычислением значения $\Psi(T, g_0, D(0,T))$ — суммарного штрафа на оптимальном расписании.

В процессе вычислений следует фиксировать решение в ситуации (t, g, S_t) — объект α^*, на котором достигается минимум. Оптимальное расписание восстанавливается при обратном проходе по заполненной таблице, начиная от финальной ситуации $(T, g_0, D(0,T))$.

Ниже в таблице приведены усредненные данные вычислительных экспериментов по оценке продолжительности синтеза оптимального расписания, сек.

$n \setminus m$	2	4	6
16	0,4	1,0	1,6
18	2,2	3,5	6,9
20	10,3	20,5	29,7
22	46,1	91,4	128,8

Доклад подготовлен по результатам исследований, выполненных при финансовой поддержке Российского фонда фундаментальных исследований в рамках проекта № 15-07-03141.

Список литературы

[1] Коган Д. И., Федосенко Ю. С. Задача диспетчеризации: анализ вычислительной сложности и полиномиально разрешимые подклассы // Дискретная математика. — 1996. — Т. 8, № 3. — С. 135–147.

[2] Беллман Р., Дрейфус С. Прикладные задачи динамического программирования. — М.: Наука, 1965. — 460 с.

Транзитивные семейства автоматных отображений

Тяпаев Ливат Борисович

НИ Саратовский государственный университет им. Н. Г. Чернышевского, e-mail: tiapaevlb@info.sgu.ru

Автоматные преобразования над алфавитом $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, где p простое число, совпадают с непрерывными в p-адической метрике преобразованиями кольца целых p-адических чисел $\mathbb{Z}_p$, удовлетворяющими p-адическому условию Липшица с константой равной 1. Объектом исследования является транзитивное семейство таких отображений, важное для криптографии.

Автомат это шестерка $\mathcal{A} = (\mathfrak{I}, \mathcal{S}, \mathcal{O}, S, O, s_0)$, где $\mathfrak{I}$ — входной алфавит, $\mathcal{S}$ — множесто состояний, $\mathcal{O}$ — выходной алфавит, $S : \mathfrak{I} \times \mathcal{S} \to \mathcal{S}$ — функция переходов, $O : \mathfrak{I} \times \mathcal{S} \to \mathcal{O}$ — функция выходов, $s_0 \in \mathcal{S}$ — начальное состояние. Заметим, что алфавиты $\mathfrak{I}, \mathcal{O}$ автомата $\mathcal{A}$ суть конечные множества, однако множество $\mathcal{S}$ состояний не обязательно конечно. В дальнейшем будем рассматривать достижимые автоматы: любое состояние $s \in \mathcal{S}$ автомата $\mathcal{A}$ достижимо из начального

состояния s_0 после подачи на вход автомата слова $u \in \mathfrak{I}^*$ конечной длины. Положим $\mathfrak{I} = \mathcal{O} = \mathbb{F}_p$. С автоматом $\mathcal{A}$ ассоциировано преобразовние f_{s_0} кольца $\mathbb{Z}_p$. Выбирая различные состояния $s \in \mathcal{S}$ в качестве начальных, получим семейство автоматных отображений $\mathcal{F} = \{f_s : s \in \mathcal{S}\}$.

Семейство $\mathcal{F}$ преобразований множества M называется транзитивным, если для любой пары $(a, b) \in M$ найдется $f \in \mathcal{F}$ такое, что $f(a) = b$. Автомат $\mathcal{A}$ вполне транзитивен, если семейство $f_s \mod p^n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, $s \in \mathcal{S}$ транзитивно на $\mathbb{Z}/p^n\mathbb{Z}$ для всех $n = 1, 2, 3, \ldots$.

Известно, что автомат $\mathcal{A}$ вполне транзитивен тогда и только тогда, когда мера Лебега $\alpha(f_{s_0})$ замыкания множества точек $(\frac{x \mod p^k}{p^k}, \frac{f_{s_0} \mod p^k}{p^k})$, $x \in \mathbb{Z}_p$, $k = 1, 2, 3, \ldots$ единичного квадрата $\mathbb{E}^2 = [0, 1] \times [0, 1] \subset \mathbb{R}^2$ равна 1 [1].

Занумеруем символы алфавита $\mathbb{F}_p$ натуральными числами $\alpha_i \in \mathbb{F} = \{1, \ldots, p\}$. Слову $u = \alpha_{k-1} \ldots \alpha_1\alpha_0$ в алфавите $\mathbb{F}$ сопоставим рациональное число: $\vec{u} = \alpha_0 + \frac{\alpha_1}{p+1} + \ldots + \frac{\alpha_{k-1}}{(p+1)^{k-1}}$. На множестве $\Gamma = [1, p+1) \times [1, p+1) \subset \mathbb{R}^2$ рассмотрим все точки плоскости с координатами $(\vec{u}, f_{s_0}(\vec{u}))$, где u пробегает все конечные слова. Множество $\Omega(f_{s_0}) \subset \Gamma$ таких точек называется геометрическим образом [2]. Геометрические образы $\Omega(f_{s_0})$ изучались в контексте метрической и аффинной эквивалентности [2]—[5]. В частности, определены коэффициенты для аффинных преобразований геометрических образов конечных автоматов [5].

Представляет интерес задача описания транзитивного семейства автоматных отображений вполне транзитивного автомата на языке геометрических образов.

С каждым состоянием $s \in \mathcal{S}$ автомата $\mathcal{A}$ ассоциировано отображение $R_s : \mathbb{F}_p \to \mathbb{F}_p$, которое каждому входному символу $x \in \mathbb{F}_p$ сопоставляет некоторую выходную реакцию $y \in \mathbb{F}_p$ из состояния s. Отметим, что R_s не обязательно сюръективное отображение.

Рассмотрим автомат $\mathcal{A}$ и семейство $\{R_s : s \in \mathcal{S}\}$. Сопоставление каждому состоянию $s \in \mathcal{S}$ некоторого отображения R'_s порождает новый автомат $\mathcal{B}$. Рассмотрим класс $\mathcal{K}(\mathcal{A})$ автоматов построенный указанным образом. Геометрический образ автомата $\mathcal{B}$ обозначим $\Omega_{\mathcal{B}}(f_s)$.

Теорема. *Автомат $\mathcal{A}$ вполне транзитивен тогда и только тогда, когда существуют автомат $\mathcal{B} \in \mathcal{K}(\mathcal{A})$ и геометрические образы $\omega(f_{s_0}) \subset \Omega(f_{s_0})$, $\omega(f_s) \subset \Omega_{\mathcal{B}}(f_s)$ такие, что $\omega(f_{s_0})$ и $\omega(f_s)$ аффинно эквивалентны.*

Доказательство (скетч). Необходимость. Если рассматривать слова конечной длины k как префиксы бесконечных слов над алфавитом $\mathbb{F}_p$, которые в свою очередь суть элементы колька целых p-адических чисел $\mathbb{Z}_p$, то совпадение этих префиксов означает, что расстояние между бесконечными словами в метрическом пространстве $\mathbb{Z}_p$ в p-адической метрике равно p^{-k}. А это означает, что расстояние между их f_s-образами не более p^{-k} в силу 1-липшицевости отображения $f_s : \mathbb{Z}_p \to \mathbb{Z}_p$. Кроме того, все такие бесконечные слова имеющие общий префикс длины $k \geq 0$ как целые p-адические числа попадают в шар $B_{p^{-k}} = \{z \in \mathbb{Z}_p : |z - a|_p \leq p^{-k}\}$ радиуса p^{-k} с центром в $a \in \mathbb{Z}_p$. Более того, слово u длины k как префикс $z \in \mathbb{Z}_p$ есть

редукция z по модулю p^k, то есть $u \in \mathbb{Z}/p^k\mathbb{Z}$. Далее, если $f_{s_0}(z) \equiv f_s(z) \pmod{p^k}$, то $f_{s_0}(z)$, $f_s(z)$ попадают в один шар и точки в $\Omega(f_{s_0})$ и $\Omega(f_s)$ соответствующие вход/выходным словам длины k совпадают и составляют элементы множеств $\omega(f_{s_0})$, $\omega(f_s)$. Очевидно, что $f_{s_0}(z) \equiv f_s(z) \pmod{p^k}$ влечет $f_{s_0}(z) \equiv f_s(z) \pmod{p^\ell}$ для всех $\ell = 1, \ldots, k-1$, следовательно, точки образов слов длины ℓ совпадают. Случай $f_{s_0}(z) \not\equiv f_s(z) \pmod{p}$ означает, что $f_{s_0}(z)$, $f_s(z)$ попадают в различные шары радиуса p^{-1}, а точки в $\omega(f_{s_0})$ и $\omega(f_s)$ соответсвующие вход/выходным словам длины 1 совместимы аффинным преобразованием $\phi_1 : (\vec{u}, f_s(\vec{u})) \mapsto (\vec{u}, f_{s_0}(\vec{u}) + d)$, $d \in \mathbb{Z}$. Если $f_{s_0}(z) \not\equiv f_s(z) \pmod{p^k}$, но при этом $f_{s_0}(z) \equiv f_s(z) \pmod{p^{k-1}}$, то $f_{s_0}(z), f_s(z) \in B_{p^{k-1}}$ и точки образов $\omega(f_{s_0})$ и $\omega(f_s)$ слов длины k совместимы преобразованием $\phi_k : (\vec{u}, f_s(\vec{u})) \mapsto (\vec{u}, f_{s_0}(\vec{u}) + d)$, $d \in \mathbb{Q}$. Транзитивность семейства $\mathcal{F}$ для автомата $\mathcal{A}$ означает, что для данной пары u, w слов длины k найдется слово v конечной длины, переводящее автомат из состояния s_0 в состояние s такое, что $f_s(\vec{u}) = \vec{w}$. Функции R'_s порождают автомат $\mathcal{B} \in \mathcal{K}(\mathcal{A})$ такой что, точка $(\vec{u}, f_{s_0}(\vec{u})) \in \omega(f_{s_o})$ переводится в точку $(\vec{u}, \vec{w}) \in \omega(f_s) \subset \Omega_{\mathcal{B}}(f_s)$ преобразованием $\phi : (\vec{u}, fs_0(\vec{u})) \mapsto (\vec{u}, cf_{s_0}(\vec{u}) + d)$, $c, d \in \mathbb{Q}$. Достаточность. Если $\omega(f_{s_0})$, $\omega(f_s)$ совпадают, то $f_{s_0}(\vec{u}) \equiv f_s(\vec{u}) \pmod{p^k}$, для некоторого u длины k, и $f_s \in \mathcal{F}$. Если $\omega(f_{s_0})$, $\omega(f_s)$ ϕ-эквивалентны, то $f_s \in \mathcal{F}$. **Теорема доказана.**

Каждому входному слову $u = \ldots x_{n-1} \ldots x_1 x_0$, $x_i \in \mathbb{F}_p$ сопоставим число $\overleftarrow{x} = \ldots x_{n-1} \ldots x_1 x_0$, записанное в системе счисления по основанию $\beta > 1$, например, по основанию $\beta = \sqrt{2}$. Для неотрицательного действительного числа z и действительного $\beta > 1$ запись $z = \ldots + z_{n-1}\beta^{n-1} + \ldots + z_1\beta + z_0 + z_{-1}\beta^{-1} + z_{-2}\beta^{-2} + \ldots + z_{-m}\beta^{-m}$, где $z_i \in \{0, 1, \ldots, \lfloor \beta \rfloor\}$, $\beta^m \leq z < \beta^{m+1}$, $m \in \mathbb{Z}$ называется β-представлением z. В. С. Анашиным предложено рассматривать автоматные отображения с использованрем β-представлений. А именно, слову $x = x_{n-1} \ldots\ x_1 x_0$, $x_i \in \mathbb{F}_p$ сопоставим точку $\overleftarrow{x} = \frac{x_{n-1}\beta^{n-1} + \ldots + x_1\beta + x_0}{\beta^n} \pmod{1}$ из интервала $[0, 1)$. Рассматривая все точки $(\overleftarrow{x}, f_{s_0}(\overleftarrow{x}))$, где x пробегает все конечные слова, получим множество точек с рациональными координатами в единичном евклидовом квадрате $\mathbb{E}^2$. Замыкание этого множества $\Psi(f_{s_0})$ суть геометрический образ автомата $\mathcal{A}$ в β-представлении. Вопрос характеризации транзитивных семейств автоматных отображений, заданных с помощью геометрических образов в β-представлении остается открытым.

Список литературы

[1] Anashin V., Khrennirov A. Applied Algebraic Dynamics. — Walter de Gruyter, Berlin–New York, 2009.

[2] Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика, механика, математическая кибернетика. Сб. науч. тр. — Саратов: Изд-во Сарат. ун-та, 1999. — С. 139–143.

[3] Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. — 2006. — Т. 6., вып. 1/2 — С. 121–133.

[4] Тяпаев Л. Б. Геометрические образы автоматов и динамические системы // Дискретная математика и ее приложения. Материалы X Межд. семинара. Под ред. О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2010. — С. 510–513.

[5] Матов Д. О. Аффинные преобразования геометрических образов конечных автоматов // Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. — 2012. — Т. 12, вып. 3 — С. 104–108.

Анализ кибернетической дискретной системы адаптивного управления потоками требований

Федоткин Михаил Андреевич, Кудрявцев Евгений Владимирович

Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: fma5@rambler.ru, evgkudryavcev@gmail.com

В данной работе рассматривается процесс управления конфликтными неординарными пуассоновскими потоками в классе адаптивных алгоритмов. Для такой системы, используя подход Ляпунова–Яблонского, выделены ее структурные блоки и дано их описание. Анализ системы сводится к изучению многомерной случайной последовательности.

Описание системы

В работах [1] и [2] описана кибернетическая управляющая система обслуживания, вероятностная модель которой представляется в виде упорядоченной тройки $(\Omega, \mathfrak{F}, \mathbf{P}(\cdot))$. Здесь Ω — множество описаний ω элементарных исходов управляющей системы, $\mathfrak{F}$ — сигма-алгебра исходов $A \subset \Omega$ и $\mathbf{P}(\cdot)$ — вероятность на $\mathfrak{F}$. Система рассматривается в дискретные моменты $\tau_i(\omega), i = 0, 1, \ldots$ смены состояний обслуживающего устройства и в ней выделены блоки:

1) первый тип входных полюсов — конфликтные входные неординарные пуассоновские потоки Π_1 и Π_2 (см. (1) из [2]);

2) второй тип входных полюсов — потоки насыщения Π_1^* и Π_2^* (выходные потоки системы при ее максимальной загрузке и эффективном функционировании);

3) внешняя память — неограниченные накопители очередей O_1 и O_2 по входным потокам Π_1 и Π_2, $\kappa_{1,i}(\omega)$ и $\kappa_{2,i}(\omega)$ — количество требований в накопителях O_1 и O_2 в момент τ_i;

4) блок по переработке внешней памяти — экстремальная стратегия обслуживания (см. (2) из [1]), при которой из накопителей O_1 и O_2 на обслуживание выбирается максимально возможное число заявок;

5) внутренняя память — обслуживающее устройство, состояния $\Gamma^{(1)}, \Gamma^{(2)}, \ldots, \Gamma^{(8)}$ которого составляют множество Γ;

6) блок по переработке информации внутренней памяти — адаптивный алгоритм (см. (1) из [1]) смены состояний обслуживающего устройства.

Алгоритм смены состояний обслуживающего устройства задается графом, представленном на рис. 1.

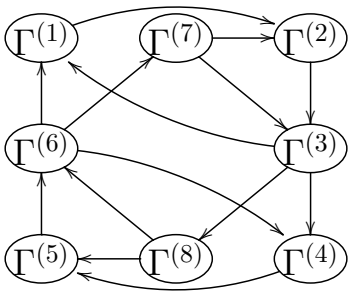

Рис. 1. Граф смены состояний обслуживающего устройства.

Состояние системы на i-м такте времени $[\tau_i, \tau_{i+1})$ описывается случайным элементом $(\Gamma_i(\omega), \kappa_i(\omega)), i = 0, 1, \ldots,$ где Γ_i — состояние обслуживающего устройства на $[\tau_i, \tau_{i+1})$, $\kappa_i = (\kappa_{1,i}, \kappa_{2,i})$ — векторный размер очереди в момент τ_i. Для данной последовательности доказана ее марковость и проведена классификация ее состояний.

Свойства системы

Теорема 1. *Случайная векторная последовательность* $\{(\Gamma_i, \kappa_i); i = 0, 1, \ldots\}$ *с заданным начальным распределением вектора* $\{(\Gamma_0, \kappa_0)\}$ *является марковской.*
Теорема 2. *Пусть* $j, s = 1, 2, j \neq s, x = (x_1, x_2) \in X^2$ (X — *множество целых неотрицательных чисел*)*, и пусть*

$$G = \{(\Gamma^h, x) : \Gamma^h \in \Gamma, x \in X^2\},$$
$$G^{(3j-2)} = \{(\Gamma^{(3j-2)}, x_s y_s) : x_s < K_s - l_{3s}\},$$
$$G^{(3j-1)} = \{(\Gamma^{(3j-1)}, x_s y_s) : x_s < K_s - l_{3s}\},$$
$$G^{(6+j)} = \{(\Gamma^{(6+j)}, x) : x_j > 0\} \cup \{(\Gamma^{(6+j)}, x) : x_s \geq K_s - l_{3s}\},$$
$$G_j = \begin{cases} G^{(6+j)} \cup G^{(3j-2)}, l_{3j-2} > 0, \\ G^{(6+j)} \cup G^{(3j-2)} \cup G^{(3j-1)}, l_{3j-2} = 0, \end{cases}$$

где $K_j, l_{3j}, l_{3j-1}, l_{3j-2}, j = 1, 2,$ — *некоторые параметры системы,* $y_1 = (1, 0)$, $y_2 = (0, 1)$.

Тогда состояния из G_j *являются несущественными и класс* $G_0 = G \backslash (G_1 \cup G_2)$ *является неразложимым апериодическим классом существенных состояний.*

Для любого $i \geq 0, r = \overline{1, 8}; x \in X^2$ обозначим:

$$Q_i^{(r)}(x) = \mathbf{P}(\Gamma_i = \Gamma^{(r)}, \kappa_i = x).$$

В [2] приведены рекуррентные соотношения для $Q_i^{(r)}(x)$. Обозначим

$$Q^{(r)}(x) = \lim_{i \to \infty} Q_i^{(r)}(x), r = \overline{1, 8}, x \in X^2.$$

Если существует предельное распределение $\{(\Gamma_i, \kappa_i); i \geq 0\}$, т. е. последовательность $\{(\Gamma_i, \kappa_i); i \geq 0\}$ сходится при $i \to \infty$ по распределению к некоторому

случайному элементу (Γ^*, κ^*), где $\Gamma^* \in \Gamma$, $\kappa^* = (\kappa_1^*, \kappa_2^*) \in X^2$, и для любого $r = \overline{1,8}, x \in X^2$ имеем $\mathbf{P}(\Gamma^* = \Gamma^{(r)}, \kappa^* = x) = Q^{(r)}(x)$. Тогда справедливы следующие утверждения.

Лемма 1. *Если существует предельное распределение марковской последовательности* $\{(\Gamma_i, \kappa_i); i \geq 0\}$*, то для любых значений* $r = \overline{1,8}$; $x_j \in X$ *имеет место предельное равенство:*

$$\lim_{i\to\infty} \mathbf{P}(\Gamma_i = \Gamma^{(r)}, \kappa_{j,i} = x_j) = \mathbf{P}(\Gamma^* = \Gamma^{(r)}, \kappa_j^* = x_j).$$

Лемма 2. *Если существует предельное распределение марковской последовательности* $\{(\Gamma_i, \kappa_i); i \geq 0\}$*, то имеют место предельные равенства:*

$$\lim_{i\to\infty} \mathbf{P}(\kappa_{j,i} = x_j) = \mathbf{P}(\kappa_j^* = x_j), j = 1, 2; x_j \in X.$$

Работа выполнена в ННГУ при финансовой поддержке госбюджетной темы «Математическое моделирование и анализ стохастических эволюционных и процессов принятия решений», госрегистрация № 01201456585, и государственной программы «Поддержка ведущих университетов РФ в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров»

Список литературы

[1] Кудрявцев Е. В, Федоткин М. А. Кибернетический подход к изучению вероятностной модели адаптивного управления конфликтными потоками // Проблемы теоретической кибернетики. Материалы XVII международной конференции. — Казань: Отечество, 2014. — С. 158–161.

[2] Кудрявцев Е. В, Федоткин М. А. Построение математической модели адаптивного управления неординарными потоками // Теория вероятностей, случайные процессы, математическая статистика и приложения. — Минск, 2015.

Построение иерархии классов сложности булевых функций вычислимых детерминированными, недетерминированными и вероятностными k-OBDD

Хадиев Камиль Равилевич

Казанский федеральный университет, e-mail: kamilhadi@gmail.com

В данной работе рассматривается известная модель ветвящихся программ — k-$OBDD$. Ветвящиеся программы и их модификации $OBDD$ и k-$OBDD$ определены в книге [1].

$OBDD$ на множестве переменных $X = \{x_1, x_2, \ldots, x_n\}$ — это ветвящаяся программа, обладающая следующими свойствами. Ее вершины разбиты на n

уровней $1, \ldots, n$ таким образом, что из вершин уровня i ребра ведут только в вершины уровня $(i+1)$. На каждом уровне i считывается значение только одной переменной x_{j_i}. На любом пути вычисления каждая переменная считывается один раз. Говорят, что $OBDD$ P читает переменные в порядке $\theta = (i_1, \ldots, i_n)$. Различные $OBDD$ могут использовать различные порядки θ считывания переменных. Вершины последнего уровня называются финальными и помечаются символами из $\{0, 1\}$.

k-$OBDD$ — это ветвящаяся программа P, которую можно разделить на k слоев, каждый из которых является $OBDD$, причем порядок θ чтения переменных во всех слоях программы P одинаковый. k-$NOBDD$ (недетерминированные k-$OBDD$) — это k-$OBDD$, в которой разрешены недетерминированные переходы. k-$POBDD$ (вероятностная k-$OBDD$) — это k-$OBDD$, в которой разрешены вероятностные переходы.

Говорят, что k-$OBDD$ $P(X)$ вычисляет булеву функцию $f(X)$ ($f : \{0, 1\}^n \to \{0, 1\}$), если для любого набора $\nu \in \{0, 1\}^n$, такого, что $f(\nu) = 1$ в $P(X)$ есть путь из начальной вершины в финальную 1-вершину. В противном случае такого пути нет. В случае k-$NOBDD$ для любого набора $\nu \in \{0, 1\}^n$, такого, что $f(\nu) = 1$, в $P(X)$ есть хотя бы один путь из начальной вершины в финальную 1-вершину. В случае k-$POBDD$ — в $P(X)$ вероятность попасть из начальной вершины в финальную 1-вершину, больше, чем $0.5 + \delta$, а для $f(\nu) = 0$ такая вероятность $0.5 - \delta$, для некоторого $\delta > 0$. В этом случае говорят, что k-$POBDD$ P вычисляет функцию f с δ изолированной точкой сечения.

Ширина $w(P)$ $OBDD$ (k-$OBDD$, k-$NOBDD$ или k-$POBDD$) P — это максимум от количества вершин на уровне, взятый по всем уровням P. Сложность $S(P)$ — это число ее внутренних вершин. Заметим, что непосредственно из определения для рассмотренных моделей имеем $w(P) \leq S(P) \leq k \cdot w(P) \cdot n$.

Через $\mathbf{k\text{-}OBDD_{POLY}}$ обозначим класс булевых функций, которые вычислимы k-$OBDD$ полиномиальной ширины (или что то же самое полиномиальной сложности). Вычислимые k-$OBDD$ константнной ширины — $\mathbf{k\text{-}OBDD_{CONST}}$, где $CONST = \{w : w > 20, w = const\}$, полилогорифмической ширины — $\mathbf{k\text{-}OBDD_{POLYLOG}}$, где $POLYLOG$ — множество линейных комбинаций над W, где $W = \{(\log_2 n)^{t_1} : t_1 = const\}$, сублинейной ширины — $\mathbf{k\text{-}OBDD_{SUBLINEAR}}$, где $SUBLINEAR_\alpha = \{w : w > 20, w \leq n^\alpha\}$. Аналогично для k-$NOBDD$ и k-$PBDD$.

В работе [2] доказана следующая иерархия (иерархия Bolling-Sauerhoff-Sieling-Wegener): для $k = o(n^{1/2}/\log^{3/2} n)$ выполняется собственное включение: $\mathbf{(k-1)\text{-}OBDD_{POLY}} \subsetneq \mathbf{k\text{-}OBDD_{POLY}}$. Доказательство иерархии Bolling-Sauerhoff-Sieling-Wegener основано на нижней оценке вычисления булевых функций в k-раундовых коммуникационных протоколах [3].

Используя метод представления k-$OBDD$ в виде специального коммуникационного протокола, рассмотренный в работе [4], была уточнена иерархия Bolling-Sauerhoff-Sieling-Wegener для малой ширины. Кроме того, исполь-

зуя ту же технику, были получены результаты для k-$NOBDD$ и k-$NOBDD$.

Теорема 1. *Справедливы следующие иерархии.*

Для $k = o(n/\log_2 n)$*:*

$$(\mathbf{k}/\log_{\mathbf{2}}\log_{\mathbf{2}}\mathbf{n})\text{-}\mathbf{OBDD_{CONST}} \subsetneq \mathbf{k}\text{-}\mathbf{OBDD_{CONST}},$$

$$(\mathbf{k}/\log_{\mathbf{2}}\log_{\mathbf{2}}\mathbf{n})\text{-}\mathbf{NOBDD_{CONST}} \subsetneq \mathbf{k}\text{-}\mathbf{NOBDD_{CONST}}.$$

Для $k = o(n/\log_2 n)$*:*

$$\big(\mathbf{k}/(\log_{\mathbf{2}}\mathbf{n}\log_{\mathbf{2}}\log_{\mathbf{2}}\mathbf{n})\big)\text{-}\mathbf{POBDD_{CONST}} \subsetneq \mathbf{k}\text{-}\mathbf{POBDD_{CONST}}.$$

Для $\varepsilon > 0, k = o(n^{1-\varepsilon}), n^{\varepsilon} < k$*:*

$$(\mathbf{k}/\mathbf{n}^{\varepsilon})\text{-}\mathbf{OBDD_{POLYLOG}} \subsetneq \mathbf{k}\text{-}\mathbf{OBDD_{POLYLOG}},$$

$$(\mathbf{k}/\mathbf{n}^{\varepsilon})\text{-}\mathbf{NOBDD_{POLYLOG}} \subsetneq \mathbf{k}\text{-}\mathbf{NOBDD_{POLYLOG}},$$

$$(\mathbf{k}/\mathbf{n}^{\varepsilon})\text{-}\mathbf{POBDD_{POLYLOG}} \subsetneq \mathbf{k}\text{-}\mathbf{POBDD_{POLYLOG}}.$$

Для $0 < \alpha < 0.49, k > n^{\alpha}(\log_2 n)^2, k = o(n^{1-\alpha}/\log_2 n)$*:*

$$\Big(\mathbf{k}/\big(\mathbf{n}^{\alpha}\big(\log_{\mathbf{2}}\mathbf{n}\big)^{\mathbf{2}}\big)\Big)\text{-}\mathbf{OBDD_{SUBLINEAR_{\alpha}}} \subsetneq \mathbf{k}\text{-}\mathbf{OBDD_{SUBLINEAR_{\alpha}}}.$$

Для $0 < \alpha < 0.32, k > n^{2\alpha}(\log_2 n)^2, k = o(n^{1-\alpha}/\log_2 n)$*:*

$$\Big(\mathbf{k}/\big(\mathbf{n}^{\mathbf{2}\alpha}\big(\log_{\mathbf{2}}\mathbf{n}\big)^{\mathbf{2}}\big)\Big)\text{-}\mathbf{NOBDD_{SUBLINEAR_{\alpha}}} \subsetneq \mathbf{k}\text{-}\mathbf{NOBDD_{SUBLINEAR_{\alpha}}},$$

Для $0 < \alpha < 0.32, k > n^{2\alpha}(\log_2 n)^3, k = o(n^{1-\alpha}/\log_2 n)$*:*

$$\Big(\mathbf{k}/\big(\mathbf{n}^{\mathbf{2}\alpha}(\log_{\mathbf{2}}\mathbf{n})^{\mathbf{3}}\big)\Big)\text{-}\mathbf{POBDD_{SUBLINEAR_{\alpha}}} \subsetneq \mathbf{k}\text{-}\mathbf{POBDD_{SUBLINEAR_{\alpha}}},$$

Таким образом, при ширине менее, чем $n^{1/3}$, иерархия справедлива для k, больших, чем в работе [2], в частности, наибольшее продвижение получаем при константной ширине. Кроме того, были улучшены результаты для недетерминированного случая [5].

Работа выполнена при поддержке РФФИ (проект № 14-07-00557-а). Работа выполнена за счет средств субсидии, выделенной в рамках государственной поддержки Казанского (Приволжского) федерального университета в целях повышения его конкурентоспособности среди ведущих мировых научно-образовательных центров.

Список литературы

[1] Wegener I. Branching Programs and Binary Decision Diagrams: Theory and Applications / I. Wegener — Philadelphia: Society for Industrial and Applied Mathematics, 2000.

[2] Bolling B. Hierarchy Theorems For kOBDDs And kIBDDs / B. Bolling, M. Sauerhoff, D. Sieling, I. Wegener // Theoretical Computer Science. — 1998. — V. 205, Iss. 1–2. — P. 45–56.

[3] Nisan N., Widgerson A. Rounds In Communication Complexity Revisited // SIAM Journal on Computing. — 1993. — V. 22. — P. 211–219.

[4] Ablayev F., Khadiev K. Extension of the hierarchy for k-OBDDs of small width // Russian Mathematics. — 2013. — V. 57, N 3. — P. 46–50.

[5] Okol'nishnikova E. On the hierarchy of nondeterministic branching k-programs // Fundamentals of computation theory // 11th International Symposium, FCT'97 Kraków, Poland, September 1–3, 1997, Proceedings. — Volume of Lecture Notes in Computer Science, Springer, 1997. — V. 1102. — P. 376–387.

Иерархия для двусторонних детерминированных и недетерминированных автоматов

Хадиев Камиль Равилевич, Ибрагимов Ришат Наримanович

Казанский федеральный университет, e-mail: kamilhadi@gmail.com, rishat.ibrahimov@yandex.ru

В данной работе рассматривается известная модель — двусторонние автоматы. В частности, двусторонние конечные детерминированные (2КДА) и недетерминированные (2КНА) автоматы.

Приведем формальное определение. Двусторонний конечный детерминированный автомат (2КДА) D, работающий на входном слове $X = (x_1, \ldots, x_n)$, с левым (\$) и правым ограничителями (#), — это шестерка $D = (\Sigma, S, s_1, \delta, s_a, s_r)$, где Σ — входной алфавит, мы будем рассматривать только алфавит $\Sigma = \{0, 1\}$; S — множество состояний автомата, причем $|S| = const$, количество состояний $|S|$ будем называть размером автомата; s_1 — начальное состояние, причем $s_1 \in S$; $\delta : S \times \Sigma \cup \{\$, \#\} \to S \times \{\leftarrow, \downarrow, \rightarrow\}$, причем $\delta(s, \$) = (s, \rightarrow)$, $\delta(s', \#) = (s', \leftarrow)$, для любого $s \in S, s' \in S \backslash \{s_a, s_r\}$, где $\leftarrow$ означает, что читающая головка перемещается влево, $\rightarrow$ — вправо, $\downarrow$ — остается на месте. s_a — принимающее состояние, причем $s_a \in S$; s_r — отвергающее состояние, причем $s_r \in S$.

Опишем работу автомата D на слове $\nu \in \Sigma^n$. Первоначально автомат обозревает первую ячейку и находится в состоянии s_1. Затем применяется функция переходов $\delta(s_1, x_1) = (s', di)$, где $s' \in S$, $di \in \{\leftarrow, \downarrow, \rightarrow\}$. Читающая головка перемещается в соответствии с направлением di, при этом автомат переходит в состояние s' и так далее.

Автомат D принимает входное слово (выдает результат 1), если попадает в состояние s_a. Автомат D отвергает входной набор (выдает результат 0), если попадает в состояние s_r или попадает в бесконечный цикл. Причем, если автомат обозревает ячейку с номером i, где $i \in \{0, \ldots, n\}$, и находится в состоянии s_r или s_a, то автомат переводит читающую головку в конец слова без изменения состояния и завершает работу.

Аналогично можно определить недетерминированную модель 2КНА.

Вопрос об отношении классов языков, распознаваемых автоматами разного размера, рассматривался уже давно. К примеру, Sakoda и Sipser в работе [8] показали, что любой 2КНА может быть смоделирован 2КДА экспоненциального размера. Кроме того двухсторонние автоматы моделировались односторонними и лучшие вариант был в работах [2], [4]. Исследователи получали улучшали оценки только для модифицированных моделей [3], [5], [6], [7].

На основе коммуникационного метода представления 2КДА и 2КНА, аналогичного методу, рассмотренному в работе [1], нами была получена нижняя оценка для ранга языка (количества классов Майхилла-Нероуда), распознаваемого приведенными моделями. Эта нижняя оценка связывает размер модели с рангом языка.

Теорема 1. *Для языка L, распознаваемого 2КДА A размера d и языка L', распознаваемого 2КНА A' размера d' справедливы следующие соотношения:*

$$Rank(L) \leq (d+1)^{d+1}, \qquad Rank(L') \leq 2^{(d'+1)^2},$$

где $Rank(L)$ — ранг (количества классов Майхилла-Нероуда) языка L.

Используя сложностные свойства языка $2 - USAF_w$, определение которого основывается на определении функции, приведенной в работе [1], а также Теорему 1 была получена следующая иерархия (Теорема 2) для классов языков распознаваемых 2КДА размера d и 2КНА размера d.

Определим эти классы $\mathbf{2DFA(d)} = \{L$: существует 2КДА D размера d, распознающий язык $L\}$, $\mathbf{2NFA(d)} = \{L$: существует 2КНА D размера d, распознающий язык $L\}$. И приведем иерархию для этих классов относительно величины d:

Теорема 2. *Для некоторого целого числа d справедливы следующие собственные включения:*

$$\mathbf{2DFA}(\lfloor \frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} \rfloor - \mathbf{4}) \subsetneq \mathbf{2DFA(d)},$$

$$\mathbf{2NFA}(\lfloor \sqrt{\frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} - \mathbf{4}} \rfloor) \subsetneq \mathbf{2NFA(d)}.$$

Очевидно, что $\mathbf{2DFA}(\lfloor \frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} \rfloor - \mathbf{4}) \subseteq \mathbf{2DFA(d)}$, $\mathbf{2NFA}(\lfloor \sqrt{\frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} - \mathbf{4}} \rfloor) \subseteq \mathbf{2NFA(d)}$. Достаточно доказать, что

$$\mathbf{2DFA}(\lfloor \frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} \rfloor - \mathbf{4}) \neq \mathbf{2DFA(d)},$$

$$\mathbf{2NFA}(\lfloor \sqrt{\frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} - \mathbf{4}} \rfloor) \neq \mathbf{2NFA(d)}.$$

Для этого был построен 2КДА A ширины $12w^2 + 21w + 4$, распознающий язык $2 - USAF_w$ для некоторого целого w, следовательно $2 - USAF_{\lfloor \frac{\sqrt{249+48d}-21}{24} \rfloor} \in \mathbf{2DFA(d)}$, $2 - USAF_{\lfloor \frac{\sqrt{249+48d}-21}{24} \rfloor} \in \mathbf{2NFA(d)}$.

При этом мы доказали, что $Rank(2 - USAF_w) \geq w^{w-1}$, таким образом согласно Теореме 1 получаем, что

$$2 - USAF_{\lfloor \frac{\sqrt{249+48d}-21}{24} \rfloor} \notin \mathbf{2DFA}(\lfloor \frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} \rfloor - \mathbf{4}),$$

$$2 - USAF_{\lfloor \frac{\sqrt{249+48d}-21}{24} \rfloor} \notin \mathbf{2NFA}(\lfloor \sqrt{\frac{\sqrt{\mathbf{249+48d}}-\mathbf{21}}{\mathbf{24}} - \mathbf{4}} \rfloor).$$

Отсюда получаем неравенства классов, а значит и доказательство собственных включений.

Список литературы

[1] Ablayev F., Khadiev K. Extension of the hierarchy for k-OBDDs of small width // Russian Mathematics. — 2013. — V. 57, N 3. — P. 46–50.

[2] Chrobak M. Finite automata and unary languages // Theoretical Computer Science. — 1986. — V. 47(0). — P. 149–158.

[3] Geffert V., Guillon B., Pighizzini G. Two-way automata making choices only at the endmarkers // Language and Automata Theory and Applications volume of Lecture Notes in Computer Science. — Springer, 2012. — V. 7183. — P. 264–276.

[4] Kapoutsis C. A. Removing bidirectionality from nondeterministic finite automata // MFCS volume of Lecture Notes in Computer Science. — Springer, 2005. — V. 3618. — P. 544–555.

[5] Kapoutsis C. A. Nondeterminism is essential in small two-way finite automata with few reversals // Information and Computation. — 2013. — V. 222(0). — P. 208–227.

[6] Kapoutsis C. A., Královic R., Mömke T. Size complexity of rotating and sweeping automata // Journal of Computer and System Sciences. — 2012. — V. 78, N 2. — P. 537–558.

[7] Leung H. Tight lower bounds on the size of sweeping automata // Journal of Computer and System Sciences. — 2001. — V. 63, N 3. — P. 384–393.

[8] Salomaa A., Soittola M. Automata-Theoretic Aspects of Formal Power Series. Series: Texts and monographs in computer science. — N. Y.: Springer-Verlag, 1978.

Модель случайного геометрического графа для беспроводных самоорганизующихся сетей

Хорошеньких Сергей Николаевич[1], **Дайняк Александр Борисович**[2]

[1] Московский физико-технический институт, e-mail: khoroshenkikh@phystech.edu

[2] Московский физико-технический институт, e-mail: dainiak@phystech.edu

Введение

В настоящее время большой практический интерес представляют *самоорганизующиеся сети* — децентрализованные беспроводные сети передачи дан-

ных. Передача трафика (*маршрутизация*) в распределенных сетях — сложная инженерная и алгоритмическая задача. Наиболее изученной моделью таких сетей является *случайный геометрический граф Гилберта* [1,2], а одна из алгоритмических проблем, возникающих в рамках маршрутизации — отыскание минимального связного доминирующего множества (minimal connected dominating set, mCDS) на графе сети [3].

Отличительная особенность беспроводных сетей — их геометрические свойства (которые в свою очередь диктуются физическими принципами распространения сигналов). Это позволяет рассматривать вершины графа как точки в евклидовом пространстве. Далее в настоящей работе термины “вершина графа” и “точка” могут отождествляться там, где это не вызовет недоразумений.

Модель Гилберта основана на предположении, что вершины графа появляются в пространстве одновременно и независимо друг от друга. В настоящей работе предлагается новая модель случайного графа для беспроводной сети, основанная на иных предположениях. Во-первых, вершины добавляются в граф последовательно (т. е. рассматриваеися процесс роста сети). Во-вторых, каждая новая вершина появляется в той и только в той области пространства, где уже присутствует “сигнал” сети. Наконец, в-третьих, место появления новой вершины заранее неизвестно. Все эти предположения будут формализованы ниже.

Предлагаемая модель

Введем модель случайного графа на n вершинах, обозначаемого далее $G(n)$. Множество вершин такого графа (обозначим его $V(n)$) состоит из n точек в $\mathbb{R}^d$, порождаемых следующим случайным процессом:

1. $V(1) = \{\mathbf{0}\}$ (первая вершина графа лежит в начале координат)
2. $V(n+1) = V(n) \cup \{\xi_n\}$, где ξ_n — реализация d-мерной случайной величины, равномерно распределенной в области $\bigcup\limits_{v \in V(n)} B(v)$, где $B(v)$ — шар единичного объема с центром в точке v.

Множество рёбер $E(n)$ графа $G(n)$ задается следующим образом: $\{v_1, v_2\} \in E(n) \iff v_1 \in B(v_2)$.

Меру множества $\bigcup\limits_{v \in V(n)} B(v)$ будем обозначать $\sigma(n)$ и называть *покрытием* графа $G(n)$. Покрытие — случайная величина, ее математическое ожидание $S(n) = \mathsf{E}\sigma(n)$ будем называть *средним покрытием* графа $G(n)$.

Алгоритм построения mCDS

Модель графа $G(n)$ обладает простым свойством, которое позволяет строить связное доминирующее множество с помощью жадного алгоритма. Введем обозначение: $d(i), 1 \le i \le n$ — математическое ожидание степени i-й вершины (т.е. вершины, которая появилась в графе i-й по счету).

Утверждение 1. *$\forall i, j : 1 \le i < j \le n$ справедливо неравенство $d(i) > d(j)$.*

Алгоритм работает в предположении, что для каждой пары вершин можно определить, какая из них появилась в графе раньше. В реальных сетях

это предположение выполнено, если узлы синхронизованы, и каждый узел распространяет информацию о своем времени подключения к сети.

Обозначим $D(n)$ множество, построенное на графе из n вершин. Множество соседей вершины v будем обозначать $N(v)$. Для произвольного $S \subseteq V(n)$ обозначим $\mathrm{oldest}(S)$ вершину из S, добавленную в граф раньше всех остальных.

- **Инициализация.** $D(1) = V(1)$.
- **Шаг алгоритма при появлении в графе новой вершины** v_{n+1}.
  Если $D(n) \cap N(v_{n+1}) = \varnothing$, то вершина $\mathrm{oldest}\,(N(v_{n+1}))$ добавляется в $D(n+1)$, в противном случае полагаем $D(n+1) = D(n)$.

Некоторые результаты для одномерного случая

В одномерном случае ($d = 1$) вершины соединяются ребром, если они находятся на расстоянии не более $\frac{1}{2}$ друг от друга. Любое множество вершин, порождающее связный подграф, будет покрывать отрезок на числовой прямой.

Заметим, что в любой реализации одномерного случайного графа $G(n)$ размер доминирующего множества будет не меньше, чем $\sigma(n) - 1$ (столько отрезков единичной длины нужно, чтобы покрыть все вершины графа). Значит, средний размер доминирующего множества в графе на n вершинах есть величина порядка $\Omega(S(n))$. Поэтому исследование случайной величины $\sigma(n)$ представляет интерес.

Можно показать, что последовательность случайных величин $\{\sigma(n)\}_{i\geq 1}$ представляет собой марковский случайный процесс с переходной плотностью

$$\Pr\left(\sigma(i+1)|\sigma(i)\right) = \frac{\sigma(i)-1}{\sigma(i)}\delta(\sigma(i+1)-\sigma(i)) +$$

$$+\frac{1}{\sigma(i)} I\left(\sigma(i) < \sigma(i+1) < \sigma(i) + \frac{1}{2}\right).$$

Используя марковское свойство, можно получить оценки на среднее покрытие и дисперсию покрытия.

Теорема 1. $S(n) = \Theta(\sqrt{n})$.

Схема доказательства. Проиллюстрируем используемую при доказательстве технику на примере “клеточной” модели одномерного графа: вершины графа появляются в целочисленных точках вещественной оси, а “окрестность” вершины — две ближайшие к ней точки на решетке. Будем искать количество точек, покрываемых этим графом.

Рекуррентное соотношение на покрытие такого графа получается из следующего соображения: покрытие увеличивается на единицу если и только если новая вершина появляется в одной из двух граничных точек, т.е. $S(k+1) = S(k) + \dfrac{2}{S(k)}$. Преобразуем это уравнение и просуммируем по

k: $\sum\limits_{k=1}^{n} S(k) \cdot (S(k+1) - S(k)) = 2n$. Сумма слева асимптотически равна $\int\limits_{1}^{S(n)} x dx \sim \dfrac{S^2(n)}{2}$. Отсюда $S(n) \sim 2\sqrt{n}$.

Теорема 2. $\mathrm{Var}[\sigma(n)] = O(\sqrt{n})$.

Список литературы

[1] Penrose M. Random geometric graphs. (Series: Oxford Studies in Probability, Book 5). -– Oxford: Oxford University Press, 2003. — 344 p.

[2] Surveys in Combinatorics 2011 / Chapman R. (ed.). — Cambridge University Press, 2011. — 446 p.

[3] Das B., Bharghavan V. Routing in ad-hoc networks using minimum connected dominating sets // Communications, 1997. ICC'97 Montreal, Towards the Knowledge Millennium. 1997 IEEE International Conference on. — IEEE, 1997. — V. 1. — P. 376–380.

Критические корневые диаграммы систем автоматического управления

Чехонадских Александр Васильевич

Новосибирский государственный технический университет, e-mail: alexander_cheh@mail.ru

Система автоматического управления (САУ) в классическом понимании представляет собой пару *объект* $\leftrightarrow$ *регулятор* с отрицательной обратной связью. Объект предполагается полностью заданным, а структура регулятора и его параметры p задаются так, чтобы обеспечить наилучшее подавление возмущений в процессах, происходящий в объекте. Описание линейной САУ после преобразования Лапласа принимает алгебраическую форму, а её принципиальные свойства (устойчивость, колебательность и др.) обеспечиваются расположением на комплексной плоскости полюсов системы $z_1, \ldots, z_m$, т. е. корней её характеристического многочлена $f_p(s) = s^m + a_{m-1}(p)s^{m-1} + \ldots + a_1(p)s + a_0(p)$.

В САУ полного порядка оказывается возможным обеспечить любое расположение полюсов. Однако в промышленности и технике преобладают регуляторы пониженного порядка с существенно более простой структурой [1]. В этом случае произвольное расположение полюсов не достижимо, и задача синтеза управления принимает оптимизационный вид: обеспечение возможно лучшего расположение полюсов САУ за счёт выбора структуры регулятора и значения p^* его параметров. Типичными для практики оказываются такие подходы к оптимальному расположению полюсов [2]:

1) максимизация Гурвицевой устойчивости ("степени", или "запаса устойчивости") за счет минимизации функции $H(p) = \max\{\mathrm{Re}\, z_1, \ldots, \mathrm{Re}\, z_m\}$, при этом полюса окажутся в самой левой из полуплоскостей $\{s \mid \mathrm{Re}\, s \le H(p)\}$;

2) снижение колебательности системы с учетом устойчивости за счет минимизации функции $K(p) = \max(\mathrm{Re}\, z_k + |\mathrm{Im}\, \mathrm{z_k}|)$, при этом полюса окажутся в самом левом из конусов семейства $\{s \mid \mathrm{Re}\, s + |\mathrm{Im}\, s| \le K(p)\}$;

3) увеличение запаса устойчивости системы с учетом колебательности, связанное с минимизацией функции $G(p) = \max\left(\mathrm{Re}\, z_k + \sqrt{L^2 + \mathrm{Im}^2 z_k}\right) - L$, в результате чего полюса окажутся во внутренности самой левой ветви гиперболы $\mathrm{Re}\, z + \sqrt{L^2 + \mathrm{Im}^2 z} - L \le G(p)$.

Число a, в этих примерах равное $H(p)$, $K(p)$ и $G(p)$ соответственно, называется *R-градуировкой* данного набора полюсов; минимизация R-градуировки как функции $a(p)$ параметров регулятора обеспечивает самое левое расположение границы всего набора полюсов САУ [3].

Точка p^0 в пространстве параметров P оказывается критической, если n степеней свободы пространства P связываются условием расположения наибольшего числа действительных и комплексносопряженных полюсов на правой границе области расположения всех полюсов; в общем случае это записывается n равенствами относительно действительных и мнимых частей граничных полюсов [4]. Схема расположения действительных полюсов и нескольких комплексных пар различной кратности на правой границе критической области, отвечающее n задающим равенствам, именуется *критической корневой диаграммой.*

Например, при 5 параметрах регулятора критическими для функции $H(p)$ оказываются расположения на вертикальной прямой (правой границе полуплоскости) шестикратного действительного корня $z_{1,\ldots,6}$, шести простых комплексных пар корней: $\mathrm{Re}\, z_{1,2} = \ldots = \mathrm{Re}\, z_{11,12}$, двух двукратных комплексных пар, трехкратной комплексной пары и простого корня $\mathrm{Re}\, z_{1,\ldots,6} = \mathrm{Re}\, z_7$, и т. д.

В силу сказанного важно установить полный перечень критических корневых расположений в зависимости от числа n задающих их действительных равенств, и указать эффективный метод их перечисления.

Рассмотрим кодировку расположения полюсов, на правой границе которого $r-1$ различная комплексная пара, в виде строки $(a_1\ a_2\ \ldots\ a_r)$, где $a_1 \ge 0$ — кратность правого действительного корня, $a_1 \ge 1$ — кратность комплексной пары с минимальной по модулю мнимой частью, $a_2 \ge 1$ — кратность комплексной пары со второй в порядке возрастания модулей мнимой частью и т. д. Равенство $a_1 = 0$ означает, что действительных корней на правой границе нет, а при отсутствии среди граничных корней комплексных пар код имеет вид (a_1).

Теорема. *Число $C(n)$ различных корневых диаграмм, задающихся n равенствами, равняется $(n+3)$-му числу Фибоначчи φ_{n+1}.*

Доказательство. Проведем полную индукцию по n. Если задающих равенств нет, справа в общем случае оказывается действительный корень или комплексная пара, коды которых (1) и $(0\ 1)$, т.е. $C(0) = 2 = \varphi_3$. Одно равенство задает наличие на правой границе двукратного действительного корня, простого корня и комплексной пары или двух комплексных пар с кодами (2), (11) и (011) со-

ответственно; при этом $C(1) = 3 = \varphi_4$. Допустим, что равенство $C(k) = \varphi_{k+3}$ верно для всех $k < n$. Рассмотрим коды, задаваемые n равенствами.

Коды, имеющие вид $(a_1 \dots a_{r-1}1)$, соответствуют случаю наибольшей по модулю мнимой части у простой комплексной пары. Исключая ее, получим всевозможные коды $(a_1 \dots a_{r-1})$, описывающиеся системой из $n-1$ равенства. По индукционному предположению их φ_{n+2}.

Коды, имеющие вид $(a_1 \dots a_{r-1}2)$, соответствуют случаю, когда наибольший модуль имеет мнимая часть двукратной комплексной пары. Ее удаление приводит к кодам, задаваемым набором $n-3$ равенств; их число равно φ_n.

И так далее. В конце возможны два варианта.

i. Если число $n = 2k+1$ нечетно, то $n+3 = 2k+4$ четно; отбрасывание правых элементов кода приведет к нечетным членам последовательности Фибоначчи и окончится на $\varphi_3 = 2$ кодах без задающих равенств. К этому добавится код одноэлементной строки $(n+1)$, отбрасывание единственного элемента которого приводит к пустой строке, не являющейся кодом. При этом в общую сумму войдет слагаемое $1 = \varphi_1$.

По известному тождеству для четных номеров последовательности Фибоначчи получаем $\varphi_1 + \varphi_3 + \varphi_5 + \ldots + \varphi_n + \varphi_{n+2} = \varphi_{n+3}$.

ii. Если же число $n = 2k$ четно, то $n+3 = 2k+3$ нечетно, и возникать будут четные члены последовательности Фибоначчи вплоть до $\varphi_4 = 3$ кодов с одним задающим равенством. К этому добавятся две строки $(n+1)$ и $(0\ k+1)$; в обоих случаях удаление элемента строки не приводит к коду. Число $n+3$ нечетно, и по аналогичному тождеству (с учетом того, что $\varphi_2 = 1$) получим $1 + \varphi_2 + \varphi_4 + \ldots + \varphi_n + \varphi_{n+2} = \varphi_{n+3}$. **Теорема доказана.**

Следствие. *Число критических диаграмм* $C(n)$ *растет асимптотически как* $((1+\sqrt{5})/2)^n$.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ, по государственному заданию № 2014/138, проект 1052.

Список литературы

[1] Kano M., Ogawa M. The state of the art in chemical process control in Japan: Good practice and questionnaire survey // Journal of Process Control. — 2010. — V. 20, Iss. 9. — P. 969–982.

[2] Чехонадских А. В. Метрика, градуировка и оптимизация расположения характеристических корней системы автоматического управления // Науч. вестн. НГТУ. — 2009. — Т. 34, № 1. — С. 165–182.

[3] Воевода А. А., Чехонадских А. В. Преодоление недифференцируемости при оптимизационном синтезе систем автоматического управления // Автометрия. — 2010. — Т. 46, № 5. — С. 11–17.

[4] Чехонадских А. В. Экстремальные расположения полюсов систем автоматического управления с регулятором пониженного порядка // Автоматика и телемеханика. — 2014. — № 10. — С. 6–24.

Применение методов целочисленной оптимизации для решения задач компьютерной алгебры

Чирков Александр Юрьевич[1], **Грибанов Дмитрий Владимирович**[2]

[1] Нижегородский госуниверситет им. Н. И. Лобачевского, e-mail: chir7@yandex.ru
[2] НИУ ВШЭ, Нижний Новгород; ННГУ им. Н. И. Лобачевского, e-mail: dimitry.gribanov@gmail.com

Представим некоторые задачи компьютерной алгебры как задачи двумерной целочисленной оптимизации:

1) Найти наибольший общий делитель (НОД) двух целых чисел a и b, тогда НОД$(a,\, b)$ совпадает с минимумом следующей задачи:

$$\min |ax + by|,$$
$$\begin{cases} |ax + by| \neq 0, \\ x, y \in Z. \end{cases}$$

2) Пусть $M = m_a m_b$, где m_a, m_b натуральные, взаимно простые числа, пусть также заданы целые числа a, b, такие что $0 \leq a < m_a$ и $0 \leq b < m_b$. Тогда задачу восстановления целого числа по остаткам можно сформулировать как задачу поиска x удовлетворяющего системе:

$$\begin{cases} x \equiv a \pmod{m_a}, \\ x \equiv b \pmod{m_b}, \\ 0 \leq x < m_a m_b, \\ x \in Z. \end{cases}$$

Данная система эквивалентна следующей задаче оптимизации:

$$\min |a - b + x m_a - y m_b|,$$
$$\begin{cases} x < m_b, \\ x, y \in Z_+. \end{cases}$$

3) Пусть $a \in Z$, $m \in N$, тогда задачей восстановления рационального числа в системе вычетов называется задача поиска таких $x \in N$ и $y \in Z$, что $ax \equiv y \pmod{m}$. Множество возможных x, y бесконечно и возникает вопрос поиска минимальных в каком-то смысле значений x, y. Пусть $f(x, y)$ двумерная строго выпуклая симметричная функция. Тогда исходную задачу восстановления дроби можно дополнить:

$$\min f(x, y),$$
$$\begin{cases} ax \equiv y \pmod{m}, \\ x \in N, \\ y \in Z. \end{cases}$$

Условие $xa \equiv y \pmod{m}$ эквивалентно тому, что $xa - y = mz$, где z есть некоторое целое число. Исключив переменную y получаем:

$$\min f(x,\, ax - mz),$$
$$\begin{cases} x, z \in Z, \\ x \neq 0. \end{cases}$$

Для приведенных задач компьютерной алгебры разработан универсальный подход, основанный на методах минимизации двумерных симметричных квазивыпуклых функций на целочисленной решетке [1]. Подход позволяет получить субквадратичные алгоритмы для данных задач. Построенный алгоритм минимизации имеет асимптотически оптимальную трудоемкость по количеству сравнений, более того константа близка к оптимальной. Подробный обзор рассматриваемых задач компьютерной алгебры можно получить из работ [2, 3, 4].

Работа выполнена при поддержке лаборатории алгоритмов и анализа сетевых структур НИУ ВШЭ, грант правительства РФ дог. 11.G34.31.0067 и при поддержке РФФИ, грант 15-01-06249.

Список литературы

[1] Чирков А. Ю. Минимизация квазивыпуклой функции на двумерной целочисленной решетке // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 2003. — № 1. — С. 227–238.

[2] Грегори Р., Кришнамурти Е. Безошибочные вычисления. Методы и приложения. — М.: Мир, 1988.

[3] Möller N. On Schönhage's algorithm and subquadratic integer gcd computation // Mathematics of Computation. — January, 2008. — V. 77 (261). — P. 589–607.

[4] Brent R., Zimmermann P. Modern Computer Arithmetic. — Cambridge University Press, New York, 2010.

О минимизации одного множества булевых функций для аддитивных мер сложности

Чухров Игорь Петрович

Институт автоматизации проектирования РАН, e-mail: chip@icad.org.ru

Задача минимизации булевых функций в геометрической интерпретации связана с представлением булевой функции подмножеством вершин n-мерного единичного куба и нахождением минимального покрытия комплексом граней единичного куба этого подмножества, т. е. является разновидностью задачи о покрытии множества. При таком подходе к минимизации булевых функций размерность матрицы в задаче о покрытии может быть значительной,

так как определяется числом простых импликант функции. Предлагаемые для решения такой задачи методы [3] нацелены на кратное увеличение быстродействия алгоритмов для повышения размерности практически решаемых задач. Обоснованными методами сокращения вычислительной трудоемкости алгоритмов являются независимая минимизация для компонент связности и методы вычисления нижних границ, которые обеспечивают достаточные условия минимальности, при условии их применимости. Соответственно, актуальным становится исследование множества булевых функций, к которым такие методы не применимы. Отметим, что для локальных алгоритмов конечного индекса была показана их неприменимость при минимизации плотных булевых функций ([1, стр. 128]).

Функционал, определенный на множестве всех комплексов граней, является мерой сложности, если он удовлетворяет аксиомам неотрицательности, монотонности относительно умножения, выпуклости относительно сложения и инвариантности относительно изоморфизма [2].

Мера сложности называется аддитивной, если сложность любого комплекса граней равна сумме сложностей граней. Аддитивными являются меры сложности: l — число граней, L — сумма рангов граней, L_0 — число направлений равных 0 и L_1 — число направлений равных 1 в гранях комплекса, т. е. число переменных с отрицанием и, соответственно, без отрицания в дизъюнктивной нормальной форме.

Используемые понятия и обозначения для единичного куба B^n и множества булевых функций n переменных P_n можно найти в [1, 2]. Под $\log$ всюду понимается логарифм по основанию 2.

Для булевой функции f обозначим: $k(f)$ — число компонент связности; $m(f)$ — мощность максимального интервально независимого подмножества вершин; $l(f)$ и $l_T^{\max}(f)$ — длина кратчайшего и максимальная длина тупикового комплекса граней; $\mathcal{TM}_l(f)$ и $\mathcal{TM}_{\mathcal{L}}(f)$ — множества тупиковых кратчайших и тупиковых $\mathcal{L}$-минимальных комплексов граней.

Обозначим через $\mathcal{F}_{n,\mathcal{L}}$ подмножество функций, зависящих от n переменных и аддитивной меры сложности $\mathcal{L}$, которые обладают следующими свойствами: множество единичных вершин функции f является одной связной компонентой, $\mathcal{TM}_l(f) \cap \mathcal{TM}_{\mathcal{L}}(f) = \varnothing$ и $l(f) = m(f)$.

Максимальное число $\mathcal{L}$-минимальных комплексов граней для функций множества $\mathcal{F}_{n,\mathcal{L}}$ обозначим через $\mu(\mathcal{F}_{n,\mathcal{L}})$.

При минимизации функций из множества $\mathcal{F}_{n,\mathcal{L}}$ не удается уменьшить трудоемкость поиска решения за счет независимой минимизации для компонент связности и применения достаточных условий минимальности, которые используют интервально независимые множества вершин, для исключения просмотра всех минимальных комплексов граней.

Теорема 1. *Если для функции $f \in P_s$ и параметров s, t и $\tilde{\alpha}_{s+1,n} = (\alpha_{s+1}, \ldots, \alpha_n)$ для аддитивной меры сложности $\mathcal{L}$ выполняется*

$$l_T^{\max}(f)\,\mathcal{L}_{s+t+2}^{\max} < \mathcal{L}_{n-s}^{\max} = \mathcal{L}\left(B_{s+1,\ldots,n}^{n,\alpha_{s+1},\ldots,\alpha_n}\right) \text{ и } l(f) > 1, \text{ то}$$
$$\log \mu(\mathcal{F}_{n,\mathcal{L}}) \geq l(f) \log \left|\tilde{I}_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}\right| \text{ и } \log|\mathcal{F}_{n,\mathcal{L}}| \geq k(f)\left(\left|\tilde{I}_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}\right| - 1\right),$$

где $\mathcal{L}_r^{\max}$ — максимальная $\mathcal{L}$-сложность грани ранга r, $\tilde{I}_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}$ — пучок изоморфных граней максимальной мощности, которые имеют ранг t и содержат вершину $\tilde{\alpha}_{s+1,n-2} = (\alpha_{s+1}, \ldots, \alpha_{n-2}) \in B^{n-s-2}$.

Для конкретной аддитивной меры сложности $\mathcal{L}$ нижние оценки получаются рациональным подбором функции $f \in P_s$ и параметров преобразований s, t, $\tilde{\alpha}_{s+1,n}$, которые удовлетворяют условиям теоремы 1. При этом может быть использована оценка $\left|\tilde{I}_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}\right| \geq \frac{1}{t+1}\binom{n-2-s}{t}$.

Аддитивной линейной мерой сложности называется мера $\mathcal{L}$, если $\mathcal{L}(I) = aL_0(I) + bL_1(I)$, где $a, b \geq 0$, $\max\{a, b\} > 0$ и I — грань куба.

Теорема 2. *Для аддитивной линейной меры сложности $\mathcal{L}$ выполняются* $\log \mu(\mathcal{F}_{n,\mathcal{L}}) \gtrsim n \log n$ *и* $\log|\mathcal{F}_{n,\mathcal{L}}| \geq \Theta(2^n/\sqrt{n})$ *при* $n \to \infty$.

Аддитивной полиномиальной мерой сложности называется мера $\mathcal{L}$, если $\mathcal{L}(I) = q(L_0(I), L_1(I))$, где $q(x, y)$ — многочлен не ниже 2-ой степени с положительными коэффициентами и I — грань куба.

Теорема 3. *Для аддитивной полиномиальной меры сложности $\mathcal{L}$ выполняются* $\log \mu(\mathcal{F}_{n,\mathcal{L}}) \geq (\mathcal{L}_n^{\max})^{1-o(1)} \log n$ *и* $\log|\mathcal{F}_{n,\mathcal{L}}| \geq \Theta\left(2^n/n^{3/2}\right)$ *при* $n \to \infty$.

Построение функции из множества $\mathcal{F}_{n,\mathcal{L}}$ при выполнении условий теоремы 1 осуществляется по следующей схеме преобразования функций.

Первое преобразование $\Phi : P_s \to P_{n-2}$ функции $f \in P_s$ ставит в соответствие функцию:

$$f_\Phi\left(\tilde{x}^{n-2}\right) = f(\tilde{x}^s)\, Z_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}(\tilde{x}_{s+1,n-2}) \vee x_{s+1}^{\alpha_{s+1}} \ldots x_{n-2}^{\alpha_{n-2}},$$

где функция $Z_{t,\tilde{\alpha}}^n \in P_n$, для $1 \leq t \leq n$, состоит из простых импликант соответствующих пучку граней максимальной мощности, которые имеют ранг t и содержат вершину $\tilde{\alpha} \in B^n$, а функция $Z_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}(\tilde{x}_{s+1,n-2})$ получается подстановкой векторов переменных $\tilde{x}_{s+1,n-2} = (x_{s+1}, \ldots, x_{n-2})$ и значений $\tilde{\alpha}_{s+1,n-2} = (\alpha_{s+1}, \ldots, \alpha_{n-2})$ в функцию $Z_{t,\tilde{\alpha}}^{n-2-s} \in P_{n-2-s}$.

Второе преобразование $\Psi : P_{n-2} \to P_n$ функции $f_\Phi \in P_{n-2}$ ставит в соответствие функцию:

$$f_{\Phi,\Psi}(\tilde{x}^n) = x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}\left(f_1\left(\tilde{x}^{n-2}\right) \vee f_2\left(\tilde{x}^{n-2}\right)\right) \vee \lambda(\tilde{x}^n)\, f_2\left(\tilde{x}^{n-2}\right), \text{ где}$$
$$f_\Phi\left(\tilde{x}^{n-2}\right) = f_1\left(\tilde{x}^{n-2}\right) \vee f_2\left(\tilde{x}^{n-2}\right),$$
$$f_1\left(\tilde{x}^{n-2}\right) = f(\tilde{x}^s)\, x_{s+1}^{\alpha_{s+1}} \ldots x_{n-2}^{\alpha_{n-2}},$$
$$f_2\left(\tilde{x}^{n-2}\right) = \bar{f}(\tilde{x}^s)\, x_{s+1}^{\alpha_{s+1}} \ldots x_{n-2}^{\alpha_{n-2}} \vee$$
$$\vee f(\tilde{x}^s)\left(x_{s+1}^{\bar{\alpha}_{s+1}} \vee \ldots \vee x_{n-2}^{\bar{\alpha}_{n-2}}\right) Z_{t,\tilde{\alpha}_{s+1,n-2}}^{n-2-s}(\tilde{x}_{s+1,n-2}),$$
$$\lambda(\tilde{x}^n) = x_{n-1}^{\alpha_{n-1}} x_n^{\bar{\alpha}_n}(x_1 \oplus \ldots \oplus x_{n-2}) \vee x_{n-1}^{\bar{\alpha}_{n-1}} x_n^{\alpha_n}(x_1 \oplus \ldots \oplus x_{n-2} \oplus 1).$$

Различные функции из множества $\mathcal{F}_{n,\mathcal{L}}$ получаются если к компонентам связности функции $f \in P_s$ независимо применяются преобразования с функциями, которые соответствуют произвольному подмножеству простых импликант функции $Z^{n-2-s}_{t,\tilde{\alpha}_{s+1,n-2}}(\tilde{x}_{s+1,n-2})$. В силу суммируемости для компонент связности тупиковых комплексов граней и сложности комплексов граней для аддитивных мер при выполнении условий теоремы 1 справедливо утверждение о принадлежности получаемых функций множеству $\mathcal{F}_{n,\mathcal{L}}$.

Работа выполнена при поддержке РФФИ (проект № 13-01-00958).

Список литературы

[1] Васильев Ю. Л., Глаголев В. В. Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики. Т. 1. — М.: Наука, 1974. — С. 99–148.

[2] Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискрет. анализ и исслед. операций. — 2013. — Т. 20, № 6. — С. 77–94.

[3] Coudert O., Sasao T. Two-level logic minimization // Logic Synthesis and Verification. — Kluwer Academic Publishers, 2001. — P. 1–21.

Сложность вычисления нелинейной полиномиальной функции над полем Галуа вида $GF(2^k)$ в базисе булевых функций от $2k$ переменных

Шалагин Сергей Викторович

Казанский национальный исследовательский технический университет им. А. Н. Туполева, e-mail: sshalagin@mail.ru

Решена задача оценки сложности вычисления нелинейной полиномиальной функции (НПФ) над полем $GF(2^k)$, $k \geq 2$, по количеству булевых функций от $2k$ переменных в зависимости от количества переменных указанной НПФ.

Получены оценки временной и аппаратной сложности распределенного вычисления нелинейной полиномиальной функции от m переменных — НПФ(m), определенной над $GF(2^k)$ вида:

$$f(x_1, ..., x_m) = \sum_{i_1=0}^{w} ... \sum_{i_m=0}^{w} a_{i_1 ... i_m} x_1^{i_1} ... x_m^{i_m}, \qquad (1)$$

где $a_{i_1 ... i_m} x_1^{i_1} \dots x_m^{i_m} \in GF(2^k)$ — элементарный полином (ЭП), $i_j = \overline{0, 2^k - 1}$, $j = \overline{1, m}$, $w = 2^k - 1$, $\sum$ обозначает операцию вычисления поразрядной суммы по модулю два. Наличие коэффициентов $a_{i_1 ... i_m} = 0$ позволяет не производить вычисление значений соответствующих ЭП. Рассмотрим процесс вычисления (1) на основе ярусно-параллельного графа (ЯПГ), описываемого определенными числовыми характеристиками [1]. Булевы функции от $2k$ переменных

обозначим БФ($2k$). Введем в рассмотрение параллельные регистры на k разрядов — $RG(k)$, $k = 2, 3, \ldots$. Обозначим $t_{\Gamma\Phi(2k)}$, $t_{RG(k)}$ и t_{IC} времена задержки функционирования БФ($2k$), $RG(k)$ и межсоединений (МС) между БФ($2k$) и $RG(k)$.

Определение 1. *Процесс вычисления* (1) *описывается ЯПГ G с вершинами v_{01}, v_{02}, …, v_{0w}, v_{10}, v_{11}, v_2 и v_D, которым соответствуют следующие операции над элементами $GF(2^k)$ — cx, x^2, …, x^w, x^1x^2, cx^1x^2, сумма по модулю два от $2k$ операндов и сохранение элемента $GF(2^k)$ в параллельном регистре, соответственно, $w = 2^k - 1$.*

Множество вершин ЯПГ G v_{01}, v_{02}, …, v_{0w}, v_{10}, v_{11} и v_2 обозначим как V. Дугам G соответствуют МС, требуемые для вычисления (1). Для выполнения операций, которым соответствуют вершины G из V, требуется по k БФ($2k$) на каждую операцию, а которым соответствуют v_D — $RG(k)$. Обозначим как t^{out}_{IOB} и t^{in}_{IOB} — времена задержек ввода переменных и вывода значения НПФ(m), соответственно.

Определение 2. *При конвейерном вычислении* (1) *с сохранением промежуточных результатов операций, описываемых на каждом ярусе G, верхняя оценка временной сложности вычислений на одной ступени конвейера составляет:*

$$t_{\text{БФ}(2k)} + t_{RG(k)} + T, \text{где } T = max(t_{IC}, t^{out}_{IOB}, t^{in}_{IOB}). \qquad (2)$$

Вычисление ЭП $a_{i_1\ldots i_m}x_1^{i_1}\ldots x_m^{i_m}$ отображено при использовании множества подграфов G — ЯПГ $G(m, P)$, где множество $P = \{p_0, p_1, \ldots, p_w\}$, $p_t \geq 0$ —- количество x_j^t, $t = \overline{0, w}$, $j = \overline{1, m}$, $\sum_{t=0}^{w} p_t = m$, $w = 2^k - 1$.

Определение 3. *Количество ярусов подграфа $G(m, P)$, при условии, что $p_0 \in [0, (m-1)]$, равно $h(G(m, P)) = 1+]log_2(]p_1/2[+p_2 + \ldots + p_w)[$, причем $h = max(h(G(m, P))) = 1+]log_2 m[$. Если для $G(m, P)$ $p_1 = 0$, то множество вершин первого яруса $G(m, P)$ — пустое.*

Определение 4. *Процесс вычисления операций, соответствующих v_2, описывается графом G_2, который является подграфом ЯПГ G.*

Теорема 1. *Количество вершин $G(m, P)$ на l-м ярусе — $N_l(G(m, P)) = N_l^{(V)}(G(m, P)) + N_l^{(D)}(G(m, P))$, где $N_l^{(V)}(G(m, P))$ — количество вершин из V, $N_l^{(D)}(G(m, P))$ — количество вершин вида v_D, $p_0 \in [0, (m-1)]$.*

Теорема 2. *Количество вершин G_2 на l-м ярусе — $N_l(G_2) = N_l^{(V)}(G_2) + N_l^{(D)}(G_2)$, где $N_l^{(V)}(G_2)$ и $N_l^{(D)}(G_2)$ — количество вершин вида v_2 и v_D, соответственно, причем $N_0(G_2) = N_1(G_2) = 0$.*

На основе теоремы 2 предложен алгоритм вычисления значений $N_l^{(V)}(G_2)$ и $N_l^{(D)}(G_2)$ при заданных коэффициентах в (1).

Оценка аппаратной сложности вычисления (1) сводится к оценке количества вершин G, в частности — на каждом из ярусов G. Возможен подсчет количества ярусов G в зависимости от значений $a_{i_1\ldots i_m} \in GF(2^k)$, $i_j = \overline{0, w}$, $j = \overline{1, m}$,

$w = 2^k - 1$. Пусть $Q(G(m,P))$ — множество ЭП в (1), соответствующих $G(m,P)$, подграфу ЯПГ G. Справедлива

Теорема 3. $|Q(G(m,P))| = q - z$, *где* $q = \frac{m!}{(m-\sum_{t=1}^{w} p_t)!P_1!\ldots p_w!}$, z — *количество нулевых коэффициентов во множестве ЭП, соответствующих* $G(m,P)$, $w = 2^k - 1$.

Множества P, а также $|Q(G(m,P))|$ вычисляемы на основе заданных значений коэффициентов в (1).

Список литературы

[1] Поспелов Д. А. Введение в теорию вычислительных систем. — М.: Советское радио, 1972. — 280 с.

О методе декомпозиции мультифункций

Шаранхаев Иван Константинович

Бурятский государственный университет, e-mail: goran5@mail.ru

Функции, заданные на конечном множестве A и принимающих в качестве своих значений подмножества множества A, в том числе $\varnothing$, в последнее время принято называть мультифункциями (мультиоперациями) на A.

Естественным является вопрос выразимости произвольной мультифункции через мультифункции меньшей размерности. Автором сформулирован и доказан критерий декомпозиции мультифункций на $\{0,1\}$, в том числе разделительной декомпозиции, который обобщает результат Г. Н. Поварова о функциональной разделимости булевых функций [1] и дает метод получения представлений мультифункций с помощью мультифункций меньшей размерности. В качестве приложений метода на его основе можно строить алгоритмы нахождения бесповторных представлений мультифункций на $\{0,1\}$ в различных базисных множествах.

Отметим, что терминология, используемая здесь для мультифункций, практически полностью сохранена из теории булевых функций, которую можно посмотреть, например, в [2]. Будут использоваться следующие обозначения: переменные обозначаются символами x, u, v, w, возможно, с индексами; константы обозначаются символами α, β, σ, возможно, с индексами; символом $\tilde{x}$ обозначается набор $(x_1,\ldots,x_n)$; $|\tilde{x}|$ – длина набора $\tilde{x}$.

Пусть $|A|$ — мощность множества A, 2^A — множество всех подмножеств A, $E_2 = \{0,1\}$. Определим следующие множества функций:

$P^{\overline{*}}_{2,n} = \{f | f : E_2^n \to 2^{E_2}\}$, $P^{\overline{*}}_2 = \bigcup\limits_n P^{\overline{*}}_{2,n}$,

$P_{2,n} = \{f | f \in P^{\overline{*}}_{2,n}$ и $|f(\tilde{\alpha})| = 1$ для всех $\tilde{\alpha} \in E_2^n\}$, $P_2 = \bigcup\limits_n P_{2,n}$.

Функции из P_2 называют булевыми функциями, а из $P^{\overline{*}}_2$ — мультифункциями на E_2. Далее мультифункции на E_2 будем называть просто мультифункциями.

Для того, чтобы суперпозиция $f(f_1(x_1,\ldots,x_m),\ldots,f_n(x_1,\ldots,x_m))$, где f, f_1, ..., $f_n \in P^{\overline{*}}_2$, определяла некоторую мультифункцию $g(x_1,\ldots,x_m)$, зададим значения мультифункции на наборах из подмножеств множества E_2.

Если $(\alpha_1, \ldots, \alpha_m) \in E_2^m$, то по определению

$$g(\alpha_1, \ldots, \alpha_m) = \begin{cases} \varnothing, \text{ если } f_i(\alpha_1, \ldots, \alpha_m) = \varnothing \text{ для некоторого } i \in \{1, \ldots, m\}; \\ \bigcup\limits_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n), \text{ в противном случае.} \end{cases}$$

Мультифункция, получаемая из $f(x_1, ..., x_n)$ подстановкой вместо некоторой переменной x_i константы $\sigma \in \{0, 1\}$, называется остаточной и обозначается $f_{x_i}^{\sigma}$. Индуктивно это определение распространяется на подмножество переменных.

Для произвольных n-местных мультифункций f и g определим мультифункцию $f \cup g$ следующим образом:

$(f \cup g)(\alpha_1, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n) \cup g(\alpha_1, \ldots, \alpha_n)$ для любого $(\alpha_1, \ldots, \alpha_n)$.

Мультифункция f при разбиении множества переменных на $\tilde{u}, \tilde{v}, \tilde{w}$ допускает *декомпозицию*, если существуют мультифункции h и g такие, что выполняется $f(\tilde{u}, \tilde{v}, \tilde{w}) = h(\tilde{u}, \tilde{w}, g(\tilde{u}, \tilde{v}))$.

Если $\tilde{u} = \varnothing$, то такая декомпозиция называется *разделительной*

Теорема. *Произвольная мультифункция f допускает декомпозицию при разбиении множества переменных на $\tilde{u}, \tilde{v}, \tilde{w}$ тогда и только тогда, когда для любого набора $\tilde{\alpha}$ ($|\tilde{\alpha}| = |\tilde{u}|$) среди всех остаточных мультифункций от $f_{\tilde{u}}^{\tilde{\alpha}}$ по переменным $\tilde{v}$ не более четырех различных, причем каждая из них равна либо $*$, либо некоторой мультифункции f_0, либо некоторой мультифункции f_1, либо $f_0 \cup f_1$.*

Следствие (критерий разделительной декомпозиции). *Произвольная мультифункция f допускает разделительную декомпозицию при разбиении множества переменных на $\tilde{v}, \tilde{w}$ тогда и только тогда, когда среди всех остаточных мультифункций от f по переменным $\tilde{v}$ не более четырех различных, причем каждая из них равна либо $*$, либо некоторой мультифункции f_0, либо некоторой мультифункции f_1, либо $f_0 \cup f_1$.*

Список литературы

[1] Поваров Г. Н. О функциональной разделимости булевых функций // Доклады АН СССР. — 1954. —Т. 94, № 5. — С. 801–803.

[2] Избранные вопросы теории булевых функций / Под ред. С. Ф. Винокурова и Н. А. Перязева). — М.: Физматлит, 2001. — 192 с.

Исследование грациозности графа средствами целочисленного программирования

Шерман Зоя Александровна

Институт кибернетики имени В. М. Глушкова НАН Украины, e-mail: sherman.zoya@rambler.ru

Пусть задан граф $G = (V, E)$ порядка m и размера n, не содержащий кратных ребер и петель. Функцию f называют грациозной разметкой графа

G, если f — инъекция из $V(G)$ в множество $\{0, 1, 2, ..., n\}$ и индуцируемая ею реберная разметка $f^*(u, v) = |f(u) - f(v)|$ является биекцией из $E(G)$ на множество $\{1, 2, 3, ..., n\}$.

Задачу построения грациозной разметки графа $G = (V, E)$ будем рассматривать как задачу линейного целочисленного программирования. Этой тематике посвящены работы [1–3]. Введем ряд переменных, необходимых для составления ограничений:

x_i — метка i-той вершины графа G, $i = 1, ..., m$;
e_{ij} — метка ребра ij, $e_{ij} \neq 0$, $i \neq j$;
r_{ijlp} — разность меток ребер ij и lp, $ij \neq lp$, $r_{ijlp} \neq 0$;
s_{ijlp} — сумма меток ребер ij и lp, $s_{ijlp} \neq 0$, $e_{ij} \neq -e_{lp}$;
t_{ij} — разность меток не смежных вершин i и j,
где $i, j, l, p = 1, 2, ..., m$.

Сформулируем задачу:

1) $x_i - x_j = e_{ij}$ для всех $i, j \in V(G)$, $(i, j) \in E(G)$, $i \neq j$;
2) $e_{ij} - e_{lp} = r_{ijlp}$ для всех $r_{ijlp} \neq 0$, $(i, j), (l, p) \in E(G)$, $(i, j) \neq (l, p)$;
3) $e_{ij} + e_{lp} = s_{ijlp}$ для всех $s_{ijlp} \neq 0$, $(i, j), (l, p) \in E(G)$, $(i, j) \neq (l, p)$;
4) $x_i - x_j = t_{ij}$ для всех $(i, j) \in E(G)$, $i \neq j$;
5) $0 \leq x_i \leq m$, где x_i — целые числа;
6) $e_{ij}, r_{ijlp}, s_{ijlp}, t_{ij}$ — ненулевые числа,
где $i, j, l, p = 1, 2, ..., m$.

Полученные ограничения гарантируют выполнение условий грациозности, если $e_{ij} \in \{1, 2, 3, ..., n\}$ при $i, j \in V(G)$. Число введенных ограничений 1)–4) в постановке задачи приводят к $((n-1)^2 + 0,5n^2 - (n-1) - n/2)$ уравнениям [2], что значительно затрудняет поиск решения при увеличении значения n. Предлагаемый в этой работе способ модификации метода «ветвей и границ» дает возможность не только отбросить условие целочисленности и ограничение 6), а так же особым образом выбрать переменную для ветвления. Этот выбор выполняется по стратегии “jumptracking” [2]. Согласно этой стратегии в каждое полученное решение входят все выше описанные переменные, которые заносятся в список оптимальных решений. При этом все нецелочисленные и нулевые переменные каждого текущего решения распределяются в множества: $P_1 = \{e_{ij}, t_{ij} \mid e_{ij} = 0$ или $t_{ij} = 0\}$, $P_2 = \{r_{ijlp}, s_{ijlp} \mid r_{ijlp} = 0$ или $s_{ijlp} = 0\}$, $P_3 = \{x_i \mid x_i$ имеет не целое значение$\}$. Переменная, выбранная из множества P_1, имеет больший приоритет над переменной из P_2. Аналогично, переменная из множества P_2 имеет больший приоритет над переменной из P_3. Если выбирается переменная из множеств P_1 или P_2, то решаем две новые подзадачи линейного программирования с дополнительными ограничениями (например: $x \geq 1$ и $x \leq -1$). Если выбирается переменная из множества P_3, то две новые подзадачи имеют следующие ограничения: в первой подзадаче дробную переменную x уменьшая до $\lfloor x \rfloor$, получаем дополнительное ограничение: $x \leq \lfloor x \rfloor$; во второй подзадаче дробную переменную x увеличивая до $\lfloor x \rfloor + 1$, получаем дополнительное ограничение: $x \geq \lfloor x \rfloor + 1$. Если из списка оптимальных решений несколько раз выбирается переменная, которая не приводит к нужно-

му результату, то данное решение удаляется из списка. Приведенный способ позволяет ускорить процесс нахождения оптимального решения задачи. Чем меньше мощность множества $|P_1|+|P_2|+|P_3|$ тем быстрее получим допустимое решение задачи.

Список литературы

[1] Redl T. A. Graceful graphs and graceful labelings: two mathematical and programming formulations and some other new results // Proceedings of the Thirty-Fourth Southeastern International Conference on Combinatorics, Graph Theory and Computing. — 2003. — V. 164. — P. 17–32.

[2] Eshghi K., Azimi P. Applications of mathematical programming in graceful labeling of graphs // J. Appl. Math. — 2004. — V. 1. — P. 1–8.

[3] Eshghi K., Azimi P. An Algorithm for Finding a Feasible Solution of Graph Labelling Problems // Utilitas Mathematica. — 2007. — V. 74. — P. 163–174.

Свойства энтропии недоопределенных данных в терминах лучших доопределений

Шоломов Лев Абрамович

Институт системного анализа РАН, e-mail: sholomov@isa.ru

Задан конечный алфавит $A_0 = \{a_i,\, i \in M\}$ *основных символов*. Каждому непустому $T \subseteq M$ сопоставлен символ a_T, называемый *недоопределенным*; его *доопределением* считается всякий основной символ a_i, $i \in T$. Недоопределенные символы образуют алфавит $A = \{a_T,\, T \subseteq M\}$. Символ a_M, доопределимый любым $a_i \in A_0$, называется *неопределенным* и обозначается $*$.

Рассматриваются источники $X = (A, P)$, $P = (p_T,\, T \subseteq M)$, порождающие символы $a_T \in A$ независимо с вероятностями p_T. *Энтропией источника* X называется величина

$$\mathcal{H}(X) = \mathcal{H}(P) = \min_Q \Big\{ -\sum_{T \subseteq M} p_T \log \sum_{i \in T} q_i \Big\}, \tag{1}$$

где $\log x = \log_2 x$, минимум берется по наборам вероятностей $Q = (q_i,\ i \in M)$.

Утверждение 1 [1]. *Набор вероятностей Q минимизирует* (1) *тогда и только тогда, когда при каждом $i \in M$ выполнено*

$$\sum_{T:\, i \in T} \frac{p_T}{\sum\limits_{j \in T} q_j} \le 1, \tag{2}$$

где строгое неравенство может быть лишь при тех i, для которых $q_i = 0$.

Операция доопределения источника $X = (A, P)$ задается набором условных вероятностей $p(a_i|a_T)$, $T \subseteq M$, $i \in M$, в котором $p(a_i|a_T) = 0$ для $i \notin T$. В применении к X она дает полностью определенный источник $X' = (A_0, P')$,

$P' = (p'_i,\ i \in M)$, $p'_i = \sum\limits_T p_T p(a_i|a_T)$, называемый *доопределением источника* X. На основе утверждения 1 доказывается следующий факт.

Утверждение 2. *Источник $X' = (A_0, Q)$, где Q — набор, на котором в* (1) *достигается $\mathcal{H}(X)$, доопределяет X.*

Из-за роли, которую это доопределение играет в задаче сжатия недоопределенных данных, оно называется *лучшим* [2]. Лучшее доопределение источника X, которое будем ассоциировать с набором вероятностей Q и обозначать Q_X, неединственно. Хотя свойства энтропии недоопределенных данных заметно отличаются от свойств энтропии (Шеннона) для полностью определенных данных, при формулировке в терминах лучших доопределений они оказываются подобными свойствам энтропии Шеннона. Подробнее об энтропии Шеннона см., напр., [3]. Будем использовать обозначения H для энтропии Шеннона и $\mathcal{H}$ для энтропии недоопределенных данных. Приведем примеры того, как трансформируются свойства энтропии при переходе от полностью определенных источников к недоопределенным и как свойства последних формулируются в терминах лучших доопределений.

Для полностью определенного источника $X = (A_0, P)$, $P = (p_i,\ i \in M)$, имеет место оценка $H(P) \le \log m$, $m = |M|$, которая достигается лишь в случае $P = (1/m, \ldots, 1/m)$. Соответствующая задача о максимуме энтропии недоопределенного источника $X = (A, P)$ ставится при заданном распределении $(p(t), t = 1, \ldots, m)$ числа t его доопределений, где $p(t) = \sum\limits_{T:\,|T|=t} p_T$.

Утверждение 3. *Для недоопределенного источника X справедлива оценка*

$$\mathcal{H}(X) \le \log m - \sum_{1 \le t \le m} p(t) \log t,$$

которая достигается тогда и только тогда, когда у X имеется лучшее доопределение $Q_X = (1/m, \ldots, 1/m)$.

Энтропия Шеннона строго вогнута, т. е. удовлетворяет неравенству

$$H(\theta P + (1 - \theta P')) \ge \theta H(P) + (1 - \theta) H(P'),\ 0 < \theta < 1, \tag{3}$$

которое обращается в равенство лишь для $P = P'$.

Утверждение 4. *Энтропия $\mathcal{H}$ вогнута (нестрого). Для недоопределенных источников $X = (A, P)$ и $X' = (A, P')$ она удовлетворяет неравенству, аналогичному* (3)*, которое обращается в равенство лишь в случае, когда X и X' имеют общее лучшее доопределение $Q_X = Q_{X'}$.*

Источники X и X', для которых $\mathcal{H}(XX') = \mathcal{H}(X) + \mathcal{H}(X')$, называются *независимыми*. Полностью определенные источники независимы тогда и только тогда, когда они статистически независимы, т. е. вероятностями p_{ij} совместного распределения XX' являются $p_{ij} = p_i p'_j$.

Утверждение 5. Недоопределенные источники X и X' независимы тогда и только тогда, когда для какой-либо произвольно взятой пары $(Q_X, Q_{X'})$,

$Q_X = (q_i,\, i \in M)$, $Q_{X'} = (q'_j,\, j \in M')$ их лучших доопределений набор $Q = (q_{ij},\, i \in M, j \in M')$, $q_{ij} = q_i q'_j$, является лучшим доопределением XY.

Формулировки свойств в терминах лучших доопределений являются неявными, поскольку лучшие доопределения обычно не известны. Но часто на их основе удается получать явные утверждения о недоопределенных данных. Приведем примеры.

Утверждение 3 позволяет дать явное описание всех распределений $(p(t),\, t = 1, \ldots, m)$, в рамках которых максимальное значение энтропии $\mathcal{H}(P)$ достигается на единственном наборе P.

Теорема 1. *Для заданного распределения $(p(t),\, t = 1, \ldots, m)$ числа t доопределений набор вероятностей P, максимизирующий энтропию $\mathcal{H}(P)$, единствен тогда и только тогда, когда распределение удовлетворяет условию (a) $p(1) + p(m) = 1$ или (b) $p(m-1) + p(m) = 1$.*

Полностью определенные данные подпадают под пункт (a) теоремы. Для них максимизирующий набор вероятностей единствен.

Утверждение 5 дает возможность описать все совместные распределения, соответствующие независимым частично определенным источникам. Частично определенным называется источник $X = (A, P)$, для которого $A \setminus \{*\} = A_0$. С источником X связывается параметр η_X, равный 0 или 1 в зависимости от того, совпадает A с A_0 или с $A = A_0 \cup \{*\}$.

Теорема 2. *Для частично определенных источников X и X' множество совместных распределений $P_{XY} = (p_{ij}, p_{i*}, p_{*j}, p_{**},\ i \in M, j \in M')$, соответствующих независимым источникам, совпадает с множеством неотрицательных решений системы линейных уравнений*

$$\begin{cases} p_{ij} + \dfrac{p'_j}{1 - p'_*} p_{i*} + \dfrac{p_i}{1 - p_*} p_{*j} + p_{**} = 1, \quad i \in M, j \in M', \\ \displaystyle\sum_{j \in M'} p_{*j} + p_{**} = p_*, \quad \sum_{i \in M} p_{i*} + p_{**} = p'_* \end{cases}$$

и образует многогранник размерности $d = \eta_{X'}(|M| - 1) + \eta_X(|M'| - 1) + \eta_X \eta_{X'}$.

Для полностью определенных источников $d = 0$ (ибо $\eta_X = \eta_{X'} = 0$) и независимость достигается на единственном совместном распределении.

Работа выполнена при поддержке ОНИТ РАН (проект 1.1 по Программе фундаментальных исследований).

Список литературы

[1] Шоломов Л. А. Элементы теории недоопределенной информации // Прикладная дискретная математика. Приложение № 2. — 2009. — С. 18–42.

[2] Шоломов Л. А. О правиле сложения энтропий для недоопределенных данных // Дискретный анализ и исследование операций. — 2010. — Т. 17, № 5. — С. 67–90.

[3] Колесник В. Д., Полтырев Г. Ш. Курс теории информации. — М.: Наука, 1982. — 416 с.

Об операциях с независимыми случайными величинами над конечным линейно упорядоченным множеством

Яшунский Алексей Дмитриевич
Институт прикладной математики им. М. В. Келдыша РАН, e-mail: yashunsky@keldysh.ru

Пусть $E = \{0, 1, \ldots, k-1\}$ — линейно упорядоченное множество ($0 < 1 < \ldots < k-1$) с определенными на нем операциями максимума $x \vee y$ и минимума $x \wedge y$.

Определим *формулу* с операциями $\vee, \wedge$ индуктивно: любая переменная является формулой; если Φ_1 и Φ_2 — формулы, то формулами также являются $(\Phi_1 \vee \Phi_2)$ и $(\Phi_1 \wedge \Phi_2)$. Формула называется *бесповторной*, если в ней все переменные различны.

Подставляя вместо всех переменных некоторой бесповторной формулы независимые случайные величины с известными распределениями, получаем новую случайную величину, распределение которой может быть вычислено. Рассматривается задача о том, какие распределения могут быть сколь угодно точно приближены бесповторными формулами со случайными переменными, если распределения переменных принадлежат заданному конечному множеству G.

Для $E = \{0, 1\}$ и $G = \{(p, 1-p)\}$ известно [1, 2], что любое распределение $(\eta, 1-\eta)$ может быть приближено сколь угодно точно бесповторными формулами с операциями $\vee, \wedge$. Рассмотрение случайных величин на линейно упорядоченном множестве из $k > 2$ элементов естественным образом обобщает эту рассматривавшуюся ранее задачу.

Случайной величине x соответствует *стохастический вектор* $(x_0, x_1, \ldots, x_{k-1})$ ее распределения: $x_i = \mathsf{P}\{x = i\}$. Также будем использовать обозначения $x_{\leqslant i} = x_0 + \ldots + x_i$, $x_{<i} = x_0 + \ldots + x_{i-1}$, $x_{\geqslant i} = x_i + \ldots + x_{k-1}$, $x_{>i} = x_{i+1} + \ldots + x_{k-1}$. Естественно, для любого i выполнено $x_{<i} + x_{\geqslant i} = 1$ и $x_{\leqslant i} + x_{>i} = 1$.

Далее будем рассматривать операции над распределениями, а запись $x \vee y$, $x \wedge y$ понимать как применение соответствующий операции к двум независимым случайным величинам, имеющим распределения x и y. В частности, $x \vee x$ будет пониматься как максимум двух независимых случайных величин с распределением x. Из свойств операций $\vee$ и $\wedge$ легко вывести, что

$$(x \vee y)_{\leqslant i} = x_{\leqslant i} y_{\leqslant i}, \quad (x \vee y)_{<i} = x_{<i} y_{<i}, \tag{1}$$

$$(x \wedge y)_{\geqslant i} = x_{\geqslant i} y_{\geqslant i}, \quad (x \wedge y)_{>i} = x_{>i} y_{>i}. \tag{2}$$

Теорема 1. *Пусть для некоторого $\alpha > 1$ и некоторого $i \in E$ выполнено $x_{<i} \leqslant x^{\alpha}_{\leqslant i}$ и $y_{<i} \leqslant y^{\alpha}_{\leqslant i}$. Тогда $(x \vee y)_{<i} \leqslant (x \vee y)^{\alpha}_{\leqslant i}$ и $(x \wedge y)_{<i} \leqslant (x \wedge y)^{\alpha}_{\leqslant i}$.*

Пусть для некоторого $\beta > 1$ и некоторого $i \in E$ выполнено $x_{>i} \leqslant x^{\beta}_{\geqslant i}$ и $y_{>i} \leqslant y^{\beta}_{\geqslant i}$. Тогда $(x \vee y)_{>i} \leqslant (x \vee y)^{\beta}_{\geqslant i}$ и $(x \wedge y)_{>i} \leqslant (x \wedge y)^{\beta}_{\geqslant i}$.

Доказательство. Из соотношений (1) вытекает $(x \vee y)_{<i} \leqslant x^{\alpha}_{\leqslant i} y^{\alpha}_{\leqslant i} = (x \vee y)^{\alpha}_{\leqslant i}$.

Рассмотрим $(x \wedge y)_{<i}$. С помощью (2) получаем:

$$(x \wedge y)_{<i} = 1 - (x \wedge y)_{\geqslant i} = 1 - x_{\geqslant i} y_{\geqslant i} = 1 - (1 - x_{<i})(1 - y_{<i}) =$$
$$= x_{<i} + (1 - x_{<i}) y_{<i} \leqslant x_{<i} + (1 - x_{<i}) y^{\alpha}_{\leqslant i} = y^{\alpha}_{\leqslant i} + (1 - y^{\alpha}_{\leqslant i}) x_{<i} \leqslant y^{\alpha}_{\leqslant i} + (1 - y^{\alpha}_{\leqslant i}) x^{\alpha}_{\leqslant i}.$$

Поскольку $(x \wedge y)_{\leqslant i} = y_{\leqslant i} + (1 - y_{\leqslant i}) x_{\leqslant i}$, для доказательства теоремы требуется показать, что $y^{\alpha}_{\leqslant i} + (1 - y^{\alpha}_{\leqslant i}) x^{\alpha}_{\leqslant i} \leqslant (y_{\leqslant i} + (1 - y_{\leqslant i}) x_{\leqslant i})^{\alpha}$.

Обозначим $y_{\leqslant i} = a$, $x_{\leqslant i} = t$ и покажем, что при всех $a, t \in [0; 1]$, $\alpha > 1$ неравенство выполнено. Пусть $f(t) = a + (1-a)t - (a^{\alpha} + (1-a^{\alpha})t^{\alpha})^{1/\alpha}$, величину a будем рассматривать как параметр. Доказываемое неравенство равносильно $f(t) \geqslant 0$. Легко проверить, что $f(0) = f(1) = 0$. Кроме того, при $t \in (0; 1)$ выполнено: $f''(t) = -(\alpha - 1)(1 - a^{\alpha}) a^{\alpha} t^{\alpha - 2} (a^{\alpha} + (1 - a^{\alpha}) t^{\alpha})^{\frac{1}{\alpha} - 2} < 0$, откуда следует, что $f(t) \geqslant 0$.

Сохранение множеств стохастических векторов, удовлетворяющих соотношению $x_{>i} \leqslant x^{\beta}_{\geqslant i}$, доказывается аналогично. **Теорема 1 доказана.**

Из теоремы 1 следует, что для $k > 2$ при заданном конечном множестве G *не любое* распределение может быть бесповторно приближено. Более того, можно указать такое замкнутое множество A, отличное от множества всех распределений, что все приближаемые распределения лежат в A.

Стохастический вектор $(x_0, x_1, \ldots, x_{k-1})$ будем называть *невырожденным*, если $x_i > 0$ для всех $i \in E$.

Теорема 2. *Пусть $G = \{p\}$, p — невырожденный стохастический вектор. Тогда для любого $i \in E$ и любого $\eta \in [0; 1]$ стохастический вектор $(0, \ldots, 0, \underbrace{\eta}_{i\text{-е место}}, 1 - \eta, 0, \ldots, 0)$ приближается сколь угодно точно.*

Доказательство. Пусть требуется построить приближения, имеющие точность Δ по каждой координате.

Рассмотрим последовательность распределений $p^{(0)} = p$, $p^{(m+1)} = p^{(m)} \wedge p$. Для $i \in E$ в силу (2) имеем $p^{(m)}_{>i} = (p_{>i})^m \to 0$ при $m \to \infty$, откуда вытекает, что $p^{(m)}$ приближает распределение $(1, 0, \ldots, 0)$.

В силу невырожденности p, для всех $i \neq 0$ существуют такие $\beta_i > 1$, что $p_{>i} = (p_{\geqslant i})^{\beta_i}$, что вместе с (2) дает $p^{(m)}_{>i} = (p^{(m)}_{\geqslant i})^{\beta_i}$.

Функция $f(t) = (1 - t^{\beta})^{\alpha} - 1 + t$ удовлетворяет $f(0) = 0$, $f'(0) = 1$, следовательно, при достаточно малых $t > 0$ выполнено $f(t) > 0$. Так как $p^{(m)}_{\geqslant i} \to 0$ при $m \to \infty$ и $i \neq 0$, для любого $\alpha > 1$ при достаточно больших m выполнено $(1 - (p^{(m)}_{\geqslant i})^{\beta_i})^{\alpha} > 1 - p^{(m)}_{\geqslant i}$, т. е. $(1 - p^{(m)}_{>i})^{\alpha} > p^{(m)}_{<i}$, откуда $p^{(m)}_{<i} < (p^{(m)}_{\leqslant i})^{\alpha}$.

Выберем такое $\alpha > 1$, что $(1 - \Delta/2)^{\alpha} < \Delta/2$ и по нему такое m_0, чтобы для всех $i \neq 0$ выполнялось

$$p^{(m_0)}_{<i} < (p^{(m_0)}_{\leqslant i})^{\alpha} \tag{3}$$

и $p^{(m_0)}$ приближало $(1, 0, \ldots, 0)$ с точностью Δ. Положим $q = p^{(m_0)}$ и рассмотрим последовательность распределений $q^{(0)} = q$, $q^{(n+1)} = q^{(n)} \vee q$. В силу (1) имеем $q^{(n)}_{\leqslant i} = (q_{\leqslant i})^n \to 0$ при $n \to \infty$ для всех $i \neq k - 1$. Кроме того,

$q^{(n)}_{\leqslant i} - q^{(n+1)}_{\leqslant i} = q^n_{\leqslant i}(1 - q_{\leqslant i}) < 1 - q_{\leqslant i} \leqslant 1 - q_0 < \Delta$. То есть, для каждого $i \neq k-1$ последовательность $q^{(n)}_{\leqslant i}$ убывает к нулю, при каждом увеличении n уменьшаясь на величину, меньшую Δ.

Пусть для некоторых i и n выполнено $q^{(n)}_{<i} > \Delta/2$. Из соотношений (3) и теоремы 1 вытекает, что $q^{(n)}_{>i} = 1 - q^{(n)}_{\leqslant i} < 1 - (q^{(n)}_{<i})^{1/\alpha} < 1 - (\Delta/2)^{1/\alpha}$, что в силу выбора α влечет $q^{(n)}_{>i} < \Delta/2$. Таким образом $q^{(n)}_{<i}$ с ростом n убывает, но пока $q^{(n)}_{<i} > \Delta/2$, выполняется $q^{(n)}_{>i} < \Delta/2$, откуда легко получить, что $q^{(n)}_i$ растет до $1 - \Delta$. Применяя это рассуждение последовательно для $i = 1, 2, \ldots, k-1$, получаем утверждение теоремы. **Теорема 2 доказана.**

Автор выражает благодарность О. М. Касим-Заде за внимание к работе.

Работа выполнена при поддержке РФФИ (проект № 14–01–00598) и Программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

[1] Схиртладзе Р. Л. О методе построения булевой величины с заданным распределением вероятностей // Дискретный анализ. Вып. 7. — Новосибирск: ИМ СО АН СССР, 1966. — С. 71–80.

[2] Яшунский А. Д. О преобразованиях вероятности бесповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.) — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 150–155.

Авторский указатель

Содержание