УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА

Том 156, кн. 3 Физико-математические науки *2014*

УДК 519.714

НЕКОТОРЫЕ ОСОБЕННОСТИ ЗАДАЧИ СИНТЕЗА БУЛЕВЫХ ФОРМУЛ В ПОЛНЫХ БАЗИСАХ С ПРЯМЫМИ И ИТЕРАТИВНЫМИ ПЕРЕМЕННЫМИ

В.А. Коноводов

Аннотация

В работе рассмотрены вопросы сложности формул в различных базисах, состоящих из функций алгебры логики с прямыми и итеративными переменными. Показано, что «стандартное» поведение функции Шеннона для сложности формул $(2^n/\log n)$ не всегда имеет место, приведены примеры нетривиальных семейств базисов с порядком роста этой функции, равным 2^n. Такие примеры существуют среди каждого из семейств в классификации полных базисов по их итеративным замыканиям, кроме двух, в которых функция Шеннона ведет себя стандартно. Для оператора итеративного замыкания δ, введенного в работе [*Ложкин С.А.* О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и кибернетика. – 1999. – № 3. – С. 35–41], получено новое представление.

Отдельно рассмотрен вопрос о сложности линейной функции в некоторых классах базисов и приведены примеры кардинального изменения этой сложности в различных базисах одного семейства.

Ключевые слова: булевы формулы, сложность функций, функция Шеннона, прямые и итеративные переменные.

---

1. Основные определения, обозначения и полученные результаты

Пусть $X = \{x_1, x_2, \ldots\}$ и $Y = \{y_1, y_2, \ldots\}$ – счетные множества булевых переменных, причем переменные из множества X (из множества Y) будем называть *прямыми* (*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:

1) переименование (с отождествлением) прямых переменных;

2) подстановка констант 0, 1 вместо переменных;

3) переименование (без отождествления) итеративных переменных;

4) подстановка одной из двух независимых функций вместо итеративной переменной другой функции;

5) замена итеративных переменных прямыми переменными;

6) отождествление итеративных переменных.

Пусть $A \subset P_2(X \cup Y)$ – некоторое конечное множество базисных функций. В соответствии с введенными операциями суперпозиции будем рассматривать одновыходные схемы из функциональных элементов над базисом A (см., например, [2]), в которых:

1) 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);

2) итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами;

3) неконстантным входам схемы сопоставлены некоторые переменные из множества X.

Как обычно, формулами считаются те схемы, которые не содержат ветвлений выходов элементов.

Необходимо отметить, что с точки зрения рекурсивного определения формулы как символьной записи [3] указанные выше операции 1–6 дают возможность проводить суперпозицию только по итеративным переменным базисных функций.

Систему функций A будем называть *полной*, если для любой функции f, $f \in P_2(X)$, существует формула над A указанного вида, реализующая функцию f. Критерий полноты произвольной системы функций был получен в работе [1]. Везде далее, если не указано обратное, рассматриваются только конечные полные системы функций.

Сложностью $L(\mathcal{F})$ формулы $\mathcal{F}$ будем называть число функциональных элементов в ней. Функцией Шеннона $L_A(n)$ для сложности формул в базисе A, как обычно, называется максимальное значение $L_A(f)$ среди всех функций f, $f \in P_2(\{x_1, \ldots, x_n\})$, где $L_A(f)$ – минимальная сложность формулы из рассматриваемого класса, реализующей функцию f.

Функция Шеннона $L_A^C(n)$ для сложности схем из функциональных элементов указанного вида в базисе A определяется аналогично.

Пусть $A \subseteq P_2(X \cup Y)$. Множество тех функций, которые можно получить из функций системы A в результате применения операций суперпозиции с номерами из множества T', $T' \subseteq T = \{1, 2, 3, 4, 5, 6\}$, обозначим через $[A]_{T'}$, и пусть $[A]_T = [A]$.

В работе [1] введено множество $\delta(A) = \big[[A]_{\{2\}} \cap P_2(Y)\big]_{\{3,4,6\}}$, которое будем называть *итеративным замыканием* базиса A. Заметим, что множество $\delta(A)$ является «обычным» замкнутым классом (см., например, [3]) в $P_2(Y)$, содержащим все константы, 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 (конъюнкции) переменных Y, а классы L и M состоят из линейных и монотонных функций от переменных Y соответственно. Далее через B^k обозначается k-я декартова степень множества B, то есть множество всех упорядоченных наборов длины k из элементов B.

В настоящей работе доказано, что для оператора δ справедливо более наглядное представление:

Теорема 1. *Для любой системы функций A, $A \subseteq P_2(X \cup Y)$, справедливо равенство*

$$\delta(A) = [A] \cap P_2(Y).$$

Таким образом, $\delta(A)$ определяет все те функции от итеративных переменных, которые можно получить из базисных функций рассматриваемыми операциями суперпозиции. Введение оператора δ позволяет классифицировать все системы функций от прямых и итеративных переменных по их итеративным замыканиям.

Эта классификация имеет прямое отношение к исследованию сложности формул в соответствующих базисах.

В [4] установлено, что функция Шеннона $L_A^C(n)$ для сложности схем в произвольном базисе A, $A \subseteq P_2(X \cup Y)$, имеет «стандартный» порядок роста $2^n/n$. Кроме того, в [4] указано, что в случае формул порядок роста $L_A(n)$ не более чем 2^n и не менее чем $2^n/\log n$ (здесь и далее все логарифмы рассматриваются по основанию два).

В [5] указано, что если $\delta(A) \in \{M, P_2(Y)\}$, то функция Шеннона для сложности формул при растущем значении натурального аргумента n ведет себя как $\Theta(2^n/\log n)$[1]. Кроме того, в [5] приведены примеры семейств базисов A, для которых $\delta(A) \in \{I, O\}$ и порядок роста функции Шеннона составляет 2^n.

В настоящей работе доказывается следующая теорема.

Теорема 2. *В семействе базисов с итеративным замыканием из множества $\{D, K, L\}$ существуют такие базисы A, для которых $L_A(n) = \Theta(2^n)$.*

Таким образом, примеры базисов с порядком функции Шеннона для сложности формул в них, равным 2^n, существуют среди систем, итеративное замыкание которых принадлежит множеству $\{I, O, D, K, L\}$. В базисах с итеративным замыканием вида $P_2(Y)$ или M соответствующая функция Шеннона имеет порядок роста $2^n/\log n$. Базисы с итеративным замыканием, равным B, не являются полными.

В некоторых базисах A таких, что $\delta(A) = D$ и $L_A(n) = \Theta(2^n)$, самой сложной функцией является линейная функция $l_n = x_1 \oplus \ldots \oplus x_n$, однако, как показывает следующий результат, при переходе от базиса к базису сложность функции l_n может кардинально изменяться в рамках одного и того же семейства[2].

Теорема 3. *В базисе $A_1 = \{(x_1 \oplus x_2)y_1, (x_1 \sim x_2)y_1, y_1 \vee y_2\}$ сложность линейной функции l_n удовлетворяет соотношению*

$$L_{A_1}(l_n) = \Theta(2^{n/2}),$$

а в базисах $A_2 = \{(x_1 \oplus x_2)y_1, y_1 \vee y_2\}$ и $A_3 = \{(x_1 \sim x_2)y_1, y_1 \vee y_2\}$ – соотношению

$$c_1 \cdot 2^{n/2} \leqslant L_{A_i}(l_n) \leqslant c_2 \cdot 3^{n/2}, \quad i = 1, 2,$$

где c_1, c_2 – некоторые положительные константы.

Итеративное замыкание каждого из указанных в теореме базисов образует класс D.

В работе [6] рассматривались так называемые обобщенные дизъюнктивные нормальные формы (ДНФ), из полученных в ней результатов следует, в частности, что $L_{A_2}(n) = \Omega\left(\dfrac{2^n}{n^{1/4}}\right)$.

Далее через μ_n обозначается мультиплексорная функция порядка n, $n \geqslant 1$, определяемая равенством

$$\mu_n(x_1, \ldots, x_n, z_0, \ldots, z_{2^n-1}) = \bigvee_{\sigma_1, \ldots, \sigma_n \in B} x_1^{\sigma_1} \ldots x_n^{\sigma_n} z_{\nu(\sigma_1, \ldots, \sigma_n)},$$

где $\nu(\sigma_1, \ldots, \sigma_n)$ – число, двоичная запись которого совпадает с набором $(\sigma_1, \ldots, \sigma_n)$, $z_i \in X \cup Y$ для всех i, $i = 0, \ldots, 2^n - 1$; а $x^\sigma = x \sim \sigma$, $\sigma \in B$.

[1] Для числовых функций $g(n)$ и $h(n)$ натурального аргумента n запись $h(n) = O(g(n))$ означает, как обычно, что отношение $|h(n)/g(n)|$ ограничено сверху. Эта запись равносильна записи $g(n) = \Omega(h(n))$. Запись $h(n) = \Theta(g(n))$ означает, что $h(n) = O(g(n))$ и $g(n) = O(h(n))$.

[2] Здесь и далее символом $\oplus$ обозначается сумма по модулю 2, а $x' \sim x'' = x' \oplus x'' \oplus 1$.

2. Представление оператора δ

Пусть A, $A \subseteq P_2(X \cup Y)$, – произвольное, не обязательно полное, конечное множество функций. На основе величины $\delta(A)$, введенной выше, базируется критерий полноты в работе [1]. Очевидно, $\delta(A) \subseteq [A] \cap P_2(Y)$. Покажем, что справедливо и обратное включение, тем самым доказав заявленное утверждение.

Следует отметить, что множество $[A] \cap P_2(Y)$ является «обычным» замкнутым классом в $P_2(Y)$, содержащим константы, поэтому $[A] \cap P_2(Y) \in \Delta$.

Предположим, что найдутся два различных класса δ_1, $\delta_2 \in \Delta$ таких, что $\delta(A) = \delta_1$ и $[A] \cap P_2(Y) = \delta_2$. При этом $\delta_1 \subset \delta_2$.

Для каждого δ, $\delta \in \Delta$, обозначим, согласно [1], $R(\delta) = \{f \in P_2(X \cup Y) : [\{f\}]_{\{2\}} \cap P_2(Y) \subseteq \delta\}$. Заметим, что если функция $f \in R(\delta)$ зависит от n прямых переменных, то при подстановке вместо них любых констант получится функция из δ. Это означает, что функция f может быть представлена в виде

$$f = \mu_n(x_1, \ldots, x_n, g_1, \ldots, g_{2^n}), \tag{1}$$

где $g_i \in \delta$ для всех $i = 1, \ldots, 2^n$.

Из такого определения следует, что $A \subseteq R(\delta(A)) = R(\delta_1)$. Действительно, так как $\delta(A) = \big[[A]_{\{2\}} \cap P_2(Y)\big]_{\{3,4,6\}}$, то для произвольной функции $g \in A$ справедливо включение $[\{g\}]_{\{2\}} \cap P_2(Y) \subseteq \delta(A)$, а это и означает, что $g \in R(\delta(A))$.

Далее, $\delta_2 = [A] \cap P_2(Y) \subseteq [R(\delta_1)] \cap P_2(Y) = R(\delta_1) \cap P_2(Y)$, так как $R(\delta_1)$ – замкнутый класс. Получаем, что

$$\delta_2 \subseteq R(\delta_1) \cap P_2(Y), \quad \delta_1 \subset \delta_2. \tag{2}$$

Пользуясь тем, что для любых классов δ', δ'' системы Δ из условия $\delta' \subset \delta''$ следует включение $R(\delta') \subset R(\delta'')$, покажем невозможность выполнения (2), что и докажет утверждение. Рассмотрим все случаи.

Если $\delta(A) = \delta_1 = B$, то $A \subseteq P_2(X)$, откуда $\delta_2 = B = \delta_1$, что противоречит определению классов δ_1 и δ_2.

Если $\delta(A) = \delta_1 = I$, то для $\delta_2 \in \{D, K, O\}$ (а следовательно, и для $\{M, L, P_2(Y)\}$) выполнение (2) невозможно, так как во множестве $R(I) \cap P_2(Y)$, согласно (1), отсутствуют дизъюнкции, конъюнкции двух и более итеративных переменных, а также отрицания итеративных переменных.

Если $\delta(A) = \delta_1 = O$, то для $\delta_2 = L$ (а, следовательно, и для $\delta_2 = P_2(Y)$) выполнение (2)также невозможно, так как множество $R(O) \cap P_2(Y)$ не содержит линейных функций от двух и более итеративных переменных, как следует из (1).

Если $\delta(A) = \delta_1 = D$, то для $\delta_2 = M$ (а, следовательно, и для $P_2(Y)$) выполнение (2) невозможно, так как $R(D) \cap P_2(Y)$ не содержит конъюнкцию итеративных переменных. Случай $\delta_1 = K$ аналогичен.

Если же $\delta(A) = \delta_1 \in \{M, L\}$, то $\delta_2 = P_2(Y)$, но $R(\delta_1)$ не содержит все функции итеративных переменных, потому (2) также не выполняется.

Полученные противоречия доказывают теорему 1.

3. Сложность функций в различных семействах базисов с прямыми и итеративными переменными

Рассмотрим системы функций A, $A \subseteq P_2(X \cup Y)$, такие, что $\delta(A) = D$.

Множество номеров существенных итеративных переменных функции f обозначим через $J(f)$. Из (1) следует, что любую функцию f, $f \in R(D)$, можно представить в виде

$$f = \bigvee_{j \in J(f)} y_j \varphi_j \vee \varphi_0, \tag{3}$$

где $\varphi_j \in P_2(X)$ при всех j, $j \in J(f) \cup \{0\}$.

Пусть $D^{(1)}$ и $D^{(0)}$ – множества тех функций f, $f \in R(D)$, для которых все коэффициенты φ_j, $j \in J(f)$, при переменных в разложении (3) являются монотонными и антимонотонными функциями соответственно.

Лемма 1. *Пусть*

$$A' = \{\bar{x}_1 y_1, f'_1, \ldots, f'_k, y_1 \vee y_2\},$$

где $f'_1, \ldots, f'_k \in D^{(1)}$, *и*

$$A'' = \{x_1 y_1, f''_1, \ldots, f''_k, y_1 \vee y_2\},$$

где $f''_1, \ldots, f''_k \in D^{(0)}$, *тогда*

$$L_{A'}(n) = \Theta(2^n), \quad L_{A''}(n) = \Theta(2^n).$$

Доказательство. Заметим, что $\delta(A') = \delta(A'') = D$, и системы A' и A'' являются полными.

Рассмотрим минимальную по сложности формулу $\mathcal{F}$ для линейной функции l_n в базисе A' (случай базиса A'' рассматривается аналогично). Пусть каждая функция f'_i, $i = 1, 2, \ldots, k$, представима в виде разложения (3) следующим образом: $f'_i = \bigvee\limits_{j \in J(f_i)} y_j \varphi_j^{(i)} \vee \varphi_0^{(i)}$. В символьной записи $\mathcal{F}$, принимая символы функций $\varphi_j^{(i)}$ ($i = 1, 2, \ldots, k$; $j = 1, 2, \ldots, |J(f_i)|$) за отдельные переменные, раскроем скобки, используя дистрибутивность конъюнкции относительно дизъюнкции. При этом не изменится число символов дизъюнкции, входящих в формулу. В результате получится ДНФ, конъюнкции которой состоят из отрицаний прямых переменных, а также из символов функций $\varphi_j^{(i)}$. Если хотя бы одна из таких конъюнкций обращается в единицу на более чем одном наборе, то, так как все функции $\varphi_j^{(i)}$ монотонны, такая конъюнкция обратится в единицу на двух соседних наборах, что противоречит реализации этой ДНФ линейной функции. Таким образом, каждая конъюнкция покрывает не более одного набора, а это означает, что их число не менее чем 2^{n-1}. С учетом того, что при раскрытии скобок число дизъюнкций не изменилось, а множества $J(f_1), \ldots, J(f_k)$ конечны и не зависят от n, имеем, что число элементов $y_1 \vee y_2$ в формуле $\mathcal{F}$ есть $\Omega(2^n)$, что с учетом верхней оценки из [4] доказывает лемму.

□

Далее докажем, что в базисах

$$A_1 = \{(x_1 \oplus x_2) y_1, (x_1 \sim x_2) y_1, y_1 \vee y_2\},$$
$$A_2 = \{(x_1 \oplus x_2) y_1, y_1 \vee y_2\},$$
$$A_3 = \{(x_1 \sim x_2) y_1, y_1 \vee y_2\}$$

того же семейства $\{A : \delta(A) = D\}$ сложность линейной функции сильно изменяется.

Лемма 2. *Справедливы соотношения*

$$L_{A_1}(l_n) = O\left(2^{n/2}\right),$$
$$L_{A_i}(l_n) = O\left(3^{n/2}\right), \quad i = 2, 3.$$

Доказательство. Доказательство основано на следующих рекуррентных разложениях, справедливых при любых n, $n \geqslant 3$:

$$l_n(x_1, \ldots, x_n) = (x_1 \oplus x_2) \bar{l}_{n-2}(x_3, \ldots, x_n) \vee (x_1 \sim x_2) l_{n-2}(x_3, \ldots, x_n),$$

$$l_n(x_1,\ldots,x_n)=(x_1\oplus x_2)\bar{l}_{n-2}(x_3,\ldots,x_n)\vee\bar{x}_1\bar{x}_2 l_{n-2}(x_3,\ldots,x_n)\vee x_1x_2 l_{n-2}(x_3,\ldots,x_n),$$

$$l_n(x_1,\ldots,x_n)=(x_1\sim x_2)l_{n-2}(x_3,\ldots,x_n)\vee x_1\bar{x}_2\bar{l}_{n-2}(x_3,\ldots,x_n)\vee\bar{x}_1x_2 l_{n-2}(x_3,\ldots,x_n),$$

на аналогичных разложениях для отрицания линейной функции и на том, что $x_1 = x_1\oplus 0 = x_1\sim 1$, а $\bar{x}_1 = x_1\oplus 1 = x_1 \sim 0$. □

Лемма 3. *Существует такая положительная константа* c_1, *что для любых натуральных* n *справедливы соотношения*

$$L_{A_i}(l_n)\geqslant c_1\cdot 2^{n/2},\quad i=1,2,3.$$

Доказательство. Рассмотрим конъюнкцию K некоторого числа функций вида $(x_1\oplus x_2)$, $(x_1\sim x_2)$, взятых от произвольных переменных из множества $\{x_1,\ldots,x_m\}$. Будем предполагать, что конъюнкция K зависит от всех переменных их этого множества существенно.

Построим неориентированный граф G_1, $G_1=(V,E)$, в котором $V = \{v_1,\ldots,v_m\}$ – множество вершин. Будем считать, что каждая вершина v_i, $v_i\in V$, взаимно однозначно поставлена в соответствие переменной x_i, где $i=1,2,\ldots,m$. Для каждой функции вида $(x_i\oplus x_j)$, участвующей в конъюнкции K, построим ребро (v_i,v_j) в графе G_1. Все такие ребра и будут образовывать множество E.

Пусть граф G_2 получен из графа G_1 отождествлением всех пар вершин v_i,v_j, для которых функция $(x_i\sim x_j)$ участвует в конъюнкции K.

Рассмотрим правильную (см., например, [3]) раскраску вершин графа G_2 в два цвета 0 и 1. Из построения графа следует, что набор цветов вершин $\alpha = (\alpha_1,\ldots,\alpha_m)$, по которому вершина v_i красится в цвет $\alpha_i\in B$, $i=1,\ldots,m$, при правильной раскраске обращает конъюнкцию K в единицу. И наоборот, если $K(\alpha)=1$, то набор α образует правильную раскраску графа G_2 в два цвета.

Следует отметить, что каждую компоненту связности графа можно покрасить правильно не более чем двумя способами, так как, указав цвет одной вершины (0 или 1), цвета остальных вершин этой компоненты определяются однозначно при условии, что правильная раскраска возможна. Таким образом, если граф G_2 имеет t компонент связности, то число способов раскрасить этот граф правильно в два цвета равно 2^t.

Далее, поскольку каждая вершина графа G_1 либо отождествлена, либо смежна с некоторой другой вершиной, что справедливо в силу существенной зависимости конъюнкции K от всех переменных, для t справедлива оценка $t\leqslant m/2$. Это означает, что конъюнкция K обращается в единицу на не более чем $2^{m/2}$ наборах значений своих существенных переменных.

Эта оценка не изменится, если в конъюнкцию K дополнительно будут входить сомножители вида x_i, $\bar{x}_i$, $i\notin\{1,\ldots,m\}$.

Аналогично доказательству леммы 1 рассмотрим минимальную по сложности формулу $\mathcal{F}$ в базисе A_1 для линейной функции l_n и раскроем скобки в ее символьной записи, пользуясь только тождеством дистрибутивности конъюнкции относительно дизъюнкции и тождествами подстановки констант. В результате получим формулу $\mathcal{F}'=K_1\vee\ldots\vee K_p$, в которой каждая конъюнкция K_i, $i=1,\ldots,p$, имеет вид

$$K_i = x_{u_1}^{\sigma_1}\ldots x_{u_r}^{\sigma_r}\varphi_1(x_{v_1'},x_{v_1''})\ldots\varphi_s(x_{v_s'},x_{v_s'}),$$

где $1\leqslant u_1,\ldots,u_r,v_1',v_1'',\ldots,v_s',v_s''\leqslant n$, $\sigma_1,\ldots,\sigma_r\in B$, а $\varphi_j(x',x'')$ является при каждом j, $j=1,\ldots,s$, либо функцией $x'\oplus x''$, либо функцией $x'\sim x''$.

В силу тождеств $x'(x'\sim x'')=x'x''$, $\bar{x}'(x'\sim x'')=\bar{x}'\bar{x}''$, $x'(x'\oplus x'')=x'\bar{x}''$, $\bar{x}'(x'\oplus x'')=\bar{x}'x''$ будем считать, что $\{u_1,\ldots,u_r\}\cap\{v_1',v_1'',\ldots,v_s',v_s''\}=\varnothing$.

Отметим, что $\{u_1,\ldots,u_r\}\cup\{v_1',v_1'',\ldots,v_s',v_s''\}=\{1,\ldots,n\}$ в силу реализации формулой $\mathcal{F}'$ линейной функции, поэтому каждая из конъюнкций $K_1,\ldots,K_p$

обращается в единицу на не более чем $2^{n/2}$ наборах. Следовательно, так как функция l_n равна единице на 2^{n-1} наборах, справедлива оценка $p \geqslant 2^{n/2-1}$.

По построению формула $\mathcal{F}$ содержит столько же элементов дизъюнкции, сколько и формула $\mathcal{F}'$, то есть $p-1=\Omega(2^{n/2})$, что и доказывает оценку в случае базиса A_1. Так как A_2, $A_3 \subset A_1$, то данная оценка верна и для базисов A_2, A_3. □

Теорема 3 следует из лемм 2 и 3. Аналогичные леммам 1, 2 и 3 результаты можно получить и для случая систем A таких, что $\delta(A)=K$.

Далее рассмотрим системы функций A, $A \subseteq P_2(X \cup Y)$, такие, что $\delta(A)=L$.

Лемма 4. *Для системы функций $A_4=\{x_1y_1,\, y_1 \oplus y_2\}$ выполняется соотношение*

$$L_{A_4}(n)=\Theta(2^n).$$

Доказательство. Рассмотрим произвольную формулу в базисе A_4, реализующую некоторую функцию f. Если в данной формуле раскрыть скобки и привести подобные, то получится полином Жегалкина для функции f. Такой полином единственный с точностью до перестановки слагаемых в нем. При этом число функциональных символов $\oplus$ может только уменьшиться, так как все умножения в базисе – это умножения на булеву переменную.

Для функции $d_n = x_1 \vee \ldots \vee x_n$ полином Жегалкина представляет собой сумму 2^n-1 монотонных элементарных конъюнкций, поэтому в любой формуле над базисом A_4, реализующей функцию d_n, содержится не менее 2^n-2 функциональных элементов $y_1 \oplus y_2$, значит, и сложность всей формулы не менее чем 2^n. □

Пусть базисная система функций A такова, что $\delta(A)=L$, а любая функция f системы A имеет вид

$$f=\bigoplus_{j \in J(f)} K_j y_j,$$

где каждая K_j, $j \in J(f)$, представляет собой монотонную конъюнкцию прямых переменных. Как следует из доказательства теоремы, для дизъюнкции d_n будет необходимо экспоненциальное число элементов такого базиса.

Рассмотрим систему функций $A_5=\{x_1y_1, \bar{x}_1y_1, y_1 \oplus y_2\}$. Необходимо отметить, что, в отличие от предыдущего базиса, функция d_n имеет в A_5 линейную сложность, поскольку справедливо соотношение

$$d_n = d_{n-1}\bar{x}_n \oplus x_n.$$

При аналогичном рассматриваемому в доказательстве леммы 4 раскрытию скобок в формуле над таким базисом возникает полиномиальная нормальная форма (ПНФ) – сумма по модулю два элементарных конъюнкций. Из результатов работ [7, 8] следует, что функция Шеннона для длины ПНФ (то есть для числа элементарных конъюнкций в ней) имеет порядок роста $2^n/n$. Это говорит о неэффективности применения нижней оценки числа элементов сложения для оценки снизу функции Шеннона $L_{A_5}(n)$.

Использование леммы 4 завершает доказательство теоремы 2.

Автор благодарит своего научного руководителя Ложкина Сергея Андреевича за постоянное внимание к работе и Селезневу Светлану Николаевну за предоставленные ссылки по результатам для ПНФ.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 12-01-00964-а).

Summary

V.A. Konovodov. Some Features of the Synthesis of Boolean Formulae over Complete Bases with Direct and Iterative Variables.

The paper studies some issues of complexity of Boolean formulae over different bases that consist of Boolean functions with direct and iterative variables. It is shown that the standard behavior of the Shannon function for the complexity of the formulae $(2^n/\log n)$ does not always take place; the examples of the non-trivial families of bases where this function has the order of growth of 2^n are given. Such examples exist in each family in the classification of bases according to their iterative closures, except for two bases, where the Shannon function has the standard order of growth. A new representation of the iterative closure operator δ (introduced by S.A. Lozhkin) is obtained.

The issue about the complexity of an affine function over some classes of bases is considered separately. The examples of radical changes of this complexity in different bases from one family are given.

Keywords: Boolean formulae, complexity of functions, Shannon function, direct and iterative variables.

Литература

1. *Ложкин С.А.* О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и кибернетика. – 1999. – № 3. – С. 35–41.
2. *Лупанов О.Б.* Асимптотические оценки сложности управляющих систем. – М.: Изд-во Моск. ун-та, 1984. – 136 с.
3. *Яблонский С.В.* Введение в дискретную математику. – М.: 1986. – 384 с.
4. *Ложкин С.А.* О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными переменными // Труды III Междунар. конф. «Дискретные модели в теории управляющих систем» Красновидово'98 (22–27 июня 1998 г.). – М.: Диалог-МГУ, 1998. – С. 72–73.
5. *Коноводов В.А.* О сложности булевых формул в базисах из элементов с прямыми и итеративными входами // Материалы IX молодежной науч. шк. по дискретной математике и ее приложениям (М., 16–21 сент. 2013 г.). – М.: Изд-во ИПМ РАН, 2013. – С. 57–60.
6. *Ложкин С.А.* Реализация функций алгебры логики схемами из функциональных элементов с задержками: Дис. . . . канд. физ.-мат. наук. – 1979.
7. *Кириченко К.Д.* Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная матем. – 2005. – Т. 17, № 3. – С. 80–88.
8. *Cooper J.N., Ellis R.B., Kahng A.B.* Asymmetric binary covering codes // J. Combin. Theory. Ser. A. – 2002. – V. 100, No 2. – P. 232–249.

Поступила в редакцию
04.08.14

Коноводов Владимир Александрович – аспирант факультета вычислительной математики и кибернетики, Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия.

E-mail: *vkonovodov@gmail.com*