ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2005 МАТЕМАТИКА № 11 (522)

УДК 519.714

Р.Г. МУБАРАКЗЯНОВ

ВОЗМОЖНОСТИ ВЕРОЯТНОСТНЫХ УПОРЯДОЧЕННЫХ k РАЗ ЧИТАЮЩИХ И ДЕТЕРМИНИРОВАННЫХ ОДИН РАЗ ЧИТАЮЩИХ БИНАРНЫХ ПРОГРАММ НЕСРАВНИМЫ

1. Введение

Вычислительная модель, называемая бинарной программой, хорошо известна [1]. Напомним основные определения.

Детерминированной бинарной программой (BP) P на множестве переменных $X=\{x_0,...,x_{n-1}\}$ называется ориентированный ациклический граф с одной начальной вершиной и двумя финальными вершинами. Одна из финальных вершин помечена 0 (назовем ее отвергающей, или 0-вершиной), другая — 1 (назовем ее принимающей, или 1-вершиной). Каждая нефинальная вершина этого графа помечена переменной из X, и из нее выходят ровно две дуги, помеченные 0 и 1. Процесс вычисления детерминированной BP при фиксировании значений переменных из X сводится к следующему. Вычисление начинается в корне s программы. Если переменная, которой помечен s, имеет значение $a \in \{0,1\}$, то осуществляется переход в сына s по дуге, помеченной a. Из этой вершины переход осуществляется в зависимости от значения помечающей ее переменной. Так как путь, соответствующий значениям переменных, выбирается однозначно, каждому набору значений переменных можно сопоставить пометку той финальной вершины, в которую приводит вычисление. Эта пометка является значением вычисляемой функции.

Если в определении бинарной программы добавить возможность наличия недетерминированных вершин, т. е. не помеченных никакой переменной, или вероятностных вершин, т. е. помеченных случайными переменными, принимающими значения 0 и 1 с вероятностью $1/2$, получим соответственно определения недетерминированной и вероятностной программы. Вероятностная программа P определяет функцию $c_P : \{0,1\}^n \to [0,1]$, $c_P(x)$ — вероятность того, что P, имея на входе x, достигает принимающую вершину. Назовем эту функцию характеристической функцией P. Программа P вычисляет функцию h, если $c_P(x) > 1/2$ для $h(x) = 1$, и $c_P(x) < 1/2$ для $h(x) = 0$, т. е. вероятность, что P выдает $h(x)$, больше $1/2$ для любого набора значений переменных x. Если эта вероятность больше $1-\varepsilon$ для некоторого ε, $0 \le \varepsilon < 1/2$, то вычисление называется вычислением с ограничением на ошибку (ε — ошибка вычисления).

Определим *сложность* программы P как число ее вершин. В целях получения соотношений между различными классами сложности рассматриваются ограниченные классы бинарных программ [1]. *k раз читающая* бинарная программа (BPk) — бинарная программа, которая на любом пути вычисления каждую переменную читает не более k раз. Один раз читающая BP ($BP1$) называется *упорядоченной* (обозначается $OBDD$), если переменные читаются в определенном порядке. $OBDD$ интересны в связи с возможностью их практического использования [2]. Программа BPk называется $kOBDD$, если ее можно разбить на k слоев так, что переменные в каждом слое читаются не более одного раза в соответствии с одним и тем же порядком.

Назовем бинарную программу *уровневой*, если для любой ее нефинальной вершины v все пути от корня до v имеют одинаковую длину. Такая программа может быть разбита на уровни: каждый уровень содержит нефинальные вершины, одинаково удаленные от корня. *Шириной* уровневой программы называется максимальное число вершин на одном уровне. Уровневая

программа называется *забывающей*, если все вершины одного уровня помечены одной и той же переменной. Бинарные программы ограниченной ширины рассматривались в различных исследованиях. Известно, например, что класс булевых функций, вычислимых BP константной ширины совпадает с классом сложности NC^1 [3]. Функция, вычислимая детерминированой $OBDD$ константной ширины, может быть вычислена вероятностно с ограничением на ошибку при помощи конечного количества вопросов [4]. Доказано [5], что проблема "Выполнимость" NP-сложна для вероятностной с ограничением на ошибку $OBDD$ и лежит в классе P для вероятностной с ограничением на ошибку $OBDD$ константной ширины.

В данной работе рассматриваются вероятностные $OBDD$, ширина которых ограничена некоторой функцией $\omega(n)$ (обозначим их $OBDD^{\omega(n)}$), в целях сравнения их возможностей с возможностями бинарных программ из других классов.

Обозначим классы функций, вычислимых детерминированными, недетерминированными, вероятностными с ограничением на ошибку и вероятностными общего вида бинарными программами полиномиальной сложности $P{-}BP$, $NP{-}BP$, $BPP{-}BP$ и $PP{-}BP$ соответственно. Для ограниченных классов бинарных программ в обозначениях классов сложности суффикс "$-BP$" заменим соответствующим сокращением. Класс

$$PP{-}OBDD^{\text{const}} = \bigcup_{k \geq 0} PP{-}OBDD^k$$

соответствует $OBDD$ константной ширины. Известны соотношения между классами сложности для $OBDD$ [6]–[9].

Классы бинарных программ полиномиальной сложности будем обозначать так же, как и соответствующие классы сложности. Например, вероятностные (без ограничения на ошибку) $OBDD$ полиномиального размера обозначим как $PP{-}OBDD$. Из контекста будет ясно, для чего используются обозначения: для бинарных программ или для класса сложности.

При обобщениях $P{-}OBDD$ важно, чтобы полученные бинарные программы сохраняли свойства, позволяющие эффективно работать с ними. Например, для $NP{-}BP1$ тест на выполнимость полиномиален. Известно, что классы $BPP{-}OBDD$ и $NP{-}BP1$ не сравнимы в смысле отношения включения [10]. Этим объясняется наш интерес к следующему классу: вероятностным без ограничения на ошибку $kOBDD$. Можно бы было предполагать, что один из классов $PP{-}kOBDD$ (возможно с ограничением на ошибку) и $NP{-}BP1$ (или по крайней мере класс между $P{-}OBDD$ и $NP{-}BP1$) включается в другой. В работе показывается, что данная гипотеза ложна.

Работа имеет следующую структуру. Во втором параграфе определяются различные функции, для которых удается получить высокие нижние оценки сложности для различных типов бинарных программ. Затем приводятся некоторые известные результаты, касающиеся оценок коммуникационной сложности.

В третьем параграфе рассматривается $OBDD$ константной ширины. Показано, какие функции могут быть характеристическими для $PP{-}OBDD$ и доказывается, что

$$PP{-}OBDD^{\text{const}} \setminus NP{-}BP1 \neq \emptyset.$$

В четвертом параграфе сначала показывается, что $PP{-}kOBDD = PP{-}OBDD$ и что для любых натуральных t и k выполняется

$$P{-}OBDD \setminus PP{-}kOBDD^{\text{const}} \supseteq P{-}OBDD^{n^t} \setminus PP{-}kOBDD^{(t\log(n)/4)^{\frac{1}{2k}}} \neq \emptyset.$$

Далее определяется функция, сложная для $PP{-}kOBDD$. Эта функция вычислима даже ограниченным типом детерминированных $BP1$ ($T{-}BP1$). Для таких $BP1$ порядок чтения переменных зависит от их значения и определяется деревом полиномиального размера ([11] и [12])

$$P{-}T{-}BP1 \setminus PP{-}kOBDD \neq 0.$$

2. Функции и некоторые известные результаты

Для слова $v \in \{0,1\}^*$ целое, представление которого в двоичной системе счисления есть v, обозначим через $dec(v)$. Для индексов (от 0 до $r-1$) сумма $j + dec(v)$ вычисляется по модулю r.

Целочисленная функция на натуральных числах, обозначаемая $w(n)$, будет в работе определять ширину $OBDD$.

Функция "перестановочная матрица" определяется следующим образом: $PERM_n : \{0,1\}^{m^2} \to \{0,1\}$, $n = m^2$, $PERM_n(x) = 1$ тогда и только тогда, когда в каждой строке и в каждом столбце булевой матрицы $X = (x_{11}, x_{12}, \ldots, x_{mm})$ размером $m \times m$ содержится ровно одна 1.

Функция $ip_n : \{0,1\}^{2n} \to \{0,1\}$ — скалярное произведение, т. е.

$$ip_n(x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}) = \bigoplus_{i=0,\, n-1} x_i y_i,$$

где $\oplus$ — сумма по модулю 2.

Функция SIP_n ("скалярное произведение со смещением") определена на $n = 2r + \log r$ переменных $X \cup Y \cup V$:

$$SIP(x_0, \ldots, x_{r-1}, y_0, \ldots, y_{r-1}, v_0, \ldots, v_{\log r - 1}) = \bigoplus_{0 \le j \le r-1} (x_j y_{j+dec(v)}).$$

Функция $IND_n : \{0,1\}^{2n+1} \to \{0,1\}$ (индексная функция) определена на $X \cup Y \cup \{u\}$, $|X| = |Y| = n$, следующим образом:

$$IND_n(x_0, \ldots, x_{r-1}, y_0, \ldots, y_{r-1}, u) = \begin{cases} x_i, & \text{если } u = 0 \text{ и } \sum\limits_{j=0,\, n-1} y_j = y_i = 1; \\ y_i, & \text{если } u = 1 \text{ и } \sum\limits_{j=0,\, n-1} x_j = x_i = 1; \\ 0, & \text{иначе,} \end{cases}$$

т. е., например, при $u = 0$ функция IND_n равна x_i, если среди $\{y_j\}$ ровно одна переменная равна 1 и индекс этой переменной равен i.

Пусть для целых чисел r и n верно $n = 2r + \lceil \log(r) \rceil + 1$. Для функции $w(n) < r$ функция $SIND^{w(n)}$ ("смещенная индексная функция") определена на n переменных $X \cup Y \cup V \cup \{u\}$, $|X| = |Y| = r$:

$$SIND^{w(n)}(x_0, \ldots, x_{r-1}, y_0, \ldots, y_{r-1}, v_0, \ldots, v_{n-2r-1}, u) =$$

$$= \begin{cases} x_i, & \text{если } u = 0, \sum\limits_{j=0,\, w(n)-1} y_j = y_{i+dec(v)} = 1,\ i < w(n) - 1; \\ y_i, & \text{если } u = 1, \sum\limits_{j=0,\, w(n)-1} x_j = x_{i+dec(v)} = 1,\ i < w(n) - 1; \\ 0, & \text{иначе.} \end{cases}$$

В этом определении $i + dec(v)$ — сумма по модулю $w(n)$. Таким образом, функция $SIND^{w(n)}$ не зависит от переменных x и y с индексами больше, чем $w(n) - 1$.

Так как получение нижних оценок сложности опирается на теорию коммуникационной сложности, приведем некоторые понятия из этой области. Пусть два игрока Алиса и Боб вычисляют функцию f на множестве переменных $X = \{x_1, \ldots, x_n\}$. Алиса читает переменные из подмножества $X_0 \in X$ и посылает некоторое сообщение Бобу, который читает оставшиеся переменные (из $X_1 = X - X_0$) и вычисляет функцию f. Зафиксируем разбиение переменных $U = (X_0, X_1)$, соответствующее входным переменным игроков. Вычисляемая функция f определяется коммуникационной матрицей CM_U^f, строки которой соответствуют значениям переменных Алисы, а столбцы — значениям переменных Боба соответственно, т. е. элемент $CM_U^f(a,b)$ коммуникационной матрицы равен $f(a,b)$, где a и b — значения переменных из X_0 и X_1 соответственно. Односторонняя коммуникационная сложность, которая означает минимальное число битов, которые Алиса должна послать Бобу, зависит от числа различных строк матрицы CM_U^f.

Если для некоторого целого числа k функция f имеет большую коммуникационную сложность некоторого типа (детерминированную, недетерминированную и так далее) для всех разбиений (X_0, X_1) с $|X_0| = k$, то любая $OBDD$, вычисляющая f, также имеет большую сложность.

Авторы работы [13] первыми представили характеризацию вероятностной коммуникационной сложности. Автором независимо был получен аналогичный результат для $OBDD$ [14].

Лемма 1. *Пусть f — функция на переменных X, вычислимая $OBDD$ P. Пусть эта $OBDD$ определяет разбиение множества переменных $U = (X_0, X - X_0)$, т. е. переменные из X_0 читаются перед переменными из $X - X_0$. Пусть L — множество вершин P, непосредственно предшествующих чтению переменных из $X - X_0$, и $|L| = d$. Тогда существует множество вектор-строк $\{\mu(x)\}$ размерности d и вектор-столбцов $\{\nu(y)\}$ той же размерности d таких, что*

$$CM^f_U(\mathbf{a}, \mathbf{b}) = 1 \Leftrightarrow \mu(\mathbf{a})\nu(\mathbf{b}) > 1/2,$$
$$CM^f_U(\mathbf{a}, \mathbf{b}) = 0 \Leftrightarrow \mu(\mathbf{a})\nu(\mathbf{b}) < 1/2.$$

Доказательство. Для каждого значения a из X_0 рассмотрим вероятностное распределение $\mu(a) = (\mu_1(a), \ldots, \mu_d(a))$, где $\mu_j(a)$ — вероятность попасть в j-ю вершину L из начальной вершины P, если переменные из X_0 равны a. Определим для каждого значения b из $X - X_0$ вектор-столбец $\nu(b) = (\nu_1(b), \ldots, \nu_d(b))$, где $\nu_j(b)$ — вероятность достигнуть принимающую вершину из j-й вершины L, если переменные из $X - X_0$ равны b. Элемент $CM^f_U(a, b) = 1$ тогда и только тогда, когда $c_P(a, b) = \mu(a)\nu(b) > 1/2$. А элемент $CM^f_U(a, b) = 0$ тогда и только тогда, когда $c_P(a, b) = \mu(a)\nu(b) < 1/2$. □

Для коммуникационной матрицы CM, минимальное число d, позволяющее представить CM в соответствии с леммой 1, обозначим через $d(CM)$. Согласно лемме 1, если для любого разбиения множества переменных функции f число $d(CM)$ ее коммуникационной матрицы CM велико, то f сложна для вероятностной $OBDD$.

3. Функция $PERM$ проста для PP–$OBDD$ константной ширины

В этом параграфе описывается ряд свойств, которыми обладают характеристические функции $OBDD$ константной ширины [15], [16]. Будем рассматривать при этом забывающие программы, где каждый уровень программы содержит или только детерминированные узлы, или только вероятностные узлы.

Лемма 2. *Для любой константы α, $0 \le \alpha \le 1$, если двоичное представление α имеет t позиций, то существует $OBDD$ $B(\alpha)$ ширины 1, состоящая только из t случайных вершин такая, что $c_{B(\alpha)} = \alpha$.*

Лемма 3. *Пусть c_{B_1} и c_{B_2} — характеристические функции $OBDD$ B_1 ширины w_1 и B_2 ширины w_2 соответственно с одинаковым порядком чтения переменных. Тогда существует $OBDD$ с тем же самым порядком переменных со следующими характеристическими функциями: $1 - c_{B_1}(x)$, $1/2(c_{B_1}(x) + c_{B_2}(x))$, $c_{B_1}(x)c_{B_2}(x)$. Эти $OBDD$ обозначим $1 - B_1$, $1/2(B_1 + B_2)$, B_1B_2, они имеют ширину w_1, $w_1 + w_2$, w_1w_2 соответственно.*

Если $OBDD$ B_1 и B_2 имеют непересекающиеся множества переменных, то существует $OBDD$ $1/2(B_1 + B_2)$ и B_1B_2 с характеристическими функциями $1/2(c_{B_1}(x) + c_{B_2}(x))$ и $c_{B_1}(x)c_{B_2}(x)$ ширины $\max(w_1, w_2) + 1$ и $\max(w_1, w_2)$ соответственно.

Используя лемму 1, можно доказать утверждение.

Лемма 4. *Пусть для $OBDD$ B_n ширины w и функции f_n существуют числа p_n такие, что $c_{B_n}(x) > p_n$ тогда и только тогда, когда $f_n(x) = 1$. Тогда существует $OBDD$ ширины $w + 1$, вычисляющая функцию f_n.*

Используя эти леммы, доказывается

Теорема 1. *Пусть f_n — функция от n переменных. Пусть p_n — действительное число и B — вероятностная $OBDD$ ширины w такая, что $f_n(x) = 1$, тогда и только тогда, когда $c_B(x) = p_n$. Тогда f_n вычислима вероятностной $OBDD$ ширины $w^2 + w + 1$.*

Доказательство. Пусть B имеет n' уровней. Тогда для $\varepsilon_n = (1/2)^{n'}$ неравенство $|c_B(x) - p_n| \geq \varepsilon_n$ выполняется для любого набора x такого, что $f_n(x) = 0$.

Рассмотрим два случая: $p_n > 1/2$ и $p_n \leq 1/2$. Пусть $p_n > 1/2$. Из лемм 2 и 3 следует, что для $p' = 2p_n - 1$ существует $OBDD$ $B_1 = B(\frac{1}{2}(1 - B + B(p')))$ ширины $w(w+1)$ с характеристической функцией $c_{B_1}(x) = c_B(x)(\frac{1}{2}(1 - c_B(x) + p')) = p_n c_B(x) - \frac{1}{2}(c_B(x))^2$. Функция c_{B_1} достигает максимума $p'' = p_n^2/2$, если $c_B(x) = p_n$. Если $p_n \leq 1/2$, то для $p' = 1 - 2p_n$ существует $OBDD$ $B_1 = (1 - B)(\frac{1}{2}(B + B(p')))$ ширины $w(w+1)$ с характеристической функцией $c_{B_1}(x) = (1 - c_B(x))(\frac{1}{2}(c_B(x) + p')) = \frac{1}{2}(p' - (c_B(x))^2 + 2p_n c_B(x))$. Функция c_{B_1} достигает максимума $p'' = (1 - p_n)^2/2$, если $c_B(x) = p_n$. Для обоих случаев, если $c_B(x) \neq p_n$, т. е. $f_n(x) = 0$, то $c_{B_1}(x) \leq p'' - \varepsilon_n^2/2$, и если $f_n(x) = 1$, то $c_{B_1}(x) = p'' > p''' = p'' - \varepsilon_n^2/4$. Для p''' верно $c_{B_1}(x) < p'''$, если $f_n(x) = 0$, и $c_{B_1}(x) > p'''$, если $f_n(x) = 1$. □

Известно, что функция $PERM_n$ вычислима $BPP{-}OBDD$ [10]. С другой стороны, $PERM_n$ не принадлежит $NP{-}BP1$, а следовательно, $PERM_n \notin P{-}OBDD^{\text{const}} \subset P{-}OBDD$. Так как $BPP{-}OBDD^{\text{const}} = P{-}OBDD^{\text{const}}$ [8], то $PERM_n$ не принадлежит $BPP{-}OBDD^{\text{const}}$. Покажем, что эта функция принадлежит $PP{-}OBDD^w$ для некоторой константы w.

Теорема 2. *Функция $PERM_n$ вычислима вероятностной (без ограничения на ошибку) $OBDD$ $B(PERM_n)$ константной ширины.*

Доказательство. Опишем $OBDD$ $B(PERM_n)$, вычисляющую функцию $PERM_n$ на переменных $x_{11}, x_{12}, \ldots, x_{mm}$. Для любого i, $1 \leq i \leq m$, детерминированная $OBDD$ $P_1^{(i)}$ читает i-ю строку матрицы и проверяет, содержит ли эта строка ровно одну 1. Для любого i, $1 \leq i \leq m$, вероятностная $OBDD$ $P_2^{(i)}$ делает то же самое, но перед чтением каждой переменной попадает в отвергающую вершину с вероятностью $1/2$. После того, как $P_2^{(i)}$ читает переменную x_{ij}, равную 1, программа проверяет детерминированно, содержит ли строка только одну 1. Если это так, то $P_2^{(i)}$ принимает. Если $OBDD$ находит в строке вторую переменную, равную 1, то осуществляется переход в отвергающую вершину. Таким образом, $P_2^{(i)}$ попадает в 1-вершину после чтения i-й строки с одной переменной x_{ij}, равной 1, с вероятностью $(\frac{1}{2})^j$. Можно построить такие $OBDD$ $P_1^{(i)}$ и $P_2^{(i)}$, причем они будут иметь на каждом уровне 2 вершины.

Построим вероятностную $OBDD$ P такую, что для $p_m = (\frac{1}{2})^m - (\frac{1}{2})^{2m}$ и $\varepsilon_m = (\frac{1}{2})^{2m}$ верно следующее: $c_P(x) = p_m$, если $PERM_n(x) = 1$, и $|p_m - c_P(x)| \geq \varepsilon_m$ иначе.

Корень P — вероятностная вершина, выбирающая $P_1^{(1)}$ или $P_2^{(1)}$. Принимающую вершину $P_1^{(i)}$, $1 \leq i \leq m-1$, отождествим со случайным узлом, выбирающим $P_1^{(i+1)}$ или $P_2^{(i+1)}$. Это может быть записано как $P_1^{(i)}(\frac{1}{2}(P_1^{(i+1)} + P_2^{(i+1)}))$. Принимающую вершину $P_1^{(m-1)}$ отождествим со случайным узлом, выбирающим $P_2^{(m)}$ или 0-вершину. Это можно записать как $P_1^{(m-1)}\frac{1}{2}P_2^{(m)}$. Принимающую вершину $P_2^{(i)}$, $1 \leq i < m$, отождествим со случайным узлом, дуги из которого ведут в $P_3^{(i+1)}$ и 0-вершину (т. е. $P_2^{(i)}\frac{1}{2}P_3^{(i+1)}$). $OBDD$ $P_3^{(i)}$, $2 \leq i \leq m$, — копия $P_1^{(i)}$ и отличается лишь ее связями с другими программами. Для $i < m$ 1-вершину $P_3^{(i)}$ отождествим со случайным узлом, ведущим в 0-вершину и корень $P_3^{(i+1)}$ (т. е. $P_3^{(i)} = \frac{1}{2}P_3^{(i+1)}$).

Для i, j, $1 \leq j \leq 3$, $1 \leq i \leq m$, 0-вершину $P_j^{(i)}$, которая достигается, например, если i-я строка содержит не одну переменную равную 1, отождествим с 0-вершиной P. Программа P принимает только, если для любого i, $1 \leq i \leq m$, i-я строка x содержит только один элемент x_{ij_i}, равный 1. Каждое вычисление на P, ведущее в 1-вершину, проходит $P_1^{(1)}, \ldots, P_1^{(i-1)}$ и достигает корня вероятностной $OBDD$ $P_2^{(i)}$ для некоторого i, $1 \leq i \leq m$. Вычисление достигает 1-вершины $P_2^{(i)}$ с вероятностью $(\frac{1}{2})^{j_i}$. После этого вычисление проходит $P_3^{(i+1)}, \ldots, P_3^{(m)}$. Поскольку каждая подпрограмма при вычислении выбирается случайно с вероятностью $1/2$, вероятность выбора

такого пути вычисления равна $(\frac{1}{2})^m(\frac{1}{2})^j$, где P читает единственный элемент x_{ij_i} i-й строки, равный 1, в вероятностной части $P_2^{(i)}$.

Таким образом, $c_P(x) = (\frac{1}{2})^m \sum_{i=1}^{m}(\frac{1}{2})^{j_i}$, если x — матрица с одной единицей в каждой строке. Если x соответствует матрице перестановки и $\{j_i \mid x_{ij_i} = 1,\ 1 \le i \le m\} = \{i \mid 1 \le i \le m\}$, то

$$c_P(x) = (\tfrac{1}{2})^m \sum_{i=1}^{m}(\tfrac{1}{2})^i = (\tfrac{1}{2})^m(1 - (\tfrac{1}{2})^m) = p_m.$$

Если x содержит в ряде не одну 1, то $c_P(x) = 0 = p_m - \varepsilon_m$.

Если x содержит в каждой строке ровно одну 1, но $\{j_i \mid x_{ij_i} = 1,\ 1 \le i \le m\} \ne \{i \mid 1 \le i \le m\}$, то $|p_m - c_P(x)| \ge (\frac{1}{2})^{2m}$. Из теоремы 1, следует, что можно построить искомую вероятностную $OBDD$ $B(PERM_n)$ константной ширины. □

Следствие 1. Существуют функции, вычислимые вероятностными (без ограничения на ошибку) $OBDD$ константной ширины и невычислимые недетерминированными $BP1$ полиномиальной сложности.

4. Нижние границы сложности вероятностных $OBDD$

Сначала покажем, что $PP{-}kOBDD = PP{-}OBDD$. Рассмотрим двусторонние вычисления: в этой модели Боб тоже посылает Алисе сообщения. Известно, что нижние оценки сложности односторонних и двусторонних вероятностных протоколов почти равны [13]. Этот результат не может быть непосредственно применен к $PP{-}kOBDD$. Тем не менее, верно следующее утверждение.

Теорема 3. *Для любого целого k и для любой целочисленной функции $\omega(n)$ справедливо следующее $PP{-}kOBDD^{\omega(n)} \subseteq PP{-}OBDD^{\omega(n)^{2k}}$.*

Доказательство. Пусть $PP{-}kOBDD$ P вычисляет функцию f на переменных X. Тогда P имеет k слоев таких, что в каждом слое переменные читаются по одному разу в одинаковом порядке. Пусть V_i, $i = 1, \dots, k$, — множество узлов первого уровня слоя i. Пусть $N = |V_1| \times \cdots \times |V_k|$.

$PP{-}OBDD$ P' моделирует параллельную работу всех k слоев P. Работа начинается с выбора с равной вероятностью $1/N$ вектора из множества $D = \{t, d_1, \dots, d_N\} = \{(v_1, \dots, v_k) \mid 1 \le t \le N,\ v_i \subseteq V_i,\ 1 \le i \le k\}$. Программа P' имеет узлы разных типов. Узлы первого типа имеют вид $\{(t, v_1, \dots, v_k) \mid 1 \le t \le N,\ v_i \subseteq V_i',\ i = 1, \dots, k\}$, где V_i' — уровни P, находящиеся на одинаковом расстоянии от начал слоев, и t – индекс вектора D. Если дуги, помеченные a, соединяют детерминированные узлы v_j с узлами v_j' в P для всех j, $1 \le j \le k$, то узлы $(t, v_1, \dots, v_k)$ и $(t, v_1', \dots, v_k')$ связаны дугой с той же пометкой в P'. Если один из v_j' является 0-вершиной, то дуга в P' ведет к 0-вершине. Если v_j' — принимающая вершина, то $v_l' = 1$ для $l \ge j$. Таким образом, узлы второго типа имеют вид $(t, v_1, \dots, v_j, 1, \dots, 1)$ для некоторого $1 \le j < k$. При определении поведения программы P' после прохождения узла такого типа рассматриваются только узлы $v_1, \dots, v_j$ программы P.

Узлы другого типа — случайные узлы. Поскольку вероятности выбора вершин P после случайных узлов независимы, программа P' должна иметь больше случайных уровней, чем P. Пусть V_i' – случайные уровни P, находящиеся на одном расстоянии от начал слоев, $1 \le i \le k$. Пусть V_i'' – уровни, следующие за V_i', $1 \le i \le k$. Тогда уровни V_i', $1 \le i \le k$, формируют k случайных уровней P'. Узлы j-го уровня такого типа обозначим через $(t, v_1', \dots, v_{j-1}', v_j, \dots, v_k)$, $1 \le t \le N$, $v_l' \subseteq V_i''$, $1 \le l \le j-1$, $v_l \subseteq V_i'$, $j \le l \le k$. Тогда дуга соединяет $(t, \dots, v_{j-1}', v_j, \dots)$ и $(t, \dots, v_{j-1}', v_j', v_{j+1} \dots)$, если P имеет дугу (v_j, v_j').

Узлы P' последнего типа имеют вид $\{(t, v_1, \dots, v_k) \mid 1 \le t \le d,\ v_i \subseteq V_{i+1},\ 1 \le i \le k-1\}$. Напомним, что V_{i+1} — первый уровень $(i+1)$-го слоя. Узел $(t, v_1, \dots, v_k)$ отождествим с принимающей вершиной P', если верно следующее: для $d_t = (t, v_1', \dots, v_k') \subseteq D$ существует индекс j,

$1 \le j \le k$, такой, что $v_i = v'_{i+1}$ для $1 \le i \le j-1$, и v_j является принимающей вершиной P. Узлы, для которых не выполняется это свойство, отождествим с отвергающей вершиной P'.

Определим вероятность $p(d_i, x)$ того, что вычисление P на x проходит через вершины d_i и заканчивает вычисление в принимающей вершине. Тогда $\sum\limits_{i=1}^{N} p(d_i, x) = c_P(x)$. Очевидно, $c_{P'}(x) = \sum\limits_{i=1}^{N} \frac{1}{N} p(d_i, x) = \frac{1}{N} c_P(x)$. Следовательно, для любого x, если $f(x) = 1$, то $c_{P'} > 1/(2N)$. Если $f(x)=0$, то $c_{P'} < 1/(2N)$. Пусть $\omega(n)$ — ширина P, тогда P' имеет ширину не более, чем $N(\omega(n)^k + \omega(n)^{k-1} + \cdots + \omega(n)) \le \omega(n)^{k-1}\omega(n)\frac{\omega(n)^k-1}{\omega(n)-1}$. Из леммы 4 следует, что существует $PP{-}OBDD$, вычисляющая f, ширины не более, чем $1 + \omega(n)^k \frac{\omega(n)^k-1}{\omega(n)-1} \le \omega(n)^{2k}$. □

Следствие 2. $PP{-}kOBDD = PP{-}OBDD$ для любого целого числа k.

Следствие 3. Для любых целых чисел k и c_1 верно следующее $PP{-}kOBDD^{c_1} \subseteq PP{-}OBDD^{c_2}$ для некоторой константы c_2. Поэтому $PP{-}kOBDD^{\text{const}} = PP{-}OBDD^{\text{const}}$.

Лемма 5. *Разобьем множество $2r$ переменных Z на два подмножества X и Y: $Z = X \cup Y$, $|X| = |Y| = r$. Для любых разбиений (Z_0, Z_1) множества $Z = Z_0 \cup Z_1$, $Z_1 = Z - Z_0$, $|Z_0| = |Z_1| = r$, существуют числа m, $0 \le m \le r-1$, и $j \in \{0,1\}$ и подмножество $X' = \{x_{i_1}, x_{i_2}, \ldots, x_{i_{r/4}}\} \subseteq Z_j \cup X$ такие, что $Y' = \{y_{i_{1+m}}, \ldots, y_{i_{\frac{r}{4}+m}}\} \subseteq Z_{1-j} \cap Y$, где суммы $l+m$ для индексов берутся по модулю r.*

Доказательство. Существует подмножество $Z'_0 \subset Z_0$ мощности $r/2$ переменных, принадлежащих или X, или Y. Без потери общности, пусть $Z'_0 \subset X$. Тогда найдется подмножество $Z'_1 \subseteq Y \cup Z_1$ мощности $r/2$. Отсюда $Z'_0 \times Z'_1$ размера $r^2/4$ содержит по крайней мере $r/4$ пар (x_i, y_{i+m}) для некоторого целого m, $0 \le m \le r-1$. Эти пары определяют X' и Y' соответственно. □

Теорема 4. *Пусть вероятностная $OBDD$ P вычисляет индексную функцию $IND_n(x_0, \ldots, x_{r-1}, y_0, \ldots, y_{r-1}, u)$ и при этом читает любую переменную из X прежде переменных из Y. Тогда P имеет ширину по крайней мере n. То же утверждение верно, если P читает любую переменную из X после переменных из Y.*

Доказательство. Пусть вероятностная $OBDD$ P читает все переменные из X перед любой переменной из Y. Положим $u = 0$. Рассмотрим подматрицу коммуникационной матрицы $CM_U^{IND_n}$ с разбиением $U = (X, Y)$ при $u = 0$. Ради простоты обозначим эту подматрицу CM. Пусть P содержит $n-1$ вершину, в которых читается первая переменная из Y. Согласно лемме 1

$$CM(a,b) = 1 \Leftrightarrow \mu(a)\nu(b) > 1/2; \quad CM(a,b) = 0 \Leftrightarrow \mu(a)\nu(b) < 1/2 \tag{1}$$

для некоторых $(n-1)$-мерных вектор-строк $\{\mu(a)\}$, соответствующих значениям X, и $(n-1)$-мерных вектор-столбцов $\{\nu(b)\}$, соответствующих значениям Y. Рассмотрим множество значений B переменных Y такое, что $B = \left\{ b^{(i)} \in \{0,1\}^n \,\middle|\, \sum\limits_{j=1,n} b_j^{(i)} = b_i^{(i)} = 1 \right\}$. По определению функции IND_n для любого набора значений $a \in \{0,1\}^n$ переменных из X пересечение строки a матрицы CM со столбцами CM, соответствующими B, формирует тот же самый вектор a. Другими словами, подматрица CM, определяемая B, содержит все вектор-строки из $\{0,1\}^n$.

Так как $(n-1)$-мерные векторы $\{\nu(b^{(i)})\}$ не могут быть линейно независимыми, существуют коэффициенты α_i, не все равные 0, такие, что $\sum\limits_{i=1}^{n}(\alpha_i \nu(b^{(i)})) = 0$. Предположим, что $\alpha_1 \neq 0$. Тогда возможно следующее представление $\nu(b^{(1)}) = \sum\limits_{i=2}^{n}(\alpha_i \nu(b^{(i)}))$.

Рассмотрим два случая: $\sum\limits_{i=2}^{n} \alpha_i \le 1$ и $\sum\limits_{i=2}^{n} \alpha_i > 1$.

Пусть $\sum\limits_{i=2}^{n} \alpha \leq 1$. Найдется строка $a \in \{0,1\}^n$ матрицы CM такая, что $CM(a, b^{(1)}) = 1$, и для $2 \leq i \leq n$, если $\alpha_i < 0$, то $CM(a, b^{(i)}) = 1$, и если $\alpha_i \geq 0$, то $CM(a, b^{(i)}) = 0$. Из (1) следует

$$1/2 < \mu(a)\nu(b^{(1)}) = \sum_{i=2}^{n}(\alpha_i \mu(a)\nu(b^{(i)})) < 1/2 \sum_{i=2}^{n} \alpha_i \leq 1/2.$$

Получили противоречие.

Пусть теперь $\sum\limits_{i=2}^{n} \alpha_i > 1$. Тогда существует строка $a \in \{0,1\}^n$ матрицы CM такая, что $CM(a, b^{(1)}) = 0$, и для $2 \leq i \leq n$, если $\alpha_i < 0$, то $CM(a, b^{(i)}) = 0$, и если $\alpha_i \geq 0$, то $CM(a, b^{(i)}) = 1$. Из (1) следует

$$1/2 > \mu(a)\nu(b^{(1)}) = \sum_{i=2}^{n}(\alpha_i \mu(a)\nu(b^{(i)}) > 1/2.$$

Противоречия доказывают теорему.

Если P читает все переменные из X после любой переменной из Y, рассмотрим подматрицу $CM_U^{IND_n}$ при $u = 1$. Функция IND_n определена так, что доказательство теоремы в этом случае аналогично приведенному выше. □

Теорема 5. *Для любой целочисленной функции $\omega(n)$, $\Omega(1) \leq \omega(n) \leq O(\log(n))$, вероятностная (без ограничений на ошибку) $kOBDD$, вычисляющая функцию $SIND^{\omega(n)}$, имеет ширину по крайней мере $(\omega(n)/4)^{\frac{1}{2k}}$. Функция $SIND^{\omega(n)}$ вычислима детерминированной $OBDD$, имеющей ширину $\omega(n)(2^{\omega(n)} + 2)$.*

Доказательство. Пусть P' — вероятностная (без ограничения на ошибку) $kOBDD$ ширины ω_1, вычисляющая функцию $SIND^{\omega(n)}$. По теореме 3 P' можно преобразовать в вероятностную $OBDD$ P ширины $(\omega_1)^{2k}$.

На множестве переменных $Z = \{x_0, \ldots, x_{\omega(n)-1}, y_0, \ldots, y_{\omega(n)-1}\}$ определим разбиение (Z_0, Z_1) с $|Z_0| = |Z_1| = \omega(n)$. При этом P читает переменные из Z_0 перед любой переменной из Z_1. Пусть m, j — целые числа из леммы 5. Тогда $X' \subseteq Z_j$, $Y' \subseteq Z_{1-j}$, $|X'| = |Y'| = \omega(n)/4$. Рассмотрим слово v_0 такое, что $dec(v_0) = m$. Установим значения переменных $X \cup Y \setminus (X' \cup Y')$ равными 0. Тогда функция $SIND^{\omega(n)}$ на переменных $(X' \cup Y' \cup \{u\})$ равна при $v = v_0$ функции $IND_{\omega(n)/4}$. Кроме того, все переменные из X' читаются P до или после переменных из Y'. По теореме 4 P имеет ширину по крайней мере $\omega(n)/4$. Таким образом, P' имеет ширину по крайней мере $(\omega(n)/4)^{\frac{1}{2k}}$.

Детерминированная $OBDD$ B, вычисляющая функцию $SIND^{\omega(n)}$, сначала читает v и запоминает $dec(v)$ по модулю $\omega(n)$. После этого B читает u.

Если $u = 0$, то B читает переменные x_i, $0 \leq i \leq \omega(n) - 1$, и запоминает их. Программе B нужно $\omega(n)2^{\omega(n)}$ узлов, чтобы сохранить информацию о $dec(v)$ и x. После этого B читает переменные $y_i, 0 \leq i \leq \omega(n) - 1$, находит переменную $y_j = 1$, определяет $x_{j-dec(v)}$ ($j - dec(v)$ вычисляется по модулю $\omega(n)$) и проверяет, верно ли, что $y_i = 0$ для всех $j < i < \omega(n)$.

Если $u = 1$, то B проверяет, точно ли одна переменная x_j из $\{x_i \mid 0 \leq i \leq \omega(n) - 1\}$, является равной 1 и запоминает одновременно $j - dec(v)$ по модулю $\omega(n)$. Для осуществления такого вычисления требуется $2\omega(n)$ вершин на каждом уровне (запоминается значение $dec(v)$ и значение последней прочитанной переменной x_j). Поскольку B — уровневая $OBDD$, B читает все переменные y_i, $i = 0$, $\omega(n) - 1$ и выдает $y_{j-dec(v)}$. B имеет ширину $\omega(n)(2^{\omega(n)} + 2)$. □

Следствие 4. Для любых натуральных чисел k и t функция $SIND^{t\log(n)}$ принадлежит $P\text{–}OBDD^{tn^{t+1}} \setminus PP\text{–}kOBDD^{(t\log(n)/4)^{1/2k}} \subseteq P - OBDD \setminus PP - kOBDD^{\text{const}}$.

Теорема 6 ([17]). *Для матрицы $CM_{(X,Y)}^{ip_n}$ верно*

$$d(CM_{(X,Y)}^{ip_n}) = 2^{n/2}.$$

Используя этот результат, доказываем следующую теорему.

Теорема 7. *Вероятностная (без ограничения на ошибку) $kOBDD$, вычисляющая функцию SIP_n, $n = 2r + \log r$, имеет сложность по крайней мере $2^{r/(16k)}$. Кроме того, $SIP_n \in P{-}T{-}BP1$.*

Доказательство. Пусть вероятностная $OBDD$ P вычисляет функцию SIP_n. По лемме 5 найдутся подмножества X' и Y', $|X'| = |Y'| = n/4$, такие, что все переменные из X' читаются в P до или после любой переменной из Y'. Обнулив значения других переменных, получим подфункцию SIP_n на множестве $X' \cup Y'$, которая равняется $ip_{n/4}$. Для соответствующей коммуникационной матрицы $CM_{(X',Y')}$ (или $CM_{(Y',X')}$) $d(CM_{(X',Y')}) = 2^{r/8}$. По лемме 1 P имеет ширину по крайней мере $2^{r/8}$, а эквивалентная вероятностная $kOBDD$ имеет ширину по крайней мере $2^{r/(16k)}$.

Детерминированная $T{-}BP1$ B, вычисляющая функцию SIP_n, читает сначала v, затем пары $(x_i, y_{i+dec(v)})$, $i = 0,\ r-1$. Для вычисления SIP_n программе B необходимо запомнить $dec(v)$, значение части скалярного произведения, соответствующего уже прочитанным переменным, и значение последней прочитанной переменной x_i. Поэтому B имеет максимальную ширину $4r$. □

Литература

1. Wegener I. *Branching programs and binary desicion diagrams*: *theory and applications.* – SIAM monographs on discrete mathematics and applications. – Philadelphia, USA, 2000. – 408 P.
2. Bryant R.E. *Graph-based algorithms for Boolean function manipulation* // IEEE Transact. on Comput. – 1986. – V. 35. – P. 677–691.
3. Barington D.A. *Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1* // J. Comput. and System Sci. – 1989. – V. 38. – P. 150–164.
4. Newman I. *Testing of function that have small width branching programs* // Proc. of the 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12–14 November 2000. IEEE Computer Society. – Redondo Beach, California, USA, 2000. – P. 251–258.
5. Agrawal M., Thierauf T. *The satisfiability problem for probabilistic ordered branching programs* // Theory Comput. Systems (TOCS). – 2001. – V. 34. – P. 471–487.
6. Ablayev F. *Randomization and nondeterminism are incomparable for ordered read-once branching programs* // Proc. ICALP'97, LNCS 1256, Springer. – 1997. – P. 195–202.
7. Ablayev F., Karpinski M., Mubarakzjanov R. *On BPP versus $NP \cup coNP$ for ordered read-once branching programs* // Theoret. Comput. Sci. – 2001. – V. 264. – P. 127–137.
8. Karpinski M., Mubarakzjanov R. *Some separation problems on randomized OBDDs* // Proc. of the Workshop on Computer Science and Information Technologies CSIT'99. – Moscow, Russia, 1999 (`http://msu.jurinfor.ru/CSIT99`).
9. Karpinski M., Mubarakzjanov R. *A note on Las Vegas OBDDs* //Electronical Colloquium on Computational Complexity, Trier University, Trier. – ECCC TR99-009, 1999 (`http://www.ecc.uni-trier.de/eccc/`).
10. Sauerhoff M. *Randomness and nondeterminism are incomparable for read-once branching programs* // Electronical Colloquium on Computational Complexity, Trier University, Trier. – ECCC TR98-018, 1998 (`http://www.ecc.uni-trier.de/eccc/`).
11. Gergov J., Meinel C. *Efficient Boolean manipulation with OBDDs can be extended to FBDDs* // IEEE Transact. on Comput. – 1994. – V. 43. – № 10. – P. 1197–1209.
12. Sieling D., Wegener I. *Graph driven BDDs — a new data structure for Boolean functions* // Theoret. Comput. Sci. – 1995. – V. 141. – P. 283–310.
13. Paturi R., Simon J. *Probabilistic communication complexity* // J. Comput. and System Sci. – 1986. – V. 33. – № 1. – P. 106–123.
14. Mubarakzjanov R. *Bounded-width probabilistic OBDDs and read-once branching programs are incomparable* // Electronical Colloquium on Computational Complexity, Trier University, Trier. – ECCC TR01-037, 2001 (`http://www.ecc.uni-trier.de/eccc/`).

15. Mubarakzjanov R. *On probabilistic OBDDs with constant width* // Proc. of the Workshop on Comput. Sci. and Informat. Technolog. CSIT'2000, Ufa, Russia, September 18–23, 2000. – V. 2. – P. 62–68.
16. Mubarakzjanov R. *Probabilistic OBDDs*: *on bound of width versus bound of error* // Electronical Colloquium on Computational Complexity, Trier University, Trier. – ECCC TR00-085, 2000 (`http://www.ecc.uni-trier.de/eccc/`).
17. Forster J. *A linear lower bound on the unbounded error probabilistic communication complexity* // J. Comput. and System Sci. – 2002. – V. 65. – № 4. – P. 612–625.

Казанский государственный университет

Поступила 27.12.2004