ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2006 МАТЕМАТИКА № 6 (529)

УДК 519.714

Р.Г. МУБАРАКЗЯНОВ

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ ВЕРОЯТНОСТНЫХ БИНАРНЫХ ПРОГРАММ С БОЛЬШОЙ УПОРЯДОЧЕННОЙ ЧАСТЬЮ

1. Введение

Определение детерминированных бинарных программ хорошо известно [1]. Эта модель определяется ориентированным ациклическим графом, у которого каждая вершина, за исключением двух выходов, соответствует некоторой переменной и имеет две исходящие дуги, помеченные 0 и 1. Для фиксированных значений переменных вычисление начинается в единственной начальной вершине, идет по дугам в соответствии со значениями переменных и возвращает значение, которым помечен выход. Если на каждом пути каждая переменная встречается не более одного раза, то программа называется один раз читающей ($BP1$). Кроме того, если переменные читаются в каком-то определенном порядке, то программа называется упорядоченной $BP1$, или $OBDD$.

Бинарная программа называется *недетерминированной*, если в ней допускаются недетерминированные узлы, т.е. узлы, из которых выходят две непомеченные дуги. При наличии в бинарной программе вероятностных узлов, каждый из которых соответствует случайной переменной, принимающей значения $\{0,1\}$ с вероятностью $1/2$, бинарная программа называется *вероятностной*. Для ε, $0 \le \varepsilon < 1/2$, будем говорить, что вероятностная бинарная программа B $(1-\varepsilon)$-*вычисляет* функцию h, если B выдает $h(x)$ с вероятностью не менее $1-\varepsilon$ для каждого входа x. Такое вычисление называется вероятностным с ограничением на ошибку, равным ε. Так как в данной работе рассматриваются лишь такие вычисления, будем для краткости называть их *вероятностными*. Под *сложностью* (или размером) бинарной программы подразумевается количество ее узлов.

Для вычисления типа M класс булевых функций, вычислимых детерминированными (недетерминированными) моделями полиномиального размера этого типа, обозначим P-M (NP-M). Пусть BPP_ε-M — класс функций, $(1/2-\varepsilon)$-вычислимых вероятностными бинарными программами типа M полиномиального размера. Тогда $BPP\text{-}M = \bigcup\limits_{0\le\varepsilon<1/2} BPP_\varepsilon\text{-}M$. Отношения между классами сложности P, BPP, NP в контексте $OBDD$ хорошо изучены [2]. Например, известна экспоненциальная нижняя оценка сложности вероятностных $OBDD$ [3]. Доказано также, что важная функция "целочисленное умножение" ($MULT_n$) сложна для вероятностных $OBDD$ [4] (определение $MULT_n$ будет дано позже). В то же время экспоненциальная нижняя оценка сложности вероятностных один раз читающих бинарных программ известна только в случае, если ошибка ε вычисления ограничена некоторой положительной константой [5]. В данной работе исследуется ограниченная модель $BP1$.

Определение 1. $BP1$ P на n переменных X назовем $BP1$ *с большой $OBDD$ частью или большой упорядоченной частью* (для краткости $BP1(OBDD)$), если существуют подмножество $X' \subset X$ переменных мощности $O(\log n)$ и значения d переменных из X' такие, что подпрограмма P после фиксирования значений переменных из X' равными d является $OBDD$ на $X \setminus X'$.

Чтобы объяснить интерес к $BP1(OBDD)$, заметим следующее. Существует несколько функций, например, ISA_n, ACH_n (дадим определения этих функций позднее), из класса P-$BP1$ \

P-$OBDD$, вычислимых детерминированными $BP1(OBDD)$. Для того чтобы найти более общую модель вычисления, чем $OBDD$, в [6] изучались свойства $BP1$, описанных деревом (T-$BP1$) и введенных в [7], [8]. Приводимое здесь определение обобщает этот класс $BP1$, т. к. T-$BP1$ — это $BP1(OBDD)$, и поэтому легко определить функцию из P-$BP1(OBDD) \setminus P$-T-$BP1$. Результаты данной работы аналогичны результатам работы [6], в которой изучались недетерминированные бинарные программы. В частности, в [6] показано, что NP-$OBDD \subset NP$-T-$BP1 \subset NP$-$BP1$. В данной работе доказывается, что

$$BPP\text{-}OBDD \subset BPP\text{-}BP1(OBDD) \subset BPP\text{-}BP1.$$

Кроме того, исследуются все известные (по крайней мере автору) функции, сложные для вероятностных $OBDD$, и доказывается, что почти все они также сложны для вероятностных $BP1(OBDD)$. Для этого обобщается определение k-стабильности функции, которое изучалось ранее [9], [10], и затем показывается, что несколько известных функций удовлетворяют этому обобщенному свойству. Это доказывается на основе нижних оценок сложности бинарных программ, полученных в [11], [3], [12], [13].

В заключение обобщаются результаты [4] для вероятностных $OBDD$ и [6] для недетерминированных T-$BP1$ и доказывается, что функция "целочисленное умножение" сложна для $BP1(OBDD)$.

2. Обобщение k-стабильности

Известен ряд функций, сложных для вероятностных $OBDD$ (напр., [2]). Некоторые из этих функций также являются k-стабильными [10]. Не приводя это определение сейчас, отметим лишь, что такие функции сложны и для $BP1$. Известные функции из класса P-$BP1 \setminus BPP$-$OBDD$ с более слабыми свойствами, чем k-стабильность, могут быть достаточны для доказательства высоких нижних оценок сложности вероятностных $BP1(OBDD)$. В [5] при исследовании сложности вычисления функции вероятностными $OBDD$ ее вычисление сводится к вычислению другой функции, сложной для однораундовых коммуникационных игр. В [3] представлен способ прямого (непосредственного) вычисления нижних оценок сложности вероятностных $OBDD$. Используя этот способ, покажем, что функции, удовлетворяющие обобщенной версии k-стабильности, сложны для вероятностных $OBDD$.

В следующем определении, как и в дальнейшем изложении, для простоты функции, зависящие от n, будем записывать без аргумента: например, просто k_2 вместо $k_2(n)$.

Определение 2. Пусть f — функция на множестве X, содержащем n переменных. Назовем эту функцию (k_2, k_3, k_A)-*стабильной относительно* $X_1 \subseteq X$ (или для краткости (k_2, k_3, k_A)-*стабильной*), если выполняются следующие условия: *для любых* $X_2 \subseteq X_1$, $|X_2| = k_2$, *существуют такие подмножество* $X_3 \subseteq X_2$, $|X_3| = k_3$, *значение* b *переменных из* $(X \setminus X_1) \cup (X_2 \setminus X_3)$ *и множество* A_b *наборов значений* X_3 *мощности* $|A_b| = k_A$, *что для любой переменной* $x \in X_3$ *существуют такие значения* c_x *переменных из* $X_1 \setminus X_2$ *и число* $\sigma \in \{0, 1\}$, *что для любого* $a \in A_b$

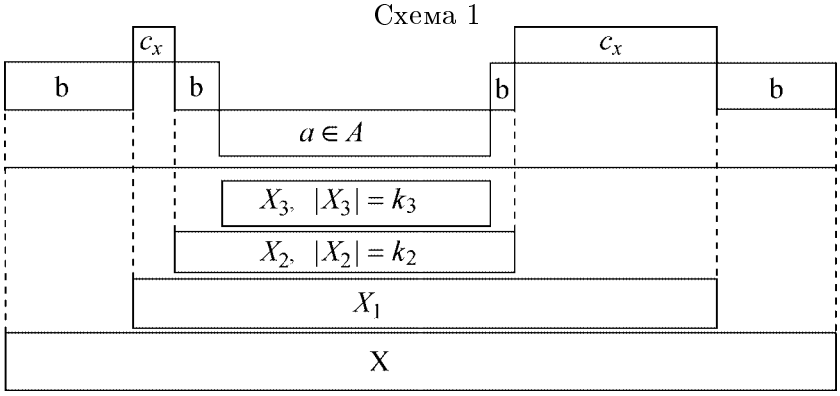
$$f(a; b; c_x) = a(x)^\sigma.$$

Здесь $a(x)$ — значение переменной x, соответствующее набору значений a (т. е. x играет роль индекса для вектора a); $(a; b; c_x)$ в данной работе означает набор значений всех переменных из X, где, например, переменные из X_3 получают значения в соответствии с a.

Схема 1 иллюстрирует разбиение множества переменных на подмножества и обозначения соответствующих наборов значений.

Чтобы понять соотношение между данным определением и определением k-стабильности, заметим, что функция k-стабильна тогда и только тогда, когда она $(k, k, 2^k)$-стабильна по отношению к X.

Схема 1



В [3] доказана

Теорема 1. *$(1-\varepsilon)$-вероятностная односторонняя коммуникационная сложность функции, описанной коммуникационной матрицей CM_U, не может быть менее*

$$\log(nrow(CM_U)) - ts(CM_U)H(1-\varepsilon) - 1.$$

Теорема 2. *Пусть h_n — (k_2, k_3, k_A)-стабильная функция от n переменных, где $k_3 = k_3(n)$ — неограниченно растущая функция, и для любого действительного $\delta < 1$ выполняется $k_A \geq 2^{\delta k_3}$ для достаточно больших n. Тогда для любого $\varepsilon \in (0, 1/2)$ существует константа $\delta' > 0$ такая, что для любого достаточно большого n вероятностная $OBDD$ $(1-\varepsilon)$-вычисляющая функция h_n имеет сложность не менее $2^{k_3\delta'}$.*

Доказательство. Теорема следует из такого факта. Пусть вероятностная $OBDD$ P $(1-\varepsilon)$-вычисляет (k_2, k_3, k_A)-стабильную функцию h_n. Тогда P имеет сложность не менее $\frac{k_A}{2^{k_3 H(1-\varepsilon)}}$, где $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ — энтропия Шеннона. Докажем это.

Рассмотрим множество Q узлов из P, достижимых после чтения ровно k_2 переменных из X_1. Тогда X можно разбить на подмножества уже прочитанных переменных L и непрочитанных переменных R. Пусть $L \cap X_1 = X_2, |X_2| = k_2$. Тогда можно найти подмножество $X_3 \subseteq X_2$, набор значений b и множество наборов значений A_b в соответствии с определением 2. Рассмотрим одностороннее коммуникационное вероятностное вычисление для частичной функции h_n^b после фиксирования значений переменных из $(X \setminus X_1) \cup (X_2 \setminus X_3)$ в соответствии с b, где первый игрок (Алиса) получает значения из X_3, а второй (Боб) из $X_1 \setminus X_2$. Вычисление возможно, если Алиса осуществляет проход по P на своей части входных данных и передает Бобу номер достигнутого ею узла P.

Чтобы сделать доказательство более полным, напомним некоторые понятия из теории коммуникационных вычислений. Установим разбиение переменных U в соответствии с тем, которое получено игроками. Вычисленная функция f описывается коммуникационной матрицей CM_U, столбцы и строки которой соответствуют значениям переменных Алисы и Боба соответственно. Элемент $CM_U(a, b)$ равен $f(a; b)$. Количество различных строк CM_U обозначим $nrow(CM_U)$. Известно, что детерминированная коммуникационная сложность, т. е. количество битов, которые Алиса должна переслать Бобу, равна $\lceil \log(nrow(CM_U)) \rceil$ (здесь $\lceil x \rceil$ — наименьшее целое, не меньшее x). Высокие нижние оценки сложности вероятностных вычислений могут быть получены тогда, когда CM_U имеет не только много разных строк, но также и подматрицу с небольшим количеством столбцов и большим количеством разных строк. Пусть A — множество значений переменных Алисы. Значения B переменных Боба называются контрольным множеством в том случае, если для любых разных $a, a' \in A$ существует набор $b \in B$ такой, что $f(a; b) \neq f(a'; b)$. Мощность минимального контрольного множества обозначим через $ts(CM_U)$.

Важно рассматривать только вычисления h_n^b, когда Алиса получает значения из A_b. Из определения 2 получаем, что соответствующая частичная функция имеет коммуникационную

матрицу CM с $nrow(CM) = k_A$ и $ts(CM) \le k_3$. Из теоремы 1 следует, что $(1-\varepsilon)$-вероятностная, односторонняя коммуникационная сложность (и, следовательно, $\log|Q|$) не меньше, чем

$$\log(k_A) - k_3 H(1-\varepsilon) - 1. \qquad (1)$$

$OBDD$ с уровнем (т. е. множеством вершин, равноудаленных от начальной) мощности t имеет не менее $t-1$ неэквивалентных узлов на предыдущих уровнях и по меньшей мере $\sqrt{t}$ на последующих. Поэтому сложность P не может быть менее, чем $2|Q| \ge 2^{\log(k_A) - k_3 H(1-\varepsilon)} = \frac{k_A}{2^{k_3 H(1-\varepsilon)}}$. □

Чтобы описать функции, сложные для вероятностных $BP1(OBDD)$, усилим условия определения 2.

Определение 3. Пусть h_n – функция от n переменных. Будем называть эту функцию *сильно (k_2, k_3, k_A)-стабильной*, если любая подфункция, полученная из h_n для фиксированных значений $O(\log n)$ переменных, будет (k_2, k_3, k_A)-стабильной.

Следствие 1. Пусть h_n — сильно (k_2, k_3, k_A)-стабильная функция от n переменных с k_3 и k_A, удовлетворяющими теореме 2. Тогда существует константа $\delta' > 0$ такая, что для любого достаточно большого n вероятностная $BP1(OBDD)$, вычисляющая функцию h_n, имеет сложность не менее $2^{k_3\delta'}$.

Доказательство использует простую идею из [6]. Вероятностная $BP1(OBDD)$ P, вычисляющая функцию h_n, имеет подграф, соответствующий вероятностной $OBDD$ P, полученный в результате фиксирования тех значений $O(\log n)$ переменных, которые превращают P в $OBDD$. Вершины, соответствующие этим переменным вместе с недостижимыми частями графа, естественным образом удаляются. Все подфункции, получаемые из h_n заменой $O(\log n)$ переменных константами, являются $(k_2(n), k_3(n), k_A(n))$-стабильными функциями. Поэтому сложность полученного подграфа, а, следовательно, и P не менее $2^{k_3(n)\delta'}$ для некоторой константы $\delta' > 0$. □

Теорема 3. *Любая k-стабильная функция f для $k = \Omega(\log n)$ является сильно-$(k_1, k_1, 2^{k_1})$-стабильной функцией для любой целочисленной функции $k_1 = k_1(n)$ такой, что $k - k_1 = \Omega(\log n)$. Следовательно, для вычисления f требуется вероятностная $BP1(OBDD)$ сложности не менее $2^{k_1(n)\delta'}$ для некоторой константы $\delta' > 0$.*

Доказательство. Любая k-стабильная функция f является $(k, k, 2^k)$-стабильной функцией: с учетом определения 2 получим $X_1 = X$, $k_2 = k$, $X_2 = X_3$, и $A = 2^{X_3}$, т. е. A — множество всевозможных наборов значений переменных из X_3. Другими словами, в коммуникационной матрице, соответствующей любому разбиению U переменных X такому, что Алиса получает значения k переменных из X, существует $2^k \times k$-подматрица CM', строки которой образуют множество всех двоичных векторов длины k. Если функция $k = \Omega(\log n)$, то k растет быстрее, чем любая функция из $O(\log n)$. Фиксирование значений любых $k_2 = O(\log n)$ переменных из X определяет подфункцию f^b на $n - k_2$ переменных со следующим свойством. Коммуникационное вычисление f, определенное выше, соответствует коммуникационному вычислению f^b, при котором Алиса получает значения не менее $k_1 = k - k_2$ переменных из X. Коммуникационная матрица, соответствующая этому вычислению, содержит $2^{k_1} \times k_1$-подматрицу CM', строки которой образуют множество всех двоичных векторов длины k_1. Следовательно, f^b — $(k_1, k_1, 2^{k_1})$-стабильная функция. □

3. Функции, сложные для вероятностных $BP1$ с большой упорядоченной частью

Итак, любая k-стабильная функция f при $k = \Omega(\log n)$ сложна для вероятностных $BP1(OBDD)$. Но и для функций, не являющихся k-стабильными, удается исследовать их сложность для вероятностных вычислений.

В этом параграфе рассматриваются четыре функции, которые не являются k-стабильными. В [11], [3], [12] и [13] получены экспоненциальные нижние оценки сложности бинарных программ

(различных типов), вычисляющих эти функции. В [14] было доказано, что эти функции сложны для вероятностных $OBDD$. Введеное в данной работе определение стабильности позволяет получить более прямое доказательство этих результатов.

Исследуем, удовлетворяют ли определениям 2 и 3 следующие функции.

1) Функция HWB_n ("скрытый взвешенный бит") на множестве переменных $X = \{x_1, ..., x_n\}$ определяется как $HWB_n(x) = x_j$, если $j = \sum\limits_{i=1}^{n} x_i > 0$; и $HWB_n(x) = 0$ иначе [11].

Лемма 1. *Функция HWB_n является $(0.6n, 0.2n, \binom{0.2n}{0.1n})$-стабильной относительно X и сильно $(0.6n - t, 0.2n - t, \binom{0.2n-t/2}{0.1n-t})$-стабильной для любого $t = \Omega(\log n)$.*

Доказательство. $(0.6n, 0.2n, \binom{0.2n}{0.1n})$-стабильность HWB_n является следствием ее сильной стабильности, доказательство которой основано на идеях [11]. Зафиксируем значения b' переменных некоторого подмножества $X' \subset X$, $t' = |X'| = O(\log n) < t$. Пусть b' содержит t_1 единиц, $0 \le t_1 \le t'$, и $X_1 = X \setminus X'$. Рассмотрим множество X_2, содержащее $0.6n - t$ элементов из X_1. Пусть $X_L = \{x_{0.1n+1}, \ldots, x_{0.5n}\}$, $X_H = \{x_{0.5n+1}, \ldots, x_{0.9n}\}$. Тогда можно выделить подмножество X_3 мощности $0.2n - \frac{t}{2}$, где либо $X_3 \subseteq X_L \cap X_2$, либо $X_3 \subseteq X_H \cap X_2$. Предполагая, что переменные X_3 читаются в бинарной программе P перед чтением других переменных, оценим сложность P.

Для случая $X_3 \subseteq X_L \cap X_2$ определим значения b переменных из $X_2 \setminus X_3$ и наборы A_b значений X_3 так, что b содержит только нули и A_b содержит $0.1n - t_1$ единиц. Итак, $(a; b; b')$ содержит 0.1 единиц для любого $a \in A_b$ и $|A_b| = \binom{0.2n-t/2}{0.1n-t_1}$. Так как $X_3 \subset X_L$ и $|X_1 \setminus X_2| = 0.4n$, то можно найти значение c_x для $X_1 \setminus X_2$ (из определения 2) для любой переменной $x \in X_3$ так, что

$$HWB_n(a; b; b'; c_x) = x. \tag{2}$$

Для случая $X_3 \subseteq X_H \cap X_2$ определим значения b переменных из $X_2 \setminus X_3$ и наборы A_b значений X_3 так, что b содержит только единицы, A_b содержит $0.1n - t_1 + t/2$ единиц. Поскольку $|X_2 \setminus X_3| = 0.4n - t/2$, то $(a; b; b')$ содержит 0.5 единиц для любого $a \in A_b$ и $|A_b| = \binom{0.2n-t/2}{0.1n-t_1+t/2}$. Так как $X_3 \subset X_H$, то можно найти значение c_x для $X_1 \setminus X_2$ для любого $x \in X_3$. Уравнение (2) снова выполняется.

В обоих случаях $|A_b| \ge \binom{0.2n-t/2}{0.1n-t}$. $\square$

2) Пусть $p[n]$ – наименьшее простое число не меньше n. Для любого целого s функция $\omega_n(s)$ определяется следующим образом. Если $1 \le s \pmod{p[n]} \le n$, то $\omega_n(s) = s \pmod{p[n]}$, в противном случае $\omega_n(s) = 1$. Функция $SZHWB_n$ ("скрытый взвешенный бит Савицкого и Жака" [15]) на множестве переменных $X = \{x_1, \ldots, x_n\}$ определяется следующим образом: для каждого $x \in \{0,1\}^n$ $SZHWB_n(x) = x_j$, где $j = \omega_n\Big(\sum\limits_{i=1}^{n} i x_i\Big)$.

Лемма 2. *Для каждого достаточно большого n функция $SZHWB_n$ является $(n - 3\sqrt{n}, n - 3\sqrt{n}, 2^{n-3\sqrt{n}}/n)$-стабильной относительно X и сильно $(n - 3\sqrt{n} - t, n - 3\sqrt{n} - t, 2^{n-3\sqrt{n}-t}/n)$-стабильной для любого $t = \Omega(\log n)$.*

Доказательство. Докажем только сильную стабильность $SZHWB_n$, опираясь на доказательство [3]. Из сильной стабильности функции следует ее $(n - 3\sqrt{n}, n - 3\sqrt{n}, 2^{n-3\sqrt{n}}/n)$-стабильность. В соответствии с [15] воспользуемся следующей теоремой для остаточного класса по модулю p, обозначенного как Z_p.

Теорема 4 ([16]). *Пусть p — простое число, а k и h — целые числа, $h \le k \le p$. Пусть $A \subseteq Z_p$, $|A| = k$. Если B — множество всех сумм из h различных элементов A, то*

$$|B| \ge \min(p, hk - h^2 + 1).$$

Рассмотрим эту теорему в интерпретации [15], см. также [3].

Следствие 2. Для любого достаточно большого n, если $A \subseteq Z_{p[n]}$ и $|A| \ge 3\sqrt{n}$, то для каждого $t \in Z_{p[n]}$ существует подмножество $B \subset A$ такое, что сумма элементов B равна t.

Это утверждение следует из предыдущей теоремы при $k = \lceil 3\sqrt{n}\,\rceil$, $h = \lfloor \frac{k}{2} \rfloor$, т. к. $p[n] = n + o(n)$. Зафиксируем значения b' переменных некоторого подмножества $X' \subset X$, $t' = |X'| = O(\log n) < t$. Пусть $t_1 = \omega_n\Big(\sum\limits_{x_i \in X'} i x_i\Big)$ и $X_1 = X \backslash X'$. Рассмотрим множество $X_3 = X_2$, содержащее $n - \lceil 3\sqrt{n}\,\rceil - t$ элементов из X_1. Разобьем множество возможных значений X_3 в соответствии со значением функции w_n на сумме взвешенных значений переменных из X_3:

$$A^{(k)} = \Big\{ a \,\Big|\, w_n\Big(\sum_{x_i \in X_3} i a(x_i) \Big) = k \Big\}.$$

Возьмем в качестве искомого множества A значений X_3 максимальное $A^{(s)}$ среди множеств $A^{(1)}, \ldots, A^{(n)}$. Заметим, что $|A| \geq \frac{2^{n - \lceil 3\sqrt{n}\,\rceil - t}}{n}$.

Из следствия 2 для любого $x_j \in X_3$ существуют такие значения c_{x_j} (из определения 2), что

$$j \equiv \Big(t_1 + s + w_n\Big(\sum_{x_i \in X_1 \backslash X_3} i c_{x_j}(x_i) \Big) \Big) \pmod{p[n]},$$

где c_{x_j} содержит ровно $h = \lfloor \frac{3\sqrt{n}}{2} \rfloor$ единиц. $\square$

3) Функция ACH_n ("Ахиллесова пята") определена на $n = 2r + \log r$ переменных $Y \cup Z \cup V$ ([17]):

$$ACH_n(y_0, \ldots, y_{r-1}, z_0, \ldots, z_{r-1}, v_0, \ldots, v_{\log r - 1}) = \begin{cases} \bigvee\limits_{0 \leq j \leq r-1} (y_j \wedge z_j), & |v| = 0; \\ \bigwedge\limits_{0 \leq j \leq r-1} (y_j \vee z_{j+|v|}), & |v| \neq 0, \end{cases}$$

где $|v|$ — целое число, двоичное представление которого равно $v = v_0 \ldots v_{\log r - 1}$, и сумма $j + |v|$ считается по модулю r.

Лемма 3. *Функция ACH_n является $(r, r/4, 2^{r/4})$-стабильной относительно $Y \cup Z$ и принадлежит P-BP1(OBDD).*

Доказательство. Опираемся на идеи [13]. С учетом определения 2 имеем $X_1 = Y \cup Z$. Если подмножество $X_2 \subset X_1$ состоит из r элементов, то можно найти подмножество $X_3' \subset X_2$ из $r/2$ переменных, принадлежащее либо Y, либо Z. Без потери общности считаем $X_3' \subseteq Y$. Далее можно найти подмножество $X_4' \subset Z \cap (X_1 \setminus X_2)$ из $r/2$ элементов. Так как подмножество $X_3' \times X_4'$ имеет мощность $r^2/4$, то оно содержит не менее $r/4$ пар (y_i, z_{i+j}) для некоторого значения j между 0 и $r - 1$. Переменные y_i и z_{i+j} в этих парах составляют X_3 и X_4 соответственно.

Определим значения переменных в соответствии с определением 2. Если $j = 0$, то $v' = 0$, иначе $v' = 1$. Подберем значение b так, что двоичное число $|b(v_0) \ldots b(v_{\log r - 1})| = j$ и любая переменная из $X_2 \setminus X_3$ эквивалентна v'. Пусть A_b — множество возможных значений X_3. Для любой переменной $x_k \in X_3$ значения c_{x_k} таковы, что $z_{i+j} = 1 - v'$ для $x_k = y_i$, все остальные переменные из X_4 и из $X_1 \setminus (X_2 \cup X_4)$ равны v'.

$BP1(OBDD)$, вычисляющая ACH_n, сначала читает $v_0 \ldots v_{\log r - 1}$, а затем пары $(y_i, z_{i+|v|})$ для i в диапазоне от 0 до $n - 1$. $\square$

4) Функция ISA_n ("непрямой доступ к хранилищу") определена на $n = 2^r + r$ переменных $X \cup Y = \{x_0, \ldots, x_{2^r - 1}\} \cup \{y_0, \ldots, y_{r-1}\}$ следующим образом [12]. Пусть двоичное число $y_0 \ldots y_{r-1}$ представляет число $i = |y_0 \ldots y_{r-1}|$. Если $i \geq \frac{2^r}{r}$, тогда ISA_n возвращает 0, иначе $ISA_n = x_j$, где $j = |x_{ir} \ldots x_{(i+1)r-1}|$.

Лемма 4. *Функция ISA_n является $(k, k, 2^k)$-стабильной относительно X для $k = \frac{2^r}{r} - 1$ и принадлежит P-BP1(OBDD).*

Доказательство. Напомним простые идеи [12]. Если $X_2 = X_3$ имеет мощность k, то найдется число $i < \frac{2^r}{r}$ такое, что $X_4 = \{x_{ir}, \ldots, x_{(i+1)r-1}\} \subset X_1 \setminus X_2$, $X = X_1$. Выберем значение b так, что $|b(y_0) \ldots b(y_{r-1})| = i$. Пусть A_b — множество всех возможных значений X_3. Для любой переменной $x_j \in X_3$ c_{x_j} устанавливает все переменные из $X \setminus (X_3 \cup X_4)$ равными нулю и все переменные из X_4 в соответствии с двоичным представлением j.

$BP1(OBDD)$ P, вычисляющая ISA, имеет следующий вид. Она сначала вычисляет число $i = |y_0 \ldots y_{r-1}|$. Если $i \geq \frac{2^r}{r}$, то программа переходит в отвергающую вершину. В противном случае P проверяет переменные $\{x_{ir}, \ldots, x_{(i+1)r-1}\}$ (соответствующее бинарное дерево имеет полиномиальный размер). Пусть значения переменных соответствуют двоичному представлению j. Если x_j еще не проверено P, то программа читает эту переменную, иначе выдается значение в соответствии с уже проверенной переменной. □

Теорема 5. $BPP\text{-}OBDD \subset BPP\text{-}BP1(OBDD) \subset BPP\text{-}BP1$.

Леммы 1–4 доказывают теорему, поскольку $ACH_n, ISA_n \in P\text{-}BP1(OBDD) \setminus BPP\text{-}OBDD$, $HWB_n \in P\text{-}BP1 \setminus BPP\text{-}BP1(OBDD)$ и $SZHWB_n \notin BPP\text{-}BP1(OBDD)$.

4. Умножение сложно для $BP1(OBDD)$

Определение 4. Пусть произведение двух n-битных двоичных чисел $x = x_{n-1} \ldots x_0$ и $y = y_{n-1} \ldots y_0$ равно $z = z_{2n-1} \ldots z_0$. Целочисленное умножение — это функция

$$MULT_n : MULT_n(x, y) = z_{n-1}.$$

Чтобы показать, что целочисленное умножение требует экспоненциальной сложности для вероятностных вычислений на $BP1(OBDD)$, потребуется

Лемма 5. *Пусть $r^{(n)}$ — целое число, двоичное представление которого имеет длину n и содержит $o(n)$ единиц и $\varepsilon \in (0, 1/2)$. Тогда вероятностная $OBDD$ $P_n(r^{(n)})$, читающая переменные, которые образуют два n-битных числа x и y, так, что x читается ранее, чем любой бит из y, и $(1-\varepsilon)$-вычисляющая, верно ли, что $|x| + |y| \geq 2^n - r^{(n)}$, имеет сложность больше, чем $a^{n/\log(n)}$ для некоторого $a > 1$ и достаточно большого n.*

Доказательство. Для определения нижней оценки сложности $P_n(r^{(n)})$ рассмотрим частичную функцию искомой функции. Пусть $x_i = y_i = 0$ для всех i таких, что $r_i^{(n)} = 1$. Остальные $l = n - o(n)$ бит x и y определяют числа x' и y'. Тогда сложность $P_n(r^{(n)})$ ограничена снизу сложностью $OBDD$, определяющей истинность $|x'| + |y'| \geq 2^l$. Соответствующая коммуникационная матрица CM размера $l \times l$, строки которой соответствуют x', а столбцы соответствуют y', является треугольной матрицей, у которой все элементы выше побочной диагонали равны нулю, а все элементы побочной диагонали и ниже ее единице. Утверждение леммы 5 получается с помощью следующей леммы.

Лемма 6. *Пусть коммуникационная матрица CM размера $l \times l$ является треугольной матрицей, у которой все элементы выше побочной диагонали равны нулю, а все элементы побочной диагонали и ниже ее равны единице. Пусть B_l — вероятностная $OBDD$, $(1-\varepsilon)$-вычисляющая функцию от $2l$ переменных, определяемую матрицей CM, причем переменные Алисы в B_l читаются перед переменными Боба. Тогда сложность B_l не менее, чем $a^{\frac{l}{\log(l)}}$ для некоторого $a > 1$ и достаточно большого l.*

Доказательство. Рассмотрим идеи [4] в интерпретации [18]. На основе B_l построим вероятностный односторонний коммуникационный протокол, позволяющий второму игроку (Бобу) определить входную последовательность первого игрока (Алисы) с малой вероятностью ошибки.

Алиса использует B_l на своих переменных t раз. Число t достаточно велико, чтобы сделать вероятность ошибки в конечном результате достаточно малой. Боб получает номера узлов $v_1, \ldots, v_t$, которых достигла Алиса. Он делает несколько предположений о значениях входной последовательности Алисы. Далее Боб проверяет свои предположения следующим образом. Сначала он фиксирует значения своих переменных соответственно среднему столбцу матрицы CM

(это и есть предположение о входе Алисы) и запускает B_l t раз, начиная с узлов $v_1, \ldots, v_t$. Если большинство результатов вычислений — нули, то Боб продолжает свои вычисления соответственно верхней правой четверти матрицы CM, иначе соответственно нижней левой четверти; т. е. Боб делает вывод, что Алиса получила на вход соответственно меньше или больше того числа, которое он подставил в качестве ее предполагаемого входа. Известно [19], что вероятность того, что его предположение неверно, не превышает $(c(\varepsilon))^t$ для некоторого фиксированного $c(\varepsilon) < 1$. Затем в соответствии со своим предположением Боб фиксирует значения своих переменных, определяемые средним столбцом подматрицы, и продолжает процедуру. Каждая такая фаза вычислений уменьшает размер матрицы CM в 2 раза. Так как исходный размер CM $2^l \times 2^l$, после l таких фаз у Боба остается лишь один столбец CM. Вероятность того, что вектор, соответствующий этому столбцу, равен входной последовательности Алисы, не менее $(1-(c(\varepsilon))^t)^l$. Для любого q такого, что $1/2 < q < 1$, если $t > \log_{c(\varepsilon)}(1-q^{1/l})$, то эта вероятность не менее q. Можно найти верхнюю оценку для t и показать, что при $t = O(\log l)$ приведенное ограничение на вероятность удовлетворяется.

Сравним $(1-(c(\varepsilon))^t)^l$ с выражением $(1-1/(bx))^x$, которое, монотонно возрастая, стремится к $(1/e)^{(1/b)}$. Выберем константу b такой, что $(1/e)^{(1/b)} > q$. Пусть $(c(\varepsilon))^t = 1/(bl)$, т. е. $t = \log_{1/c(\varepsilon)}(bl)$. Тогда для достаточно большого l Боб определяет входную последовательность первого игрока с вероятностью большей, чем q.

Пусть B_l имеет сложность не более $a^{\frac{l}{\log(l)}}$ для любого $a > 1$ и любого достаточно большого l. Любой узел v_i программы B_l может быть записан как двоичная последовательность $\log(a)\frac{l}{\log(l)}$ бит. Если $t = O(\log l)$, то для вычисления любой функции Алисе достаточно согласно указанной процедуре передать Бобу $\log a \frac{l}{\log l} O(\log l)$ бит. После этого Боб определяет вход Алисы с вероятностью более q и потом детерминированно вычисляет искомую функцию. Таким образом, односторонняя коммуникационная сложность вероятностных вычислений любой булевой функции $2l$ переменных ограничена сверху $\log a \frac{l}{\log l} O(\log l) \le a'l$ для любого $a' > 0$ и достаточно большого l, т. е. эта сложность всегда менее линейной. Это не так.

Рассмотрим такое коммуникационное вычисление для $SZHWB_n$-функции, $(n - 3\sqrt{n}, n - 3\sqrt{n}, 2^{n-3\sqrt{n}}/n)$-стабильной относительно $X = \{x_1, \ldots, x_n\}$ (лемма 2). В соответствии с (1) вероятностное одностороннее вычисление $SZHWB_n$ имеет сложность по меньшей мере $K = \log(k_A) - k_3 H(q) - 1 = n - 3\sqrt{n} - \log n - H(q)(n - 3\sqrt{n}) - 1$. Очевидно, $K > a'n$ для некоторого $a' > 0$ и достаточно большого n. Это противоречие доказывает справедливость леммы. □

Теорема 6. *Для любого $\varepsilon > 0$ вероятностная $BP1(OBDD)$ P_n, $(1-\varepsilon)$-вычисляющая $MULT_n$, имеет сложность больше, чем $a^{\frac{n}{\log^2(n)}}$ для некоторого $a > 1$ и достаточно большого n.*

В [6] показано следующее. Можно зафиксировать значения некоторых переменных так, что вычисление $MULT_n$ сводится к вычислению суммы двух чисел $x^{(1)}$ и $x^{(2)}$, а также некоторой константы r. Эта константа имеет не более $O(\log n)$ единиц, и определяется установкой этих $\log n$ бит из входящей последовательности P_n так, что P_n становится $OBDD$. Число $x^{(1)}$ читается до любого бита числа $x^{(2)}$. Оба числа имеют $O(n/\log n)$ бит. Поэтому можно использовать лемму 5:

$$a^{\frac{n/\log(n)}{\log(n/\log(n))}} a^{\frac{n}{\log(n)(\log(n)-\log(\log(n)))}} > a^{\frac{n}{\log^2(n)}}. \quad \square$$

Литература

1. Wegener I. *Branching programs and binary desicion diagrams*: *theory and applications.* – SIAM Monographs on Discrete Math. and Appl. – Philadelphia, USA, 2000. – 408 p.
2. 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.
3. Ablayev F. *Randomization and nondeterminism are incomparable for ordered read-once branching programs* // Proc. ICALP'97, LNCS 1256, Springer. – 1997. – P. 195–202.
4. Ablayev F., Karpinski M. *A lower bound for integer multiplication on randomized read-once branching programs* // Electron. Colloq. on Comput. Compl., Trier University, Trier. – ECCC TR98-011, 1998, `http://www.eccc.uni-trier.de/ECCC`

5. Sauerhoff M. *Lower bounds for randomized read-k-times branching programs* // Proc. STACS'98, LNCS 1373, Springer. – 1998. – P. 105–115.
6. Bollig B. *Restricted nondeterministic read-once branching programs and an exponential lower bound for integer multiplication* // RAIRO Theoret. Inform. Appl. – 2001. – V. 35. – P. 149–162.
7. Gergov J., Meinel C. *Efficient Boolean manipulation with OBDDs can be extended to FBDDs* // IEEE Transac. Comput. – 1994. – V. 43. – № 10. – P. 1197–1209.
8. Sieling D., Wegener I. *Graph driven BDDs — a new data structure for Boolean functions* // Theoret. Comput. Sci. – 1995. – V. 141. – P. 283–310.
9. Jukna S. *Entropy of contact circuits and lower bounds on their complexity* // Theoret. Comput. Sci. – 1988. – V. 57. – P. 113–129.
10. Jukna S., Razborov A.,Savicky P., Wegener I. *On P versus $NP \cap co\text{-}NP$ for decision trees and read-once branching programs* // Comput. Compl. – 1999. – V. 8. – P. 357–370.
11. Bryant R. E. *On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication* // IEEE Trans. Comput. – 1991. – V. C-40. – № 2. – P. 205–213.
12. Breitbard Y., Hunt III H.B., Rosenkratz D. *On the size of binary decision diagrams representing Boolean functions* // Theoret. Comput. Sci. – 1995. – V. 145. – P. 45–69.
13. Ponzio S. *A lower bound for integer multiplication with read-once branching programs* // Proc. 27-th STOC. – V. 1995. – P. 130–139.
14. Karpinski M., Mubarakzjanov R. *Some separation problems on randomized OBDDs* // Proc. of the International Workshop on Computer Science and Information Technologies, CSIT'99, Moscow, Russia. – 1999. – `http://msu.jurinfor.ru/CSIT99/`
15. Savicky P., Zak S. *A hierarchy for $(1, +k)$-branching programs with respect to k* // Proc. MFCS'97, LNCS 1295. – 1997. – P. 478–487.
16. Dias J.A., Hamidoune Y.O. *Cyclic spaces for Grassmann derivatives and additive theory* // Bull. London Math. Soc. – 1994. – V. 26. – P. 140–146.
17. Bollig B., Sauerhoff M., Sieling D., Wegener I. *On the power of different types of restricted branching programs* // Electron. Colloq. on Comput. Compl., Trier University, Trier. – ECCC TR94-026, 1994, `http://www.eccc.uni-trier.de/ECCC`
18. Mubarakzjanov R. *On probabilistic OBDDs with constant width* // Proc. of the 2nd International Workshop on Computer Science and Information Technologies, CSIT'2000, Ufa, Russia. – Ufa: USATU Publisher, 2000. – V. 2. – P. 62–68.
19. Chernoff H. *A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations* // Ann. Math. Stat. – 1952. – V. 23. – P. 493–509.

Казанский государственный университет

Поступила 26.01.2005