

О КЛАССАХ СЛОЖНОСТИ, ОПРЕДЕЛЯЕМЫХ БИНАРНЫМИ ПРОГРАММАМИ ОГРАНИЧЕННОЙ ШИРИНЫ*)

Р. Г. Мубаракзянов

Рассматриваются классы сложности, образованные булевыми функциями, реализуемыми полиномиальными один раз читающими упорядоченными бинарными программами (OBDD в англоязычной литературе). Соотношения между классами, определяемыми вероятностными, детерминированными и недетерминированными OBDD, были доказаны ранее. В данной статье доказаны все соотношения между классами сложности, возникающими при рассмотрении OBDD, ширина которых ограничена константой, а также в том случае, когда связи между слоями фиксированы. Кроме того, определена функция, вычисляемая полиномиальной вероятностной OBDD, ширина которой ограничена константой и связи между слоями фиксированы. Эта функция не принадлежит классам BPP, NP, coNP в контексте OBDD.

Введение

В последние годы в теории сложности активно изучаются свойства бинарных программ. Это связано с тем, что такая модель вычислений представляет практический интерес, а также с тем, что в результате этих исследований удалось получить экспоненциальные нижние оценки и построить иерархии классов сложности. Соответствующие результаты были получены при рассмотрении различных ограничений, накладываемых на класс бинарных программ.

Дадим основные определения. Бинарной программой от переменных из X называется ориентированный ациклический граф с одной начальной вершиной, в котором каждая вершина помечена переменной из X . Имеются две конечные вершины, помеченные 0 и 1. Из каждой неконечной вершины выходят 2 дуги, помеченные 0 и 1. Если к этому определению детерминированной бинарной программы добавить возможность

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99-01-00163).

наличия недетерминированных вершин (т. е. не помеченных никакой переменной), или вероятностных вершин (т. е. помеченных случайными переменными y_i , принимающими значения 0 и 1 с вероятностью $1/2$), получим соответственно определения недетерминированной и вероятностной бинарной программы. При вычислении бинарная программа выдает пометку той вершины, к которой приводит путь из начальной вершины в соответствии со значениями переменных. Недетерминированная (вероятностная) программа, согласуясь с классическим подходом, вычисляет 1 тогда и только тогда, когда существует принимающее вычисление (вероятность принимающего вычисления не менее фиксированного порога). В [5] показано, что без ограничения общности значение порога вероятностного вычисления можно принять равным $1/2$. Важно также выделить подкласс вероятностных вычислений, которые будем называть *рандомизированными*. Для них существует положительная константа ε (характеризующая ошибку вычисления) такая, что при любых значениях аргументов вероятность правильного значения вычисляемой функции не менее $1/2 + \varepsilon$.

Под *сложностью* бинарной программы понимается число ее вершин. Нас интересуют программы полиномиальной сложности. В дальнейшем, если не оговаривается противное, под бинарными программами будем понимать лишь программы полиномиальной сложности.

Так как не удастся получить высокие нижние оценки сложности для произвольных бинарных программ, в литературе рассматривались бинарные программы с различными ограничениями. Если принять во внимание, что наиболее общей моделью должно являться вероятностное вычисление (соответствующее классу сложности RP в классической теории сложности), то можно перечислить основные рассматриваемые ранее ограничения, накладываемые на вычисления.

1. Ограничения на ошибку вычисления и соответственно переход к вычислениям

- (a) рандомизированным (класс сложности BPP),
- (b) недетерминированным (NP, coNP),
- (c) детерминированным (P).

2. Количество считываний переменных (на каждом пути к конечной вершине любая переменная встречается не более определенного числа раз).

3. Упорядоченность считывания переменных (например, для один раз читающих переменных существует некоторый порядок чтения переменных $(x_{i_1} \dots x_{i_n})$ такой, что если переменная x_{i_j} читается перед x_{i_k} , то $j < k$).

4. Ширина бинарной программы.

Основной целью данной работы является исследование последнего ограничения, которое мы обсудим позже. Не принимая во внимание ограничение на ширину бинарной программы, заметим следующее. Если максимально ограничить класс бинарных программ на основе ограничений 2 и 3, получим класс упорядоченных один раз читающих бинарных программ, или OBDD. Переходя к ограничениям (или обобщениям относительно детерминированных OBDD) из п. 1, заметим, что в [5, 7] доказаны различные соотношения между классами сложности P, NP, coNP, BPP, PP, которые определены в контексте OBDD. В частности, показана несовместность классов NP, coNP, BPP. Итак, переходя от детерминированных к недетерминированным, либо рандомизированным, вычислениям, устанавливаем, что ни один из получаемых в результате обобщения более широкий класс сложности не поглощает другой.

Ниже будем рассматривать вычисление булевых функций, но для полноты изложения отметим, что в некоторых случаях экспоненциальные нижние оценки получаются проще при рассмотрении функций, аргументы которых заданы в алфавите мощности более 2. Так, в работе [2] рассматривалась функция, аргументы которой принимают 4 значения. Было показано, что эта функция вычислима рандомизированной полиномиальной OBDD, но сложна для недетерминированной один раз читающей бинарной программы (снято ограничение упорядочения). Но при перекодировании аргументов с целью получения булевой функции экспоненциальную оценку удалось установить лишь для детерминированных один раз читающих бинарных программ (обобщение на недетерминированный случай до сих пор не получено).

Рассмотрим последнее ограничение нашего списка: ограничение на ширину бинарной программы. Под *шириной* понимается максимальное число вершин слоя программы, представленной в слоевой форме, т. е. когда вершины программы разбиты на слои V_1, V_2, \dots так, что дуги из вершин слоя V_i ведут в V_{i+1} . Известно, что класс булевых функций, реализуемых полиномиальными бинарными программами, ширина которых ограничена константой, совпадает с $NC^1 / \text{poly}(n)$ — классом функций, реализуемых схемами из функциональных элементов логарифмической глубины [6]. Является ли это ограничение сужением класса булевых функций, реализуемых произвольными полиномиальными бинарными программами, т. е. класса, совпадающего с $\text{LogSpace} / \text{poly}(n)$, неизвестно.

Рассмотрим полиномиальные OBDD ограниченной ширины, получив таким образом наиболее узкий класс бинарных программ. Для краткости класс таких программ константной ширины обозначим через bwOBDD. Покажем следующее:

1) класс функций, характеристических для регулярных языков, является собственным подклассом множества функций, реализуемых bwOBDD с фиксированными переходами между слоями;

2) класс функций, реализуемых bwOBDD с фиксированными переходами между слоями, совпадает с классом функций, реализуемых недетерминированными и рандомизированными bwOBDD с фиксированными переходами между слоями;

3) класс функций, реализуемых детерминированными bwOBDD с фиксированными переходами между слоями, является собственным подклассом множества функций, реализуемых bwOBDD;

4) класс функций, реализуемых bwOBDD, совпадает с классом функций, реализуемых недетерминированными bwOBDD, и с классом функций, реализуемых рандомизированными bwOBDD;

5) класс функций, реализуемых детерминированными bwOBDD, является собственным подклассом множества функций, реализуемых OBDD;

6) класс функций, реализуемых детерминированными bwOBDD, является собственным подклассом множества функций, реализуемых вероятностными bwOBDD.

Более того, в данной работе доказывается, что вероятностные bwOBDD полиномиальной сложности с фиксированными переходами между слоями могут обладать «большими» возможностями даже по сравнению с недетерминированными (класс NP) и рандомизированными (BPP) полиномиальными OBDD.

1. Бинарные программы с фиксированными переходами между слоями

Прежде чем приступить к изложению, договоримся, что в каждом слое бинарной программы ограниченной ширины содержится одно и то же число вершин. Так как переход к такой форме возможен при добавлении фиктивных вершин (в том числе начальных и конечных), это не нарушает общности рассмотрения, но облегчает изложение.

Несложно обнаружить некоторую аналогию между вычислениями bwOBDD и при помощи конечного детерминированного автомата. При этом можно ограничить класс bwOBDD.

Перенумеруем вершины каждого слоя bwOBDD. Вершины, имеющие одинаковый номер, назовем *соответствующими*. Будем говорить, что bwOBDD имеет фиксированные переходы между слоями, если дуга (a, b) между первым и вторым слоем существует тогда и только тогда,

когда для любых двух соседних слоев существует дуга (a', b') , где a' соответствует a , а b' соответствует b , при этом пометки дуг (a, b) и (a', b') совпадают.

Теорема 1. *Класс функций, характеристических для регулярных языков, является собственным подклассом множества функций, реализуемых bwOBDD с фиксированными переходами между слоями.*

Доказательство. Вычисление на детерминированном автомате A можно реализовать OBDD ширины, равной количеству состояний, при чтении переменных в естественном порядке $1, 2, \dots, n$, где n — число аргументов функции. При этом переходы между любыми двумя соседними слоями одинаковы и соответствуют диаграмме автомата.

Для bwOBDD возможно чтение переменных в любом фиксированном порядке. Рассмотрим функцию $g(x_1, \dots, x_m, x_{m+1}, \dots, x_{2m})$, которая равна 1 тогда и только тогда, когда $x_i = x_{i+m}$, $1 \leq i \leq m$. Ясно, что эта функция может быть вычислена детерминированной bwOBDD ширины 3, читающей переменные в следующем порядке: $x_1, x_{1+m}, \dots, x_i, x_{i+m}, \dots, x_m, x_{2m}$. Вместе с тем g является характеристической функцией нерегулярного языка.

Если зафиксировать переходы между слоями, bwOBDD реализует работу детерминированного автомата, осуществляющего чтение букв входного слова в произвольном порядке. В связи с тем, что недетерминированные и вероятностные автоматы с изолированной точкой сечения допускают в точности регулярные языки, верно

Следствие 1. *Класс функций, реализуемых bwOBDD с фиксированными переходами между слоями, совпадает с классом функций, реализуемых недетерминированными и рандомизированными bwOBDD с фиксированными переходами между слоями.*

Ниже мы покажем, что класс реализуемых функций расширяется, если снять ограничение на ошибку вероятностного вычисления. Расширяется ли класс реализуемых функций, если не фиксировать переходы между слоями? Прежде чем ответить на этот вопрос, дадим

ОПРЕДЕЛЕНИЕ 1. Назовем bwOBDD B *регулярной*, если существуют такие константы l_1, l_2 , что переходы между слоями $V_{l_1+l_2i+j}$, $V_{l_1+l_2i+j+1}$ и $V_{l_1+l_2(i+1)+j}$, $V_{l_1+l_2(i+1)+j+1}$ одинаковы для любых i, j таких, что $0 \leq j < l_2$, $i \geq 0$ и $l_1 + l_2(i+1) + j + 1$ не превышает номера последнего слоя B .

Очевидна следующая

Лемма 1. *Любая регулярная bwOBDD B может быть преобразована в bwOBDD с фиксированными переходами между слоями, вычисляющую ту же функцию, что и B .*

Теперь можно сформулировать следующее утверждение.

Теорема 2. Множество функций, реализуемых регулярными недетерминированными bwOBDD, является собственным подклассом класса функций, реализуемых bwOBDD.

Доказательство. Рассмотрим функцию $g(x_1, \dots, x_m)$, которая равна 1 тогда и только тогда, когда аргументы в позициях $\lfloor \sqrt{m} \rfloor i$, $i = 1, 2, \dots$, равны 1, а остальные аргументы равны 0. Очевидно, что эта функция может быть вычислена детерминированной bwOBDD ширины 2, читающей переменные в порядке x_1, \dots, x_m . При этом осуществляется переход к конечной 1-вершине, если читается префикс слова, на котором функция равна 1. В остальных случаях осуществляется переход в вершину, соответствующую конечной 0-вершине.

Пусть g вычислима регулярной недетерминированной bwOBDD. Тогда в соответствии с леммой 2 и следствием 1 функция g вычислима детерминированной bwOBDD B с фиксированными переходами между слоями. Пусть B имеет ширину t . Программа B читает переменные в порядке x_{i_1}, \dots, x_{i_m} . Будем считать, что $m = n^2, t^3 + 2t < n$.

Согласно определению функции g существует единственное слово $v = x_{i_1} \dots x_{i_m}$, которое помечает путь, ведущий в конечную 1-вершину, причем длина этого пути равна m . Слово $v' = x_{i_1} \dots x_{i_m}$ получено из v при изменении порядка букв в соответствии с порядком считывания B . Чтобы получить противоречие с предположением, выделим в v' подслово u , содержащее 1, при этом u «соединяет» в B пары соответствующих вершин. В оставшейся части v найдем подслово w , содержащее лишь нули, также «соединяющее» в B пары соответствующих вершин, причем это «соединение» осуществляется такое число раз, что если удалить подслово w из v' и продублировать u необходимое число раз, длина слова v' не изменится. Полученное слово также будет допустимым для B , хотя в нем имеется более n единиц, что противоречит предположению.

Рассмотрим вершины, в которые попадает B перед прочтением очередной 1 (число которых равно n). Среди этих состояний найдется подмножество состояний, соответствующих друг другу, мощности не менее n/t . Пусть j является номером этих состояний. Следовательно, существует подслово u слова $v' = u'uu''$ длины $s \leq m/(n/t) = tn$. При этом слово u содержит хотя бы одну 1, а вершины B после прочтения u' , $u'u$ имеют номер j .

В словах u' и u'' выделим максимальные подслова w_i , состоящие из одних нулей: $w_1, w_2 \dots w_{n'}, n' \leq n + 2, w_i = 0^{k_i}$. При прочтении любого такого подслова длины более t в программе B осуществляется «циклический» переход по соответствующим вершинам: если $|w_i| > t$, то

найдутся такие числа $t'_i, t''_i, t'_i + t''_i \leq t$, $w_i = w'_i(w''_i)^{l_i}$, $|w'_i| = t'_i$, $|w''_i| = t''_i$, что после прочтения слов $w'_i(w''_i)^{l_1}$, $w'_i(w''_i)^{l_2}$, $0 \leq l_1, l_2 \leq l$, программа B переходит в пару соответствующих вершин. Подслова w''_i образуют «циклы». Подсчитаем число таких циклов длины $1, 2, \dots, t$. Каждый цикл содержит не менее

$$m - s - (n - 1) - (n + 2)(t - 1) \geq m - 2nt - 2t + 3$$

символов, ибо $|u'u''| = m - s$, $\sum_{i=1, n'} t'_i \leq (n + 2)(t - 1)$ и в слове $u'u''$ содержится не более $n - 1$ единиц.

Так как не существует цикла длины более t , то существует число $t'' \leq t$ такое, что во всех циклах длины t'' содержится не менее $(m - 2nt - 2t + 3)/t = (m + 3)/t - 2n - 2$ символов. Следовательно, число таких циклов в слове v' не менее $((m + 3)/t - 2n - 2)/t''$.

Преобразуем v' следующим образом. Удалим из него s циклов длины t'' : это возможно, так как $s \leq tn \leq ((n^2 + 3)/t - 2n - 2)/t''$ (последнее неравенство верно, так как $t^3 + 2t < n$). При этом будут удалены лишь нули. Продублируем слово u еще t'' раз. В результате длина слова v' не изменится, не изменится и вершина, в которую придет программа B по прочтении нового слова v'' , т. е. v'' допускается. Однако в v'' содержится по крайней мере на t'' больше единиц, чем в v' , что противоречит определению вычисляемой функции g .

Следствие 2. Класс функций, реализуемых bwOBDD, совпадает с классом функций, реализуемых недетерминированными bwOBDD, и с классом функций, реализуемых рандомизированными bwOBDD.

Справедливость следствия 2 объясняется теми же соображениями, которые приводились перед формулировкой следствия 1.

Теорема 3. Множество функций, реализуемых детерминированными bwOBDD, является собственным подклассом класса функций, реализуемых OBDD.

Доказательство. Рассмотрим функцию $g(x_1, \dots, x_{2m})$, которая равна 1 тогда и только тогда, когда $x_1 + x_2 + \dots + x_{2m} = m$.

OBDD, вычисляющая эту функцию, читает переменные в естественном порядке и подсчитывает разницу между числом единиц и нулей. Несложно видеть, что функция может быть вычислена OBDD сложности $(m + 1)^2 + m$ и максимальной ширины $m + 1$. В то же время OBDD, имеющая ширину, меньшую $m + 1$, не может вычислять g . Действительно, пусть это не так и существует соответствующая программа B . Рассмотрим слой в B после прочтения m переменных. Разница между количеством нулей и единиц среди прочитанных переменных может быть

равна $m, m-2, \dots, 2-m, -m$, т. е. имеется $m+1$ возможность. Так как B имеет ширину не более чем m , то существует 2 набора значений переменных с разной разницей между числом нулей и единиц среди m аргументов, прочитанных первыми. В процессе чтения этих наборов после m -го аргумента программа попадает в одну и ту же вершину. Несложно убедиться, что получаем противоречие с предположением.

2. Вероятностные программы ограниченной ширины

Чтобы доказать последний пункт из перечисленных соотношений между классами сложности, а именно, что класс функций, реализуемых детерминированными bwOBDD, является собственным подклассом множества функций, реализуемых вероятностными bwOBDD, покажем следующее. Существует функция, не вычислимая полиномиальными недетерминированными (рандомизированными) OBDD, т. е. программа без ограничений на ширину. Эта функция вычислима вероятностной bwOBDD с фиксированными переходами.

Необходимая нам функция GE_n не менее чем от $n = 4l$ переменных строится по функции f_n из [3]. Нечетные аргументы функции назовем типовыми, а четные — значащими. Скажем, что бит x_i , $i \in \{2, 4, \dots, 4l\}$, имеет тип 0 (1), если соответствующий нечетный бит x_{i-1} равен 0 (1). Обозначим через \mathbf{x}^0 (\mathbf{x}^1) подпоследовательность $\mathbf{x} \in \{0, 1\}^{4l}$, состоящую из всех четных битов типа 0 (1). Тогда $GE_n(\mathbf{x}) = 1$ тогда и только тогда, когда

- 1) либо все типовые переменные равны 1, а все значащие равны 0,
- 2) либо \mathbf{x} имеет не менее одного бита типа 1 и не менее одного бита типа 0 и $0, \mathbf{x}^0 \geq 0, \mathbf{x}^1$, где $0, \mathbf{y}$ — дробь в двоичной системе счисления.

Теорема 4. Функция GE_{4l} может быть вычислена вероятностной OBDD ширины 2^3 с фиксированными переходами между слоями. Любая недетерминированная или рандомизированная OBDD, вычисляющая GE_{4l} или ее отрицание, имеет экспоненциальный размер.

Доказательство. Рассмотрим следующую бинарную вероятностную программу B_n от n переменных. Она имеет слоевую форму. Начальная вершина соответствует случайной переменной и определяет 0-й слой. Первый слой содержит вершины a_0^1, a_2^1 , помеченные переменной x_n . Второй слой содержит две вероятностные вершины a_0^2, a_1^2 . Дуги (a_0^1, a_0^2) и (a_2^1, a_0^2) помечены нулем, а дуги (a_0^1, a_1^2) и (a_2^1, a_1^2) помечены

единицей. Программа B_n имеет регулярную структуру. Каждый четный слой имеет две случайные вершины a_0^{2k}, a_1^{2k} , $k = 1, 2, \dots, n-1$. Нечетный слой с номером $2k+1$, $k = 1, 2, \dots, n-1$, имеет три вершины: $a_0^{2k+1}, a_1^{2k+1}, a_2^{2k+1}$, $k = 1, \dots, n-1$. Конечная вершина a_1^{2n} помечена единицей, а вершина a_0^{2n} помечена нулем. Дуги (a_i^j, a_i^{j+1}) , где $i = 0, 1$ и $j = 2, 3, \dots, 2n-1$, и дуги (a_2^{2k+1}, a_0^{2k+2}) при $k = 1, 2, \dots, n-1$ помечены нулем. Дуги (a_1^{2k}, a_2^{2k+1}) , где $i = 0, 1$ и $k = 1, 2, \dots, n-1$, дуги (a_i^{2k+1}, a_i^{2k+2}) , где $i = 0, 1$ и $k = 1, 2, \dots, n-1$, и дуги (a_2^{2k+1}, a_1^{2k+2}) при $k = 1, 2, \dots, n-1$ помечены единицей.

Для удобства дальнейшего рассмотрения «регулярность» данной бинарной программы распространим на первые два слоя, добавив вершины a_1^0 и a_1^1 вместе с соответствующими дугами, выходящими из них.

Приведенная бинарная программа является новым представлением известного автомата Рабина [8] (см. также [1]). Легко видеть, что на слове $x_1 x_2 \dots x_n = \sigma_1 \sigma_2 \dots \sigma_n$ вероятность достижения конечной 1-вершины программой B_n следующая. Представление этой вероятности в двоичной системе счисления есть $0, \sigma_1 \sigma_2 \dots \sigma_n$. Пусть B'_n совпадает с B_n за исключением того, что пометки конечных вершин меняются местами.

Чтобы определить бинарную программу $B(GE_{4l})$ для вычисления GE_{4l} , программе B_{2l} (B'_{2l}) поставим в соответствие такую программу C_{4l} (C'_{4l}), которая работает на четных битах типа 0 (1). Если нет четного бита типа 0 (1), то C_{4l} (C'_{4l}) не достигнет конечной 1-вершины. Начальной вершиной программы $B(GE_{4l})$ является случайная вершина, из которой дуги ведут в начальные вершины C_{3l} и C'_{3l} .

Более подробно опишем структуру программы C_{4l} . Сначала она читает типовой бит x_{4l-1} , затем x_{4l-3} , затем x_{4l-5} и т. д. Если все биты равны 1, то бинарная программа приходит в конечную 0-вершину. Параллельно этим проверкам осуществляется построение слоев программы, соответствующей B_{2l} . Дуга, помеченная 0 и выходящая из вершины, помеченной $x_{4l-2t+1} = 0$ для некоторого t , $1 \leq t \leq 2l$, направлена в вершину программы, которая соответствует вершине a_0^{t-1} программы B_{2l} . В этой части проверяется четный бит, соответствующий прочитанному перед этим типовому биту, равному 0. Работа осуществляется в соответствии с B_{2l} . Затем последовательно читаются типовые биты. Если значение типового бита равно 1, соответствующий четный бит игнорируется.

Чтобы перевести C_{4l} в слоевую форму (которая отсутствует в связи с типовыми битами, равными 1), в программу можно добавить «фиктивные» вершины: после тестирования типового бита при равенстве его 1 осуществляется переход в случайную вершину, из которой

происходит переход на тестирование соответствующего четного бита (с переходом в одну вершину). После такого преобразования C_{4l} будет иметь ширину 6: первая вершина слоя осуществляет «поиск» типового бита, равного 0. После его нахождения возникают две параллели «фиктивных» вычислений, призванные хранить информацию о номере слоя, в котором закончилась работа в соответствии с B_{2l} .

Таким образом, $B(GE_{4l})$ имеет ширину 12. Причем данная bwOBDD регулярна и в соответствии с леммой 2 может быть преобразована в bwOBDD с фиксированными переходами между слоями. Для краткости не будем приводить подробности этого построения. Отметим лишь, что при таком преобразовании части C_{4l} и C_{4l} преобразуются в программы ширины 14, а ширина всей программы станет равной 29: 29-я вершина соответствует начальной вершине исходной программы.

Если переменные не содержат битов типа 1, то в части C_{4l} программы $B(GE_{4l})$ вероятность достижения конечной 0-вершины строго больше 0, а в части C'_{4l} детерминировано достигается 0-вершина. Таким образом, в этом случае вычисление программой $B(GE_{4l})$ закончилось в конечной 1-вершине с вероятностью строго меньше $1/2$. Если все типовые переменные равны 1, то в части C'_{4l} программы $B(GE_{4l})$ вероятность достижения конечной 0-вершины строго больше 0 тогда и только тогда, когда хотя бы один значащий бит равен 1, а в части C_{4l} детерминировано достигается 0-вершина. Таким образом, в этом случае вся программа $B(GE_{4l})$ достигнет конечной 1-вершины с вероятностью строго меньше $1/2$, за исключением случая, когда все типовые переменные равны 1, а все значащие — 0.

Пусть $x_1, \dots, x_k, y_1, \dots, y_t, k + t = 2l$, четные биты типа 0 и 1 соответственно. Тогда вероятность того, что $B(GE_{4l})$ достигнет конечной 1-вершины, равна

$$1/2(0, x_1 \dots x_k + 1 - 0, y_1 \dots y_t).$$

Эта вероятность не меньше $1/2$ тогда и только тогда, когда $0, x_1 \dots x_k \geq 0, y_1 \dots y_t$.

При получении экспоненциальной нижней оценки сложности недетерминированной OBDD B' , вычисляющей GE_{4l} , воспользуемся идеей, изложенной, например, в [5]. Пусть B' читает переменные в порядке τ . Обозначим через $\tau^0 = \{i_1, i_2, \dots, i_l\}$ подпоследовательность τ , содержащую первые l четных битов τ . Соответственно через $\tau^1 = \{j_1, j_2, \dots, j_l\}$ обозначим подпоследовательность τ , содержащую последние l четных битов τ .

Слово $\bar{\sigma} \in f_n^{-1}(1)$ назовем τ -сложным, если все четные биты σ_i , $i \in \tau^0$, имеют «тип» 0, а все четные биты σ_j , $j \in \tau^1$, имеют «тип» 1.

Обозначим

$$X^\tau = \{\bar{\sigma} \in \{0, 1\}^{4l} \mid \sigma^0 = \sigma^1, \bar{\sigma} \text{ } \tau\text{-сложно}\}.$$

Рассмотрим часть B'' программы B' , соответствующую путям, порожденным множеством X^τ . Пусть Q — множество вершин B'' , когда прочитано в точности l четных битов. Множество слов X^τ , с равными прочитанными l значащими битами, соответствует одной вершине из Q , а если прочитанные l значащих битов разные, то соответствующие вершины Q различны. Следовательно, мощность множества Q не менее 2^l .

При доказательстве высокой нижней оценки сложности рандомизированной OBDD B'' , вычисляющей функцию GE_{4l} , используем идею [4]. Если B'' имеет порядок чтения переменных τ , опять рассмотрим множество X^τ . Рассмотрим вычисление на этом множестве функции GE_{4l} двумя вычислителями. Первый вычислитель получает на вход те переменные, которые читаются программой B'' до того момента, когда оказываются прочитанными первые l четных битов. Это множество переменных обозначим через X_1 . Коммуникационная матрица $CM(GE_{4l})$ порядка l для вычисления GE_{4l} на X^τ , строки которой соответствуют переменным из X_1 с четными индексами, а столбцы — переменным с четными индексами из $X \setminus X_1$, является треугольной булевой матрицей, т. е. в ней элементы над главной диагональю равны 0, а на диагонали и под ней равны 1. Те же соображения, что приведены в [4], доказывают экспоненциальную нижнюю оценку сложности B'' .

Автор выражает благодарность Ф. М. Аблаеву за полезное обсуждение результатов работы.

ЛИТЕРАТУРА

1. Трахтенброт Б. А., Барздинь Я. М. Конечные автоматы (поведение и синтез). М.: Наука, 1970.
2. Ablayev F., Karpinski M. On the power of randomized ordered branching programs // Univ. Bonn, 85181-CS. 1997.
3. Ablayev F., Karpinski M. On the power of randomized ordered branching programs // ECCC TR98-004, 1998, available at <http://www.ecc.uni-trier.de/eccc>.
4. Ablayev F., Karpinski M. A lower bound for integer multiplication on randomized read-once branching programs // ECCC TR98-011, 1998, available at <http://www.ecc.uni-trier.de/eccc>.
5. Ablayev F., Karpinski M., Mubarakzjanov R. On BPP versus $NP \cup coNP$ for ordered read-once branching programs // Proc. Randomized Algorithms. Brno, 1998.

6. **Barrington M.** Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 // J. Comput. Systems Sci. 1989. V. 38, N 1. P. 150–164.
7. **Karpinski M., Mubarakzjanov R.** Some separation problems on randomized OBDDs // Univ. Bonn, 85196-CS. 1998.
8. **Rabin M. O.** Probabilistic automata // Inform. and Control. 1963. V. 6, N 3. P. 230–245. (Рус. пер.: Кибернетический сборник. М.: Мир, 1964. Вып. 9. С. 123–141.)

Адрес автора:

Казанский

государственный университет,

ул. Кремлевская, 18,

420008 Казань, Россия.

E-mail: rustam@ksu.ru

Статья поступила

7 декабря 1999 г.