

УДК 519.7

## О ФУНКЦИЯХ, ВЫЧИСЛИМЫХ БУЛЕВЫМИ СХЕМАМИ ЛОГАРИФМИЧЕСКОЙ ГЛУБИНЫ И ВЕТВЯЩИМИСЯ ПРОГРАММАМИ СПЕЦИАЛЬНОГО ВИДА

*А. В. Васильев*

Д. М. Баррингтон доказал совпадение класса функций  $NC^1$ , реализуемых схемами из функциональных элементов логарифмической глубины, с классом функций, представимых ветвящимися программами BWBP константной ширины и полиномиальной длины. В статье уточняется структура ветвящихся программ, получаемых предложенным Баррингтоном методом. А именно, доказывается, что с помощью  $k$ -OBDD полиномиальной сложности и ширины 5 можно реализовать все функции из класса  $NC^1$  и только их. Это утверждение можно переформулировать следующим образом:  $\text{poly}(n)\text{-OBDD}_5 = NC^1$ .

### 1. Предварительные сведения

При описании результатов Баррингтона из [1] будем пользоваться монографией Вегенера [3]. Приведём определение стандартных ветвящихся программ.

#### 1.1. Стандартные ветвящиеся программы

**Определение 1.** Ветвящаяся программа (ВП) на множестве переменных  $X_n = \{x_1, \dots, x_n\}$  — это ориентированный ациклический граф  $G = (V, E)$ , состоящий из выделенной начальной вершины, внутренних вершин, помеченных переменными из  $X_n$ , а также конечных вершин, помеченных константами из  $\{0, 1\}$ . Каждая внутренняя вершина имеет две исходящих дуги, помеченных 0 и 1 соответственно, начальная вершина не имеет входящих дуг, а у конечных вершин нет исходящих дуг. Вычисления начинаются из начальной вершины, также являющейся внутренней. При достижении внутренней вершины, помеченной переменной  $x_i$ , осуществляется переход по дуге, помеченной константой 0 (1), если  $i$ -й входной бит равен 0 (1). Вычисления заканчиваются по достижении одной из конечных вершин.

**Определение 2.** Говорят, что ветвящаяся программа  $G$  *вычисляет* функцию  $f \in B_n$ , если на входном наборе  $a = (a_1, \dots, a_n)$  вычисление, начинающееся из начальной вершины программы  $G$ , заканчивается в конечной вершине, помеченной  $f(a)$ .

**Определение 3.** *Сложностью* программы  $G$  называется величина  $\text{size}(G)$ , равная числу её внутренних вершин.

**Определение 4.** *Длиной (глубиной)* ветвящейся программы  $G$  называется величина  $\text{length}(G)$ , равная числу внутренних вершин на самом длинном пути в  $G$ .

**Определение 5.** Ветвящаяся программа называется *уровневой*, если для каждой вершины  $v$  и каждой конечной вершины  $w$ , достижимой из  $v$ , все пути от  $v$  до  $w$  имеют одинаковую длину.

**Определение 6.** *Шириной* уровневой ветвящейся программы  $G$  называется величина  $\text{width}(G)$ , равная максимальному числу вершин на уровне.

**Определение 7.**  $k$ -OBDD ( $k$ -BDD,  $k$  раз читающая OBDD) — это ветвящаяся программа, в которой на каждом пути из начальной вершины в конечную переменные считываются (используются в качестве меток вершин) не более  $k$  раз каждая, причём в порядке, представляющем собой  $k$ -кратное повторение порядка переменных  $(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \dots, x_{\pi^{-1}(n)})$ , где  $\pi$  есть некоторая подстановка индексов переменных.

## 1.2. Перестановочные ветвящиеся программы

Для формулировки доказываемой теоремы потребуется определение ветвящихся программ специального типа.

Пусть  $S_n$  — группа подстановок  $n$ -й степени с композицией подстановок в качестве групповой операции.

**Определение 8.** Подстановку  $\tau \in S_5$  назовём *5-циклом*, если  $\tau^i(j) \neq j$  для  $i \in \{1, \dots, 4\}$  и  $j \in \{1, \dots, 5\}$ , т. е. если  $\tau$  состоит из единственного цикла длины 5. Такие подстановки будем представлять строками вида  $(a_1 a_2 a_3 a_4 a_5)$ , где  $\tau(a_i) = a_{i+1}$  при  $i \leq 4$  и  $\tau(a_5) = a_1$ .

**Определение 9.** Перестановочную ветвящуюся программу (ПВП) ширины  $k$  и длины (или глубины)  $l$  будем задавать последовательностью инструкций вида  $\langle x_{j(i)}, g_i, h_i \rangle$ , где  $x_{j(i)}$  — переменная из  $\{x_1, \dots, x_n\}$ ,  $g_i, h_i \in S_k$  для всех  $i$ ,  $1 \leq i \leq l$ . На  $i$ -м уровне,  $1 \leq i \leq l + 1$ , такая ПВП содержит  $k$  вершин  $v_{i,1}, \dots, v_{i,k}$ . На уровне  $i = 1, \dots, l$  реализуется подстановка  $\sigma_i(x) = g_i$ , если  $x_{j(i)} = 0$ , в противном случае  $\sigma_i(x) = h_i$ , т. е.

для всех  $m$ ,  $1 \leq m \leq k$ , две дуги, помеченные 0 и 1, ориентированы из вершины  $v_{i,m}$  к вершинам  $v_{i+1,g_i(m)}$  и  $v_{i+1,h_i(m)}$  соответственно. Последний  $(l+1)$ -й уровень содержит конечные вершины, отображающие результаты вычислений. ПВП на входном наборе  $x$  вычисляет композицию подстановок  $\sigma(x) = \sigma_1(x)\sigma_2(x) \dots \sigma_l(x) \in S_k$ .

Обозначим через  $\text{id}$  тождественную подстановку.

**Определение 10.** Говорят, что ПВП вычисляет функцию  $f_n \in B_n$  посредством подстановки  $\tau$ , если  $\sigma(x) = \text{id}$  для  $x \in f_n^{-1}(0)$  и  $\sigma(x) = \tau \neq \text{id}$  для  $x \in f_n^{-1}(1)$ .

Следующая лемма устанавливает связь перестановочных и стандартных ветвящихся программ.

**Лемма 1.** Пусть  $G$  — перестановочная ветвящаяся программа ширины  $k$  и длины  $l$ , вычисляющая функцию  $f$ . Тогда существует стандартная ветвящаяся программа ширины  $k$  и длины  $kl$ , вычисляющая функцию  $f$ .

**ДОКАЗАТЕЛЬСТВО.** Для каждой из  $k$  вершин на первом уровне ПВП построим ветвящуюся программу ширины  $k$  и длины  $l$ : все вершины на уровне  $i$  помечаются переменной  $x_{j(i)}$ , а дуги, направленные на следующий уровень, соответствуют подстановкам  $g_i$  и  $h_i$ , т. е. ведут из вершины  $v_{i,m}$  к вершинам  $v_{i+1,g_i(m)}$  и  $v_{i+1,h_i(m)}$  соответственно. Вершины на последнем уровне заменяются конечными, а именно: в  $r$ -й ветвящейся программе  $\tau(r)$ -я вершина последнего уровня заменяется на 1, остальные — на 0. Полученная ветвящаяся программа вычисляет 1 тогда и только тогда, когда  $\sigma(x)(r) = \tau(r)$ . Таким образом,  $f(x) = 1$  тогда и только тогда, когда все построенные ветвящиеся программы вычисляют 1, т. е.  $\sigma(x) = \tau$ . Для получения конечного результата достаточно соединить ветвящиеся программы следующим образом: единичная конечная вершина  $r$ -й программы заменяется на начальную вершину  $(r+1)$ -й программы и так далее. Итоговая ветвящаяся программа сохраняет ширину  $k$ , а длина увеличивается до  $kl$ . Лемма 1 доказана.

### 1.3. Результаты Баррингтона

В данном подразделе приводится теорема Баррингтона, которая имитирует работу функционального элемента AND, используя коммутаторы подстановок. В результате для схемы из функциональных элементов глубины  $d$  индуктивно вырабатывается ПВП длины  $4^d$ , вычисляющая ту же функцию, что и исходная схема. Это означает, что для любой функции из  $\text{NC}^1$  существует ПВП полиномиальной длины, её вычисляющая.

Для доказательства теоремы Баррингтона потребуются некоторые вспомогательные утверждения.

**Лемма 2.** Если ПВП  $G$  вычисляет некоторую функцию  $f$  посредством 5-цикла  $\tau$ , а  $\rho$  — другой 5-цикл, то существует ПВП  $G'$  той же длины что и  $G$ , вычисляющая  $f$  посредством  $\rho$ .

ДОКАЗАТЕЛЬСТВО. Из элементарной теории групп следует существование такой подстановки  $v \in S_5$ , что  $\rho = v\tau v^{-1}$ . Непосредственная проверка показывает, что этому соотношению удовлетворяют подстановки вида

$$v = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ t_1 & t_2 & t_3 & t_4 & t_5 \end{pmatrix},$$

где  $(t_1 t_2 t_3 t_4 t_5)$  и  $(p_1 p_2 p_3 p_4 p_5)$  — циклические представления  $\tau$  и  $\rho$  соответственно.

Искомая ПВП  $G'$  получается из  $G$  заменой подстановок  $g_i$  и  $h_i$  в последовательности инструкций на  $vg_i v^{-1}$  и  $vh_i v^{-1}$  соответственно. В процессе выполнения  $G'$  вырабатывает подстановку

$$\sigma'(x) = v\sigma_1(x)v^{-1}v\sigma_2(x)v^{-1} \dots v\sigma_l(x)v^{-1} = v\sigma(x)v^{-1}.$$

Таким образом, выходные подстановки  $\text{id}$  и  $\tau$  заменяются на  $v \text{id} v^{-1} = \text{id}$  и  $v\tau v^{-1} = \rho$  соответственно. Лемма 2 доказана.

**Лемма 3.** Если ПВП  $G$  вычисляет некоторую функцию  $f$  посредством 5-цикла  $\tau$ , то существует ПВП  $G'$  той же длины, вычисляющая  $\neg f$  посредством  $\tau^{-1}$ , которая также является 5-циклом.

ДОКАЗАТЕЛЬСТВО. Очевидно, что  $\tau^{-1}$  является 5-циклом. Далее,  $G'$  получается из  $G$  заменой последней инструкции на  $\langle x_{j(l)}, g_l \tau^{-1}, h_l \tau^{-1} \rangle$ . В таком случае  $G'$  на входном наборе  $x$  вычисляет подстановку  $\sigma'(x) = \sigma(x)\tau^{-1}$ . Следовательно,  $\sigma'(x) = \tau^{-1}$  при  $x \in f^{-1}(0)$  и  $\sigma'(x) = \text{id}$  при  $x \in f^{-1}(1)$ . Таким образом,  $G'$  вычисляет  $\neg f$  посредством  $\tau^{-1}$ . Лемма 3 доказана.

**Лемма 4.** Существуют такие 5-циклы  $\tau_1$  и  $\tau_2$ , что подстановка  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$  является 5-циклом.

ДОКАЗАТЕЛЬСТВО.  $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5\ 4\ 2)(5\ 4\ 3\ 2\ 1)(2\ 4\ 5\ 3\ 1) = (1\ 3\ 2\ 5\ 4)$ .

**Теорема 1** [3]. Пусть функция  $f$  может быть представлена схемой из функциональных элементов  $S$  глубины  $d$  относительно базиса  $\{\wedge, \neq\}$ . Тогда существует ПВП  $G$  ширины 5 и длины  $4^d$ , вычисляющая  $f$  посредством некоторого 5-цикла.

ДОКАЗАТЕЛЬСТВО. Применим индукцию по глубине схемы  $d$ .

При  $d = 0$  функция  $f$  существенно зависит не более чем от одной переменной. Пусть  $f = x_k$ . В таком случае инструкция  $\langle x_k, \text{id}, \tau \rangle$ , где

$\tau$  — произвольный 5-цикл, будет искомой ПВП. В случае  $f = c = \text{const}$  такими ПВП будут  $\langle x_i, \text{id}, \text{id} \rangle$  при  $c = 0$  и  $\langle x_i, \tau, \tau \rangle$  при  $c = 1$  (для них выбор переменной  $x_i$  произволен).

Пусть предположение теоремы справедливо для всех  $l \leq d$ . Для индукционного шага предположим, что последним в  $S$  является элемент AND и  $f = f_1 \wedge f_2$  (по лемме 3 это не уменьшает общности, так как ПВП для  $\neg f$  можно легко получить из ПВП для  $f$ ). По индукционному предположению существуют ПВП  $G_1$  и  $G_2$  длины  $4^{d-1}$  каждая, вычисляющие  $f_1$  и  $f_2$  посредством 5-циклов  $\rho_1$  и  $\rho_2$  соответственно. Используя леммы 2 и 4, можно заменить их на  $\tau_1$  и  $\tau_2$ , для которых подстановка  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$  является 5-циклом. Более того, из леммы 2 также следует существование ПВП  $G_3$  и  $G_4$  длины  $4^{d-1}$  каждая, вычисляющих  $f_1$  и  $f_2$  посредством 5-циклов  $\tau_1^{-1}$  и  $\tau_2^{-1}$  соответственно. Последовательно соединяя  $G_1$ ,  $G_2$ ,  $G_3$  и  $G_4$ , получаем ПВП  $G$  длины  $4^d$ . Покажем, что она вычисляет функцию  $f$ .

Пусть на входном наборе  $x$  ПВП  $G$  вычисляет подстановку  $\sigma(x) = \sigma_1(x)\sigma_2(x)\sigma_3(x)\sigma_4(x)$ , где  $\sigma_i(x)$  — подстановка, вычисляемая ПВП  $G_i$  ( $i \in \{1, 2, 3, 4\}$ ) на входном наборе  $x$ . Возможны четыре случая:

- 1)  $f_1(x) = f_2(x) = 0$ . Следовательно,  $\sigma_1(x) = \dots = \sigma_4(x) = \text{id}$ . Поэтому  $\sigma(x) = \text{id}$ .
- 2)  $f_1(x) = 0, f_2(x) = 1$ . В таком случае  $\sigma_1(x) = \sigma_3(x) = \text{id}, \sigma_2(x) = \tau_2, \sigma_4 = \tau_2^{-1}$ . Поэтому  $\sigma(x) = \text{id}$ .
- 3)  $f_1(x) = 1, f_2(x) = 0$ . Тогда  $\sigma(x) = \text{id}$  (аналогично предыдущему случаю).
- 4)  $f_1(x) = 1, f_2(x) = 1$ . Здесь имеем  $\sigma(x) = \tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$ , которая является 5-циклом, а значит не равна  $\text{id}$ .

Таким образом,  $G$  вычисляет функцию  $f$ , имеет ширину 5 и длину  $4^d$ . Теорема 1 доказана.

**Замечание 1.** Отметим, что подстановка  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$ , называемая коммутатором подстановок  $\tau_1$  и  $\tau_2$ , ведёт себя точно так же, как моделируемый ею функциональный элемент AND: если хотя бы одна из подстановок  $\tau_1, \tau_2$  равна тождественной подстановке, то их коммутатор будет равен  $\text{id}$ , т. е. булевой константе 0 при интерпретации ПВП.

**Замечание 2.** Выбранная ширина 5 является в определённом смысле минимальной по следующим соображениям. Известно, что при  $n \geq 5$

группа  $S_n$  является неразрешимой, т. е. некоммутативной в очень сильном смысле. Если же использовать разрешимую группу, то на некотором шаге окажется, что невозможно выбрать пару некоммутирующих элементов группы, т. е. для любых доступных элементов  $\tau_1$  и  $\tau_2$  будет выполняться равенство  $\tau_1\tau_2 = \tau_2\tau_1$ , а значит, их коммутатор  $\tau_1\tau_2\tau_1^{-1}\tau_2^{-1}$  будет вырождаться в единичный элемент (тождественную подстановку). Таким образом, неразрешимость используемой группы обеспечивает возможность конструирования ПВП по методу Баррингтона.

**Пример.** В качестве примера построим ПВП для частного случая функции  $\text{MULT}_n^k$  при  $n = k = 2$ :

$$f(x_0, x_1, y_0, y_1) = \text{MULT}_2^2 = (\neg(x_0 \wedge y_0)) \wedge (x_1 \wedge y_1).$$

В общем случае функция  $\text{MULT}_n^k$  вычисляет  $k$ -й бит в произведении двух  $n$ -битных чисел, т. е.  $\text{MULT}_n^k = z_k$ , где  $z = z_{2n-1} \dots z_1 z_0$  и  $z = x \cdot y$ , а двоичные разложения  $x = x_{n-1} \dots x_1 x_0$  и  $y = y_{n-1} \dots y_1 y_0$  вместе образуют список аргументов функции  $\text{MULT}_n^k$ .

Используем обозначения  $\tau_1 = (1\ 2\ 3\ 4\ 5)$ ,  $\tau_2 = (1\ 3\ 5\ 4\ 2)$  из леммы 4.

- 1) Для элементарных функций  $x_0, x_1, y_0, y_1$  выберем, например, ПВП  $\langle x_1, \text{id}, \tau_1 \rangle$ ,  $\langle y_1, \text{id}, \tau_2 \rangle$ ,  $\langle x_0, \text{id}, \tau_1 \rangle$  и  $\langle y_0, \text{id}, \tau_2 \rangle$  соответственно.
- 2) Далее, объединим эти ПВП для представления функций  $x_1 \wedge y_1$  и  $x_0 \wedge y_0$ :

$$\begin{array}{ll} \langle x_1, \text{id}, \tau_1 \rangle & \langle x_0, \text{id}, \tau_1 \rangle \\ \langle y_1, \text{id}, \tau_2 \rangle & \langle y_0, \text{id}, \tau_2 \rangle \\ \langle x_1, \text{id}, \tau_1^{-1} \rangle & \langle x_0, \text{id}, \tau_1^{-1} \rangle \\ \langle y_1, \text{id}, \tau_2^{-1} \rangle & \langle y_0, \text{id}, \tau_2^{-1} \rangle. \end{array}$$

- 3) Пусть  $\tau = \tau_1\tau_2\tau_1^{-1}\tau_2^{-1} = (1\ 3\ 2\ 5\ 4)$ . Тогда  $\tau^{-1} = (4\ 5\ 2\ 3\ 1)$ . Согласно лемме 3 в этих обозначениях ПВП для  $\neg(x_0 \wedge y_0)$  имеет следующий вид:

$$\begin{array}{l} \langle x_0, \text{id}, \tau_1 \rangle \\ \langle y_0, \text{id}, \tau_2 \rangle \\ \langle x_0, \text{id}, \tau_1^{-1} \rangle \\ \langle y_0, \tau^{-1}, \tau_2^{-1}\tau^{-1} \rangle. \end{array}$$

- 4) Теперь преобразуем ПВП, вычисляющую  $x_1 \wedge y_1$  посредством  $\tau$ , так, чтобы она вычисляла данную функцию посредством подстановки

$\tau_1$ . Для этого сначала вычислим подстановку  $v$  такую, что  $\tau_1 = v\tau v^{-1}$ . По лемме 2 это может быть подстановка

$$v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

Замечая, что  $v = v^{-1}$ , или непосредственно вычисляя произведения подстановок, получаем:  $v\tau_1 v^{-1} = (1\ 3\ 2\ 5\ 4) = \tau$ ,  $v\tau_2 v^{-1} = (2\ 4\ 5\ 3\ 1) = \tau_2^{-1}$ ,  $v\tau_1^{-1} v^{-1} = (4\ 5\ 2\ 3\ 1) = \tau^{-1}$ ,  $v\tau_2^{-1} v^{-1} = (1\ 3\ 5\ 4\ 2) = \tau_2$ . Таким образом, по лемме 2 получаем, что ПВП

$$G_1 \begin{array}{l} \langle x_1, \text{id}, \tau \rangle \\ \langle y_1, \text{id}, \tau_2^{-1} \rangle \\ \langle x_1, \text{id}, \tau^{-1} \rangle \\ \langle y_1, \text{id}, \tau_2 \rangle \end{array}$$

вычисляет функцию  $x_1 \wedge y_1$  посредством подстановки  $\tau\tau_2^{-1}\tau^{-1}\tau_2 = \tau_1$ .

Введём дополнительные обозначения  $\tau_3 = (1\ 4\ 2\ 3\ 5)$ ,  $\tau_4 = (1\ 2\ 5\ 3\ 4)$ ,  $\tau_5 = (1\ 3\ 4\ 2\ 5)$  и аналогично получаем следующие ПВП:

$$\begin{array}{ccc} G_2 & \begin{array}{l} \langle x_0, \text{id}, \tau_3 \rangle \\ \langle y_0, \text{id}, \tau_4 \rangle \\ \langle x_0, \text{id}, \tau_3^{-1} \rangle \\ \langle y_0, \tau_2, \tau_1 \rangle \end{array} & G_3 \begin{array}{l} \langle x_1, \text{id}, \tau^{-1} \rangle \\ \langle y_1, \text{id}, \tau_3^{-1} \rangle \\ \langle x_1, \text{id}, \tau \rangle \\ \langle y_1, \text{id}, \tau_3 \rangle \end{array} & G_4 \begin{array}{l} \langle x_0, \text{id}, \tau_3^{-1} \rangle \\ \langle y_0, \text{id}, \tau_5 \rangle \\ \langle x_0, \text{id}, \tau_3 \rangle \\ \langle y_0, \tau_2^{-1}, \tau \rangle \end{array} \end{array},$$

где  $G_3$  вычисляет  $x_1 \wedge y_1$  посредством подстановки  $\tau^{-1}\tau_3^{-1}\tau\tau_3 = \tau_1^{-1}$ , а  $G_2$  и  $G_4$  используются для вычисления  $\neg(x_0 \wedge y_0)$  посредством  $\tau_2$  и  $\tau_2^{-1}$  соответственно.

- 5) На заключительном этапе остаётся последовательно соединить ПВП  $G_1$ ,  $G_2$ ,  $G_3$  и  $G_4$ , чтобы получить ПВП  $G$ , вычисляющую исходную функцию  $f$  посредством подстановки  $\tau$ .

## 2. $\text{NC}^1 = \text{poly}(n)\text{-OBDD}_5$

Согласно предложенному Баррингтоном методу по схеме из функциональных элементов глубины  $d$  можно получить перестановочную ветвящуюся программу ширины 5 и глубины  $4^d$ , по которой, в свою очередь, можно построить стандартную ветвящуюся программу той же ширины и глубины  $5 \cdot (4^d)$ . Возникает вопрос, а сколько раз и в каком порядке читаются переменные в результирующей ветвящейся программе?

Ответ на данный вопрос содержится в следующей теореме.

Пусть  $\text{poly}(n)\text{-OBDD}_5$  — класс функций, представимых  $k\text{-OBDD}$  ширины 5, где  $k = \text{poly}(n) = n^{O(1)}$  — некоторый полином от  $n$ .

**Теорема 2.**  $\text{poly}(n)\text{-OBDD}_5 = \text{NC}^1$ .

**ДОКАЗАТЕЛЬСТВО.** Из теоремы 1 и леммы 1 следует, что получаемая из схемы ветвящаяся программа является забывающей, т. е. на каждом вычислительном пути порядок считывания переменных  $s$  один и тот же. Метод Баррингтона позволяет определить его рекурсивным образом:  $s$  соответствует последнему элементу схемы (на глубине  $d$ ) и представляет собой конкатенацию  $s_1 \circ s_2 \circ s_1 \circ s_2$ , где  $s_1$  и  $s_2$  точно также соответствуют последним элементам подсхем глубины  $d-1$ . Здесь можно отметить, что ПВП, вычисляющая некоторую функцию  $f_1$  посредством подстановки  $\tau_1$  и полученная из неё по лемме 2 ПВП, использующая подстановку  $\tau_1^{-1}$ , используют один и тот же порядок переменных  $s_1$ . Поэтому в приведённом разложении  $s_1$  и  $s_2$  повторяются.

Коммутативность функционального элемента AND даёт альтернативное представление порядка считывания  $s = s_2 \circ s_1 \circ s_2 \circ s_1$ . Таким образом, на глубине 1, на которой задаются порядки считывания пар переменных, можно переставить их так, чтобы эти элементарные порядки на парах переменных подчинялись бы одному фиксированному порядку на  $n$  переменных, задаваемому некоторой подстановкой  $\pi$ . Действительно, если некоторая упорядоченная пара переменных  $(x_{i_1}, x_{i_2})$  нарушает этот порядок, т. е.  $\pi(i_2) < \pi(i_1)$ , то ничто не мешает заменить эту пару на  $(x_{i_2}, x_{i_1})$  — результат конъюнкции будет тот же.

Получаемая ПВП глубины  $4^d$  содержит  $4^d/2$  пар переменных, которые, как было показано, подчиняются одному и тому же порядку считывания. Моделируя её стандартной ветвящейся программой, имеем  $k(d)\text{-OBDD}$  ширины 5, где  $k(d) \leq 5 \cdot 2^{-1} \cdot 4^d$ .

В частности,  $d = O(\log(n))$  для класса функций из  $\text{NC}^1$ , т. е. результирующая ветвящаяся программа находится в классе  $\text{poly}(n)\text{-OBDD}_5$ . Значит,  $\text{NC}^1 \subseteq \text{poly}(n)\text{-OBDD}_5$ .

Обратная теорема Баррингтона [3] демонстрирует включение класса функций, представимых ветвящимися программами константной ширины и полиномиальной сложности, в класс  $\text{NC}^1$ , т. е.  $BWBP \subseteq \text{NC}^1$ .

Таким образом, предшествующие рассуждения, а также тот факт, что  $\text{poly}(n)\text{-OBDD}_5 \subseteq BWBP$ , доказывают утверждение теоремы. Теорема 2 доказана.



## ЛИТЕРАТУРА

1. **Barrington D. M.** Bounded-width polynomial-size branching programs recognize exactly those languages in NC // J. Comput. and System Sci. 1989. V. 38, N 4. P. 150–164. русский перевод: **Баррингтон Д.** Ветвящиеся программы ограниченной ширины, имеющие полиномиальную сложность, распознают в точности языки из  $NC^1$  // Кибернетический сборник. Новая серия. Вып. 28. М.: Мир, 1991. С. 94–113.
2. **Vollmer H.** Introduction to circuit complexity. A uniform approach. Berlin: Springer-Verlag, 1999.
3. **Wegener I.** The complexity of Boolean functions. Stuttgart: John Wiley & Sons Ltd., and B. G. Teubner, 1987.
4. **Wegener I.** Branching programs and binary decision diagrams // Philadelphia, CA: SIAM, 2000.

Адрес автора:

Казанский государственный университет,  
ул. Кремлевская, 18,  
420008 Казань,  
Россия.  
E-mail: vaslo@mail.ru

Статья поступила

20 октября 2006 г.

Переработанный вариант —

18 мая 2007 г.