

О СРАВНЕНИИ СЛОЖНОСТЕЙ БИНАРНЫХ k -ПРОГРАММ*)

Е. А. Окольников

В работе сравниваются сложности реализации булевых функций бинарными k -программами при различных значениях k . Показано, что для любого натурального k , $k \geq 2$, существуют натуральное s_k и последовательность булевых функций такие, что сложность реализации каждой функции из этой последовательности в классе бинарных k -программ в экспоненциальное число раз (по числу переменных булевой функции) превосходит сложность реализации той же функции в классе бинарных s_k -программ. В качестве s_k можно взять k^2 ; более точная оценка для s_k приводится перед леммой 5.

Введение

Проблема нахождения нетривиальных нижних оценок сложности реализации конкретных последовательностей булевых функций — одна из наиболее важных в математической теории синтеза и сложности схем. Получение таких оценок является сложной задачей. В настоящее время лишь для небольшого числа функций получены нетривиальные нижние оценки сложности реализации. Поэтому представляет интерес выявление факторов, в той или иной мере влияющих на сложность схем, реализующих булевы функции.

В настоящей работе изучаются факторы, влияющие на сложность бинарных программ. Бинарные программы — это логические схемы, которые хорошо моделируют вычисления с помощью одного процессора, читающего не более одного бита информации в единицу времени (определение бинарной программы будет дано в § 2, см. также [1]). Впервые этот класс схем изучал В. А. Кузьмин [2]. Он получил асимптотику функции Шеннона для бинарных программ, реализующих булевы функции. В последние два десятилетия получен ряд интересных результатов по сложности бинарных программ. Подробный обзор результатов по нижним оценкам сложности таких программ можно найти в [3, 4].

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-01-16009).

Бинарная программа называется бинарной k -программой, если в ней каждая переменная на любом пути от входной вершины к выходной проверяется не более чем k раз. Такие программы в [5] названы *синтаксическими k -программами*. Возможное альтернативное определение k -программы состоит в том, что ограничение на число проверок накладывается не на все пути программы, а только на пути, соответствующие хотя бы одному возможному набору входных переменных. В работах [5, 6] получены экспоненциальные нижние оценки сложности реализации последовательностей конкретных булевых функций в классе (детерминированных) синтаксических k -программ [6] и в более широком классе недетерминированных синтаксических k -программ [5]. Нетривиальные нижние оценки для класса бинарных несинтаксических k -программ при $k > 1$ в настоящее время неизвестны. В дальнейшем речь пойдет только о синтаксических k -программах.

В связи с тем, что одну и ту же булеву функцию можно реализовать бинарными k -программами с различными значениями k , возникает вопрос о выяснении соотношений сложностей реализации одной и той же булевой функции бинарными k_1 - и k_2 -программами. В работах [5, 7–10] показано, что сложность реализации некоторых последовательностей булевых функций бинарными 1-программами в экспоненциальное число раз (по числу переменных булевых функций) превышает сложность реализации тех же булевых функций бинарными 2-программами.

В данной работе показано, что для любого натурального k , $k \geq 2$, существует натуральное s_k и конкретная последовательность булевых функций такие, что сложность реализации каждой функции из этой последовательности в классе бинарных k -программ в экспоненциальное число раз (по числу переменных булевой функции) превосходит сложность реализации той же функции в классе бинарных s_k -программ. В качестве s_k можно взять k^2 ; более точная оценка для s_k приводится перед леммой 5. Ранее в [6] была показана возможность использования нижних оценок сложности бинарных k -программ для получения нижних оценок сложности бинарных программ без ограничений на структуру. Таким образом, сложность бинарных k -программ оказывается связанной со сложностью обычных бинарных программ.

Для получения нижних оценок сложности в работе предложена некоторая модификация метода из [6]. Этот метод основан на использовании мощностного подхода по отношению к частям бинарной программы и функции и может быть применим к функции со следующим свойством: ее подфункции в основном «плохо» представимы в форме

$$\bigvee_i f_i(X) \& g_i(Y),$$

где X и Y — некоторые непересекающиеся подмножества переменных, $|X|$ и $|Y|$ не малы.

Структура статьи следующая. В § 1 дан ряд определений, связанных с бинарными программами, а также приводятся некоторые простейшие свойства бинарных программ. В § 2 определяется последовательность булевой функции $F_{n,s}$, для которой будет доказан экспоненциальный рост сложности при переходе от реализации булевой функции $F_{n,s}$ бинарными s_k -программами к реализации этой же булевой функции бинарными k -программами. В § 3 каждой конъюнкции K из некоторого подмножества \mathcal{X}_0 допустимых для бинарной функции $F_{n,s}$ конъюнкций будет поставлена в соответствие последовательность $\Psi(K)$ бинарной программы. В § 4 для любой последовательности B бинарной программы оценивается мощность множества $\Psi^{-1}(B)$. При этом оказывается, что $|\Psi^{-1}(B)| \ll |\mathcal{X}_0|$. Это позволяет в § 5 доказать основную теорему о том, что для любого натурального k , $k \geq 2$, существует натуральное число s_k такое, что сложность реализации булевой функции $F_{n,s}$ бинарными k -программами в экспоненциальное число раз (по числу переменных булевой функции) больше сложности реализации $F_{n,s}$ бинарными s_k -программами.

§ 1. Определения, предварительные сведения

Напомним, что *бинарная программа* — это ориентированный граф без циклов, состоящий из *входной вершины* (нет входящих дуг и имеется ровно две выходящие дуги), *внутренних вершин* (не меньше одной входящей дуги и ровно две выходящие дуги) и *выходных вершин* (нет выходящих дуг). Входная вершина и каждая внутренняя вершина помечены булевой переменной из множества $X = \{x_1, \dots, x_n\}$, каждая выходная вершина — булевой константой 0 или 1. Одна дуга, выходящая из входной или внутренней вершины, помечена 0, другая — 1.

Пусть задан входной набор $\tilde{a} = (a_1, \dots, a_n)$, $a_i \in \{0, 1\}$, $i = 1, 2, \dots, n$. Бинарная программа \mathcal{P} по набору \tilde{a} вычисляет значение $P(\tilde{a})$, равное 0 или 1, следующим образом. Вычисление начинается во входной вершине. Если достигнута вершина, которой приписана переменная x_i , то осуществляется переход к следующей вершине по дуге, помеченной 1, если $a_i = 1$, и по дуге, помеченной 0, если $a_i = 0$. Поскольку из каждой невыходной вершины выходит одна дуга, помеченная 0, а другая — 1, и бинарная программа — это ориентированный граф без циклов, в конце концов будет достигнута выходная вершина, помеченная 0 или 1. Полученное значение определяется как $P(\tilde{a})$.

Говорят, что бинарная программа \mathcal{P} *вычисляет булеву функцию* $f(X)$, если для любого набора $\tilde{a} = (a_1, \dots, a_n)$ значений входных пере-

менных из X выполняется равенство $P(\bar{a}) = f(\bar{a})$.

Бинарную программу, в которой любой путь от входной вершины к выходной содержит не более k вершин, помеченных одной и той же переменной, будем называть *бинарной k -программой* (k -программой).

k -программу назовем *однородной*, если для любой вершины и любой переменной число проверок по этой переменной на любом пути, идущем от входа к рассматриваемой вершине, не зависит от пути (по разным переменным может быть разное число проверок). Кроме того, число проверок по любой переменной на любом пути, идущем от входной вершины к выходной, должно быть равно k .

Сложность $B(\mathcal{P})$ бинарной программы \mathcal{P} определяется как число вершин бинарной программы \mathcal{P} , в которых осуществляется проверка переменных (это входная и внутренние вершины бинарной программы). Обозначим через $Bk(f)$ сложность минимальной k -программы, реализующей булеву функцию f , а через $UBk(f)$ — сложность минимальной однородной k -программы, реализующей булеву функцию f .

Рассмотрим бинарную программу \mathcal{P}_f , реализующую булеву функцию f . Каждому пути в бинарной программе, идущему от входной вершины к выходной, естественным образом можно поставить в соответствие конъюнкцию K : если на этом пути после прохождения вершины, помеченной переменной x_i , выбрана дуга, помеченная 1, то в конъюнкцию K включается x_i , если эта дуга помечена 0, то в K включается \bar{x}_i . При этом конъюнкции, соответствующие некоторым путям бинарной программы \mathcal{P}_f , могут содержать одновременно переменную и ее отрицание, т. е. могут быть тождественно равны нулю.

Будем говорить, что вершина a_i *предшествует* вершине a_j в бинарной программе \mathcal{P} , если в \mathcal{P} существует путь, идущий от a_i к a_j .

Множество вершин a_1, \dots, a_t (не обязательно различных) бинарной программы \mathcal{P} назовем *последовательностью вершин*, если в \mathcal{P} существует путь от входной вершины к выходной, проходящий через вершины a_1, \dots, a_t , и на этом пути вершина a_i предшествует вершине a_j при $i < j$ или a_i совпадает с a_j .

Ясно, что если конъюнкция K соответствует некоторому пути бинарной программы \mathcal{P}_f , то она является *допустимой* для булевой функции f , т. е. $N_K \subseteq N_f$. (Здесь, как обычно, через N_f обозначено множество точек n -мерного единичного куба, в которых булева функция f равна единице.)

§ 2. Определение и свойства булевой функции $F_{n,k}$

Определим последовательность булевых функций и в § 5 докажем, что сложность реализации каждой функции из этой последовательности

бинарными s_k -программами в экспоненциальное число раз (по числу переменных функции) меньше сложности реализации той же функции k -программами.

Пусть n и s — натуральные числа, n — кратно s , и пусть $X_{n,s} = \{x_{i_1, i_2, \dots, i_s} \mid 1 \leq i_1 < i_2 < \dots < i_s \leq n\}$ — множество переменных. Ясно, что

$$|X_{n,s}| = \binom{n}{s} \stackrel{\text{def}}{=} N. \quad (1)$$

Обозначим через W_i множество переменных из $X_{n,s}$, у которых один из индексов равен i . Определим булеву функцию $F_{n,s}(X_{n,s})$ следующим образом:

$$F_{n,s} = \bigwedge_{i=1}^n \left(\bigvee_{x_{i_1, \dots, i_s} \in W_i} x_{i_1, \dots, i_s} \right). \quad (2)$$

ПРИМЕР 1. При $n = 4$ и $s = 2$ имеем $X_{4,2} = \{x_{1,2}, x_{1,3}, x_{1,4}, x_{2,3}, x_{2,4}, x_{3,4}\}$; $W_1 = \{x_{1,2}, x_{1,3}, x_{1,4}\}$, $W_2 = \{x_{1,2}, x_{2,3}, x_{2,4}\}$, $W_3 = \{x_{1,3}, x_{2,3}, x_{3,4}\}$ и $W_4 = \{x_{1,4}, x_{2,4}, x_{3,4}\}$. Тогда

$$F_{4,2} = (x_{1,2} \vee x_{1,3} \vee x_{1,4}) \& (x_{1,2} \vee x_{2,3} \vee x_{2,4}) \& (x_{1,3} \vee x_{2,3} \vee x_{3,4}) \& (x_{1,4} \vee x_{2,4} \vee x_{3,4}).$$

Нетрудно видеть, что булева функция $F_{n,s}$ может быть реализована бинарной s -программой сложности не более

$$n|W_i| = n \binom{n-1}{s-1} = s \binom{n}{s} = s|X_{n,s}|. \quad (3)$$

Семейство функций $F_{n,2}$ нами было рассмотрено в [8] для сравнения сложностей бинарных 1- и 2-программ, а в [11,12] — для сравнения сложностей реализации булевых функций схемами из функциональных элементов с ограничениями на структуру схемы и без ограничений.

Введем несколько определений.

Пусть $D \subset X_{n,s}$. Обозначим через $V(D)$ множество индексов (без учета кратности), которые имеются у переменных из D . В частности, $V(X_{n,s}) = \{1, 2, \dots, n\}$.

Для конъюнкции K , содержащей некоторые переменные или отрицания переменных из $X_{n,s}$, через $R(K)$ обозначим множество переменных, которые входят в конъюнкцию K без отрицания. Через $V(K)$ обозначим множество индексов, которые имеются у переменных из $R(K)$. Ясно, что

$$V(K) = V(R(K)).$$

ПРИМЕР 2. Для конъюнкции $K_1 = x_{1,2} \& \bar{x}_{1,3} \& x_{2,4} \& \bar{x}_{3,5}$ имеем $V(K_1) = V(x_{1,2}, x_{2,4}) = \{1, 2, 4\}$.

Конъюнкцию K , зависящую от всех переменных из множества $X_{n,s}$, назовем *непересекающейся*, если любое число от 1 до n встречается в качестве индекса у переменных из $R(K)$ точно один раз. Ясно, что $V(K) = \{1, 2, \dots, n\}$ для любой непересекающейся конъюнкции.

Пусть $\Phi(n, s)$ обозначает число непересекающихся конъюнкций переменных из $X_{n,s}$. Легко проверить, что

$$\Phi(n, s) = \frac{n!}{(s!)^{n/s} (n/s)!}.$$

Рассмотрим некоторые свойства булевой функции $F_{n,s}$, а также конъюнкций, получаемых на выходе произвольной бинарной программы, реализующей $F_{n,s}$.

Из (2) легко следует

Лемма 1. Конъюнкция K , зависящая от некоторых переменных из множества $X_{n,s}$, является допустимой для $F_{n,s}$ тогда и только тогда, когда $V(K) = \{1, 2, \dots, n\}$.

ПРИМЕР 3. Для $F_{4,2}$ конъюнкции $x_{1,2} \& x_{1,3} \& \bar{x}_{1,4} \& x_{2,3} \& \bar{x}_{2,4} \& \bar{x}_{3,4}$ и $x_{1,2} \& x_{1,3} \& \bar{x}_{2,4}$ не являются допустимыми, конъюнкция $x_{1,2} \& x_{1,3} \& \bar{x}_{1,4} \& x_{3,4}$ — допустимая, а конъюнкция $x_{1,2} \& \bar{x}_{1,3} \& \bar{x}_{1,4} \& \bar{x}_{2,3} \& \bar{x}_{2,4} \& x_{3,4}$ — допустимая и непересекающаяся.

Из леммы 1 вытекает

Следствие 1. Пусть \mathcal{P}_0 — однородная k -программа, реализующая $F_{n,s}$. Тогда для любой непересекающейся конъюнкции K существует путь от входной вершины к выходной, по которому реализуется конъюнкция K .

Доказательство. Из определения непересекающейся конъюнкции и леммы 1 следует, что для любой элементарной конъюнкции из совершенной дизъюнктивной нормальной формы булевой функции $F_{n,s}$ в \mathcal{P}_0 существует путь, по которому эта конъюнкция реализуется. Утверждение доказано.

Замечание 1. Задание булевой функции $F_{n,s}$ посредством переменных из $X_{n,s}$ позволяет использовать гиперграфы с n вершинами для описания булевой функции $F_{n,s}$ (определение гиперграфа см., например, [13, гл. XI]). Каждой конъюнкции $K(X_{n,s})$ поставим в соответствие гиперграф $G(K)$ с n вершинами $1, 2, \dots, n$ следующим образом: s -ребро (i_1, \dots, i_s) входит в гиперграф $G(K)$ тогда и только тогда, когда $x_{i_1, \dots, i_s} \in R(K)$. Тогда для $F_{n,s}$ допустимыми являются те и только те конъюнкции переменных из $X_{n,s}$, которым соответствуют гиперграфы без изолированных вершин. В гиперграфе, соответствующем непересекающейся конъюнкции, нет изолированных вершин и каждая вершина

инцидентна только одному s -ребру. Такие гиперграфы являются аналогами совершенных паросочетаний в обычных графах.

На языке гиперграфов множество $V(K)$ можно определить как совокупность тех вершин в гиперграфе $G(K)$, соответствующем конъюнкции K , которые инцидентны хотя бы одному ребру гиперграфа.

§ 3. Построение последовательности $\Psi(K)$

По лемме 1 из [9] любую k -программу \mathcal{P} , реализующую булеву функцию f от N переменных, можно преобразовать в однородную k -программу \mathcal{P}_0 , реализующую функцию f и такую, что сложность программы \mathcal{P}_0 не более чем в $2kN$ раз превышает сложность первоначальной k -программы \mathcal{P} , т. е.

$$Bk(\mathcal{P}_0) \leq (2kN)Bk(\mathcal{P}).$$

Из этого факта следует, что для любой булевой функции f

$$UBk(f) \leq (2kN)Bk(f). \quad (5)$$

Пусть \mathcal{P}_0 — однородная k -программа, реализующая булеву функцию f . Тогда любой путь в \mathcal{P}_0 реализует либо некоторую элементарную конъюнкцию от переменных из X , либо конъюнкцию, тождественно равную нулю. Пусть α — путь в \mathcal{P}_0 , реализующий ненулевую конъюнкцию K . Будем говорить, что *переменная x встречается на отрезке (b, c) пути α* , если на отрезке (b, c) пути α между вершинами b и c есть дуга, которая исходит из вершины программы \mathcal{P}_0 , помеченной переменной x . Аналогично будем говорить, что *переменная y без отрицания встречается на отрезке (b, c) пути α* , если на отрезке (b, c) пути α между вершинами b и c есть дуга, которая помечена 1 и исходит из вершины программы \mathcal{P}_0 , помеченной переменной y . Ясно, что $y \in R(K)$.

Пусть a_1, a_2, \dots, a_{2m} — последовательность вершин однородной k -программы \mathcal{P}_0 , лежащих на пути α . Через $R_\alpha^1(a_1, a_2, \dots, a_{2m})$ (соответственно $Q_\alpha^1(a_1, a_2, \dots, a_{2m})$) обозначим множество переменных без отрицания (соответственно множество переменных как с отрицаниями, так и без них), которые встречаются хотя бы на одном из отрезков $(a_1, a_2), \dots, (a_{2m-1}, a_{2m})$ пути α и не встречаются вне этих отрезков на этом пути. Обозначим через $R_\alpha^2(a_1, a_2, \dots, a_{2m})$ (соответственно $Q_\alpha^2(a_1, a_2, \dots, a_{2m})$) множество переменных без отрицания (соответственно множество переменных как с отрицаниями, так и без них), которые встречаются только вне указанных выше отрезков пути α . Обозначим через $R_\alpha^0(a_1, a_2, \dots, a_{2m})$ (соответственно $Q_\alpha^0(a_1, a_2, \dots, a_{2m})$) множество переменных без отрицания (соответственно множество переменных как с отрицаниями, так и без них), которые встречаются как на указанных выше отрезках пути α , так и вне их.

Ясно, что множества $R_\alpha^j(a_1, a_2, \dots, a_{2m})$, $j = 0, 1, 2$, попарно не пересекаются и их объединение совпадает с множеством всех переменных без отрицания, которые встречаются на пути α . Множества R_α^j зависят не только от последовательности a_1, a_2, \dots, a_{2m} , но и от пути α , которому эта последовательность принадлежит.

Так как \mathcal{P}_0 — однородная k -программа, то на любом пути, проходящем через ее вершины b и c , множество переменных, которые встречаются на отрезке (b, c) этого пути, не зависит от пути. Поэтому множества $Q_\alpha^j(a_1, a_2, \dots, a_{2m})$, $j = 0, 1, 2$, зависят только от последовательности вершин a_1, a_2, \dots, a_{2m} и не зависят от пути. Поэтому индекс α при Q_α^j можно опустить. Ясно, что множества $Q^j(a_1, a_2, \dots, a_{2m})$, $j = 0, 1, 2$, попарно не пересекаются и их объединение совпадает с множеством всех переменных булевой функции f . Очевидно, что $R_\alpha^j(a_1, a_2, \dots, a_{2m}) \subseteq Q^j(a_1, a_2, \dots, a_{2m})$, $j = 0, 1, 2$, для любого пути α , проходящего через последовательность вершин a_1, a_2, \dots, a_{2m} .

Лемма 2. Пусть \mathcal{P}_0 — однородная k -программа, реализующая булеву функцию $F_{n,s}$; m, t — натуральные числа такие, что $k \leq m \leq t$. Тогда любой непересекающейся конъюнкции K можно поставить в соответствие последовательность $\Psi(K)$ из $2m$ вершин такую, что

а) все вершины последовательности $\Psi(K)$ принадлежат некоторому пути $\alpha(K)$, реализующему конъюнкцию K ;

$$\text{б) } |R_\alpha^1(\Psi(K))| = \left[(n/s) \binom{t-k}{m-k} / \binom{t}{m} \right];$$

$$|R_\alpha^2(\Psi(K))| \geq n/s - m \lceil kn/(ts) \rceil + (k-1) \left[(n/s) \binom{t-k}{m-k} / \binom{t}{m} \right];$$

$$|R_\alpha^0(\Psi(K))| \leq m \lceil kn/(ts) \rceil - k \left[(n/s) \binom{t-k}{m-k} / \binom{t}{m} \right].$$

Доказательство. По следствию 1 леммы 1 в \mathcal{P}_0 существует путь $\alpha(K)$ от входной вершины к выходной, по которому реализуется конъюнкция K . Так как \mathcal{P}_0 — однородная k -программа, то любая переменная встречается на любом пути точно k раз. Поэтому на пути $\alpha(K)$ есть точно kn/s дуг, помеченных единицей. На пути $\alpha(K)$ выберем $t+1$ таких вершин a_0, a_1, \dots, a_t , что вершина a_i предшествует вершине a_j ($0 \leq i < j \leq t$) и число дуг, помеченных единицей между вершинами a_i и a_{i+1} ($i = 0, 1, \dots, t-1$), не превышает $\lceil kn/(ts) \rceil$.

Любые m вершин a_{i_1}, \dots, a_{i_m} , $0 \leq i_1 < i_2 < \dots < i_m \leq t-1$, из множества $\{a_0, a_1, \dots, a_{t-1}\}$ задают m отрезков пути $\alpha(K)$: (a_{i_1}, a_{i_1+1}) , (a_{i_2}, a_{i_2+1}) , \dots , (a_{i_m}, a_{i_m+1}) . Множество концов этих отрезков обозначим через A_{i_1, i_2, \dots, i_m} , т. е. $A_{i_1, i_2, \dots, i_m} = \{a_{i_1}, a_{i_1+1}, a_{i_2}, a_{i_2+1}, \dots, a_{i_m}, a_{i_m+1}\}$. Множество A_{i_1, i_2, \dots, i_m} является последовательностью вершин бинарной программы \mathcal{P}_0 .

В конце доказательства этой леммы будет показано, что среди все-

возможных последовательностей вершин A_{i_1, i_2, \dots, i_m} можно выбрать такую, что ее незначительная модификация (последовательность B) удовлетворяет условиям леммы 2.

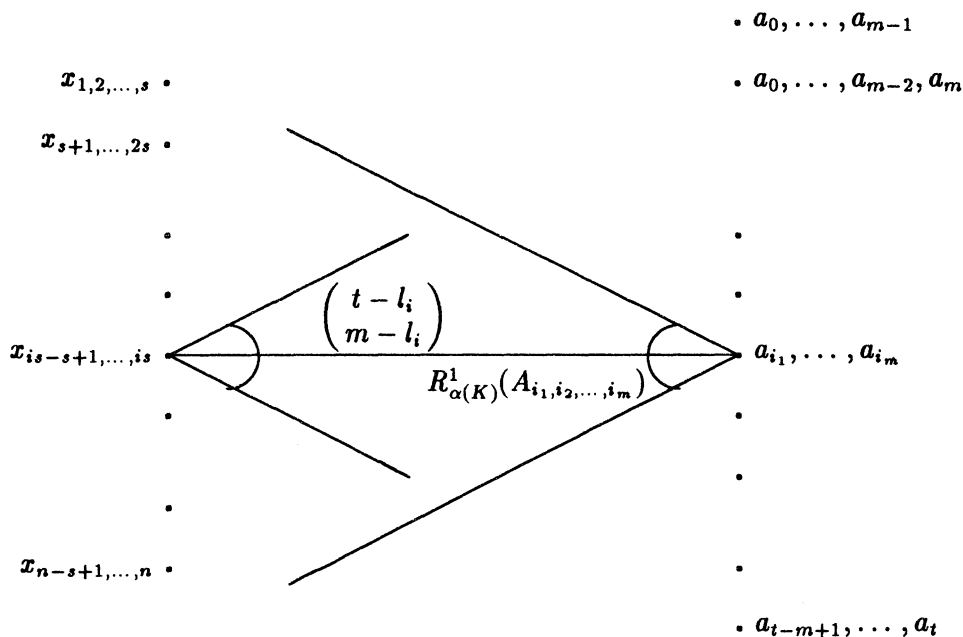


Рис. 1

Без ограничения общности можно считать, что

$$K = x_{1, \dots, s} \& x_{s+1, \dots, 2s} \& \dots \& x_{n-s+1, \dots, n}.$$

Рассмотрим граф G (рис. 1), содержащий два множества вершин: n/s вершин, помеченных переменными $x_{1, \dots, s}, x_{s+1, \dots, 2s}, \dots, x_{n-s+1, \dots, n}$, и $\binom{t}{m}$ вершин, помеченных всевозможными n -элементными выборками $\{a_{i_1}, \dots, a_{i_m}\}$ из множества $\{a_0, a_1, \dots, a_{t-1}\}$, а значит, и всевозможными выборками последовательностей A_{i_1, i_2, \dots, i_m} . Вершину, помеченную переменной $x_{(i-1)s+1, \dots, is}$, соединим с вершиной, помеченной подмножеством $\{a_{i_1}, a_{i_2}, \dots, a_{i_m}\}$, $0 \leq i_1 < i_2 < \dots < i_m \leq t-1$, в том и только в том случае, когда $x_{(i-1)s+1, \dots, is} \in R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})$, т. е. когда эта переменная входит без отрицания хотя бы в один из отрезков пути $(a_{i_1}, a_{i_1+1}), (a_{i_2}, a_{i_2+1}), \dots, (a_{i_m}, a_{i_m+1})$, но не входит в остальные отрезки пути. Пусть l_i — число отрезков (a_{i_j}, a_{i_j+1}) , $0 \leq j \leq t-1$, в которые входит переменная $x_{(i-1)s+1, \dots, is}$. Тогда вершина, помеченная переменной $x_{(i-1)s+1, \dots, is}$, в графе G соединена со всеми подмножествами, содержащими эти отрезки. Число таких подмножеств равно $\binom{t-l_i}{m-l_i}$. Вместе

с тем вершина, помеченная подмножеством $\{a_{i_1}, \dots, a_{i_m}\}$, соединена в графе G с $|R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})|$ вершинами, которые соответствуют переменным. Поскольку число ребер, выходящих из вершин, расположенных в двудольном графе G слева (см. рис. 1), равно числу ребер, выходящих из вершин, расположенных в графе G справа, то

$$\sum_{i_1, \dots, i_m} |R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})| = \sum_{i=1}^{n/s} \binom{t-l_i}{m-l_i}. \quad (6)$$

Так как на любом пути бинарной программы \mathcal{P}_0 любая переменная встречается точно k раз, то $l_i \leq k$. Поэтому $\binom{t-l_i}{m-l_i} \geq \binom{t-k}{m-k}$. Отсюда и из (6) следует, что

$$\sum_{i_1, \dots, i_m} |R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})| \geq (n/s) \binom{t-k}{m-k}.$$

Значит, существуют вершины a_{i_1}, \dots, a_{i_m} такие, что имеет место неравенство

$$|R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})| \geq (n/s) \binom{t-k}{m-k} / \binom{t}{m}.$$

Так как $|R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})|$ — целое число, то

$$|R_{\alpha(K)}^1(A_{i_1, i_2, \dots, i_m})| \geq \left\lceil (n/s) \binom{t-k}{m-k} / \binom{t}{m} \right\rceil. \quad (7)$$

Если неравенство (7) — строгое, то, постепенно уменьшая отрезки (т. е. сближая на пути $\alpha(K)$ концы отрезков $(a_{i_j}, a_{i_{j+1}})$), от последовательности A_{i_1, i_2, \dots, i_m} можно перейти к последовательности $B = (b_1, \dots, b_{2m})$ такой, что

$$|R_{\alpha(K)}^1(B)| = \left\lceil (n/s) \binom{t-k}{m-k} / \binom{t}{m} \right\rceil. \quad (8)$$

Общее число переменных без отрицания, входящих в отрезки (b_1, b_2) , (b_3, b_4) , \dots , (b_{2m-1}, b_{2m}) , т. е. величина $|R_{\alpha(K)}^1(B) \cup R_{\alpha(K)}^0(B)|$ удовлетворяет неравенству

$$|R_{\alpha(K)}^1(B) \cup R_{\alpha(K)}^0(B)| \leq \lceil kn/(ts) \rceil m - (k-1) |R_{\alpha(K)}^1(B)|. \quad (9)$$

Поскольку

$$|R_{\alpha(K)}^2(B)| = n/s - |R_{\alpha(K)}^1(B) \cup R_{\alpha(K)}^0(B)|,$$

из (8), (9) следует, что

$$\begin{aligned} |R_{\alpha(K)}^2(B)| &\geq n/s - \lceil kn/(ts) \rceil m + (k-1) |R_{\alpha(K)}^1(B)| \\ &\geq n/s - \lceil kn/(ts) \rceil m + (k-1) \left\lceil (n/s) \binom{t-k}{m-k} / \binom{t}{m} \right\rceil. \end{aligned}$$

Так как $|R_{\alpha(K)}^0(B)| + |R_{\alpha(K)}^1(B)| + |R_{\alpha(K)}^2(B)| = n/s$, то требуемая оценка имеет место и для $|R_{\alpha(K)}^0(B)|$.

Таким образом, последовательность вершин $\Psi(K) = B$ удовлетворяет условию б) леммы 2. Условию а) леммы 2 последовательность B удовлетворяет по построению. Лемма 2 доказана.

§ 4. Оценка мощности множества $\Psi^{-1}(B)$

Пусть ψ — последовательность вершин бинарной программы, реализующей булеву функцию $F_{n,s}$ от переменных из $X_{n,s}$. Из определения множеств $Q^j(\psi)$, $j = 0, 1, 2$, следует, что $X_{n,s} = Q^0(\psi) \cup Q^1(\psi) \cup Q^2(\psi)$ и $Q^i(\psi) \cap Q^j(\psi) = \emptyset$ при $i \neq j$. Пусть \mathcal{X} — конъюнкция, существенно зависящая от всех переменных из множества $X_{n,s}$. Тогда \mathcal{X} можно единственным образом представить в виде $\mathcal{X} = \mathcal{X}^0(Q^0(\psi)) \& \mathcal{X}^1(Q^1(\psi)) \& \mathcal{X}^2(Q^2(\psi))$, где конъюнкция $\mathcal{X}^i(Q^i(\psi))$ существенно зависит от всех переменных из множества $Q^i(\psi)$, т. е. конъюнкция \mathcal{X} по последовательности ψ однозначно определяет конъюнкции $\mathcal{X}^i(Q^i(\psi))$, $i = 0, 1, 2$.

Пусть ψ — последовательность вершин бинарной программы. Через $T(\psi)$ обозначим множество таких непересекающихся конъюнкций, существенно зависящих от переменных из $X_{n,s}$, что для каждой из них существует реализующий эту конъюнкцию путь (от входной вершины к выходной), проходящий через последовательность вершин ψ .

Лемма 3. Пусть $\psi = (a_1, a_2, \dots, a_{2m})$ — последовательность вершин однородной k -программы \mathcal{P}_0 ; конъюнкции \mathcal{A}, \mathcal{B} принадлежат $T(\psi)$ и являются такими, что $\mathcal{A} = \mathcal{A}^0(Q^0(\psi)) \& \mathcal{A}^1(Q^1(\psi)) \& \mathcal{A}^2(Q^2(\psi))$ и $\mathcal{B} = \mathcal{B}^0(Q^0(\psi)) \& \mathcal{B}^1(Q^1(\psi)) \& \mathcal{B}^2(Q^2(\psi))$. Тогда если $\mathcal{A}^0(Q^0(\psi)) = \mathcal{B}^0(Q^0(\psi))$, то $V(\mathcal{A}^1(Q^1(\psi))) = V(\mathcal{B}^1(Q^1(\psi)))$ и $V(\mathcal{A}^2(Q^2(\psi))) = V(\mathcal{B}^2(Q^2(\psi)))$.

Доказательство. Пусть α и β — пути в \mathcal{P}_0 от входной вершины к выходной, каждая из которых содержит последовательность вершин из $\psi = (a_1, a_2, \dots, a_{2m})$, и α реализует конъюнкцию из \mathcal{A} , а β — конъюнкцию из \mathcal{B} .

Через α_1 (аналогично β_1) обозначим такую часть пути α (аналогично β), что α_1 содержит отрезки $(a_1, a_2), (a_3, a_4), \dots, (a_{2m-1}, a_{2m})$. Через α_2 (аналогично β_2) обозначим такую часть пути α (аналогично β), что α_2 проходит вне указанных выше отрезков.

Так как \mathcal{A} — непересекающаяся конъюнкция (по определению множества $T(\psi)$), то множества $V(\mathcal{A}^0(Q^0(\psi)))$, $V(\mathcal{A}^1(Q^1(\psi)))$ и $V(\mathcal{A}^2(Q^2(\psi)))$ взаимно не пересекаются и их объединение совпадает с $\{1, 2, \dots, n\}$. Аналогичное утверждение верно и для конъюнкции \mathcal{B} . Так как $\mathcal{A}^0(Q^0(\psi)) = \mathcal{B}^0(Q^0(\psi))$, то $V(\mathcal{A}^0(Q^0(\psi))) = V(\mathcal{B}^0(Q^0(\psi)))$. Поэтому $V(\mathcal{A}^1(Q^1(\psi))) \cup V(\mathcal{A}^2(Q^2(\psi))) = V(\mathcal{B}^1(Q^1(\psi))) \cup V(\mathcal{B}^2(Q^2(\psi)))$. Предположим, что $V(\mathcal{A}^1(Q^1(\psi))) \neq V(\mathcal{B}^1(Q^1(\psi)))$. Без ограничения общ-

ности можно предположить, что $V(\mathcal{A}^1(Q^1(\psi))) \not\subseteq V(\mathcal{B}^1(Q^1(\psi)))$, т. е. существует такой индекс i , что $i \in V(\mathcal{A}^1(Q^1(\psi)))$ и $i \notin V(\mathcal{B}^1(Q^1(\psi)))$. Рассмотрим путь γ (на рис. 2 изображен штрихом),

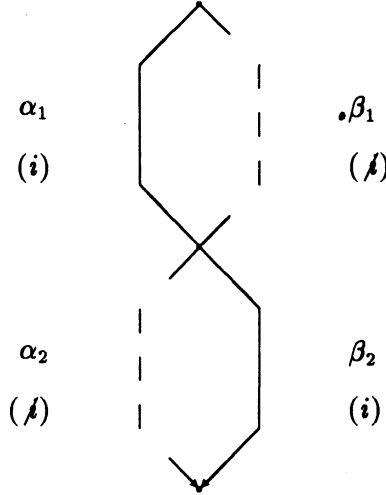


Рис. 2

проходящий по дугам из β_1 пути β и по дугам из α_2 пути α . Так как $\mathcal{A}^0(Q^0(\psi)) = \mathcal{B}^0(Q^0(\psi))$, то значения переменных, которые встречаются как на отрезке β_1 , так и на отрезке α_2 , совпадают. Поэтому путь γ реализует ненулевую конъюнкцию

$$\mathcal{C} = \mathcal{A}^0(Q^0(\psi)) \& \mathcal{B}^1(Q^1(\psi)) \& \mathcal{A}^2(Q^2(\psi)).$$

Так как \mathcal{A} — непересекающаяся конъюнкция, то из $i \in V(\mathcal{A}^1(Q^1(\psi)))$ следует, что $i \notin V(\mathcal{A}^2(Q^2(\psi)))$ и $i \notin V(\mathcal{A}^0(Q^0(\psi)))$. По предположению $i \notin V(\mathcal{B}^1(Q^1(\psi)))$. Поэтому $i \notin V(\mathcal{C})$. Следовательно, по лемме 1 конъюнкция \mathcal{C} не является допустимой для булевой функции $F_{n,s}$. Полученное противоречие доказывает лемму 3.

Ниже всюду будем полагать, что

$$n_1 = s \left\lceil (n/s) \binom{t-k}{m-k} / \binom{t}{m} \right\rceil; \quad (10)$$

$$n_0 = sm \lceil kn/(ts) \rceil - sk \left\lceil (n/s) \binom{t-k}{m-k} / \binom{t}{m} \right\rceil; \quad (11)$$

$$n_2 = n - n_0 - n_1. \quad (12)$$

Лемма 4. Пусть $B = (b_1, b_2, \dots, b_{2m})$ — последовательность вершин однородной k -программы \mathcal{P}_0 , реализующей булеву функцию $F_{n,s}$. Тогда при фиксированных значениях k, m, t ($k \leq m, kt \leq t$) справедливо соотношение

$$\Psi^{-1}(B) \leq \binom{n}{n_0} \Phi(n_0, s) \Phi(n_1, s) \Phi(n_2, s),$$

где Φ задается формулой (4).

Доказательство. Последовательность вершин B задает разбиение множества $X_{n,s}$ на три попарно непересекающихся подмножества $Q^j(B)$, $j = 0, 1, 2$. Отображение Ψ , удовлетворяющее лемме 2, является отображением множества всех непересекающихся конъюнкций переменных из $X_{n,s}$ в множество последовательностей вершин бинарной программы \mathcal{P}_0 . При этом если $K \in \Psi^{-1}(B)$, то, по построению отображения Ψ , для пути $\alpha(K)$, проходящего через последовательность вершин B и реализующего непересекающуюся конъюнкцию K , справедливы соотношения

$$|R_{\alpha(K)}^1(B)| = |R(K) \cap Q^1(B)| = n_1/s,$$

$$|R_{\alpha(K)}^0(B)| = |R(K) \cap Q^0(B)| \leq n_0/s$$

и

$$|R_{\alpha(K)}^2(B)| = |R(K) \cap Q^2(B)| \geq n_2/s.$$

Из определения множества $T(B)$ и леммы 2 следует, что $\Psi^{-1}(B) \subseteq T(B)$ и для любых конъюнкций K из $\Psi^{-1}(B)$, для которых совпадают множества переменных $(R(K) \cap Q^0(B))$, совпадают также и множества индексов $(V(R(K) \cap Q^1(B)))$ и $(V(R(K) \cap Q^2(B)))$. Таким образом, для конъюнкций из $\Psi^{-1}(B)$ множество индексов $\{1, 2, \dots, n\} \setminus (V(R(K) \cap Q^0(B)))$ делится на 2 непересекающихся подмножества $V_1 = V(R(K) \cap Q^1(B))$ и $V_2 = V(R(K) \cap Q^2(B))$; при этом $|V(R(K) \cap Q^0(B))| \leq n_0$, $|V_1| = n_1$ и $|V_2| = n - n_1 - |V(R(K) \cap Q^0(B))|$.

Любая конъюнкция K , существенно зависящая от всех переменных из $X_{n,s}$, однозначно определяется множеством $R(K)$. Так как все конъюнкций из $\Psi^{-1}(B)$ — непересекающиеся, то для любой конъюнкции K из $\Psi^{-1}(B)$ переменные, входящие в множество $R(K)$, попарно не имеют общих индексов. Оценим сверху число способов построения множества $R(K)$ для конъюнкций из $\Psi^{-1}(B)$. Это можно сделать следующим способом.

1. Из множества переменных $Q^0(B) \cup Q^2(B)$ выбирается подмножество U такое, что

а) переменные из U попарно не содержат общих индексов;

б) $|U| = n_0/s$.

Число способов выбора подмножества U из $Q^0(B) \cup Q^2(B)$ не превосходит числа способов выбора подмножества, состоящего из n_0/s переменных, попарно не содержащих общих индексов из $X_{n,s}$, т. е. не превосходит величины $\binom{n}{n_0} \Phi(n_0, s)$.

Пусть $R_0 = U \cap Q^0(B)$. Ясно, что $|R_0| \leq n_0/s$. По лемме 3 для конъюнкций K из $\Psi^{-1}(B)$, для которых $R(K) \cap Q_0(K) = R_0$, однозначно определены множества $V_1(R_0) = V(Q^1(B) \cap R(K))$ и $V_2(R_0) = V(Q^2(B) \cap R(K))$.

2. Если $|V_1(R_0)| \neq n_1$, то процесс построения множества $R(K)$ обрывается. Если $|V_1(R_0)| = n_1$, то из множества $Q^1(B)$ выбирается подмножество U_1 такое, что

- а) переменные из U_1 попарно не содержат общих индексов;
- б) $V(R_0) = V_1(R_0)$.

Число способов выбора U_1 не превосходит величины $\Phi(n_1, s)$.

3. Если $V(U \cap Q^2(B)) \not\subseteq V_2(R_0)$, то процесс построения множества $R(K)$ обрывается. Если $V(U \cap Q^2(B)) \subseteq V_2(R_0)$, то из множества $Q^2(B)$ выбирается подмножество U_2 такое, что

- а) переменные из U_2 попарно не содержат общих индексов;
- б) $|U_2| = n_2$;
- в) $V(U_2) = V_2(R_0) \setminus V(U \cap Q^2(B))$.

Число способов выбора U_2 не превосходит величины $\Phi(n_2, s)$.

Легко видеть, что любая конъюнкция из $\Psi^{-1}(B)$ была учтена в пп. 1–3. Поэтому

$$\Psi^{-1}(B) \leq \binom{n}{n_0} \Phi(n_0, s) \Phi(n_1, s) \Phi(n_2, s).$$

Лемма 4 доказана.

Пусть k — натуральное число, $k \geq 2$. Введем обозначения:

$$s_k^0 = \frac{k^2 \ln k - (k^k - k) \ln(1 - k^{-k+1}) - (k-1) \ln(k-1)}{k \ln k - (k-1) \ln(k-1)}; \quad (13)$$

$$s_k = \lfloor s_k^0 \rfloor + 1;$$

$$\varepsilon_k = s_k - s_k^0.$$

Ясно, что

$$0 < \varepsilon_k \leq 1. \quad (14)$$

Лемма 5. При любом k , $k \geq 2$, величина s_k удовлетворяет неравенству

$$s_k \leq k^2.$$

ДОКАЗАТЕЛЬСТВО. Так как $s_2 = 4$, то при $k = 2$ лемма верна. При любом $k \geq 3$ имеем

$$\begin{aligned} -(k-1)\ln(k-1) &= -(k-1)\ln k - (k-1)\ln(1-1/k) \\ &= -(k-1)\ln k - (k-1)\sum_{i=1}^{\infty} \frac{1}{ik^i} \\ &= -(k-1)\ln k + 1 - \sum_{i=1}^{\infty} \frac{1}{i(i+1)k^i} < -(k-1)\ln k + 1 \end{aligned} \quad (15)$$

и

$$-(k-1)\ln(k-1) > -(k-1)\ln k + 1 - 1/k. \quad (16)$$

Аналогично можно убедиться в том, что

$$-(k^k - k)\ln(1 - 1/k^{k-1}) < k. \quad (17)$$

Из (14)–(17) следует, что при $k \geq 3$

$$s_k \leq \frac{k^2 \ln k + k - (k-1)\ln k + 1}{\ln k + 1 - 1/k} + 1 \leq \frac{(k^2 - k + 1)\ln k + k + 2}{\ln k + 1 - 1/k} < k^2. \quad (18)$$

Лемма 5 доказана.

Пусть \mathcal{P}_0 — однородная k -программа, реализующая булеву функцию $F_{n,s}$. Обозначим через $\omega_{\mathcal{P}_0}(n, s, k, 2m)$ число $2m$ -элементных последовательностей в \mathcal{P}_0 .

Пусть

$$m_k = \lceil k^3/\varepsilon_k \rceil. \quad (19)$$

Лемма 6. Пусть $k \geq 2$, $n \geq 3k^{k+5}/\varepsilon_k$ и \mathcal{P}_0 — однородная k -программа, реализующая булеву функцию F_{n,s_k} . Тогда

$$\omega_{\mathcal{P}_0}(n, s_k, k, 2m_k) \geq \frac{\exp(n\varepsilon_k/k^2)}{(2n)^{m_k k^2}}.$$

ДОКАЗАТЕЛЬСТВО. Так как каждой непересекающейся конъюнкции K поставлена в соответствие $2m$ -элементная последовательность вершин $\Psi(K)$, то из леммы 4 и (4) при фиксированных n, k, t, m и $s = s_k$ следует, что

$$\begin{aligned} \omega_{\mathcal{P}_0}(n, s_k, k, 2m) &\geq \frac{\Phi(n, s)}{\binom{n}{n_0} \Phi(n_0, s) \Phi(n_1, s) \Phi(n_2, s)} \\ &= \frac{(n_0/s)! (n_1/s)! (n_2/s)! (n_1 + n_2)!}{(n/s)! n_1! n_2!}, \end{aligned}$$

где n_0, n_1, n_2 определены в (10)–(12).

Отсюда с использованием формулы Стирлинга получаем

$$\omega_{\mathcal{D}_0}(n, s_k, k, 2m) \geq \sqrt{\frac{2\pi n_0(n_1 + n_2)}{ns^2}} \frac{n_0^{n_0/s} n_1^{n_1/s} n_2^{n_2/s} (n_1 + n_2)^{n_1 + n_2}}{n^{n/s} n_1^{n_1} n_2^{n_2} e^{s/(12n) + 1/(12n_1) + 1/(12n_2)}}. \quad (20)$$

Положим

$$m = m_k, \quad t = m_k k, \quad (21)$$

где m_k взято из (19).

Представим n_1 в виде

$$n_1 = an. \quad (22)$$

Тогда из (10)–(12) следует, что

$$n - kan \leq n_0 \leq n - kan + ms, \quad (23)$$

$$(k-1)an - sm \leq n_2 \leq (k-1)an. \quad (24)$$

В свою очередь, пользуясь равенствами (10), (21) и (22), имеем

$$\begin{aligned} a &\geq \binom{t-k}{m-k} / \binom{t}{m} = \prod_{i=0}^{k-1} \frac{m-i}{t-i} > \frac{1}{k^k} \prod_{i=0}^{k-1} \left(1 - \frac{i}{m}\right) \\ &> \frac{1}{k^k} \left(1 - \frac{k}{m}\right)^{k/2} > \frac{1}{k^k} \left(1 - \frac{k^2}{2m}\right). \end{aligned} \quad (25)$$

С другой стороны, из (22), (10), леммы 5 и (19) следует, что при n , удовлетворяющих условию леммы 6,

$$\begin{aligned} a &\leq \prod_{i=0}^{k-1} \frac{m-i}{mk-i} + \frac{s}{n} = \frac{1}{k^k} \prod_{i=0}^{k-1} \frac{1-i/m}{1-i/(km)} + \frac{s}{n} \\ &< \frac{1}{k^k} \frac{1-(k-1)/m}{1-(k-1)/(km)} + \frac{k^2}{n} \leq \frac{1}{k^k} \frac{1-(k-1)/m + k^{k+2}/n}{1-(k-1)/(km)} \\ &\leq \frac{1}{k^k} - \frac{(k-1)/m - k^{k+2}/n - (k-1)/(km)}{1-(k-1)/(km)} \leq \frac{1}{k^k}. \end{aligned} \quad (26)$$

Если n удовлетворяет условию леммы 6, то из (22)–(24), леммы 5, (25) и (19) имеем

$$\begin{aligned} \sqrt{\frac{2\pi n_0(n_1 + n_2)}{ns^2}} \frac{1}{e^{s/(12n) + 1/(12n_1) + 1/(12n_2)}} &\geq \sqrt{\frac{2\pi(n-kan)(kan-sm)}{nk^4 e}} \\ &\geq \sqrt{\frac{(1-k/k^k)(kn/k^k - k^2 m)}{k^4}} > 1. \end{aligned} \quad (27)$$

При любом $b > 0$ функция x^{bx} возрастает при $x > 1/e$. Поэтому из (20), (22)–(24) и (27) следует, что

$$\begin{aligned}\omega_{\mathcal{D}_0} &\geq \frac{(n - kan)^{(n - kan)/s} (na)^{na/s} ((k - 1)an)^{(k-1)an/s} (kan - ms)^{kan - ms}}{n^{n/s} (na)^{na} ((k - 1)an)^{(k-1)an}} \\ &= \left(\frac{(1 - ka)^{(1 - ak)} a^{ak} (k - 1)^{a(k-1)} k^{aks}}{(k - 1)^{as(k-1)}} \right)^{n/s} \frac{(1 - sm/(kan))^{kan - sm}}{n^{ms} (ka)^{ms}}. \quad (28)\end{aligned}$$

Если n удовлетворяет условию леммы 6, то из (13), (19) и (25) следует, что при $k \geq 2$

$$sm/(kan) < \frac{k^2 k^3 / \varepsilon_k}{kk^{-k}(1 - k^2/(2m))3k^{k+5}/\varepsilon_k} \geq \frac{1}{3k(1 - k^2/(2k^3))} < \frac{1}{4}.$$

Поэтому при $k \geq 2$ имеем

$$\begin{aligned}(1 - sm/(kan))^{kan - sm} / (ka)^{ms} &= \exp\left(-(kan - sm) \sum_{i=1}^{\infty} \frac{1}{i} \left(\frac{sm}{kan}\right)^i\right) / (ka)^{ms} \\ &\geq \exp\left(-(kan - sm) \left(\frac{sm}{kan} + \left(\frac{sm}{kan}\right)^2\right)\right) / (ka)^{ms} \\ &> \frac{e^{-sm}}{(ka)^{ms}} \geq \left(\frac{k^{k-1}}{e}\right)^{ms} > \left(\frac{1}{2}\right)^{ms}.\end{aligned}$$

Из этого факта и (28) следует, что

$$\omega_{\mathcal{D}_0} \geq (2n)^{-ms} \exp\{(n/s)f(n, k, a)\}, \quad (29)$$

где

$$\begin{aligned}f(n, k, a) &= (1 - ak) \ln(1 - ak) + ak \ln a + a(k - 1) \ln(k - 1) \\ &\quad + as(k \ln k - (k - 1) \ln(k - 1)).\end{aligned}$$

Поскольку $s = s_k^0 + \varepsilon_k$, пользуясь (14), получаем

$$\begin{aligned}f(n, k, a) &= (1 - ak) \ln(1 - ak) + ak \ln a \\ &+ a(k^2 \ln k - (k^k - k) \ln(1 - k^{-k+1})) + \varepsilon_k(k \ln k - (k - 1) \ln(k - 1)). \quad (30)\end{aligned}$$

Воспользовавшись (19), (25) и (26), при $k \geq 2$ имеем

$$\begin{aligned}(1 - ak) \ln(1 - ak) - a(k^k - k) \ln(1 - k^{-k+1}) \\ &= (1 - ak) \ln \frac{1 - ak}{1 - k^{-k+1}} + (1 - ak^k) \ln(1 - k^{-k+1}) \\ &\geq (1 - ak^k) \ln(1 - k^{-k+1}) \geq -(1 - ak^k) 2k^{-k+1} \\ &\geq -(k^2/m) 2^{-k+1} \geq -(k^2/k^3) 2^{-k+1} \geq -\varepsilon_k/4. \quad (31)\end{aligned}$$

Кроме того, по аналогии с (15) из (25) следует, что

$$ak \ln a + ak^2 \ln k = ak \ln(ak^k) \geq \frac{1}{k^{k-1}} \left(1 - \frac{k^2}{2m}\right) \ln \left(1 - \frac{k^2}{2m}\right) \geq -\frac{k^2}{2mk^{k-1}} \geq -\frac{\varepsilon_k}{8}. \quad (32)$$

Функция $x \ln x - (x-1) \ln(x-1)$ возрастает при $x > 1$, поэтому при $k \geq 2$

$$k \ln k - (k-1) \ln(k-1) \geq 2 \ln 2. \quad (33)$$

Из (30)–(33) получаем

$$f(n, k, a) \geq \varepsilon_k.$$

Отсюда, из (29) и леммы 5 следует, что

$$\omega_{\mathcal{P}_0} \geq \frac{\exp(n\varepsilon_k/k^2)}{(2n)^{mk^2}}.$$

Лемма 6 доказана.

§ 6. Доказательство основного результата

Пусть $\lambda_{k,s}(f) = Bk(f)/Bs(f)$, $\lambda_{k,s}(n) = \max \lambda_{k,s}(f)$, где максимум берется по всем булевым функциям от n переменных.

Теорема 1. Для булевой функции F_{n,s_k} справедливо соотношение

$$Bk(F_{n,s_k}) \geq \exp(\alpha_k n),$$

где $\alpha_k = \varepsilon_k^2/(2k^5)$.

Доказательство. Из (5) следует, что

$$Bk(F_{n,s_k}) \geq UBk(F_{n,s_k})(2kN)^{-1}, \quad (34)$$

где N — число переменных функции F_{n,s_k} — задается (1). Так как согласно лемме 5 $s \leq k^2$, то имеем

$$N \leq n^{k^2}. \quad (35)$$

Пусть \mathcal{P}_0 — однородная k -программа минимальной сложности, реализующая булеву функцию F_{n,s_k} , т. е. сложность \mathcal{P}_0 равна $UBk(F_{n,s_k})$. Тогда число различных $2m_k$ -элементных последовательностей в \mathcal{P}_0 не превышает $UBk(F_{n,s_k})^{2m_k}$. Отсюда и из леммы 6 следует, что

$$UBk(F_{n,s_k})^{2m_k} \geq \frac{\exp(n\varepsilon_k/k^2)}{(2n)^{mk^2}}. \quad (36)$$

Из (34)–(36) получаем

$$Bk(F_{n,s_k}) \geq \frac{e^{n\varepsilon_k/(k^2 m_k)}}{(2n)^{k^2} 2kn^{k^2}} \geq \frac{e^{n\varepsilon_k^2/(k^5)}}{(2n)^{2k^2}}. \quad (37)$$

Следовательно,

$$Bk(F_{n,s_k}) \geq \exp(\alpha_k n),$$

где $\alpha_k = \varepsilon_k^2/(2k^5)$. Теорема 1 доказана.

Теорема 2. Для любого $k, k \geq 2$, существует положительная константа β_k , зависящая только от k , такая, что

$$\lambda_{k,s_k}(N) \geq \exp(\beta_k N^{1/k^2}).$$

ДОКАЗАТЕЛЬСТВО. В §3 показано (см. (3)), что $Bs_k(F_{n,s_k}) \leq s_k N$. Из этого факта, (35) и теоремы 1 следует, что

$$\lambda_{k,s_k}(N) \geq Bk(F_{n,s_k})/Bs_k(F_{n,s_k}) \geq \exp(\alpha_k N^{1/k^2})/(k^2 N) \geq \exp(\beta_k N^{1/k^2}),$$

где $\beta_k = \varepsilon_k^2/(3k^5)$. Теорема 2 доказана.

Пусть $s_k^1 = \lceil s_k^0 \rceil + 1$. Можно доказать, что имеет место

Теорема 3. Справедливо соотношение

$$\lambda_{k,s_k^1}(N) \geq \exp(N^{1/k^2}/(2k^5)).$$

Ниже приводится таблица значений величин s_k^0, s_k и s_k^1 для небольших значений k .

k	2	3	4	5	6	7	8	9	10
s_k^0	3	5,93	10,16	15,86	23,10	31,92	42,29	54,36	67,82
s_k	4	6	11	16	24	32	43	55	68
s_k^1	4	7	12	17	25	33	44	56	69

В заключение автор благодарит А. Д. Коршунова за помощь в редактировании этой статьи, а также рецензента за ряд ценных замечаний.

ЛИТЕРАТУРА

1. Wegener I. The complexity of Boolean functions. Stuttgart: B. G. Teubner; Chichester: John Wiley & Sons, 1987.
2. Кузьмин В. А. Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ // Методы дискретного анализа в теории кодов и схем: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1976. Вып. 29. С. 11–39.
3. Razborov A. A. Lower bounds for deterministic and nondeterministic branching programs // Fundamentals of Computation Theory. Berlin: Springer-Verl., 1991. P. 47–60. (Lecture Notes in Comput. Sci.; V. 529).
4. Sieling D., Wegener I. New lower bounds and hierarchy results from restricted branching programs // Graph-theoretical Concepts in Computer Science. Berlin: Springer-Verl., 1995. P. 359–370. (Lecture Notes in Comput. Sci.; V. 903).

5. Borodin A., Razborov A., Smolensky R. On lower bounds for read- k -times branching programs // Comput. Complexity. 1993. V. 3, N 1. P. 1–18.
6. Окольнішнікова Е. А. Нижні оцінки складності реалізації характеристических функцій двоичних кодів бінарними програмами // Методи дискретного аналізу в синтезі реалізацій булевих функцій: Сб. науч. тр. Новосибирск: Ін-т математики СО АН СССР, 1991. Вып. 51. С. 61–83. (Пер.: Okol'nishnikova E. A. Lower bounds on branching programs // Siberian Adv. Math. 1993. V. 3, N 1. P. 152–166.)
7. Žak S. An exponential lower bound for one-time only branching programs // Mathematical Foundations of Computer Science. Berlin: Springer-Verl., 1984. P. 562–566. (Lecture Notes in Comput. Sci.; V. 199).
8. Dunne P. E. Lower bounds on the complexity of 1-time only branching programs (preliminary version) // Fundamentals of Computation Theory. Berlin: Springer-Verl., 1985. P. 90–99. (Lecture Notes in Comput. Sci.; V. 199).
9. Babai L., Hajnal P., Szemerédi E., Turán G. A lower bound for read-once-only branching programs // J. Comput. System Sci. 1987. V. 35, N 2. P. 153–162.
10. Окольнішнікова Е. А. Об одном соотношении сложностей булевых функций // VIII Всесоюз. конф. по проблемам теоретической кибернетики. Тез. докл. Горький: Горьк. гос. ун-т, 1988. С. 63.
11. Окольнішнікова Е. А. Схеми из функціональних елементів з мінімально достаточними кон'юнкціями // Методи дискретного аналізу в розв'язанні екстремальних задач: Сб. науч. тр. Новосибирск: Ін-т математики СО АН СССР, 1979. Вып. 33. С. 53–67.
12. Окольнішнікова Е. А. О влиянии одного типа ограничений на сложность схем из функциональных элементов // Методи дискретного аналізу в дослідженні функціональних систем: Сб. науч. тр. Новосибирск: Ін-т математики СО АН СССР, 1981. Вып. 36. С. 46–58.
13. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука. 1990.

Адрес автора:

Россия,
630090 Новосибирск,
Университетский пр., 4,
Институт математики
им. С. Л. Соболева СО РАН

Статья поступила

3 мая 1995 г.