

УДК 519.714

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФОРМУЛАМИ ПРОИЗВЕДЕНИЙ БУЛЕВЫХ ФУНКЦИЙ*)

Д. Ю. Черухин

Рассматривается операция бесповторного произведения булевых функций как обобщение степени булевой функции, введенной Б. А. Субботовской в 1963 г. и использованной ею и автором при решении задачи сравнения булевых базисов. Дан критерий реализуемости последовательности произведений булевых функций формулами в базисе Б с линейной сложностью.

1. Постановка задачи и формулировка результата

Произведение функций можно рассматривать как обобщение степени функции, введенной Б. А. Субботовской [2] и использованной ей и автором [3] при решении задачи сравнения булевых базисов. Данная работа является развитием статьи [5], в которой аналогичный результат был доказан для степеней булевых функций, т. е. произведений с одинаковыми сомножителями.

Понятия и обозначения, используемые в работе без определений, можно найти в [3]. Пусть $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_m)$ — булевы функции. *Бесповторным произведением* функций f и g называется функция

$$(f \otimes g)(x_1, \dots, x_{nm}) = f(g(x_1, \dots, x_m), \dots, g(x_{(n-1)m+1}, \dots, x_{nm})).$$

Функция

$$f^{(m)} = \underbrace{f \otimes \dots \otimes f}_m$$

называется *m -й степенью* функции f . Булева функция $f(x_1, \dots, x_n)$ называется *линейной*, если она представима в виде $a_1x_1 \oplus \dots \oplus a_nx_n \oplus a_0$, где a_0, a_1, \dots, a_n — булевы константы. Булева функция f называется

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01175), Федеральной целевой программы «Интеграция» (объединенный проект АО-110), программы «Университеты России» (проект 992206) и Программы поддержки ведущих научных школ РФФИ (проект 00-15-96103).

обобщенно-монотонной, если по каждой своей переменной функция f либо возрастает, либо убывает.

Конечная система булевых функций называется *базисом*, если каждая булева функция может быть выражена в виде формулы через функции данной системы. Базис, состоящий только из обобщенно-монотонных функций, называется *обобщенно-монотонным*. Булева функция f называется *бесповторно выражимой* в базисе B , если она представима формулой в базисе B , содержащей ровно одно вхождение каждой существенной переменной функции f . Базис называется *линейным*, если в нем бесповторно выразима функция $x \oplus y$. Число вхождений символов переменных в формулу называется *сложностью* формулы. Будем говорить, что последовательность функций f_1, f_2, \dots имеет *линейную сложность* в базисе B , если существует такая константа C , что для любого n сложность функции f_n в классе формул в базисе B не более чем в C раз превосходит число существенных переменных функции f_n .

Теорема 1 [5]. Пусть f — произвольная булева функция, B — произвольный базис. Тогда последовательность функций $f^{(1)}, f^{(2)}, \dots$ имеет в базисе B линейную сложность только в следующих случаях:

- а) функция f существенно зависит не более чем от одной переменной;
- б) функция f линейна, существенно зависит не менее чем от двух переменных и B — не обобщенно-монотонный базис;
- в) функция f нелинейна и бесповторно выразима в базисе B .

Пусть f_1, \dots, f_n — булевы функции. Произведение $f_i \otimes \dots \otimes f_j$, $1 \leq i \leq j \leq n$, называется *линейным блоком* в произведении $f_1 \otimes \dots \otimes f_n$, если

- 1) каждая из функций f_i, \dots, f_j линейна;
- 2) хотя бы одна из функций f_i, \dots, f_j существенно зависит не менее чем от двух переменных;
- 3) если $i > 1$, то функция f_{i-1} нелинейна; если $j < n$, то функция f_{j+1} нелинейна.

Пусть B — базис. Введем обозначение $N_B(f_1 \otimes \dots \otimes f_n)$ следующим образом:

- i) если B — линейный или обобщенно-монотонный базис, то через $N_B(f_1 \otimes \dots \otimes f_n)$ обозначим число таких номеров i , $1 \leq i \leq n$, что функция f_i не выразима бесповторно в B ;
- ii) если базис B нелинеен и не обобщенно-монотонен, то через $N_B(f_1 \otimes \dots \otimes f_n)$ обозначим сумму числа таких номеров i , $1 \leq i \leq n$, что функция f_i нелинейна и не выразима бесповторно в B , и числа линейных блоков в произведении $f_1 \otimes \dots \otimes f_n$.

Ниже доказана следующая

Теорема 2. Пусть B — базис, f_1, f_2, \dots — последовательность булевых функций и для каждого n функция f_n представлена в виде $f_n^1 \otimes \dots \otimes f_n^{k(n)}$. Пусть число существенных переменных каждой из функций f_n^i больше нуля и ограничено сверху некоторой константой, не зависящей ни от n , ни от i . Тогда в базисе B последовательность f_1, f_2, \dots имеет линейную сложность в том и только в том случае, когда величина $N_B(f_n^1 \otimes \dots \otimes f_n^{k(n)})$ ограничена сверху некоторой константой, не зависящей от n .

Сложность формулы F будем обозначать через $L(F)$, сложность функции f в базисе B — через $L_B(f)$, число существенных переменных функции f — через $\text{nes}(f)$, отношение $L_B(f)/\text{nes}(f)$ при $\text{nes}(f) \neq 0$ (называемое *средней сложностью* функции f в базисе B) — через $M_B(f)$.

Докажем три вспомогательных факта.

2. Вспомогательные утверждения

Лемма 1. Пусть B — базис, содержащий константы, f_1, \dots, f_n — булевы функции, существенно зависящие хотя бы от одной переменной, k — натуральное число, $k \leq n$. Тогда найдется такая подфункция φ функции f_k , $\varphi \in \{x, \bar{x}\}$, что выполнено неравенство

$$M_B(f_1 \otimes \dots \otimes f_{k-1} \otimes \varphi \otimes f_{k+1} \otimes \dots \otimes f_n) \leq M_B(f_1 \otimes \dots \otimes f_n).$$

ДОКАЗАТЕЛЬСТВО. Пусть $g = f_1 \otimes \dots \otimes f_{k-1}$ ($g = x$ при $k = 1$) и $h = f_{k+1} \otimes \dots \otimes f_n$ ($h = x$ при $k = n$). Таким образом, $f_1 \otimes \dots \otimes f_n = g \otimes f_k \otimes h$. Обозначим $f = g \otimes f_k \otimes h$. Функцию f представим в виде

$$f = g\left(f_k(h(x^1), \dots, h(x^p)), \dots, f_k(h(x^{(q-1)p+1}), \dots, h(x^{pq}))\right),$$

где x^1, \dots, x^{pq} — наборы, состоящие из попарно различных переменных.

Пусть F — формула в базисе B , реализующая функцию f с наименьшей сложностью. Так как базис B содержит константы, то в формулу F не входят несущественные переменные. Для каждого числа i , $1 \leq i \leq p$, обозначим через L_i суммарное число вхождений в формулу F переменных из наборов $x^i, x^{p+i}, \dots, x^{(q-1)p+i}$. Пусть L_{i_0} — наименьшее из чисел L_i , $1 \leq i \leq p$, отличных от нуля. Тогда переменная x_{i_0} существенна для функции $f_k(x_1, \dots, x_p)$. Следовательно, при некоторых константах $c_1, \dots, c_{i_0-1}, c_{i_0+1}, \dots, c_p$ функция $f_k(c_1, \dots, c_{i_0-1}, x, c_{i_0+1}, \dots, c_p)$ существенно зависит от x . Обозначим ее через φ .

Функция h существенно зависит хотя бы от одной переменной. Поэтому при некоторой подстановке констант вместо всех переменных функции f , не входящих в наборы $x^{i_0}, x^{p+i_0}, \dots, x^{(q-1)p+i_0}$, получится

функция $g \otimes \varphi \otimes h$. При той же подстановке констант в формулу F получится некоторая формула G , реализующая функцию $g \otimes \varphi \otimes h$. При этом

$$L(G) = L_{i_0} \leq \frac{1}{\text{nes}(f_k)} \sum_{i=1}^p L_i = \frac{1}{\text{nes}(f_k)} L(F).$$

Следовательно,

$$\begin{aligned} M_B(g \otimes \varphi \otimes h) &\leq \frac{L(G)}{\text{nes}(g \otimes \varphi \otimes h)} \\ &\leq \frac{L(F)}{\text{nes}(f_k) \cdot \text{nes}(g) \cdot \text{nes}(h)} = \frac{L_B(f)}{\text{nes}(g \otimes f_k \otimes h)} = M_B(f). \end{aligned}$$

Лемма 1 доказана.

Следующая лемма является обобщением леммы 1 из [3] (которая также приведена в работе [5] в качестве леммы 2).

Лемма 2. Пусть f_1, \dots, f_n — булевы функции, существенно зависящие хотя бы от одной переменной, Y — множество, состоящее из некоторых существенных переменных функции $f_1 \otimes \dots \otimes f_n$ и

$$|Y| > \prod_{i=1}^n (\text{nes}(f_i) - 1). \quad (1)$$

Тогда для некоторого числа k , $1 \leq k \leq n$, функцию f_k можно получить из функции $f_1 \otimes \dots \otimes f_n$, подставив в нее константы вместо всех существенных переменных, не входящих в Y , а также вместо некоторых других переменных, навесив отрицания на некоторые переменные и (возможно) на функцию.

Доказательство. Проведем индукцию по n .

Базис индукции: $n = 1$. В этом случае (1) равносильно равенству $|Y| = \text{nes}(f_1)$, т. е. Y есть множество существенных переменных функции f_1 . Не применив никаких преобразований, из функции f_1 получим f_1 .

Индуктивный переход: $n > 1$. Пусть $g = f_2 \otimes \dots \otimes f_n$ и $f = f_1 \otimes g$. Функцию f представим в виде $f = f_1(g(x^1), \dots, g(x^p))$, где x^1, \dots, x^p — наборы, состоящие из попарно различных переменных. Пусть Y_i — множество всех переменных из Y , входящих в набор x^i , $1 \leq i \leq p$, I — множество таких индексов i , $i \in \{1, \dots, p\}$, что переменная x_i существенна для функции $f_1(x_1, \dots, x_p)$. Возможны два случая: 1) для каждого i , $i \in I$, множество Y_i непусто; 2) одно из множеств Y_i , $i \in I$, пусто.

Случай 1. Выберем переменные y_1, \dots, y_p из наборов x^1, \dots, x^p следующим образом: если $i \in I$, то в качестве y_i возьмем переменную

из множества Y_i , в противном случае в качестве y_i возьмем любую переменную из набора x^i . При $i \in I$ функция $g(x^i)$ существенно зависит от y_i . Поэтому из нее при некоторой подстановке констант вместо всех остальных переменных получится функция y_i или \bar{y}_i . При $i \notin I$ подставим произвольные константы вместо всех переменных из x^i , отличных от y_i . В результате этих подстановок констант получим функцию, отличающуюся от f_1 только навешиванием отрицаний на некоторые переменные. При этом константы подставлены вместо всех существенных переменных, не принадлежащих множеству Y . В случае 1 лемма доказана.

Случай 2. Одно из множеств Y_i , $i \in I$, пусто. В этом случае мощность хотя бы одного множества Y_{i_0} с учетом (1) допускает оценку

$$|Y_{i_0}| \geq \frac{|Y|}{|I| - 1} > \frac{1}{\text{nes}(f_1) - 1} \prod_{i=1}^n (\text{nes}(f_i) - 1) = \prod_{i=2}^n (\text{nes}(f_i) - 1),$$

что соответствует неравенству (1) для функции $g = f_2 \otimes \dots \otimes f_n$ и множества Y_{i_0} . Применив к функции $g(x^{i_0})$ и множеству Y_{i_0} предположение индукции, получим, что для некоторого k , $1 \leq k \leq n$, функция f_k может быть получена из $g(x^{i_0})$ с помощью допустимых в условии леммы преобразований. В свою очередь, функция $g(x^{i_0})$ может быть получена из f путем подстановки констант вместо всех переменных, не входящих в набор x^{i_0} и (возможно) навешиванием отрицания на функцию. Таким образом, функция f_k получается из f допустимым способом и случай 2 рассмотрен. Лемма 2 доказана.

Лемма 3. Пусть B — базис, содержащий константы, f_1, \dots, f_n — булевы функции, у каждой из которых число существенных переменных больше нуля и не больше n . Тогда найдется такое k , $1 \leq k \leq n$, что для любой подфункции g функции f_k выполнено неравенство

$$M_B(g) \leq 2M_B(f_1 \otimes \dots \otimes f_n).$$

Доказательство. Пусть $f = f_1 \otimes \dots \otimes f_n$ и F — формула в базисе B , реализующая функцию f с минимальной сложностью. Так как базис B содержит константы, то в формуле F присутствуют только существенные переменные. Пусть Y — множество существенных переменных, каждая из которых входит в F не более $2M_B(f)$ раз. Поскольку существенная переменная входит в F в среднем $M_B(f)$ раз, имеем

$$|Y| \geq \frac{1}{2} \text{nes}(f). \quad (2)$$

Покажем, что выполнено неравенство (1). По условию леммы 3 для любого i , $1 \leq i \leq n$, выполнено неравенство $\text{nes}(f_i) \leq n$. Отсюда следует,

что

$$\frac{\text{nes}(f_i)}{\text{nes}(f_i) - 1} \geq \frac{n}{n - 1}. \quad (3)$$

Используя неравенство $\ln(1 + x) \leq x$, $x > -1$, получаем

$$2\left(\frac{n-1}{n}\right)^n = 2 \cdot e^{n \ln(1-1/n)} \leq 2 \cdot e^{n(-1/n)} = \frac{2}{e} < 1.$$

Отсюда, а также из (2) и (3) следует, что

$$|Y| \geq \frac{1}{2} \text{nes}(f) = \frac{1}{2} \prod_{i=1}^n \text{nes}(f_i) \geq \frac{1}{2} \left(\frac{n}{n-1}\right)^n \prod_{i=1}^n (\text{nes}(f_i) - 1) > \prod_{i=1}^n (\text{nes}(f_i) - 1).$$

Таким образом, неравенство (1) выполнено. Из леммы 2 следует, что для некоторого k , $1 \leq k \leq n$, функция f_k может быть получена из f с помощью операций подстановки констант вместо переменных (обязательно подставляются константы вместо существенных переменных, не входящих в множество Y), навешивания отрицаний на некоторые переменные и (возможно) функцию. Любая подфункция g функции f_k может быть получена из f с помощью аналогичных преобразований. Произведем эти преобразования с формулой F . Кроме того, подставим константы вместо всех переменных, несущественных для g . В результате получим формулу G , реализующую функцию g . Так как базис B содержит константы, то в нем отрицание реализуется со сложностью 1, а значит, навешивание отрицаний не увеличивает сложности. Поскольку каждая переменная, входящая в G , принадлежит множеству Y , число ее вхождений в G не превосходит $2M_B(f)$. Окончательно получаем

$$M_B(g) \leq \frac{L(G)}{\text{nes}(g)} \leq \frac{2M_B(f) \cdot \text{nes}(g)}{\text{nes}(g)} = 2M_B(f).$$

Лемма 3 доказана.

3. Доказательство теоремы 2

Можно считать, что базис B содержит константы. Действительно, поскольку константы неповторно выразимы в любом базисе, множества функций, неповторно выразимых в базисах B и $B \cup \{0, 1\}$, совпадают. Следовательно, базисы B и $B \cup \{0, 1\}$ одновременно являются или не являются линейными. Они также одновременно являются или не являются обобщенно-монотонными. Таким образом, для любых функций $\varphi_1, \dots, \varphi_n$ величины $N_B(\varphi_1 \otimes \dots \otimes \varphi_n)$ и $N_{B \cup \{0, 1\}}(\varphi_1 \otimes \dots \otimes \varphi_n)$ совпадают. Наконец, эти базисы эквивалентны [2, 3]. Поэтому любая последовательность функций, имеющая в одном из них линейную сложность, имеет также линейную сложность в другом базисе.

Обозначим через A наибольшее число существенных переменных у функций f_n^i , $n = 1, 2, \dots$, $i = 1, \dots, k(n)$.

Доказательство разбивается на две части. Сначала докажем верхнюю оценку, т. е. убедимся, что из соотношения

$$N_B(f_n^1 \otimes \dots \otimes f_n^{k(n)}) = O(1), \quad n \rightarrow \infty, \quad (4)$$

следует соотношение

$$L_B(f_n) = O(\text{nes}(f_n)), \quad n \rightarrow \infty, \quad (5)$$

а затем — нижнюю оценку: из невыполнения соотношения (4) выведем невыполнение (5).

Верхняя оценка. Пусть B — наибольшая сложность (в базисе B) функции, имеющей не более A существенных переменных, C — верхняя грань чисел $N_B(f_n^1 \otimes \dots \otimes f_n^{k(n)})$, $n = 1, 2, \dots$. Так как базис B содержит константы, то произвольная функция f бесповторно выражима в B тогда и только тогда, когда ее сложность в B равна числу существенных переменных. Кроме того, для любых функций f и g выполнено неравенство

$$L_B(f \otimes g) \leq L_B(f) \cdot L_B(g). \quad (6)$$

Сначала рассмотрим случай, когда базис B линейный или обобщенно-монотонный. Пусть $W(n)$ — множество таких индексов i , $1 \leq i \leq k(n)$, что функция f_n^i не выражима бесповторно в базисе B . Тогда $|W(n)| \leq C$. Сложность каждой функции, бесповторно выражимой в B , равна числу ее существенных переменных, а сложность функции f_n^i , не выражимой бесповторно в B , не больше B . Поэтому в силу (6) имеем

$$\begin{aligned} L_B(f_n) &= L_B(f_n^1 \otimes \dots \otimes f_n^{k(n)}) \leq B^{|W(n)|} \cdot \prod_{i \notin W(n)} \text{nes}(f_n^i) \\ &\leq B^C \cdot \prod_{i=1}^{k(n)} \text{nes}(f_n^i) = B^C \text{nes}(f_n), \end{aligned}$$

откуда следует (5).

Пусть теперь B — нелинейный и не обобщенно-монотонный базис. Известно [1, 4], что в любом не обобщенно-монотонном базисе сложность последовательности линейных функций $x_1 \oplus \dots \oplus x_t$, $t = 1, 2, \dots$, линейна. Пусть D — такая константа, что для любого t сложность функции $x_1 \oplus \dots \oplus x_t$ в базисе B не больше Dt . Обозначим через $W(n)$ множество таких индексов i , $1 \leq i \leq k(n)$, что функция f_n^i нелинейна и не выражима бесповторно в B , через $P(n)$ — количество линейных блоков в произведении $f_n^1 \otimes \dots \otimes f_n^{k(n)}$, а через $Q(n)$ — множество таких индексов i , что функция f_n^i входит в некоторый линейный блок. Тогда

$|W(n)| + |P(n)| \leq C$, сложность функции f_n^i , $i \in W(n)$, не больше B , сложность функции f_n^i , $i \notin W(n) \cup Q(n)$, равна $\text{nes}(f_n^i)$ и сложность каждого линейного блока не превосходит константы D , умноженной на число существенных переменных в этом блоке, которое равно произведению чисел $\text{nes}(f_n^i)$ по всем функциям f_n^i , входящим в блок.

Функция f_n распадается в произведение линейных блоков, нелинейных функций f_n^i , не выражимых бесповторно в Б, и функций f_n^i , бесповторно выражимых в Б. Поэтому в силу (6) имеем

$$\begin{aligned} L_B(f_n) &\leq D^{|P(n)|} \prod_{i \in Q(n)} \text{nes}(f_n^i) \cdot B^{|W(n)|} \cdot \prod_{i \notin W(n) \cup Q(n)} \text{nes}(f_n^i) \\ &\leq (D + B)^{|P(n)| + |W(n)|} \prod_{i=1}^{k(n)} \text{nes}(f_n^i) \leq (D + B)^C \text{nes}(f_n). \end{aligned}$$

Неравенство (5) доказано, тем самым установлена верхняя оценка.

Нижняя оценка. Пусть B_1 — число функций, существенно зависящих не более чем от A переменных (с точностью до добавления и изъятия несущественных переменных), C_1 — произвольная константа. Найдем такое число t , что $M_B(f_t) \geq C_1$. Тем самым нижняя оценка будет доказана.

Рассмотрим произвольную функцию θ , существенно зависящую не более чем от A^2 переменных, для которой и данного базиса Б не выполнено ни одно из условий а)–в) теоремы 1. Тогда по теореме 1 последовательность $\theta^{(1)}, \theta^{(2)}, \dots$ имеет нелинейную сложность в базисе Б. Следовательно, существует такое число $m(\theta)$, что $M_B(\theta^{(m(\theta))}) \geq 2C_1$.

Обозначим через m максимальное из чисел $m(\theta)$ по всем функциям θ , существенно зависящим не более чем от A^2 переменных (заметим, что функции, отличающиеся только фиктивными переменными, имеют одну и ту же сложность). Положим $D_1 = 2B_1^2 m A^{4m} + B_1$. Так как величина $N_B(f_n^1 \otimes \dots \otimes f_n^{k(n)})$ неограничена при $n \rightarrow \infty$, то существует такое число n_0 , для которого она не меньше D_1 . В качестве t выберем n_0 .

Построим такую подфункцию φ функции f_n , что $M_B(\varphi) \leq M_B(f_t)$ и φ представима в виде

$$\varphi = \varphi_0 \otimes g \otimes \varphi_1 \otimes g \otimes \dots \otimes g \otimes \varphi_p, \quad (7)$$

где функции $\varphi_0, \dots, \varphi_p$ принадлежат множеству $\{x, \bar{x}\}$, g является произведением одной или двух функций из f_t^i , $1 \leq i \leq k(t)$, и некоторого числа функций одной переменной и g для данного базиса Б не удовлетворяет ни одному из условий а)–в) теоремы 1.

Для построения функции φ будем применять лемму 1, а именно в произведении $f_t^1 \otimes \dots \otimes f_t^{k(t)}$ будем заменять ненужные сомножители

функциями x, \bar{x} так, чтобы на каждом шаге средняя сложность полученной функции была не больше $M_B(f_t)$. Если базис B нелинейный и не обобщенно-монотонный, то сначала из каждого линейного блока удалим все функции, существенно зависящие не менее чем от двух переменных, кроме одной из них. Полученное произведение обозначим через $g_t^1 \otimes \dots \otimes g_t^{k(t)}$. Если базис B линейный или обобщенно-монотонный, то исходное произведение $f_t^1 \otimes \dots \otimes f_t^{k(t)}$ обозначим через $g_t^1 \otimes \dots \otimes g_t^{k(t)}$.

Таким образом, для любого базиса B величина $N_B(g_t^1 \otimes \dots \otimes g_t^{k(t)})$ равна $N_B(f_t^1 \otimes \dots \otimes f_t^{k(t)})$ и равна числу сомножителей g_t^i , не выражимых бесповторно в B . Далее будем работать с произведением $g_t^1 \otimes \dots \otimes g_t^{k(t)}$. Среди сомножителей, не выражимых бесповторно в B , выделим тот, который входит в полученное произведение наибольшее число раз (функции, отличающиеся только фиктивными переменными, не различаем). Обозначим его через h . Рассмотрим два случая: 1) функция h нелинейна либо базис B обобщенно-монотонен; 2) функция h линейна и B не обобщенно-монотонен.

Случай 1. Функцию h примем за g , все функции из произведения, существенно зависящие не менее чем от двух переменных и отличные от g , заменим функциями x, \bar{x} , идущие подряд функции одного аргумента объединим в одну и получим требуемое представление (7). Поскольку функция g не выражима бесповторно в B , она существенно зависит не менее чем от двух переменных. Ясно, что либо функция g нелинейна и не выражима бесповторно в B , либо функция g линейна и базис B обобщенно-монотонен. Поэтому ни одно из условий а)–в) теоремы 1 не выполнено.

Случай 2. Так как функция h не выражима бесповторно в B , то базис B нелинеен. Кроме того, B не обобщенно-монотонен. Выше для такого базиса B в каждом линейном блоке мы оставили ровно по одной функции, существенно зависящей не менее чем от двух переменных. Поэтому различные экземпляры функции h принадлежат разным линейным блокам. Следовательно, между ними есть хотя бы одна нелинейная функция. Оставим в произведении сомножители h и по одной нелинейной функции между ними; остальные сомножители заменим функциями одной переменной. Объединим функции одного аргумента с нелинейными функциями. Таким образом, получим подфункцию функции f_t вида

$$\varphi' \otimes h \otimes \psi_1 \otimes h \otimes \psi_2 \otimes \dots \otimes \psi_s \otimes h \otimes \varphi'', \quad (8)$$

где φ' и φ'' — функции одной переменной и ψ_1, \dots, ψ_s — нелинейные функции.

Среди функций ψ_1, \dots, ψ_s выберем такую, которая встречается наибольшее число раз (функции, отличающиеся только фиктивными переменными, считаем равными), и обозначим ее через ψ . Положим

$g = h \otimes \psi$. В произведении (8) крайний справа сомножитель h и все пары соседних сомножителей вида $h \otimes \psi_j$, для которых $\psi_j \neq \psi$, заменим функциями x, \bar{x} . Объединив идущие подряд функции одной переменной, получим искомую функцию вида (7). Функция g нелинейна (так как ψ нелинейна) и не выражима бесповторно в B (так как h не выражима). Таким образом, ни одно из условий а)–в) теоремы 1 не выполнено.

Оба случая рассмотрены, и функция φ построена. В процессе построения функции φ мы не более двух раз применяли процедуру выбора одной функции из B_1 возможных. Кроме того, перед вторым выбором число сомножителей уменьшили на 1 за счет крайнего правого сомножителя h . Поэтому число p сомножителей g в произведении (7) удовлетворяет неравенству (используем определение D_1 и выбор числа t)

$$\begin{aligned} p &\geq \frac{1}{B_1} \left(\frac{1}{B_1} N_B(g_t^1 \otimes \dots \otimes g_t^{k(t)}) - 1 \right) = \frac{1}{B_1^2} N_B(f_t^1 \otimes \dots \otimes f_t^{k(t)}) - \frac{1}{B_1} \\ &\geq \frac{1}{B_1^2} D_1 - \frac{1}{B_1} = \frac{1}{B_1^2} (2B_1^2 mA^{4m} + B_1) - \frac{1}{B_1} = 2mA^{4m}. \end{aligned}$$

Заметим, что в (7) можно уменьшить число сомножителей g , заменив некоторые из них функциями одной переменной и введя новые функции φ_j . Поэтому можно считать, что $p = 2mA^{4m}$. Кроме того, можно считать, что функция g в качестве подфункции содержит тождественную функцию x . Действительно, в противном случае функция \bar{g} содержит подфункцию x и g можно заменить на $\bar{x} \otimes \bar{g}$, принять \bar{g} за g и ввести новые функции φ_j . При этом снова получим вид (7).

Воспользовавшись тождеством $g \otimes \bar{x} = \bar{x} \otimes g^*$ (здесь g^* — функция, двойственная к g , определяемая тождеством $g^* = \bar{x} \otimes g \otimes \bar{x}$), все отрицания в (7) можно перенести влево и привести функцию φ к виду

$$\varphi = \varphi''' \otimes g_1 \otimes \dots \otimes g_p,$$

где φ''' — функция одной переменной, каждая функция g_j , $j = 1, \dots, p$, равна либо g , либо g^* . Пусть $\chi = \varphi''' \otimes \varphi$. Тогда $\chi = g_1 \otimes \dots \otimes g_p$. Так как базис B содержит константы, то отрицание реализуется в нем со сложностью 1, а значит, функции φ и χ имеют одинаковую сложность в B . Таким образом, $M_B(\chi) = M_B(\varphi)$.

Пользуясь равенством $p = 2mA^{4m}$, произведение $g_1 \otimes \dots \otimes g_p$ разобьем на A^{4m} блоков G_1, \dots, G_q (где $q = A^{4m}$) по $2m$ множителей в каждом так, чтобы выполнялось равенство $\chi = G_1 \otimes \dots \otimes G_q$. Так как $\text{pes}(g^*) = \text{pes}(g) \leq A^2$, то $\text{pes}(G_j) = \text{pes}(g)^{2m} \leq A^{4m} = q$, $j = 1, \dots, q$. Применив к функциям G_1, \dots, G_q лемму 3, получим, что для некоторого j_0 и любой подфункции G функции G_{j_0} выполнено неравенство $M_B(G) \leq 2M_B(\chi)$.

Обозначим через g' такую функцию из множества $\{g, g^*\}$, которая входит в блок G_{j_0} наибольшее число раз. Это число не меньше m . Заметим, что $\text{pes}(g') \leq A^2$, функция g , а значит, и функция g' для данного

базиса B не удовлетворяют ни одному из условий а)–в) теоремы 1. Поэтому определено число $m(g')$ и оно не превосходит m . Таким образом, функция g' встречается в блоке G_{j_0} не менее $m(g')$ раз. Так как функция g содержит подфункцию x , то и функция g' содержит подфункцию x . Удалив из блока G_{j_0} лишние сомножители, заменив их тождественными подфункциями, получим функцию $(g')^{(m(g'))}$. Обозначим ее через G' .

Итак, G' является подфункцией функции G_{j_0} . По определению числа $m(g')$ средняя сложность функции G' не меньше $2C_1$. Таким образом, имеем

$$M_B(f_i) \geq M_B(\varphi) = M_B(\chi) \geq \frac{1}{2} M_B(G') \geq \frac{1}{2} \cdot 2C_1 = C_1.$$

Нижняя оценка установлена. Теорема 2 доказана.

Автор благодарит чл.-корр. РАН О. Б. Лупанова за внимание к работе.

ЛИТЕРАТУРА

1. **Перязев Н. А.** Сложность представлений булевых функций формулами в немонотонных базисах // Дискретная математика и информатика. Вып. 2. Иркутск: Изд-во Иркут. ун-та, 1995.
2. **Субботовская Б. А.** О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, № 4. С. 784–787.
3. **Черухин Д. Ю.** Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 77–122.
4. **Черухин Д. Ю.** О сложности реализации линейной функции формулами в конечных булевых базисах // Дискрет. математика. 2000. Т. 12, вып. 1. С. 135–144.
5. **Черухин Д. Ю.** О сложности реализации формулами степеней булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8, № 4. С. 103–111.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва, Россия.

E-mail:

dyucher@mech.math.msu.su

Статья поступила
25 июля 2001 г.