ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2001. Серия 1. Том 8, № 4, 103–111

УДК 519.714

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФОРМУЛАМИ СТЕПЕНЕЙ БУЛЕВЫХ ФУНКЦИЙ*)

Д. Ю. Черухин

Рассматриваются операция бесповторного произведения булевых функций и порожденная ею операция возведения булевой функции в степень. Степени булевой функции были рассмотрены Б. А. Субботовской (впервые в 1963 г.) и автором при решении задачи сравнения булевых базисов. В настоящей статье дан критерий, позволяющий установить, реализуется ли последовательность степеней функции f формулами в базисе Б с линейной или нелинейной сложностью.

1. Постановка задачи и формулировка результата

Степень булевой функции была введена Б. А. Субботовской [4] и впоследствии рассмотрена ею же [1] и автором [5–7] для решения задачи сравнения булевых базисов. В данной статье степень функции выступает как самостоятельный предмет исследования. В работах [1, 5–7] для достаточно широкого множества функций f и базисов Б были получены нелинейные нижние оценки сложности последовательности степеней функции f при реализации формулами в базисе Б. В настоящей статье получен критерий, позволяющий для произвольной функции f и полного конечного базиса Б указать, реализуется ли последовательность степеней функции f с линейной или нелинейной сложностью формулами в базисе Б. Данная работа во многом опирается на статью [7].

Дадим необходимые определения. Понятия и обозначения, используемые без определений, можно найти в [7]. Конечная система булевых функций называется *базисом*, если каждая булева функция может быть выражена в виде формулы через функции данной системы. *Сложностью*

*) 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).

формулы считаем число вхождений в нее символов переменных. Сложность формулы F обозначим через $L(F)$, сложность функции f в базисе Б — через $L_{\text{Б}}(f)$, число существенных переменных функции f — через $\text{nes}(f)$, отношение $L_{\text{Б}}(f)/\text{nes}(f)$ при $\text{nes}(f) \neq 0$ — через $M_{\text{Б}}(f)$. Будем говорить, что в базисе Б последовательность функций $f_1, f_2, \ldots$ имеет *линейную сложность*, если $M_{\text{Б}}(f_m) = O(1)$ при $m \to \infty$. В противном случае будем говорить, что в Б эта последовательность функций имеет *нелинейную сложность*. Будем говорить, что в базисе Б последовательность функций имеет *строго нелинейную сложность*, если сложность в Б любой ее подпоследовательности нелинейна.

Пусть $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_k)$ — булевы функции. Определим *бесповторное произведение* функций f и g следующим образом:

$$(f \otimes g)(x_1, \ldots, x_{nk}) = f(g(x_1, \ldots, x_k), \ldots, g(x_{(n-1)k+1}, \ldots, x_{nk})).$$

Функция

$$f^{(m)} = \underbrace{f \otimes f \otimes \ldots \otimes f}_{m}$$

называется *m-й степенью* функции f. Функции $f^{(m)}$ впервые рассмотрела Б. А. Субботовская [4].

Булева функция f называется *линейной*, если она представима в виде $f(x_1, \ldots, x_n) = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_0$, где $a_0, a_1, \ldots, a_n$ — некоторые булевы константы; в противном случае функция f называется *нелинейной*. Скажем, что функция f *бесповторно выразима* [4] в базисе Б (через множество функций M), если существует такая формула F в базисе Б (над множеством M), реализующая функцию f, что каждая существенная переменная функции f входит в F ровно один раз. Такая формула F называется *бесповторной*. Функция f называется *монотонной*, если она возрастает (нестрого) по каждой переменной; *антимонотонной*, если f убывает по каждой переменной; и *обобщенно-монотонной*, если по некоторым переменным (возможно, ни по одной) f возрастает, а по остальным (возможно, ни по одной) — убывает.

Основным результатом данной работы является следующая

Теорема. *Пусть f — произвольная булева функция, Б — произвольный базис. Тогда в базисе Б последовательность функций $f^{(1)}$, $f^{(2)}, \ldots$ имеет 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 в базисе Б существует функция, не являющаяся обобщенно-монотонной;*

в) *функция f нелинейна и бесповторно выразима в базисе Б.*

В любом другом случае последовательность $f^{(1)}, f^{(2)}, \ldots$ *в базисе* Б *имеет строго нелинейную сложность.*

2. Вспомогательные утверждения

Для доказательства теоремы введем вспомогательные понятия и докажем ряд утверждений. Функция g называется *подфункцией* функции f, если g может быть получена из f подстановкой некоторых констант вместо некоторого (возможно, пустого) множества переменных. Функция вида $x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k}$, $i_1 < i_2 < \ldots < i_k$, $k \geqslant 2$, называется *конъюнкцией*; функция вида $x_{i_1} \vee x_{i_2} \vee \ldots \vee x_{i_k}$, $i_1 < i_2 < \ldots < i_k$, $k \geqslant 2$, называется *дизъюнкцией.*

Лемма 1. *Пусть* f *— такая нелинейная булева функция, что* f *и* $\bar{f}$ *отличны от дизъюнкций и конъюнкций. Тогда при некотором числе* $m(f)$, $m(f) \leqslant 3$, *среди подфункций функции* $f^{(m(f))}$ *имеются конъюнкция двух переменных и дизъюнкция двух переменных.*

Доказательство. Рассмотрим три случая: 1) функция f монотонна; 2) функция f антимонотонна; 3) функция f не является ни монотонной, ни антимонотонной.

Случай 1. Пусть f является монотонной функцией от n переменных. Набор $\sigma \in \{0,1\}^n$ назовем *нижним единичным* набором функции f, если $f(\sigma) = 1$, и $f(\tau) = 0$ для любого набора τ, строго меньшего σ (при покоординатном сравнении). Пусть $\sigma^1, \ldots, \sigma^k$ — все различные нижние единичные наборы функции f, $\sigma^i = (\sigma_1^i, \ldots, \sigma_n^i)$, $1 \leqslant i \leqslant k$. Значение функции f на произвольном наборе равно единице тогда и только тогда, когда этот набор не меньше хотя бы одного из нижних единичных наборов. Поэтому

$$f(x_1, \ldots, x_n) = \bigvee_{i=1}^{k} \left(\bigwedge_{j:\, \sigma_j^i = 1} x_j \right) \tag{1}$$

(здесь $\wedge$ — конъюнкция).

Так как функция f тождественно не равна единице, то в каждом из нижних единичных наборов есть хотя бы одна единица. Если в каждом из этих наборов имеется ровно одна единица, то согласно (1) функция f является дизъюнкцией, что противоречит условию леммы. Таким образом, имеется нижний единичный набор, в котором содержится не меньше двух единиц. Без ограничения общности можно считать, что $\sigma_1^1 = \sigma_2^1 = 1$. Рассмотрим функцию g, полученную из f при подстановке констант $\sigma_3^1, \ldots, \sigma_n^1$ вместо переменных $x_3, \ldots, x_n$ соответственно. Имеем $g(1,1) = f(\sigma^1) = 1$. Вместе с тем для любого набора (τ_1, τ_2),

отличного от $(1,1)$, набор $(\tau_1, \tau_2, \sigma_3^1, \ldots, \sigma_n^1)$ строго меньше набора σ^1. Поэтому $g(\tau_1, \tau_2) = f(\tau_1, \tau_2, \sigma_3^1, \ldots, \sigma_n^1) = 0$. Итак, $g(x_1, x_2) = x_1 x_2$ — конъюнкция двух переменных.

Рассуждая двойственным образом, найдем подфункцию функции f, являющуюся дизъюнкцией двух переменных.

В качестве числа $m(f)$ возьмем 1. В случае 1 лемма доказана.

Случай 2. Функция $\bar{f}$ монотонна и по условию леммы не является ни конъюнкцией, ни дизъюнкцией. В силу уже рассмотренного случая 1 среди подфункций функции $\bar{f}$ есть конъюнкция двух переменных и дизъюнкция двух переменных. Далее, функция f существенно зависит хотя бы от одной переменной и убывает по ней. Поэтому среди подфункций функции f есть отрицание. Тогда функция $\bar{f}$ является подфункцией функции $f^{(2)}$. Значит, конъюнкция двух переменных и дизъюнкция двух переменных суть подфункции функции $f^{(2)}$. Положив $m(f) = 2$, завершим рассмотрение случая 2.

Случай 3. Так как функция f нелинейна, то у нее существует нелинейная подфункция от двух переменных. Пусть g — такая подфункция. Любая нелинейная функция двух переменных, в том числе конъюнкция и дизъюнкция, представима в виде $g(x_1 \oplus \tau_1, x_2 \oplus \tau_2) \oplus \tau_0$ при некоторых константах τ_0, τ_1, τ_2. Функция f возрастает хотя бы по одной существенной переменной и убывает хотя бы по одной существенной переменной. Поэтому отрицание и тождественная функция являются ее подфункциями. Тогда функция $g(x_1 \oplus \tau_1, x_2 \oplus \tau_2) \oplus \tau_0$ является подфункцией функции $g(f(x^1), f(x^2)) \oplus \tau_0$ (здесь x^1 и x^2 — наборы переменных, x^1 содержит x_1, x^2 содержит x_2, все переменные в наборе (x^1, x^2) попарно различны), которая есть подфункция функции $f^{(2)} \oplus \tau_0$. Последняя функция является подфункцией функции $f^{(3)}$. Итак, конъюнкция двух переменных и дизъюнкция двух переменных являются подфункциями функции $f^{(3)}$. Положим $m(f) = 3$. Случай 3 рассмотрен. Лемма 1 доказана.

В работе [7] (см. также [5, предложение 1]) сформулирована (в иных терминах) и доказана

Лемма 2 [7, лемма 1, с. 83–84]. *Пусть f — булева функция, существенно зависящая от всех своих n переменных, $n \geqslant 2$; m — натуральное число; Y — подмножество множества переменных функции $f^{(m)}$ и*

$$|Y| > (n-1)^m. \tag{2}$$

Тогда существует такая подфункция g функции $f^{(m)}$, что все переменные подфункции g принадлежат множеству Y, и f может быть получена из g удалением несущественных переменных, переименованием переменных, навешиванием отрицаний на некоторые переменные и (возможно) навешиванием отрицания на функцию.

Лемма 3. *Пусть* Б — *произвольный базис,* f — *булева функция,* h — *ее подфункция, и пусть в базисе* Б *последовательность* $f^{(1)}, f^{(2)}, \ldots$ *имеет линейную сложность. Тогда в* Б *последовательность* $h^{(1)}, h^{(2)}, \ldots$ *имеет линейную сложность.*

Доказательство. Базис Б эквивалентен базису Б $\cup \{1, 0, \bar{x}\}$ [4–7]. Если последовательность функций имеет линейную сложность в некотором базисе, то она имеет линейную сложность в любом эквивалентном ему базисе. Поэтому достаточно доказать лемму в случае, когда базис Б содержит отрицание и константы. Далее, можно считать, что функция f существенно зависит от всех своих переменных. Действительно, можно рассмотреть подфункцию φ, полученную из f удалением несущественных переменных. Тогда сложности функций $f^{(m)}$ и $\varphi^{(m)}$ равны, также равны количества их существенных переменных. Наконец, можно считать, что число переменных функции f не меньше двух. В противном случае число переменных функции h меньше двух. В этом случае последовательность $h^{(1)}, h^{(2)}, \ldots$ имеет линейную сложность.

Итак, $M_{\text{Б}}(f^{(m)}) = O(1)$ при $m \to \infty$. Поэтому существует такая константа C, что для любого m справедливо неравенство $M_{\text{Б}}(f^{(m)}) \leqslant C$. Рассмотрим произвольное натуральное число m_0. Покажем, что $M_{\text{Б}}(h^{(m_0)}) \leqslant 2C$. Тем самым лемма будет доказана. Обозначим через n число существенных переменных функции $f^{(m_0)}$ и положим $m_1 = m_0 n$. Пусть F — формула в базисе Б, реализующая функцию $f^{(m_1)}$ со сложностью, не превосходящей $C \cdot \operatorname{nes}(f^{(m_1)})$. Обозначим через Y множество существенных переменных функции $f^{(m_1)}$, каждая из которых входит в формулу F не более $2C$ раз. Тогда

$$|Y| \geqslant \frac{1}{2}\operatorname{nes}(f^{(m_1)}). \tag{3}$$

Используя неравенство $\ln(1+x) \leqslant x$, $x > -1$, имеем

$$\ln\left(1 - \frac{1}{n}\right)^n = n \ln\left(1 - \frac{1}{n}\right) \leqslant -n\frac{1}{n} < -\ln 2 = \ln\frac{1}{2}.$$

Следовательно,

$$(n-1)^n = n^n\left(1 - \frac{1}{n}\right)^n < \frac{1}{2}n^n. \tag{4}$$

Представим функцию $f^{(m_1)}$ в виде $(f^{(m_0)})^{(n)}$. Тогда из (3) и (4) следует, что

$$|Y| \geqslant \frac{1}{2}\operatorname{nes}(f^{(m_0)})^n = \frac{1}{2}n^n > (n-1)^n. \tag{5}$$

К функции $f^{(m_0)}$, степени $m = n$ и множеству Y применим лемму 2. Из (5) следует требуемое неравенство (2). Согласно лемме 2 существует такая подфункция g функции $f^{(m_1)}$, содержащая только переменные из

множества Y, что из нее можно получить функцию $f^{(m_0)}$ с помощью операций удаления несущественных переменных, переименования переменных, навешивания отрицаний на переменные и функцию. Наконец, функция $h^{(m_0)}$ является подфункцией функции $f^{(m_0)}$.

Подставим в формулу F те же константы вместо переменных, которые подставлялись в функцию $f^{(m_1)}$ для получения подфункции g. Полученную формулу обозначим через G. Каждая существенная переменная функции g, входящая в G, принадлежит множеству Y, а значит, входит в G не более $2C$ раз. Затем с формулой G произведем необходимые преобразования: подстановку констант вместо переменных, переименование переменных, навешивание на них отрицаний, навешивание отрицания на всю формулу так, чтобы получить формулу H, реализующую функцию $h^{(m_0)}$ и содержащую только существенные переменные (вместо несущественных переменных можно подставить одинаковые константы).

Так как базис Б содержит отрицание и константы, то H — формула в базисе Б. Каждая переменная входит в H не большее число раз, чем она входила в формулу G, т. е. не больше $2C$ раз. Поэтому $L(H) \leqslant 2C \cdot \mathrm{nes}(h^{(m_0)})$. Следовательно, $M_{\text{Б}}(h^{(m_0)}) \leqslant 2C$. Лемма 3 доказана.

Пусть $\circ$ — любая из операций $\&, \vee, \oplus$. Тогда через $\circ_p$ обозначим функцию $x_1 \circ x_2 \circ \ldots \circ x_p$. Базис называется *линейным*, если в нем бесповторно выразима функция $\oplus_2$. В противном случае базис называется *нелинейным*.

3. Доказательство теоремы

Необходимо и достаточно доказать следующие утверждения: (i) при выполнении любого из условий а)–в) последовательность степеней функции f имеет линейную сложность в базисе Б; (ii) при одновременном невыполнении условий а)–в) последовательность степеней функции f имеет строго нелинейную сложность в базисе Б. Доказательство пункта (i) достаточно очевидно (для условия б) оно содержится, например, в [3, 8]; для условия в) формулу, реализующую степень функции f, можно построить из бесповторной формулы в базисе Б, реализующей f). Доказательство пункта (ii) разбивается на два случая: (ii.а) функция f линейна, существенно зависит не менее чем от двух переменных и все функции из базиса Б обобщенно-монотонны; (ii.б) функция f нелинейна и невыразима бесповторно в базисе Б.

Случай (ii.а). Последовательность $f^{(1)}, f^{(2)}, \ldots$ есть некоторая подпоследовательность последовательности линейных функций $\oplus_1, \oplus_2, \ldots$ Строгая нелинейность сложности для последовательности линейных функций в соответствующих базисах была доказана Н. А. Перязевым [3] (для некоторых из этих базисов ее доказала Б. А. Мучник [2];

результат из [3] доказан также в [8]). Так как сложность последовательности $\oplus_1, \oplus_2, \ldots$ строго нелинейна, то сложность ее подпоследовательности $f^{(1)}, f^{(2)}, \ldots$ строго нелинейна.

Случай (ii.б). Конъюнкции, дизъюнкции и их отрицания бесповторно выразимы в любом базисе [4], а f невыразима бесповторно в базисе Б. Поэтому ни f, ни $\bar{f}$ не равна ни конъюнкции, ни дизъюнкции. Кроме того, f нелинейна. Согласно лемме 1 существует такое число $m(f)$, что в качестве подфункций функция $f^{(m(f))}$ содержит конъюнкцию и дизъюнкцию двух переменных. Подфункцией конъюнкции является тождественная функция. Таким образом, конъюнкция, дизъюнкция и тождественная функция являются подфункциями функции $f^{(m(f))}$, которую мы обозначим через g.

Рассмотрим теорему 12 из [7, с. 116–118]. В качестве $Б_1$ возьмем базис Б, а в качестве $Б_2$ — либо множество $\{g, 0, 1, \bar{x}\}$, если функция g монотонна, либо множество $\{g, 0, 1\}$ в противном случае. Заметим, что множество $Б_2$ является базисом (функция g нелинейна, как степень нелинейной функции f, 0 не сохраняет единицы и несамодвойственна, 1 не сохраняет нуля, g или $\bar{x}$ немонотонна). Не все функции из базиса $Б_2$ бесповторно выразимы в $Б_1$. Например, функция g, как степень функции f, невыразима бесповторно в $Б_1$. Положим $\varepsilon = 1$. Согласно теореме 12 существует такая функция f_1, что в базисе $Б_1$ последовательность ее степеней имеет нелинейную сложность. Рассмотрим доказательство теоремы 12 и покажем, что выбранная в нем функция f_1 бесповторно выразима через функции $g, 0, 1$. Как и в доказательстве теоремы 12, рассмотрим два случая: 1) базис $Б_2$ линеен, базис $Б_1$ нелинеен; 2) либо базис $Б_2$ нелинеен, либо базис $Б_1$ линеен.

В **случае 1** выбирается число t_1 и в качестве f_1 берется функция $\&_2 \otimes \oplus_{t_1}$. Заметим, что если функция g монотонна, то все функции из базиса $Б_2$ обобщенно-монотонны, а значит, все их бесповторные суперпозиции обобщенно-монотонны. В то же время функция $\oplus_2$ не обобщенно-монотонна. Поэтому она невыразима бесповторно в базисе $Б_2$, т. е. базис $Б_2$ нелинеен, что не соответствует рассматриваемому случаю. Таким образом, функция g немонотонна, поэтому $Б_2 = \{g, 0, 1\}$. Функции $\&_2$ и $\oplus_2$ бесповторно выразимы в базисе $Б_2$. Следовательно, функция f_1 бесповторно выразима в $Б_2$, т. е. через множество функций $g, 0, 1$.

В **случае 2** в качестве θ берется функция из $Б_2$, невыразимая бесповторно в базисе $Б_1$. Такая функция единственна: g. Поэтому $\theta = g$. Далее берется подфункция ψ функции θ, полученная отбрасыванием несущественных переменных, выбирается число t_1 и в качестве f_1 берется функция $\vee_{t_1} \otimes \&_{t_1} \otimes \psi$. Функции $\&_2$, $\vee_2$ и ψ являются подфункциями функции g, а значит, бесповторно выразимы через $g, 0, 1$. Следовательно, функция f_1 бесповторно выразима через $g, 0, 1$.

Итак, случаи 1 и 2 рассмотрены. Функция f_1 бесповторно выразима через $g, 0, 1$. Покажем, что f_1 есть подфункция некоторой степени функции g. Действительно, рассмотрим формулу F, бесповторно выражающую f_1 через $g, 0, 1$. Все несущественные переменные в F заменим одинаковыми константами, затем все константы заменим попарно различными переменными, ранее не присутствовавшими в формуле. Далее, пользуясь тем, что тождественная функция есть подфункция функции g, будем заменять переменные, лежащие не на максимальной глубине в построенной формуле, на элементарные формулы $g(y_1, \ldots, y_k)$ (содержащие попарно различные переменные $y_1, \ldots, y_k$, ранее в формулу не входившие) до тех пор, пока все переменные не окажутся на одной глубине. Полученная формула реализует некоторую степень функции g, а при некоторой подстановке констант из нее получается формула, реализующая функцию f_1. Таким образом, функция f_1 является подфункцией некоторой степени функции g. Поскольку функция g есть некоторая степень функции f, f_1 есть также подфункция функции $f^{(m_0)}$ для некоторого m_0.

Как следует из теоремы 12 [7], последовательность степеней функции f_1 имеет нелинейную сложность в базисе Б_1, т. е. в базисе Б. Применив отрицание леммы 3, получим, что в базисе Б последовательность степеней функции $f^{(m_0)}$ имеет нелинейную сложность. Каждая степень функции $f^{(m_0)}$ является также степенью функции f. Согласно утверждению 4 [7, с. 116] величина $M_{\text{Б}}(f^{(m)})$ возрастает по m. Так как сложность некоторой подпоследовательности последовательности $f^{(1)}, f^{(2)}, \ldots$ нелинейна, то сложность всей этой последовательности строго нелинейна. Теорема доказана.

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

ЛИТЕРАТУРА

1. **Мучник Б. А.** Об одном критерии сравнимости базисов при реализации функций алгебры логики формулами // Мат. заметки. 1967. Т. 1, вып. 5. С. 515–524.

2. **Мучник Б. А.** Оценка сложности реализации линейной функции формулами в некоторых базисах // Кибернетика. 1970. № 4. С. 29–38.

3. **Перязев Н. А.** Сложность представлений булевых функций формулами в немонолинейных базисах // Дискрет. математика и информатика. Вып. 2. Иркутск: Изд-во Иркут. ун-та, 1995.

4. **Субботовская Б. А.** О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, № 4. С. 784–787.

5. **Черухин Д. Ю.** Об одной бесконечной последовательности улучшающихся булевых базисов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 79–95.

6. **Черухин Д. Ю.** О предплохих булевых базисах // Дискрет. математика. 1999. Т. 11, вып. 2. С. 118–160.

7. **Черухин Д. Ю.** Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 77–122.

8. **Черухин Д. Ю.** О сложности реализации линейной функции формулами в конечных булевых базисах // Дискрет. математика. 2000. Т. 12, вып. 1. С. 135–144.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва, Россия.
E-mail:
dyucher@mech.math.msu.su

Статья поступила
25 июля 2001 г.