Дискретная математика

том 30 выпуск 4 * 2018

УДК 519.714.4 DOI https://doi.org/10.4213/dm1513

Обобщенная сложность линейных булевых функций

© 2018 г. Н. П. Редькин*

Изучается обобщенная (по базисам) сложность реализации линейных булевых функций схемами из функциональных элементов в произвольных функционально полных базисах; сложность всякой схемы при этом определяется числом функциональных элементов в ней. Пусть $L^*(n)$ — наименьшее возможное число элементов, достаточное для реализации произвольной линейной булевой функции от n переменных схемой в любом функционально полном базисе. Устанавливается, что $L^*(0) = L^*(1) = 3$ и $L^*(n) = 7(n-1)$ при любом натуральном $n \geqslant 2$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 18.01.00337 "Проблемы синтеза, сложности и надежности в теории управляющих систем").

Ключевые слова: булева функция, схема из функциональных элементов, сложность булевой функции, функция Шеннона

Введение

Данная работа посвящена исследованию сложности реализации индивидуальных булевых функций схемами из функциональных элементов [1]. Для сложности схем будем использовать классическую меру сложности: сложность схемы S в базисе B измеряем числом функциональных элементов в S и обозначаем через $L_B(S)$. Число $L_B(f) = \min L_B(S)$, где минимум берётся по всем схемам в базисе B, реализующим булеву функцию f, считаем сложностью (реализации) функции f в базисе B. Как и в [2], введем обобщенную функцию Шеннона $L^*(f)$, полагая $L^*(f) = \sup L_B(f)$, где верхняя грань берется по всем функционально полным конечным базисам; обобщенную функцию Шеннона $L^*(f)$ будем также называть обобщенной сложностью функции f. В нашем случае при рассматриваемой мере сложности верхняя грань достигается (см. [2]) и „sup” можно заменить на „max”.

В качестве конкретных функций рассматриваются линейные булевы функции, которые занимают особое место среди индивидуальных булевых функций. Среди булевых функций, существенно зависящих от n переменных $x_1, ..., x_n$, всего две линейные: $l_n(\widetilde{x}) = x_1 \oplus ... \oplus x_n$ и $\overline{l_n}(\widetilde{x}) = x_1 \oplus ... \oplus x_n \oplus 1$. Но при этом линейные булевы функции составляют один (самый „жидкий”) из пяти предполных классов [3]

*Место работы: МГУ имени М. В. Ломоносова, e-mail: npredkin@mail.ru

и весьма часто встречаются в теории и на практике, например, в исследованиях по функциональной полноте, в различных представлениях булевых функций, при построении легкотестируемых схем из функциональных элементов с моделированием полиномов Жегалкина, в помехоустойчивом кодировании. В исследованиях ряда авторов [4–11] получены окончательные результаты по сложности реализации линейных булевых функций схемами из функциональных элементов, имеющих не более двух входов, причем в [7–11] помимо сложности устанавливается еще и структура минимальных схем в рассматриваемых базисах.

Ниже находится обобщенная сложность линейных функций.

Теорема 1. *Для любого натурального* $n \geqslant 2$

$L^*(x_1 \oplus ... \oplus x_n) = L^*(x_1 \oplus ... \oplus x_n \oplus 1) = 7(n-1)$;
при $n = 0 : L^*(0) = L^*(1) = 3$,
при $n = 1 : L^*(x) = 0, L^*(x \oplus 1) = 3$.

Доказательство. Верхние оценки $L^*(0) \leqslant 3, L^*(1) \leqslant 3, L^*(x \oplus 1) \leqslant 3$ очевидно следуют из рассуждений при доказательстве теоремы 7 (о функциональной полноте) в [3]. Более того, из этих же рассуждений следует

Утверждение 1. *В любом функционально полном базисе можно построить схему из трех функциональных элементов, реализующую обе булевы константы и инверсию.*

Нетрудно также заметить, что для базисов $B_1 = \{xy, \overline{x}\}, B_2 = \{x \vee y, \overline{x}\}, B_3 = \{x(y \vee \overline{z}), 0, 1\}$ выполняются соответственно оценки $L_{B_1}(0) \geqslant 3$, $L_{B_2}(1) \geqslant 3$, $L_{B_3}(\overline{x}) \geqslant 3$ (при доказательстве первых двух неравенств достаточно перебрать неизоморфные схемы с одним входом из одного элемента и из двух элементов, а при обосновании последнего неравенства достаточно обратить внимание на тот факт, что функция $\overline{x}$ не сохраняет 0, не сохраняет единицу и существенно зависит от одной переменной, а потому в построении схемы для $\overline{x}$ должны участвовать все три элемента из B_3). Следовательно, $L^*(0) = L^*(1) = L^*(\overline{x}) = 3$; тривиальное равенство $L^*(x) = 0$ следует из того очевидного факта, что тождественную функцию x можно реализовать схемой с одним входом, не содержащей функциональных элементов.

Для базиса $B_1 = \{x\&y, \overline{x}\}$ в [4], в частности, установлено, что $L_{B_1}(x_1 \oplus ... \oplus x_n) = L_{B_1}(x_1 \oplus ... \oplus x_n \oplus 1) = 7(n-1)$ при $n \geqslant 2$, откуда следуют нижние оценки $L^*(x_1 \oplus ... \oplus x_n) \geqslant 7(n-1)$ и $L^*(x_1 \oplus ... \oplus x_n \oplus 1) \geqslant 7(n-1)$. Для завершения доказательства теоремы достаточно для любого функционально полного конечного базиса B подтвердить верхние оценки $L_B(x_1 \oplus ... \oplus x_n) \leqslant 7(n-1)$ и $L_B(x_1 \oplus ... \oplus x_n \oplus 1) \leqslant 7(n-1)$ при $n \geqslant 2$, которые, очевидно, следуют из оценок $L^*(x_1 \oplus x_2) \leqslant 7$ и $L^*(x_1 \oplus x_2 \oplus 1) \leqslant 7$.

Последние неравенства и устанавливаются в нижеследующих разделах.

1. Схемы в базисах, содержащих линейные функции, отличные от констант

Как и в [2], далее будем рассматривать расширения базисов [12]. Под расширением базиса B будем понимать всякий базис $B', B' \supseteq B$, любая функция которого либо

совпадает с какой-нибудь функцией из B, либо может быть получена отождествлением переменных из какой-нибудь функции из B. Каждому элементу расширения B', реализующему отсутствующую в B функцию, можно сопоставить эквивалентную ему (т. е. реализующую ту же самую функцию) схему из одного элемента базиса B, получающуюся из некоторого элемента базиса B „склеиванием" некоторых его входов. Отсюда вытекает, что для произвольной функции f выполняется равенство $L_B(f) = L_{B'}(f)$ и для получения верхних оценок сложности реализации булевых функций схемами над B достаточно получить эти оценки для схем над произвольным расширением B' базиса B. Как обычно, предполагаем, что если $\phi(x_1, ..., x_k)$ — некоторая функция базиса, то ей отвечает и некоторый элемент данного базиса с k входами, реализующий эту функцию. Ниже через B' будем обозначать максимальное (по мощности, т. е. по числу содержащихся в B' функций) расширение исходного базиса B.

Если B' содержит линейную функцию от двух или более переменных, то верхние оценки $L(x \oplus y) \leqslant 7, L(x \sim y) \leqslant 7$ легко получаются с учетом утверждения 1. Далее будем считать, что B' содержит $\overline{x}$, но не содержит линейных функций от двух или более переменных.

Предположим, что B' содержит нелинейную булеву функцию $\phi(x, y)$, которая существенно зависит от двух переменных, т. е.
$\phi(x, y) \in \{xy, x\overline{y}, \overline{x}y, \overline{x}\,\overline{y}, x \vee y, x \vee \overline{y}, \overline{x} \vee y, \overline{x} \vee \overline{y}\}$. Во всех таких случаях из элементов „$\overline{x}$", „$\phi(x, y)$" (т. е. из элементов, реализующих $\overline{x}, \phi(x, y)$) легко построить схему, реализующую любую линейную функцию от двух переменных и содержащую не более семи элементов (это подтверждается также и в работах [4–11]). Далее считаем, что в B' нет нелинейных булевых функций от двух переменных.

Булеву функцию $xy \oplus xz \oplus yz \oplus \alpha x \oplus \beta y \oplus \gamma z \oplus \varepsilon$, где $\alpha, \beta, \gamma, \varepsilon \in \{0, 1\}$, назовем особенной.

Лемма 1 ([12]). *Из всякой нелинейной и неособенной функции от трех или более переменных отождествдением переменных можно получить либо нелинейную функцию от двух переменных, либо особенную функцию.*

Поскольку B' обладает функциональной полнотой и по нашему условию не содержит нелинейных булевых функций от двух переменных, то в B' в соответствии с леммой 1 должна быть особенная функция. Легко заметить, что в качестве такой особенной функции можно рассмотреть одну из следующих функций:
1) $\phi_1(x, y, z) = xy \oplus xz \oplus yz \oplus x \oplus y \oplus z \oplus \varepsilon$,
2) $\phi_2(x, y, z) = xy \oplus xz \oplus yz \oplus x \oplus y \oplus \varepsilon$,
3) $\phi_3(x, y, z) = xy \oplus xz \oplus yz \oplus x \oplus \varepsilon$,
4) $\phi_4(x, y, z) = xy \oplus xz \oplus yz \oplus \varepsilon$
(из всякой иной особенной функции переименованием переменных получается одна из функций $\phi_1, ..., \phi_4$). Случай вхождения в B' особенной функции $\phi_1(x, y, z)$ исключается, так как $\phi_1(x, x, z) = x \oplus z \oplus \varepsilon$, а в B' линейной функции от двух переменных нет.

Утверждение 2. *Базис B' содержит элемент, реализующий булеву константу.*

Утверждение 2 следует из леммы 1 работы [2].

Предположим теперь, что в B' есть $\phi_2(x,y,z) = xy \oplus xz \oplus yz \oplus x \oplus y \oplus \varepsilon$. Используя один элемент, реализуем (согласно утверждению 2) булеву константу. При подстановке в $\phi_2(x,y,z)$ нуля вместо y получаем $\phi_2(x,0,z) = xz \oplus x \oplus \varepsilon$, а при подстановке единицы вместо y получаем $\phi_2(x,1,z) = xz \oplus z \oplus \varepsilon \oplus 1$; в обоих случаях получается либо импликация, либо отрицание импликации. Отсюда следует, что если на вход „y" элемента E, реализующего $\phi_2(x,y,z)$, подавать константу, а на входы „x" и „z" подавать, скажем так, „свободные" переменные x и z, то элемент E будет реализовывать импликацию (или отрицание импликации) от свободных переменных. Но при наличии в базисе элемента, реализующего импликацию (или отрицание импликации), и элемента, реализующего инверсию, уже можно как нетрудно заметить, построить схему из не более чем пяти элементов, реализующую любую линейную булеву функцию от двух переменных. В итоге получаем, что в рассматриваемом случае любую линейную булеву функцию от двух переменных можно реализовать схемой, содержащей не более шести элементов.

Случай, когда B' содержит $\phi_3(x,y,z) = xy \oplus xz \oplus yz \oplus x \oplus \varepsilon$ исключается, так как при отождествлении $y \equiv z$ получаем $\phi_3(x,y,y) = x \oplus y \oplus \varepsilon$, а в B' по предположению нет линейных булевых функций от двух переменных.

Рассмотрим последний случай, когда B' содержит $\phi_4(x,y,z) = xy \oplus xz \oplus yz \oplus \varepsilon$. Согласно лемме 1 из [2] с использованием двух элементов из B' реализуем обе булевы константы. Если $\varepsilon = 1$, то, подавая на вход „z" элемента E, реализующего $\phi_4(x,y,z)$, константу 0, получим на выходе элемента E функцию $\overline{xy}$ (штрих Шеффера). Поскольку схемой из пяти элементов „штрих Шеффера" уже можно реализовать любую линейную булеву функцию от двух переменных, то в итоге получается, что и схемой в базисе B', насчитывающей не более семи элементов, можно реализовать любую линейную функцию от двух переменных.

Если $\varepsilon = 0$, то подавая на входы „z" элементов, реализующих $\phi_4(x,y,z)$, константы 0 и 1, получим на выходах этих элементов функции xy и $x \vee y$. Поскольку из конъюкторов, дизъюнкторов и инверторов уже можно строить схемы , насчитывающие по четыре элемента и реализующие линейные функции от двух переменных, то получается, что и в базисе B' можно стоить схемы, насчитывающие по шесть элементов и реализующие линейные булевы функции от двух переменных.

Далее будем считать, что в B' инверсия отсутствует.

2. Схемы в базисах, не содержащих инверсию и линейные функции от двух и более переменных

Для любой булевой константы $\sigma, \sigma \in \{0,1\}$, в B' есть функция, не сохраняющая σ. При отождествлении переменных этой функции может получиться либо инверсия, либо константа $\overline{\sigma}$. Поскольку инверсии в B' нет, то это означает, что в B' есть константа $\overline{\sigma}$, а так как в качестве σ можно выбрать как 0, так и 1, то выполняется следующее утверждение.

Утверждение 3. *Расширение B' содержит обе булевы константы.*

Среди булевых функций от одной переменной немонотонной является только инверсия, которая по предположению отсутствует в B'. Но в силу функциональной

полноты B' содержит немонотонную функцию. Значит, в B' имеется немонотонная функция ϕ, существенно зависящая не менее чем от двух переменных.

Предположим, что в B' имеется немонотонная функция $\phi(x, y)$, существенно зависящая от двух переменных. Эта функция не может быть шефферовой (т. е. $\overline{xy}$ или $\overline{x \vee y}$), поскольку при отождествлении переменных шефферовой функции получается инверсия, а инверсии в B' нет. Учитывая, что $\phi(x, y)$ не может быть и линейной функцией (линейных функций от двух переменных в B' нет), получаем, что $\phi(x, y)$ —одна из функций $x^\sigma y^{\overline{\sigma}}, x^\sigma \vee y^{\overline{\sigma}}$, где $\sigma \in \{0, 1\}$.

При имеющихся условиях для B' справедливо следующее утверждение.

Утверждение 4. *Любую линейную булеву функцию от двух переменных можно реализовать схемой над B', сложность которой не превосходит* 6.

Доказательство. Схему над B', реализующую линейную булеву функцию $x \oplus y \oplus c, c \in \{0, 1\}$, строим так. Согласно утверждению 3 с использованием двух элементов E_0 и E_1 из B' реализуем булевы константы 0 и 1. В B' есть элемент E_ϕ, реализующий немонотонную булеву функцию ϕ. Если теперь (в соответствии с леммой о немонотонной функции [3, стр. 37]) выделить некоторый вход этого элемента и подать на него x, а на остальные входы подходящим образом подать булевы константы, то на выходе данного элемента получим $\overline{x}$; таким образом, элемент E_ϕ далее при построении схемы можно использовать еще и как инвентор. Из элементов же, реализующих инверсию и одну из функций $x^\sigma y^{\overline{\sigma}}, x^\sigma \vee y^{\overline{\sigma}} (\sigma \in \{0, 1\})$, как нетрудно заметить, уже можно построить схему, содержащую четыре элемента и реализующую заданную линейную функцию $x \oplus y \oplus c$. С учетом элементов E_0 и E_1, реализующих константы, можем получить схему из шести элементов, реализующую заданную линейную булеву функцию от двух переменных. Утверждение доказано.

С учетом последнего утверждения остается рассмотреть еще один случай, когда (дополнительно к прежним условиям) B' еще и не содержит немонотонных функций от двух переменных. Но тогда в силу полноты системы B' в ней должна быть некоторая немонотонная функция $\phi(x_1, ..., x_k)$, которая существенно зависит не менее чем от трех переменных (по условиям на B'). Коль скоро ϕ — немонотонная функция, существуют такие переменная x_i и набор значений $(\sigma_1, ..., \sigma_{i-1}, \sigma_{i+1}, ..., \sigma_k)$ остальных переменных, что $\phi(\sigma_1, ..., \sigma_{i-1}, x_i, \sigma_{i+1}, ..., \sigma_k) = \overline{x_i}$. Без ограничения общности будем считать, что $i = 1$, а в наборе $\sigma_2, ..., \sigma_k$ первые l разрядов – нули, а остальные $k - l - 1$ разрядов – единицы. Из функции ϕ путем отождествлений и переобозначений переменных $x_2 \equiv ... \equiv x_{l+1} = y, x_{l+2} \equiv ... \equiv x_k \equiv z, x_1 \equiv x$ получим некоторую немонотонную функцию $\psi(x, y, z)$, существенно зависящую от трех переменных, и эта функция имеется в B' (с учетом определения максимального расширения).

Представим функцию ψ полиномом Жегалкина P:

$$P = \alpha_1 xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus \alpha_5 x \oplus \alpha_6 y \oplus \alpha_7 z \oplus \alpha_8,$$

где $\alpha_1, ..., \alpha_8 \in \{0, 1\}$.

Утверждение 5. *Из функции $\psi(x, y, z)$ подстановкой вместо какой-нибудь переменной подходящей булевой константы можно получить немонотонную булеву функцию, существенно зависящую от двух переменных.*

Доказательство. Рассмотрим следующие варианты значений коэффициентов полинома P, представляющего функцию $\psi(x, y, z)$. Предположим, что $\alpha_8 = 1$. Пусть, далее, хотя бы один из коэффициентов $\alpha_2, \alpha_3, \alpha_4$, например, α_2 равен единице. Подставим в P вместо z константу 0. Получим полином $xy \oplus \alpha_5 x \oplus \alpha_6 y \oplus 1$, который, как легко заметить, представляет (при любых значениях α_5, α_6) немонотонную булеву функцию, существенно зависящую от переменных x, y. Предположим теперь, что $\alpha_2 = \alpha_3 = \alpha_4 = 0$. По условиям $\psi(x, y, z)$ существенно зависит от всех трех переменных и не является линейной функцией. Значит, $\alpha_1 = 1$ и функцию ψ представляет полином $P = xyz \oplus \alpha_5 x \oplus \alpha_6 y \oplus \alpha_7 \oplus 1$. Но в таком случае при отождествлении $y \equiv z$ получаем полином $xy \oplus \alpha_5 x \oplus (\alpha_6 \oplus \alpha_7) y \oplus 1$, представляющий немонотонную булеву функцию, существенно зависящую от двух переменных x и y, которая (по условиям) отсутствует в расширении B'. Полученное противоречие исключает последнее преположение.

Будем считать ниже $\alpha_8 = 0$. В зависимости от значений коэффициентов $\alpha_5, \alpha_6, \alpha_7$ рассмотрим следующие основные случаи: а) $\alpha_5 = \alpha_6 = \alpha_7 = 1$, б) $\alpha_5 = \alpha_6 = 1$, $\alpha_7 = 0$, в) $\alpha_5 = 1$, $\alpha_6 = \alpha_7 = 0$, г) $\alpha_5 = \alpha_6 = \alpha_7 = 0$ (любой другой набор значений коэффициентов $\alpha_5, \alpha_6, \alpha_7$ переименованием переменных сводится к одному из указанных в случаях а)$\div$ г)).

а) Имеем $P = \alpha_1 xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus x \oplus y \oplus z$. Случай $\alpha_1 = ... = \alpha_4 = 1$ исключается, так как полином $P = xyz \oplus xy \oplus xz \oplus yz \oplus x \oplus y \oplus z$ представляет дизъюнкцию $x \vee y \vee z$, а функция $\psi(x, y, z)$ по предположению немонотонная. Следовательно, хотя бы один из коэффициентов $\alpha_1 \div \alpha_4$ равен 0. Допустим, что $\alpha_1 = 0$. Если при этом $\alpha_2 = \alpha_3 = \alpha_4 = 0$, то $P = x \oplus y \oplus z$ и при подстановке $z \equiv 0$ получаем немонотонную функцию $x \oplus y$. А если хотя бы один из коэффициентов $\alpha_2, \alpha_3, \alpha_4$ отличен от нуля, например $\alpha_2 = 1$, то $P = xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus x \oplus y \oplus z$ и при подстановке $z \equiv 1$ получаем из P полином $xy \oplus (\alpha_3 \oplus 1)x \oplus (\alpha_4 \oplus 1)y \oplus 1$, представляющий, как нетрудно заметить, немонотонную булеву функцию, существенно зависящую от переменных x и y.

Допустим, что $\alpha_1 = 1$. Поскольку случай $\alpha_1 = ... = \alpha_4 = 1$ исключается, то хотя бы один из коэффициентов $\alpha_2, \alpha_3, \alpha_4$, скажем, α_4 равен нулю. В таком случае $P = xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus x \oplus y \oplus z$ и при подстановке $x \equiv 0$ получаем полином $y \oplus z$, представляющий немонотонную булеву функцию от двух переменных.

б) Имеем $P = \alpha_1 xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus x \oplus y$. Поскольку ψ существенно зависит от всех трех переменных, то в полиноме P присутствует хотя бы одно слагаемое, содержащее z, т. е. $\alpha_1 + \alpha_3 + \alpha_4 \geqslant 1$. Если $\alpha_4 = 1$, то при $x \equiv 0$ получим полином $yz \oplus y$, представляющий немонотонную булеву функцию от переменных y, z. Аналогично, если $\alpha_3 = 1$, то при $y \equiv 0$ опять же получаем полином $xz \oplus x$, представляющий немонотонную булеву функцию от переменных x, z. Предположим, что $\alpha_3 = \alpha_4 = 0$; в таком случае $\alpha_1 = 1$ (так как ψ зависит существенно от трех переменных) и $P = xyz \oplus \alpha_2 xy \oplus x \oplus y = xy(z \oplus \alpha_2) \oplus x \oplus y$. При подстановке $z \equiv \alpha_2$ получаем немонотонную функцию $z \oplus y$.

в) Имеем $P = \alpha_1 xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus x$. Пусть $\alpha_2 + \alpha_3 \geqslant 1$ и, без ограничения общности, $\alpha_2 = 1$. Тогда $P = \alpha_1 xyz \oplus xy \oplus \alpha_3 xz \oplus \alpha_4 yz \oplus x$ и при $z \equiv 0$ получаем полином $xy \oplus x$, представляющий немонотонную булеву функцию от двух переменных. Допустим, что $\alpha_2 + \alpha_3 = 0$. Тогда $P = \alpha_1 xyz \oplus \alpha_4 yz \oplus x$ и в силу

существенной зависимости функции ψ от трех переменных хотя бы один из коэффициентов α_1, α_4 не равен нулю. Возможны три набора, задающие коэффициенты α_1, α_4: (0, 1), (1, 0), (1, 1). В первом случае (при $(\alpha_1, \alpha_4) = (0, 1)$) получим полином $yz \oplus x$, из которого подстановкой $z \equiv 1$ получаем немонотонную функцию $x \oplus y$. Во втором случае получаем полином $xyz \oplus x$; этот случай следует исключить, так как из полинома $xyz \oplus x$ отождествлением переменных $y \equiv z$ получается нелинейная и немонотонная функция $xy \oplus x$, которой не должно быть в B'. В третьем случае получаем полином $xyz \oplus yz \oplus x$, который задает функцию $yz(x \oplus 1) \oplus x = \overline{x}yz \oplus x = x \vee yz$, являющуюся монотонной; но функция $\psi(x, y, z)$ не является монотонной и потому этот случай исключается.

г) Имеем $P = \alpha_1 xyz \oplus \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz$. Предположим, что $\alpha_1 = 1$. Поскольку $\psi(x, y, z)$ — немонотонная функция, должно выполняться условие $\alpha_1 + \alpha_2 + \alpha_3 \geqslant 1$.

В зависимости от значений коэффициентов $\alpha_1, \alpha_2, \alpha_3$ рассмотрим далее три подслучая:
1) $\alpha_2 = 1, \alpha_3 = \alpha_4 = 0$,
2) $\alpha_2 = \alpha_3 = 1, \alpha_4 = 0$,
3) $\alpha_2 = \alpha_3 = \alpha_4 = 1$
(все остальные наборы значений коэффициентов $\alpha_2, \alpha_3, \alpha_4$ сводятся к указанным переименованием переменных).

Для первого подслучая $P = xyz \oplus xy$. При подстановке $y = 1$ получаем полином $xz \oplus x$, представляющий немонотонную функцию $x\overline{z}$. Второй подслучай исключается, так как ему отвечает полином, представляющий монотонную булеву функцию $xyz \oplus xy \oplus xz = x(yz \oplus y \oplus z) = x(y \vee z)$. Третьему подслучаю отвечает полином $P = xyz \oplus xy \oplus xz \oplus yz$, из которого подстановкой $z \equiv 1$ получается немонотонная функция $x \oplus y$.

Предположим теперь, что $\alpha_1 = 0$, т. е. $P = \alpha_2 xy \oplus \alpha_3 xz \oplus \alpha_4 yz$. Поскольку функция $\psi(x, y, z)$ существенно зависит от всех трех переменных и не является монотонной, должны выполняться условия $\alpha_1 + \alpha_2 + \alpha_3 \geqslant 2$ и $\alpha_1 + \alpha_2 + \alpha_3 \neq 3$, из которых следует $\alpha_1 + \alpha_2 + \alpha_3 = 2$. Предположим (без ограничения общности), что $\alpha_2 = \alpha_3 = 1$, $\alpha_4 = 0$. Получим $P = xy \oplus xz$; полагая $x \equiv 1$, получаем немонотонную функцию $y \oplus z$. Утверждение доказано.

Завершая доказательство теоремы, схему S для любой заданной булевой функции $x \oplus y \oplus \varepsilon$, где $\varepsilon \in \{0, 1\}$, строим следующим образом. С использованием двух элементов E_0 и E_1 из B' в соответствии с утверждением 3 реализуем обе булевы константы. Подавая на один из входов элемента E_ψ, реализующего $\psi(x, y, z)$, подходящую константу (с выхода одного из элементов E_0, E_1) согласно утверждению 5 получаем на выходе этого элемента какую-то немонотонную булеву функцию ψ^*. Если $\psi^* \in \{\overline{xy}, \overline{x \vee y}\}$, то из пяти элементов E_ψ можно достроить подсхему, реализующую $x \oplus y \oplus \varepsilon$; всего в схеме S окажется (с учетом E_0 и E_1) не более семи элементов. Если же ψ^* — функция вида $x\overline{y}$ или $x \vee \overline{y}$, то, подавая на вход «x» элемента E_ψ подходящую булеву константу, можем получить на выходе этого элемента инверсию $\overline{y}$ и использовать данный элемент в качестве инвертора. Из элементов, реализующих одну из функций $x\overline{y}$, $x \vee \overline{y}$ и инверсию, уже можно составить подсхему не более чем из четырех элементов, реализующую $x \oplus y \oplus \varepsilon$; всего в схеме S окажется не более шести элементов. Теорема доказана.

Список литературы

1. Лупанов О.Б., *Асимптотические оценки сложности управляющих систем*, М.: Изд-во МГУ, 1984, 138 с.
2. Редькин Н.П., “Об одном обобщении функции Шеннона”, *Дискретная математика*, **29**:2 (2017), 70–83; англ. пер.: Redkin N. P., “A generalization of Shannon function”, *Discrete Math. Appl.*, **28**:5 (2018), 309–318.
3. Яблонский С.В., *Введение в дискретную математику*, М.: Высшая школа, 2003, 384 с.
4. Редькин Н.П, “Доказательство минимальности некоторых схем из функциональных элементов”, *Проблемы кибернетики*, 1970, № 23, 83–101.
5. Редькин Н.П., “О минимальной реализации линейной функции схемой из функциональных элементов”, *Кибернетика*, 1971, № 6, 31–38.
6. Шкребела И.С., “О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$”, *Дискретная математика*, **15**:4 (2003), 100–112; англ. пер.: Shkrebela I. S., “On complexity of realisation of linear Boolean functions by circuits of functional elements over the basis $\{x \to y, \overline{x}\}$”, *Discrete Math. Appl.*, **13**:5 (2003), 483–496.
7. Комбаров Ю.А., “О минимальных схемах для линейных булевых функций”, *Вестн. Моск. ун-та. Матем. Мех.*, 2011, № 6, 41–44; англ. пер.: Kombarov Yu. A., “The minimal circuits for linear Boolean functions”, *Moscow University Mechanics Bulletin*, **66**:6 (2011), 260–263.
8. Комбаров Ю.А., “О минимальных реализациях линейных булевых функций”, *Дискретный анализ и исследование операций*, **19**:3 (2012), 39–57.
9. Комбаров Ю.А., “О минимальных схемах для линейных функций в некоторых базисах”, *Дискретная математика*, **25**:1 (2013), 33–44; англ. пер.: Kombarov Yu. A., “On minimal circuits for linear functions over some bases”, *Discrete Math. Appl.*, **23**:1 (2013), 39–51.
10. Комбаров Ю.А., “О сложности реализации линейной булевой функции в базисе Шеффера”, *Вестн. Моск. ун-та. Матем. Мех.*, 2013, № 2, 49–53; англ. пер.: Kombarov Yu. A., “Complexity of realization of a linear Boolean function in Sheffer’s basis”, *Moscow Univ. Math. Bull.*, **68**:2, 114–117.
11. Комбаров Ю.А., “О минимальных схемах в базисе Шеффера для линейных булевых функций”, *Дискретный анализ и исследование операций*, **20**:4 (2013), 65–87.
12. Редькин Н.П., “О полных проверяющих тестах для схем из функциональных элементов”, *Математические вопросы кибернетики*, 1989, № 2, 198–222.

Статья поступила 03.04.2018.