Краткие сообщения

УДК 519.95

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ РЕАЛИЗАЦИИ ЛИНЕЙНЫХ ФУНКЦИЙ СХЕМАМИ В ОДНОМ БАЗИСЕ ИЗ МНОГОВХОДОВЫХ ЭЛЕМЕНТОВ

Ю. А. Комбаров [1]

Заметка посвящена реализации линейных булевых функций схемами из функциональных элементов в базисе U_∞, состоящем из всех элементов, реализующих функции вида $x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k}$. Доказано, что всякая схема в базисе U_∞, реализующая линейную булеву функцию от n переменных, состоит не менее чем из $2\frac{1}{9}n+\Theta(1)$ элементов.

Ключевые слова: схемы из функциональных элементов, сложность схем, линейная булева функция, минимальная схема.

The paper is focused on realization of parity functions by circuits in the basis U_∞. This basis contains all functions of the form $x_1^{\sigma_1}\&\ldots\&x_k^{\sigma_k}$. It is proved that every circuit over U_∞ computing a parity function of n variables contains at least $2\frac{1}{9}n+\Theta(1)$ gates.

Key words: Boolean circuits, circuit complexity, parity function, minimal circuit.

Введение. Работа посвящена изучению схем из функциональных элементов [1], реализующих линейные булевы функции (однородную линейную функцию $l_n(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n$ и неоднородную линейную функцию $\overline{l_n}(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n\oplus 1$). Базис (т.е. множество функциональных элементов, из которых разрешается строить схемы), схемы в котором мы рассматриваем, определяется следующим образом:

$$U_\infty=\{x_1^{\sigma_1}\&\ldots\&x_n^{\sigma_n}\mid n\in\mathbb{N},\,\sigma_1,\ldots\sigma_n\in\{0,1\}\}.$$

Другими словами, базис U_∞ состоит из конъюнкторов с произвольным количеством входов, любой вход которых может быть инвертирован.

В работе [2] были получены первые оценки сложности реализации линейных функций схемами в базисе U_∞:

$$2n+\Theta(1)\leqslant L_{U_\infty}(l_n)=L_{U_\infty}(\overline{l_n})\leqslant 2.5n+\Theta(1)$$

(через $L_B(f)$ обозначается сложность реализации булевой функции f в базисе B, определяемая как минимальное количество функциональных элементов, достаточное для реализации функции f схемой в базисе B). В [3] была улучшена верхняя оценка: $L_{U_\infty}(l_n)=L_{U_\infty}(\overline{l_n})\leqslant 2\frac{1}{3}n+\Theta(1)$. Настоящая работа посвящена улучшению нижней оценки. Основной результат работы — следующая теорема.

Теорема. *Имеет место оценка* $L_{U_\infty}(l_n)=L_{U_\infty}(\overline{l_n})\geqslant 2\frac{1}{9}n+\Theta(1)$.

В доказательстве теоремы используется метод забивающих констант. Опишем основную идею этого подхода.

Пусть задана схема, для которой нам требуется доказать, что ее сложность велика. Выберем в схеме один или несколько входов и подадим на них константы. После этого появится возможность удаления нескольких элементов (например, элементов, реализующих константы или функции одной переменной). Будем продолжать шаги подстановки констант и удаления элементов индуктивно до тех пор, пока константы не будут поданы на все или почти на все входы схемы. Общее число элементов, которые были удалены во время этого процесса, и будет нижней оценкой сложности схемы.

Метод забивающих констант используется практически во всех доказательствах нижних оценок сложности схем в полных конечных базисах (см., например, [4–9]). При этом характерной чертой доказательств, использующих метод, является значительный объем: как правило, приходится рассматривать множество вариантов строения схемы и для каждого варианта указывать подходящую подстановку констант.

[1] *Комбаров Юрий Анатольевич* — канд. физ.-мат. наук, ассист. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: yuri.kombarov@gmail.com.

Kombarov Yuri Anatol'evich — Candidate of Physical and Mathematical Sciences, Assistant, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

В настоящей работе используется обобщение метода забивающих констант, предложенное в [8] и связанное с применением вспомогательной меры сложности схем и выбором такой меры путем решения задачи линейного программирования.

Сложность линейных функций установлена для многих базисов, как состоящих из двухвходовых элементов [5, 6, 9], так и содержащих элементы с произвольным числом входов [2, 10, 11].

Определения и вспомогательные утверждения. Приведем определение схемы из функциональных элементов в базисе U_∞ (далее — просто схемы), которое мы будем использовать. Это определение отличается от определения, данного в [1], но эквивалентно ему.

Схемой будем называть ориентированный граф без ориентированных циклов, каждому ребру которого приписано число из $\{0, 1\}$, а каждой вершине нулевой входной степени — переменная из алфавита переменных $\{x_1, x_2, \ldots\}$ (никаким двум вершинам нулевой входной степени не приписаны одинаковые метки). Одна из вершин схемы дополнительно выделена и называется *выходной* вершиной. Вершины схемы, которым приписаны переменные, называются *входами*, все остальные вершины — *элементами*. Число, приписанное ребру, будем называть *знаком* ребра. Число ребер, исходящих из входа, будем называть *степенью* этого входа.

Каждой вершине схемы можно индуктивно сопоставить булеву функцию, *реализуемую* этой вершиной. Функция, реализуемая входом, есть переменная, приписанная этому входу. Пусть E — элемент схемы, $e_1, \ldots, e_k$ — все ребра схемы, входящие в E, а $V_1, \ldots, V_k$ — вершины схемы, из которых выходят ребра $e_1, \ldots, e_k$. Если $\varphi_1, \ldots, \varphi_k$ — булевы функции, реализуемые вершинами $V_1, \ldots, V_k$, а $\sigma_1, \ldots, \sigma_k$ — знаки ребер $e_1, \ldots, e_k$ соответственно, то элемент E реализует функцию $\varphi_1^{\sigma_1} \& \ldots \& \varphi_k^{\sigma_k}$ (здесь через φ^σ обозначается функция φ, если $\sigma = 1$, и функция $\overline{\varphi}$, если $\sigma = 0$). Говорят, что схема *реализует* булеву функцию f, если выходная вершина схемы реализует эту функцию.

Пусть S — схема. Введем обозначения для некоторых ее числовых характеристик, которые необходимо отслеживать при доказательстве теоремы:

$L(S)$ — число элементов в S;

$F(S)$ — сумма степеней всех входов S;

$T(S)$ — число входов в S степени, большей трех или равной трем.

Число $L(S)$ будем называть *сложностью* схемы S. *Мерой* схемы S будем называть величину

$$\mu(S) = L(S) + \alpha_F F(S) + \alpha_T T(S),$$

где α_F и α_T — положительные числовые параметры, значения которых будут выбраны позднее.

Схема S называется *приведенной*, если в S все ребра, ведущие из элементов, имеют знак 0 (другими словами, все элементы подаются только на инвертированные входы конъюнкторов).

Далее будут сформулированы три леммы. Доказательства первых двух несложны, доказательство третьей представляет заметную трудность. В целях экономии объема приводятся лишь эскизы доказательств.

Лемма 1. *Пусть S — схема, реализующая функцию f. Тогда существует приведенная схема S', также реализующая f, такая, что $L(S) - L(S') \geqslant 0$.*

Для доказательства леммы 1 достаточно заметить, что пару конъюнкторов, соединенных положительным ребром, можно заменить на один конъюнктор, такой, что на его входы подаются все вершины схемы, которые подавались на входы исходной пары конъюнкторов.

Лемма 2. *Пусть S — приведенная схема, реализующая линейную функцию от n переменных ($n \geqslant 2$). Пусть S содержит вход x, из которого исходят не менее трех ребер одного знака. Тогда существует приведенная схема S', реализующая линейную функцию от $n-1$ переменной, такая, что $L(S) - L(S') \geqslant 3$.*

Пусть x — вход схемы S, из которого исходят три ребра одного знака (без ограничения общности знака 1). Подадим на вход x константу нуль. После этого три элемента, на которые подается вход x, также будут реализовывать константу нуль. Такие элементы могут быть удалены из схемы без изменения реализуемой схемой функции. Лемма 2 доказана.

Лемма 3. *Пусть S — приведенная схема, реализующая линейную функцию от n переменных ($n \geqslant 2$). Тогда существует приведенная схема S', реализующая линейную функцию от $n-k$ переменных ($k \geqslant 1$), такая, что величина $\frac{1}{k}(\mu(S) - \mu(S'))$ больше или равна одной из следующих величин:*

$$3 + \alpha_F - \alpha_T; \quad 2\frac{2}{3} + 1\frac{2}{3}\alpha_F - \frac{1}{3}\alpha_T; \quad 2.5 + 2\alpha_F; \quad 2\frac{1}{3} + 2\frac{2}{3}\alpha_F + \frac{2}{3}\alpha_T;$$

$$2.25 + 3\alpha_F + \alpha_T; \quad 2 + 6\alpha_F + \alpha_T; \quad 2 + 3.5\alpha_F + 1.5\alpha_T; \quad 1 + 7\alpha_F + 5\alpha_T.$$

Доказательство леммы 3 проводится следующим образом. В схеме S выбирается вход x. Далее рассматривается множество (более 40) случаев возможного соединения входа x и "близких" к нему элементов и входов. Для некоторых случаев доказывается, что они невозможны в схеме, реализующей линейную функцию (например, подстановка константы вместо какой-либо переменной приводит к тому, что выходная функция схемы становится независимой от какой-то другой переменной). Для остальных случаев предъявляется подстановка констант вместо каких-то k входов схемы S. Доказывается, что после подстановки из схемы можно удалить несколько элементов (например, реализующих константы) и несколько ребер, исходящих из входов (например, исходящих из входа, на который подана константа, или ведущих в удаленные элементы). В каждом случае снижение меры схемы (на один забитый константой вход) оказывается больше или равно одной из перечисленных в формулировке леммы 3 величин.

Отметим, что выбор входа x, с которого начинается перебор случаев, нетривиален. Во многих аналогичных работах (см., например, [5–7, 11]) перебор может быть начат с любого входа, подающегося на элемент, на который подаются лишь другие входы, или с входа, наиболее удаленного от выходного элемента схемы. В данной ситуации (как и в [9]) предложен алгоритм обхода вершин схемы, который обнаруживает вход, подходящий для начала перебора.

Доказательство теоремы. Пусть S — схема, реализующая линейную функцию от n переменных. Преобразуем схему S в приведенную схему S_1, реализующую ту же функцию, согласно лемме 1. Верно, что $L(S) - L(S_1) \geqslant 0$.

Схема S_1 может содержать входы, из которых исходят не менее трех ребер одного знака. Согласно лемме 2 каждый такой вход может быть удален с уменьшением сложности не менее чем на три. Пусть S_2 — схема, которая получается из S_1 после последовательного применения леммы 2. В схеме S_2 нет входов, которые подаются на три и более входа элемента одного знака, схема S_2 реализует линейную функцию и является приведенной. Пусть n_2 — число входов схемы S_2. Верно, что

$$L(S) - L(S_2) \geqslant 3(n - n_2), \tag{1}$$

$$F(S_2) \leqslant 4n_2, \quad T(S_2) \leqslant n_2. \tag{2}$$

К схеме S_2 будем последовательно применять лемму 3, удаляя входы и уменьшая значение меры схемы не менее чем на δ на каждый удаленный вход, где

$$\delta \geqslant \min(3 + \alpha_F - \alpha_T,\, 2\frac{2}{3} + 1\frac{2}{3}\alpha_F - \frac{1}{3}\alpha_T,\, 2.5 + 2\alpha_F,\, 2\frac{1}{3} + 2\frac{2}{3}\alpha_F + \frac{2}{3}\alpha_T,$$

$$2.25 + 3\alpha_F + \alpha_T,\, 2 + 6\alpha_F + \alpha_T,\, 2 + 3.5\alpha_F + 1.5\alpha_T,\, 1 + 7\alpha_F + 5\alpha_T),$$

до тех пор, пока число входов схемы не станет меньше двух. Поэтому

$$\mu(S_2) = L(S_2) + \alpha_F F(S_2) + \alpha_T T(S_2) \geqslant \delta(n_2 - 1).$$

Учитывая неравенства (2), имеем

$$L(S_2) \geqslant (\delta - 4\alpha_F - \alpha_T)n_2 - \delta.$$

Выберем значения параметров, дающие наибольшую нижнюю оценку сложности S_2, решив следующую задачу линейного программирования:

$$\text{maximize:} \quad \delta - 4\alpha_F - \alpha_T;$$

$$\text{subject to:} \quad \begin{cases} \delta \geqslant \min(3 + \alpha_F - \alpha_T,\, 2\frac{2}{3} + 1\frac{2}{3}\alpha_F - \frac{1}{3}\alpha_T,\, 2.5 + 2\alpha_F, \\ \qquad 2\frac{1}{3} + 2\frac{2}{3}\alpha_F + \frac{2}{3}\alpha_T,\, 2.25 + 3\alpha_F + \alpha_T, \\ \qquad 2 + 6\alpha_F + \alpha_T,\, 2 + 3.5\alpha_F + 1.5\alpha_T,\, 1 + 7\alpha_F + 5\alpha_T), \\ \delta,\, \alpha_F,\, \alpha_T \geqslant 0. \end{cases}$$

Зафиксируем значения параметров, соответствующие оптимальному решению задачи:

$$\delta = 2\frac{11}{18}, \quad \alpha_F = \frac{1}{18}, \quad \alpha_T = \frac{5}{18}.$$

При выбранных параметрах нижняя оценка сложности S_2 примет следующий вид:

$$L(S_2) \geqslant 2\frac{1}{9}n_2 - 2\frac{11}{18}.$$

Тогда, учитывая (1), получаем

$$L(S) \geqslant 3(n-n_2) + L(S_2) \geqslant 3(n-n_2) + 2\frac{1}{9}n_2 - 2\frac{11}{18} \geqslant 2\frac{1}{9}n - 2\frac{11}{18}.$$

Теорема доказана.

Работа выполнена при поддержке РФФИ (проект № 18–01–00337).

СПИСОК ЛИТЕРАТУРЫ

1. *Лупанов О.Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
2. *Wegner I.* The complexity of the parity function in unbounded fan-in, unbounded depth circuits // Theor. Comput. Sci. 1991. **85**. 155–170.
3. *Комбаров Ю.А.* Верхняя оценка сложности реализации линейных функций схемами в одном базисе из многовходовых элементов // Вестн. Моск. ун-та. Матем. Механ. 2015. № 5. 47–50.
4. *Клосс Б.М., Малышев В.А.* Оценки сложности некоторых классов функций // Вестн. Моск. ун-та Матем. Механ. 1965. № 4. 44–51.
5. *Редькин Н.П.* Доказательство минимальности некоторых схем из функциональных элементов // Пробл. кибернетики. 1970. **23**. 83–101.
6. *Редькин Н.П.* О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. 1971. № 6. 31–38.
7. *Iwama K., Lachish O., Morizumi H., Raz R.* An explicit lower bound of $5n - o(n)$ for Boolean circuits // Proc. 33d STOC. Heraklion, 2001. 399–408.
8. *Find M., Golovnev A., Hirsch E., Kulikov A.* A better-than-3n lower bound for the circuit complexity of an explicit function // 2016 IEEE 57th Annual Symp. on Foundations of Computer Science (FOCS). New Brunswick, 2016. 89–98.
9. *Комбаров Ю.А.* О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискретн. анализ и исслед. опер. 2013. **20**, № 4. 65–87.
10. *Подольская О.В.* Сложность реализации симметрических булевых функций схемами в базисе антицепных функций // Дискретн. матем. 2015. **27**, № 3. 95–107.
11. *Lai H. Ch., Muroga S.* Logic networks with a minimum number of NOR (NAND) gates for parity functions of n variables // IEEE Trans. Comput. 1987. **C**-36, N 2. 157–166.

Поступила в редакцию
21.10.2020

УДК 515.12

НОРМАЛЬНЫЕ ФУНКТОРЫ И ПАРАНОРМАЛЬНОСТЬ

А. А. Иванов[1]

Доказано, что если для какого-нибудь нормального функтора $\mathcal{F} : \mathcal{P} \longrightarrow \mathcal{P}$ степени $\geqslant 3$ в категории $\mathcal{P}$ паракомпактных p-пространств и совершенных отображений пространство $\mathcal{F}(X)$ наследственно паранормально, то пространство X метризуемо.

Ключевые слова: нормальный функтор, паракомпактное p-пространство, наследственная паранормальность, метризуемость.

It is proved that if $\mathcal{F} : \mathcal{P} \longrightarrow \mathcal{P}$ is a normal functor of degree $\geqslant 3$ in the category $\mathcal{P}$ of

[1] *Иванов Андрей Александрович* — студ. каф. общей топологии и геометрии мех.-мат. ф-та МГУ, e-mail: an98iv@yandex.ru.

Ivanov Andrey Aleksandrovich — Student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of General Topology and Geometry.