Сложность и строение схем для линейных функций

Ю. А. КОМБАРОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: yuri.kombarov@gmail.com

УДК 519.95

Ключевые слова: схемы из функциональных элементов, линейная функция.

Аннотация

Работа посвящена изучению схем из функциональных элементов, реализующих линейные булевы функции. Приведён обзор результатов, в которых устанавливается сложность реализации линейных функций схемами в различных базисах. Для некоторых базисов дано описание всех минимальных схем, реализующих линейные функции. Также описана верхняя оценка сложности линейных функций в одном бесконечном базисе.

Abstract

Yu. A. Kombarov, Complexity and structure of circuits for parity functions, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 6, pp. 147—153.

The paper is devoted to circuits implementing parity functions. A review of results establishing exact values of the complexity of parity functions is given. The structure of optimal circuits implementing parity functions is described for some bases. For one infinite basis, an upper bound for the complexity of parity functions is given.

1. Основные определения

Пусть B — множество булевых функций. *Схемой из функциональных элементов* в базисе B называется ориентированный граф без ориентированных циклов, вершины которого подписаны. Каждая вершина входной степени 0 подписана некоторой переменной из алфавита переменных $\{x_1, \ldots, x_n, \ldots\}$. Каждая вершина входной степени k подписана некоторой k-местной функцией из B. Одна из вершин также дополнительно помечена специальным символом $*$. Эта вершина называется *выходной* вершиной схемы.

Вершины, помеченные переменными, называются *входами* схемы, а вершины, помеченные функциями, называются *элементами*.

По индукции определим булеву функцию, реализуемую в каждой вершине схемы. Вершина, помеченная переменной x_i, по определению реализует функцию $g(x_1, \ldots, x_n) = x_i$. Пусть G — элемент схемы, помеченный функцией

Фундаментальная и прикладная математика, 2015, том 20, № 6, с. 147—153.

$h(x_1, \ldots, x_k)$. Пусть $G_1, \ldots, G_k$ — элементы, такие что для каждого i существует ребро, идущее из G_i в G. Тогда если элементы $G_1, \ldots, G_k$ реализуют функции $h_1, \ldots, h_k$, то G реализует функцию $h(h_1, \ldots, h_k)$.

Схема реализует функцию f тогда и только тогда, когда её выходная вершина реализует f. На рисунках элементы схемы обычно изображаются треугольниками. Пример схемы приведён на рис. 1: схема в базисе $\{x \,\&\, y,\ x \vee y,\ \overline{x}\}$, реализующая функцию $x_1 \oplus x_2 \oplus 1$. Рядом с каждым элементом на рисунке подписана функция, которую он реализует.

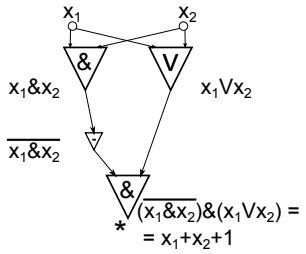

Рис. 1

Сложностью схемы C называется количество элементов в C. Сложность схемы C обозначается $L(C)$. Пусть f — булева функция. Сложность функции f в базисе B определяется как

$$L_B(f) = \min L(C),$$

где минимум берётся по всем схемам C в базисе B, реализующим f. Схема C в базисе B называется минимальной, если она реализует функцию f и $L(C) = L_B(f)$.

Пусть B — базис (т. е. произвольное множество булевых функций). Максимальное число входов элемента (функции) из B называется *входным ветвлением* базиса B. Базисы, которые для любого k содержат элемент с k входами, называются *бесконечными* базисами. Базис называется *полным*, если любая булева функция реализуется некоторой схемой в этом базисе. Полный базис называется *неизбыточным*, если никакое его собственное подмножество не является полным.

Эта заметка посвящена схемам для линейных функций. Различают однородные и неоднородные линейные функции; однородная линейная функция от n переменных определяется как

$$l_n(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n,$$

а неоднородная — как

$$\overline{l_n}(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n \oplus 1.$$

Далее будут использоваться следующие обозначения для элементарных булевых функций: через $x \to y$ обозначается функция $\overline{x} \vee y$, а через $x \mid y$ — функция $x \,\&\, y \oplus 1$.

2. Схемы для линейных функций в базисах с входным ветвлением 2

Сложность линейных функций известна для многих базисов, состоящих из элементов с не более чем двумя входами. Линейные функции были одними из первых функций, для которых были получены нетривиальные нижние оценки сложности. Первый результат в этом направлении принадлежит Н. П. Редькину, который доказал [3], что

$$L_{\{x\&y,\, x\vee y,\, \overline{x}\}}(l_n) = L_{\{x\&y,\, x\vee y,\, \overline{x}\}}\left(\overline{l_n}\right) = 4n - 4$$

и

$$L_{\{x\&y,\, \overline{x}\}}(l_n) = L_{\{x\&y,\, \overline{x}\}}\left(\overline{l_n}\right) = L_{\{x\vee y,\, \overline{x}\}}(l_n) = L_{\{x\vee y,\, \overline{x}\}}\left(\overline{l_n}\right) = 7n - 7.$$

Он также изучал сложность линейных функций в базисе $\{x \mid y\}$ и доказал [4], что

$$L_{\{x|y\}}(l_n) = 4n - 4, \quad 4n - 4 \leqslant L_{\{x|y\}}\left(\overline{l_n}\right) \leqslant 4n - 3.$$

Такие же оценки были получены для базиса $\{x \to y,\, \overline{x}\}$:

$$L_{\{x\to y,\, \overline{x}\}}(l_n) = 4n - 4, \quad 4n - 4 \leqslant L_{\{x\to y,\, \overline{x}\}}\left(\overline{l_n}\right) \leqslant 4n - 3$$

(см. [5]).

Автором данной заметки получено полное описание минимальных схем, реализующих линейные функции в некоторых базисах. Чтобы сформулировать соответствующий результат, необходимо дать следующее определение.

Определение. Пусть B — базис. *Стандартным блоком* в базисе B будем называть схему S с двумя входами, реализующую линейную функцию от двух переменных (однородную или неоднородную), если сложность схемы S в базисе B минимальна среди всех схем в базисе B, реализующих линейную функцию от двух переменных (как однородную, так и неоднородную).

Примеры стандартных блоков представлены на рис. 2.

В базисе $\{x \,\&\, y,\, x \vee y,\, \overline{x}\}$ существуют два стандартных блока (см. рис. 2.1 и 2.2), один блок реализует l_2, а второй реализует $\overline{l_2}$. В базисе $\{x \mid y\}$ существует только один стандартный блок (см. рис. 2.3), который реализует l_2; так как $L_{\{x|y\}}\left(\overline{l_2}\right) = 5$, минимальная схема, реализующая $\overline{l_2}$ в этом базисе, не является стандартным блоком по определению. Ситуация в базисе $\{x \to y,\, \overline{x}\}$ аналогична (см. рис. 2.4).

Следующие две теоремы описывают структуру минимальных схем для линейных функций.

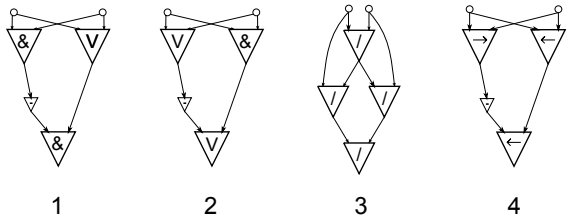

Рис. 2

Теорема 1 [1]. *Любая минимальная схема в базисе* $\{x \,\&\, y,\ x \vee y,\ \overline{x}\}$, *реализующая* l_n *или* $\overline{l_n}$, *состоит из* $n-1$ *непересекающихся стандартных блоков.*

Теорема 2 (частично в [2]). *Любая минимальная схема в одном из базисов* $\{x \mid y\}$, $\{x \to y,\ \overline{x}\}$, *реализующая* l_n, *состоит из* $n-1$ *непересекающихся стандартных блоков.*

Говоря неформально, значение теорем 1 и 2 следующее: всякая минимальная схема для линейной функции в базисе $\{x \,\&\, y,\ x \vee y,\ \overline{x}\}$ и всякая минимальная схема для однородной линейной функции в базисах $\{x \mid y\}$ и $\{x \to y,\ \overline{x}\}$ является двоичным деревом, в листьях которого находятся переменные, а во внутренних вершинах — стандартные блоки. Пример двух минимальных схем для l_4 в базисе $\{x \mid y\}$ приведён на рис. 3; теорема 2 гарантирует, что других минимальных схем для l_4 не существует.

Подход, который был использован при доказательстве теорем 1 и 2, оказался полезен для доказательства новых нижних оценок сложности для неоднородной линейной функции. Эти оценки позволили найти точные значения сложности неоднородной линейной функции в базисах $\{x \mid y\}$ и $\{x \to y,\ \overline{x}\}$.

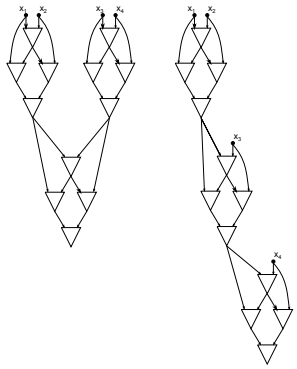

Рис. 3

Теорема 3. *Для всех $n \geqslant 2$ выполнены равенства*

$$L_{\{x|y\}}\left(\overline{l_n}\right) = L_{\{x\to y,\,\overline{x}\}}\left(\overline{l_n}\right) = 4n-3.$$

Используя теорему 3, результаты [3—5] и простые соображения, такие, как соображения двойственности, удалось определить точные значения сложности линейных функций во всех полных неизбыточных базисах, состоящих из элементов с не более чем двумя входами. Значения сложности во всех таких базисах (за исключением базисов, содержащих функцию $x \oplus y$ или $x \oplus y \oplus 1$) приведены в таблице 1 (m обозначает остаток от деления n на 2).

Таблица 1. Сложность линейных функций в полных неизбыточных базисах

Базис	$L(l_n)$	$L\left(\overline{l_n}\right)$
$\{x \,\&\, y,\, \overline{x}\}$	$7n-7$	$7n-7$
$\{x \vee y,\, \overline{x}\}$	$7n-7$	$7n-7$
$\{x \mid y\}$	$4n-4$	$4n-3$
$\{\overline{x \vee y}\}$	$4n-3-m$	$4n-4+m$
$\{x \to y,\, \overline{x} \,\&\, y\}$	$3n-3$	$3n-3$
$\{x \to y,\, \overline{x}\}$	$4n-4$	$4n-3$
$\{\overline{x} \,\&\, y,\, \overline{x}\}$	$4n-3-m$	$4n-4+m$
$\{x \to y,\, 0\}$	$4n-3$	$4n-2$
$\{\overline{x} \,\&\, y,\, 1\}$	$4n-2-m$	$4n-3+m$

3. Схемы для линейных функций в бесконечных базисах

Значения сложности линейных функций известны для небольшого количества бесконечных базисов. Первым бесконечным базисом, для которого были найдены точные значения сложности линейной функции, был базис NAND. Этот базис состоит из всех функций вида $\overline{x_1 \,\&\, \ldots \,\&\, x_k}$ ($k \in \{2,3,\ldots\}$). Этот базис можно рассматривать как «бесконечный» вариант базиса $\{x| \mid y\}$. В [6] доказано, что при $n \geqslant 3$ верно, что $L_{\mathrm{NAND}}(l_n) = L_{\mathrm{NAND}}\left(\overline{l_n}\right) = 3n-2$ (для сравнения напомним, что $L_{\{x|y\}}(l_n) = 4n-4$, $L_{\{x|y\}}\left(\overline{l_n}\right) = 4n-3$). Минимальные схемы, построенные в [6], содержат элементы с не более чем четырьмя входами. Поэтому использование элементов из NAND с более чем четырьмя входами не позволяет строить более экономные схемы.

Также известна сложность линейных функций в базисе AC, состоящем из всех антицепных функций. Булева функция называется антицепной, если любые два её единичных набора не сравнимы. Доказано [7], что $L_{\mathrm{AC}}(l_n) = \lfloor (n+1)/2 \rfloor$.

Другой пример бесконечного базиса — это базис T, состоящий из всех пороговых функций (функция $f(x_1, \ldots, x_n)$ называется пороговой, если существует k, такое что $f(x_1, \ldots, x_n) = 1$ тогда и только тогда, когда $x_1 + \ldots + x_n \geqslant k$ или $f(x_1, \ldots, x_n) = 1$ тогда и только тогда, когда $x_1 + \ldots + x_n \leqslant k$). В [8] доказано, что $L_{\mathrm{T}}(l_n) = L_{\mathrm{T}}\left(\overline{l_n}\right) = \lceil \log(n+1) \rceil$.

Также в [8] рассматриваются схемы, реализующие линейные функции в базисе U_∞. Базис U_∞ состоит из всех элементов, реализующих функции вида $(x_1^{\sigma_1} \,\&\, \ldots \,\&\, x_k^{\sigma_k})^\beta$, где $k \in \{2, 3, \ldots\}$, $\sigma_1, \ldots, \sigma_k, \beta \in \{0, 1\}$. В [8] доказано, что $2n - 1 \leqslant L_{U_\infty}(l_n) \leqslant \lfloor (5n-4)/2 \rfloor$ и $2n - 1 \leqslant L_{U_\infty}\left(\overline{l_n}\right) \leqslant \lfloor (5n-4)/2 \rfloor$.

Автору удалось улучшить верхнюю оценку сложности линейных функций в базисе U_∞. Справедлива следующая теорема.

Теорема 4. *При $n \geqslant 2$ верно, что*

$$L_{U_\infty}(l_n) \leqslant \left\lfloor \frac{7n-4}{3} \right\rfloor, \quad L_{U_\infty}\left(\overline{l_n}\right) \leqslant \left\lfloor \frac{7n-4}{3} \right\rfloor.$$

Для доказательства теоремы построена последовательность схем; i-я схема реализует l_i со сложностью $\lfloor (7i-4)/(4) \rfloor$. На рис. 4 представлена схема, реализующая l_6 (6 — это наименьшее число переменных, для которого сложность построенных схем меньше, чем верхняя оценка из [8]). Все элементы в этой схеме реализуют $x_1^{\sigma_1} \,\&\, \ldots \,\&\, x_k^{\sigma_k}$, кружок около i-го входа элемента означает, что $\sigma_i = 0$, в противном случае $\sigma_i = 1$.

При помощи перебора схем на компьютере проверено, что построенные схемы минимальны при $n \leqslant 6$. Автор предполагает, что они минимальны для любого n.

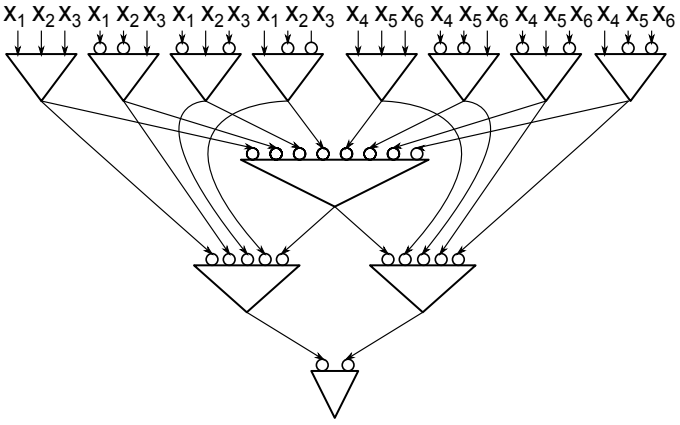

Рис. 4

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант 14-01-00598).

Литература

[1] Комбаров Ю. А. О минимальных реализациях линейных булевых функций // Дискрет. анализ и исслед. операций. — 2012. — Т. 19, № 3. — С. 39—57.

[2] Комбаров Ю. А. О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискрет. анализ и исслед. операций. — 2013. — Т. 20, № 4. — С. 65—87.

[3] Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — Т. 23. — С. 83—101.

[4] Редькин Н. П. О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — Т. 6. — С. 31—38.

[5] Шкребела И. С. О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$ // Дискрет. матем. — 2003. — Т. 15, № 4. — С. 100—112.

[6] 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. — Vol. C-36, no. 2. — P. 157—166.

[7] Podolskaya O. On circuit complexity of parity and majority functions in antichain basis. — `http://arxiv.org/abs/1410.2456`.

[8] Wegner I. The complexity of the parity function in unbounded fan-in, unbounded depth circuits // Theor. Comput. Sci. — 1991. — Vol. 85. — P. 155—170.