

на правах рукописи

Комбаров Юрий Анатольевич

СЛОЖНОСТЬ И СТРОЕНИЕ
МИНИМАЛЬНЫХ СХЕМ
ДЛЯ ЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

МОСКВА 2013

Работа выполнена на кафедре дискретной математики Механико-математического факультета Федерального государственного бюджетного образовательного учреждения высшего профессионального образования “Московский государственный университет им. М. В. Ломоносова”

Научный руководитель: доктор физико-математических наук,
профессор **Редькин Николай Петрович**

Официальные оппоненты: **Ложкин Сергей Андреевич**,
доктор физико-математических наук, профессор (ФГБОУ ВПО “Московский государственный университет им. М.В.Ломоносова“, Факультет вычислительной математики и кибернетики, кафедра математической кибернетики)

Стеценко Владимир Алексеевич,
кандидат физико-математических наук, профессор (ФГБОУ ВПО “Московский педагогический государственный университет”, кафедра теоретической информатики и дискретной математики)

Ведущая организация: ФГБУН "Институт системного анализа РАН"

Защита диссертации состоится 15 ноября 2013 г. в 16⁴⁵ на заседании диссертационного совета Д.501.001.84 при ФГБОУ ВПО “Московский государственный университет им. М. В. Ломоносова” по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО “Московский государственный университет им. М. В. Ломоносова” (Москва, Ломоносовский проспект, дом 27, сектор А, 8 этаж).

Автореферат разослан 15 октября 2013 г.

Ученый секретарь
диссертационного совета

Д.501.001.84 при ФГБОУ ВПО МГУ
доктор физико-математических наук,
профессор

А. О. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы.

Изучение свойств схем из функциональных элементов является одной из главных задач математической кибернетики. Схемы из функциональных элементов представляют собой математические модели реальных физических устройств, используемых для вычислений. Наряду с булевыми формулами, контактными схемами, конечными автоматами и машинами Тьюринга, схемы из функциональных элементов являются примерами дискретных управляющих систем. Определение схемы из функциональных элементов можно найти в книге¹.

С практической точки зрения разумно рассматривать схемы, оптимальные по какому-либо параметру (например, содержащие наименьшее количество функциональных элементов). В связи с этим вводятся такие понятия, как сложность схемы, сложность булевой функции в классе схем и функция Шеннона.

Пусть B — некоторый базис, каждому элементу E которого приписано положительное число $L(E)$, называемое *весом элемента E* . Сложностью схемы S в базисе B называют сумму весов всех входящих в S функциональных элементов, сложность схемы S обозначают через $L(S)$. Для произвольной булевой функции f *сложностью реализации функции f схемами в базисе B* называют число $L_B(f) = \min L(S)$, где минимум берется по всем схемам S в базисе B , реализующим f . Схемы в базисе B , реализующие функцию f со сложностью $L_B(f)$ называются *минимальными*. Наконец, функцией Шеннона для базиса B называют функцию $L_B(n) = \max L(f)$, где $n \in N$, а максимум берется по всем функциям f от n переменных.

Наряду со сложностью, важной характеристикой схем из функциональных элементов является их глубина. *Глубиной* схемы S с одним выходом называется число элементов, принадлежащих самой длинной ориентированной цепи, в которой некоторый вход ее первого элемента является входом схемы, а выход последнего элемента является выходом схемы. Глубина

¹Лупанов О. Б., Асимптотические оценки сложности управляющих систем. — М.: МГУ, 1984.

схемы S обычно обозначается как $D(S)$.

О.Б. Лупанов¹ предложил метод построения почти минимальных схем для почти всех булевых функций, а также нашел асимптотику для функции Шеннона. Пусть $B = \{E_1, \dots, E_k\}$ — произвольный полный конечный базис и пусть каждому элементу E_i сопоставлен положительный вес $L(E_i)$, а число входов элемента E_i обозначается как m_i . Будем называть минимальным приведенным весом базиса B величину

$$\rho_B = \min_{i \in \{1, \dots, k\}} \frac{L(E_i)}{m_i - 1}.$$

Верна следующая

Теорема (О.Б. Лупанов). *При $n \rightarrow \infty$*

$$L_B(n) \sim \rho_B \frac{2^n}{n},$$

причем среди булевых функций от n переменных x_1, \dots, x_n доля функций f таких, что $L_B(f) \leq \rho_B \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right)\right)$, стремится к нулю с ростом n .

Для доказательства верхней оценки теоремы О.Б. Лупановым предложен метод, позволяющий для любой булевой функции f , существенно зависящей от n переменных, построить схему S , реализующую f со сложностью, не превышающей $\rho_B \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right)\right)$. Однако использование метода синтеза Лупанова приводит к асимптотически наилучшим результатам лишь при построении схем для сложнореализуемых и потому малодоступных на практике булевых функций. Встречающиеся в практических приложениях функции имеют относительно небольшую сложность реализации. В связи с этим возникает задача построения минимальных схем для индивидуальных последовательностей „простых“ булевых функций и получения оценок сложности их реализации.

Приведем известные нижние оценки для сложности схем в базисе B_2 , состоящего из всех функций, существенно зависящих не более, чем от двух переменных. Для любой булевой функции f , существенно зависящей от n переменных, верна тривиальная нижняя оценка $L_{B_2}(f) \geq n - 1$ (здесь и далее сложность схем определяется числом элементов в них, т.е. вес

каждого элемента базиса принимается равным единице). Для некоторых функций эта оценка оказывается оптимальной, например, для линейной функции $l_n(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$ верно, что $L_{B_2}(l_n) = n - 1$.

К.П. Шнорр² получил оценку $L_{B_2}(f) \geq 2n - 3$ для функций f из достаточно широкого класса $Q_{2,3}^n$. Класс $Q_{2,3}^n$ определяется индуктивно: булева функция f , существенно зависящая от n переменных принадлежит классу $Q_{2,3}^n$, если среди функций, полученных после подстановки всевозможных констант вместо каких-то двух переменных функции f , найдутся хотя бы три различные функции и если любая функция, полученная после подстановки константы вместо какой-либо переменной функции f , принадлежит классу $Q_{2,3}^{n-1}$.

Опишем подход, на котором основано доказательство оценки сложности для функций из класса $Q_{2,3}^n$. Пусть S — минимальная схема, реализующая функцию f из класса $Q_{2,3}^n$. Можно доказать, что после подачи некоторой константы на определенный вход схемы S какие-то два элемента в схеме S станут излишними (например, будут реализовывать константу или функцию, которая реализована каким-либо другим элементом в схеме), и их можно удалить из схемы S . Схема, полученная из схемы S после подачи константы и удаления двух элементов будет реализовывать некоторую функцию из класса $Q_{2,3}^{n-1}$ (это следует из определения класса $Q_{2,3}^n$). С учетом этого соображения требуемая нижняя оценка получается по индукции.

Описанный прием носит название „метод забивающих констант“ („elimination method“ в англоязычной литературе). Он был предложен Н.П. Редькиным³. Значительная часть известных нижних оценок сложности булевых функций получена с помощью этого приема. В общем случае для того, чтобы доказать нижнюю оценку сложности вида $L(f) \geq kn - C$ ($k, n \in \mathbb{N}$, C - константа) для булевых функций f из класса F_n , содержащего функции, зависящие от n переменных, необходимо доказать следующее утверждение: для любой булевой функции $f(x_1, \dots, x_n) \in F_n$ существуют $i \in \{1, \dots, n\}$ и $\sigma \in \{0, 1\}$ такие, что из всякой минимальной схемы S ,

²Schnorr C. P., Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen // Computing — 1974. — 13. — P. 155-171.

³Редькин Н.П., Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — № 23. — С. 83-101.

реализующей f , после подачи на вход, соответствующий переменной x_i , константы σ можно удалить k элементов так, что полученная схема будет реализовывать функцию из F_{n-1} . После доказательства этого утверждения требуемую оценку сложности можно будет получить по индукции.

Л. Стокмейер⁴ изучал реализации симметрических функций специального вида схемами в базисе B_2 . При помощи метода забивающих констант он показал, что сложность таких функций, зависящих от n переменных, не меньше $2.5n + O(1)$. Наконец, Н. Блюм⁵ получил нижнюю оценку вида $L_{B_2}(f_n) \geq 3n - 3$ для сложности специально сконструированных функций f_n , являющихся обобщением функции выбора. Доказательство последней оценки помимо метода забивающих констант в ряде случаев использует достаточно сложный анализ структуры схемы. На настоящее время последняя оценка является самой высокой нижней оценкой для базиса B_2 .

Функции, для которых Стокмейер и Блюм получили оценки, являются в некотором роде искусственными, сконструированными специально для получения высокой нижней оценки сложности. Н.П. Редькин⁶ нашел сложность в базисе B_2 для естественно определенного и имеющего значительное практическое значение оператора суммирования. Оператор суммирования — это отображение из $\{0, 1\}^{2n}$ в $\{0, 1\}^{n+1}$ вида $p(x_1, \dots, x_n, y_1, \dots, y_n) = (p_{n+1}, p_n, \dots, p_1)$, где p_i является i -м знаком в двоичной записи числа $x + y$, а x и y — числа, двоичной записью которых являются строки (x_n, \dots, x_1) и (y_n, \dots, y_1) соответственно. Доказано, что сложность оператора суммирования в базисе B_2 составляет $5n - 3$ (необходимо отметить, что оператор суммирования является оператором от $2n$ переменных). Доказательство нижней оценки сложности оператора суммирования проводится при помощи метода забивающих констант.

Более высокие нижние оценки сложности были получены для более узких, чем B_2 , базисов. Так, в работе⁷ получена нижняя оценка сложности с

⁴Stockmeyer L., On the combinational complexity of certain symmetric Boolean functions // Math.Syst.Th. — 1977. — **10**. — P. 323-326.

⁵Blum N., A Boolean function requiring $3n$ network size // TCS. — 1984. — **28**. — P. 337-345.

⁶Редькин Н.П., О минимальной реализации двоичного сумматора // Проблемы кибернетики. — Вып. 38. М.: Наука, 1981. — С. 181-216.

⁷Iwama K., Lachish O., Morizumi H., Raz R., An explicit lower bound of $5n - o(n)$ for Boolean circuits // Proceeding of the 33rd STOC, 2001. — P. 399-408.

минорантой вида $5n - o(n)$ для сложности реализации булевых функций из некоторого множества схемами в базисе $U_2 = B_2 \setminus \{x \oplus y, x \oplus y \oplus 1\}$. В работе⁸ получено значение асимптотики сложности в базисе U_2 для другого класса булевых функций. Эта работа посвящена исследованию класса функций с малым числом единиц, т.е. класса $F_{n,k}$, содержащего все булевы функции, зависящие от n переменных и принимающие значение 1 ровно на k наборах значений переменных (k предполагается малым по сравнению с n). Приведем определение сильных переменных, которое используется в формулировке результата работы⁸.

Определение. Пусть $f(x_1, \dots, x_n)$ — некоторая функция из $F_{n,k}$, обращающаяся в единицу на наборах $\tilde{\sigma}_1, \dots, \tilde{\sigma}_k$. Функции f можно сопоставить матрицу M_f , строками которой являются наборы $\tilde{\sigma}_1, \dots, \tilde{\sigma}_k$. Будем считать, что i -ый столбец матрицы M_f соответствует переменной x_i ($i \in \{1, \dots, n\}$). Для произвольного набора $\tilde{\tau}$ через $M_{\tilde{\tau}}$ обозначим группу столбцов матрицы M_f , равных $\tilde{\tau}$ (быть может, $M_{\tilde{\tau}} = \emptyset$). Непустую группу столбцов $M_{\tilde{\tau}}$ будем считать сильной, если она содержит не менее двух столбцов и в этих столбцах содержатся как нули, так и единицы. Переменные, соответствующие столбцам из сильных групп, будем называть сильными.

В работе⁸ доказана следующая

Теорема. Пусть у булевой функции $f(x_1, \dots, x_n)$ из класса F_{n,k_n} имеется m_n сильных переменных, а для параметра k_n выполняется условие

$$1 \leq k_n \leq \log n - c \log \log n,$$

где c — произвольная константа, большая единицы. Тогда

$$L_{U_2}(f) \sim n + m_n.$$

Доказательство этой теоремы является одним из немногих примеров доказательств оценок сложности схем, не использующих метод забивающих констант.

⁸Редькин Н. П., О сложности булевых функций с малым числом единиц // Дискретная математика. — 2004. — Т. 16, вып. 4. — С. 20–31.

Настоящая работа посвящена изучению минимальных схем для линейных булевых функций $l_n(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$ и $\bar{l}_n(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n \oplus 1$ в различных базисах. Функцию l_n называют однородной линейной функцией, а функцию \bar{l}_n — неоднородной. Первый результат в этом направлении получен для класса управляющих систем, отличного от схем из функциональных элементов: в 1952 г. Кардо⁹ доказал, что всякая минимальная контактная схема, реализующая линейную функцию от n переменных содержит ровно $4n - 4$ контакта. Более простое доказательство того же результата получил С.А. Ложкин¹⁰, он же для некоторых случаев нашел число минимальных контактных схем, реализующих операторы, составленные из линейных функций. Первые результаты, в которых устанавливается значение сложности линейных функций в классе схем из функциональных элементов получил Н.П. Редькин: в работе¹¹ доказано, что $L_{\{x \& y, x \vee y, \bar{x}\}}(l_n) = L_{\{x \& y, x \vee y, \bar{x}\}}(\bar{l}_n) = 4n - 4$ и $L_{\{x \& y, \bar{x}\}}(l_n) = L_{\{x \& y, \bar{x}\}}(\bar{l}_n) = L_{\{x \vee y, \bar{x}\}}(l_n) = L_{\{x \vee y, \bar{x}\}}(\bar{l}_n) = 7n - 7$. В работе¹² установлено значение сложности функции l_n и даны оценки для сложности функции \bar{l}_n в базисе, состоящем из единственного функционального элемента — штриха Шеффера (т.е. функции $x|y = x \& y \oplus 1$). А именно, доказаны следующие утверждения: $L_{\{x|y\}}(l_n) = 4n - 4$, $4n - 4 \leq L_{\{x|y\}}(\bar{l}_n) \leq 4n - 3$. И.С. Шкребела¹³ получил аналогичный результат для базиса, состоящего из импликации и отрицания: $L_{\{x \rightarrow y, \bar{x}\}}(l_n) = 4n - 4$, $4n - 4 \leq L_{\{x \rightarrow y, \bar{x}\}}(\bar{l}_n) \leq 4n - 3$. Нижние оценки сложности линейных функций в трех вышеприведенных работах получены при помощи метода забивающих констант.

Перейдем к описанию результатов, в которых устанавливаются значения сложности для других естественно заданных булевых функций. Н.П.

⁹Cardot C., Quelques résultats sur l'application de l'algèbre de Boole à la synthèse des circuits à relais // Ann. Telecomm. — 1952. — 7, № 2. — P. 75–84.

¹⁰Ложкин С.А., Об одном методе получения нижних оценок сложности контактных схем и о некоторых минимальных схемах для линейных функций // Сборник трудов семинара семинара по дискретной математике и ее приложениям. — М.: Изд-во механико-математического факультета МГУ, 1997. — С. 113–115.

¹¹Редькин Н.П., Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — № 23. — С. 83–101.

¹²Редькин Н.П., О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — № 6. — С. 31–38.

¹³Шкребела И.С., О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \rightarrow y, \bar{x}\}$ // Дискретная математика. — 2003. — Т. 15, вып. 4. — С. 100–112.

Редькиным¹⁰ найдена сложность реализации оператора сравнения F_n и оператора совпадения R_n в базисе $\{x \& y, x \vee y, \bar{x}\}$. Операторы сравнения и совпадения — это булевы функции, определяемые следующим образом:

$$F_n(\tilde{x}, \tilde{y}) = \begin{cases} 1, & \text{если } |\tilde{x}| < |\tilde{y}| \\ 0, & \text{если } |\tilde{x}| \geq |\tilde{y}| \end{cases}, \quad R_n(\tilde{x}, \tilde{y}) = \begin{cases} 1, & \text{если } \tilde{x} = \tilde{y} \\ 0, & \text{если } \tilde{x} \neq \tilde{y} \end{cases}.$$

Здесь \tilde{x} и \tilde{y} — наборы из нулей и единиц длины n , а через $|\tilde{x}|$ обозначается целое неотрицательное число, двоичной записью которого является набор \tilde{x} . При помощи метода забивающих констант доказано, что $L_{\{x \& y, x \vee y, \bar{x}\}}(F_n) = 5n - 3$ и $L_{\{x \& y, x \vee y, \bar{x}\}}(R_n) = 5n - 1$.

Достаточно глубоко изучены минимальные реализации элементарных конъюнкций и дизъюнкций схемами в различных полных базисах. Элементарными конъюнкциями и дизъюнкциями называются булевы функции вида $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}$ и $D_{\tilde{\sigma}}^n = x_1^{\sigma_1} \vee \dots \vee x_n^{\sigma_n}$ соответственно. Е.П. Сопруненко¹⁴ было найдено значение сложности реализации функций $x_1 \& \dots \& x_n$ и $x_1 \vee \dots \vee x_n$ в базисе Шеффера: $L_{\{x|y\}}(x_1 \& \dots \& x_n) = 2n - 2$, $L_{\{x|y\}}(x_1 \vee \dots \vee x_n) = 3n - 3$. Е.С. Горелик¹⁵ обобщил эти утверждения, доказав, что $L_{\{x|y\}}(K_{\tilde{\sigma}}^n) = 3n - 2 - \|\tilde{\sigma}\|$, $L_{\{x|y\}}(D_{\tilde{\sigma}}^n) = 2n - 3 + \|\tilde{\sigma}\|$. Здесь через $\|\tilde{\sigma}\|$ обозначается число единиц в наборе $\tilde{\sigma}$.

Дальнейшие обобщения этих результатов были произведены Г.А. Кочергиной¹⁶, изучавшей реализации элементарных конъюнкций и дизъюнкций в базисах $B_{kl}^{\vee} = \{x_1 \vee \dots \vee x_k \vee \bar{x}_{k+1} \vee \dots \vee \bar{x}_{k+l}, \bar{x}\}$. В работе¹⁶ найдены значения сложности $L_{B_{kl}^{\vee}}(K_{\tilde{\sigma}}^n)$ и $L_{B_{kl}^{\vee}}(D_{\tilde{\sigma}}^n)$ при всех возможных значениях k, l, n и $\tilde{\sigma}$, а также дано описание всех минимальных схем, реализующих функцию $x_1 \& \dots \& x_n$ в базисе B_{11}^{\vee} .

Еще одной хорошо изученной функцией является универсальная функция

$$SA_n(\tilde{x}, \tilde{y}) = \bigvee_{\tilde{\sigma}=(\sigma_1, \dots, \sigma_n)} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n} \& y_{|\tilde{\sigma}|},$$

¹⁴Сопруненко Е.П., Об одном классе схем из функциональных элементов // Проблемы кибернетики. — 1965. — № 15. — 117–134.

¹⁵Горелик Е.С., О сложности реализации элементарных конъюнкций и дизъюнкций в базисе $\{x|y\}$ // Проблемы кибернетики. — 1973. — № 26. — С. 27–36.

¹⁶Кочергина Г.А., О сложности реализации элементарных конъюнкций и дизъюнкций схемами в некоторых полных базисах // Математические вопросы кибернетики. — 2002. — № 11. — С. 219–246.

где набор переменных \tilde{x} имеет длину n , набор переменных \tilde{y} имеет длину 2^n , а

$$|\tilde{\sigma}| = \sum_{i=1}^n \sigma_i 2^{n-i} + 1.$$

В. Дж. Пауль¹⁷ получил следующие оценки для сложности реализации функции SA_n в базисе B_2 :

$$2 \cdot 2^n - 2 \leq L_{B_2}(SA_n) \leq 3 \cdot 2^n - 3.$$

В. В. Коровин¹⁸ получил асимптотические значения сложности реализации функции SA_n в нескольких базисах, а именно показал, что

$$L_{B_2}(SA_n) \sim 2 \cdot 2^n, \quad L_{\{x \& y, x \vee y, \bar{x}\}}(SA_n) \sim 2 \cdot 2^n,$$

$$L_{\{x \& y, x \oplus y, 1\}}(SA_n) \sim 2 \cdot 2^n,$$

$$L_{\{x \& y, \bar{x}\}}(SA_n) = L_{\{x \vee y, \bar{x}\}}(SA_n) \sim 3 \cdot 2^n.$$

Отметим, что функция SA_n зависит от экспоненциального (по n) числа переменных, поэтому все вышеприведенные оценки остаются линейными по числу переменных.

В работе¹⁹ найдены точные значения глубины функции SA_n в базисе U_2 при $2 \leq n \leq 5$ и для $n \geq 20$. Для случая $5 < n < 20$ в работе¹⁸ получены очень точные оценки на глубину функции SA_n . Наконец, асимптотические оценки для сложности реализации функции SA_n в классе формул можно найти в работе²⁰.

В работе²¹ рассматривается некоторый подход к получению нетривиальных оценок сложности схем из функциональных элементов, основанный на замене сложных базисов на более простые с последующим использованием известных нижних оценок сложности схем в простых базисах.

¹⁷Пауль В. Дж., Оценка $2.5n$ для комбинаторной сложности булевых функций // Кибернетический сборник. — 1979. — № 16. — С. 23–44.

¹⁸Коровин В.В., О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — 1995. — Т. 7, вып. 2. — С. 95–102.

¹⁹Ложкин С.А., Власов Н.В., О глубине мультиплексорной функции // Вестн. Моск. ун-та. Вычислительная математика и кибернетика. — 2011. — № 2. — С. 40–46.

²⁰Власов Н.В., О сложности мультиплексорной функции в классе формул // Проблемы теоретической кибернетики, Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.) — Нижний Новгород, Издательство Нижегородского госуниверситета, 2011. — С. 96–97.

²¹Редькин Н.П., Об оценках сложности схем из многовыходовых функциональных элементов // Дискретная математика. — 2010. — Т. 7, вып. 1. — С. 50–57.

Эффективность этого подхода демонстрируется на примерах нахождения асимптотики, а в некоторых случаях и точного значения для сложности схем из многоходовых элементов, реализующих монотонные симметрические булевы функции и функции с малым числом единиц.

Отметим, что все вышеприведенные нижние оценки для сложности булевых функций являются линейными. Несмотря на то, что, согласно теореме Лупанова, почти все булевы функции, существенно зависящие от n переменных, имеют экспоненциальную по n сложность, до сих пор не удалось найти пример явно заданной (т.е. строящейся за полиномиальное время) последовательности булевых функций, сложность функций которой растет более, чем линейно. Задача получения нелинейных оценок сложности реализации булевых функций в полном базисе является одной из важнейших задач математической кибернетики.

В завершение приведем результат, в котором описывается структура минимальных схем. Работа²² посвящена минимальным реализациям оператора $(x_1 \& x_2 \& \dots \& x_n, \overline{x_1} \& \overline{x_2} \& \dots \& \overline{x_n})$ схемами из функциональных элементов в базисе B_2 . Показано, что всякая минимальная схема, реализующая такой оператор, разбивается на две непересекающиеся подсхемы, одна из которых является минимальной схемой для функции $x_1 \& x_2 \& \dots \& x_n$, а другая — минимальной схемой для функции $\overline{x_1} \& \overline{x_2} \& \dots \& \overline{x_n}$.

Цель работы

Целью работы является нахождение точных значений сложности реализации линейных функций схемами из функциональных элементов в базисах, состоящих из не более чем двухходовых элементов, а также описание структуры минимальных схем в таких базисах, реализующих линейные функции.

Основные методы исследования.

В диссертации используются методы дискретной математики и математической кибернетики.

²²Блом Н., Сейсен М., Характеристика всех оптимальных схем из функциональных элементов для одновременного вычисления AND и NOR // Кибернетический сборник. Новая серия. — 1990. — № 27 — С. 104–117.

Научная новизна. Все основные результаты диссертации являются новыми и состоят в следующем:

1. Получено описание минимальных схем, реализующих однородные линейные функции в базисе Шеффера.
2. Найдены точные значения сложности неоднородных линейных функций в базисе Шеффера.
3. Получено описание минимальных схем, реализующих однородные линейные функции в базисе $\{x \rightarrow y, \bar{x}\}$.
4. Найдены точные значения сложности неоднородных линейных функций в базисе $\{x \rightarrow y, \bar{x}\}$.

Апробация результатов. Результаты диссертации докладывались на семинарах „Надежность управляющих систем“ и „Диагностика управляющих систем“ под руководством профессора Н.П. Редькина (МГУ, 2009-2013гг, неоднократно), на VIII Международной конференции „Дискретные модели в теории управляющих систем“ (Москва, 2009г., 6-9 апреля), на XVI Международной конференции „Проблемы теоретической кибернетики“ (Нижний Новгород, 2011г., 20-25 июня), на XI Международном семинаре „Дискретная математика и ее приложения“ (Москва, 2012г., 18-23 июня), на Международной научных конференциях студентов, аспирантов и молодых ученых „Ломоносов-2011“ (МГУ, Москва, 2011г., 11-15 апреля), „Ломоносов-2012“ (МГУ, Москва, 2012г., 9-13 апреля) и „Ломоносов-2013“ (МГУ, Москва, 2013г., 8-12 апреля), на научных конференциях „Ломоносовские чтения“ (МГУ, Москва, 2009г., 16-24 апреля), „Ломоносовские чтения“ (МГУ, Москва, 2012г., 16-24 апреля), „Ломоносовские чтения“ (МГУ, Москва, 2013г., 15-26 апреля).

Публикации. Основные результаты диссертации опубликованы в работах автора [1 – 9], список которых приведен в конце автореферата.

Структура диссертации. Диссертация объемом 129 страниц состоит из введения, пяти глав, разбитых на параграфы, и списка литературы из 40 наименований, включая 9 работ автора.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В работе рассматриваются минимальные схемы для линейных булевых функций $l_n = x_1 \oplus \dots \oplus x_n$ и $\bar{l}_n = x_1 \oplus \dots \oplus x_n \oplus 1$ в различных базисах, состоящих из не более чем двухвходовых элементов. Для описания структуры минимальных схем вводится понятие стандартного блока.

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). На рис. 1 представлены стандартные блоки для базиса $\{x \& y, x \vee y, \bar{x}\}$, на рис. 2а представлен единственный стандартный блок для базиса $\{x|y\}$, а на рис. 2б — единственный стандартный блок для базиса $\{x \rightarrow y, \bar{x}\}$.

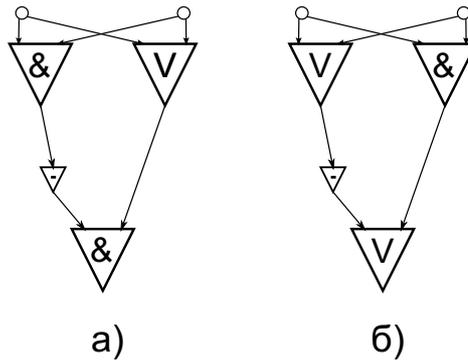


Рис. 1:

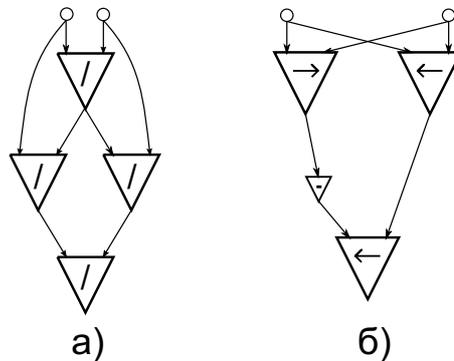


Рис. 2:

Отметим, что поскольку $L_{\{x\&y, x\vee y, \bar{x}\}}(l_2) = L_{\{x\&y, x\vee y, \bar{x}\}}(\bar{l}_2)$, для базиса $\{x\&y, x\vee y, \bar{x}\}$ существуют стандартные блоки, реализующие как однородную, так и неоднородную линейную функцию. С другой стороны, $L_{\{x|y\}}(l_2) < L_{\{x|y\}}(\bar{l}_2)$ и $L_{\{x\rightarrow y, \bar{x}\}}(l_2) < L_{\{x\rightarrow y, \bar{x}\}}(\bar{l}_2)$, поэтому в базисах $\{x|y\}$ и $\{x\rightarrow y, \bar{x}\}$ не существует стандартных блоков, реализующих неоднородную линейную функцию.

Элемент стандартного блока, реализующий линейную функцию, будем называть *выходным*. Пусть в некоторой схеме S можно выделить подсхему, являющуюся стандартным блоком. Будем говорить, что этот стандартный блок входит в схему *правильно*, если выходы всех элементов блока, за исключением выходного, не соединены со входами элементов, не принадлежащих блоку.

В главе 1 рассматриваются реализации линейных булевых функций в базисах, состоящих из инвертора и нескольких двухвходовых элементов, реализующих нелинейные функции. Сложность схем в таких базисах оценивается числом двухвходовых элементов в схеме (т.е. инвертор имеет вес равный нулю, а всякий двухвходовой элемент имеет вес равный единице). В следующей теореме содержится описание всех минимальных схем в таком базисе B , реализующих линейную функцию.

Теорема 2. *Любая минимальная схема в базисе B , реализующая l_n или \bar{l}_n , $n \geq 2$, разбивается на $n - 1$ непересекающихся стандартных блоков, каждый из которых входит в схему правильно.*

Для доказательства теоремы показывается, что $L_B(l_n) = L_B(\bar{l}_n) = 3n - 3$. Затем для всякой минимальной схемы S в базисе B , реализующей линейную функцию от n переменных и имеющей структуру, отличную от описанной в теореме, устанавливается возможность удаления четырех двухвходовых элементов таким образом, что полученная схема реализует линейную функцию от $n - 1$ переменной. Это приводит к противоречию с вышеприведенной оценкой сложности и доказывает теорему. Доказательство теоремы основано исключительно на методе забивающих констант.

Глава 2 посвящена описанию структуры минимальных схем, реализующих линейную функцию в классическом базисе $K = \{x\&y, x\vee y, \bar{x}\}$.

Доказана следующая

Теорема 3. *Любая минимальная схема в базисе K , реализующая l_n или \bar{l}_n , $n \geq 2$, разбивается на $n - 1$ непересекающихся стандартных блоков, каждый из которых входит в схему правильно.*

Доказательство теоремы опирается на результат работы¹¹, в которой устанавливается значение сложности линейных функций в базисе K . В данном случае установить структуру схем с использованием лишь метода забивающих констант не удалось; при помощи этого метода оказалось невозможным опровергнуть существование минимальных схем, содержащих подсхемы особого вида, названные *специальными блоками*. Поэтому доказательство теоремы выстраивается следующим образом: сначала при помощи метода забивающих констант доказывалось, что из всякой минимальной схемы в базисе K , реализующей линейную функцию от n переменных, можно удалить стандартный или специальный блок, получив схему, реализующую линейную функцию от $n - 1$ переменных; затем существование минимальных схем, содержащих специальные блоки, опровергается при помощи ряда соображений, основанных на подсчете числа конъюнктов и дизъюнктов в схеме.

Отметим, что аналогичную теорему, описывающую структуру минимальных схем в базисе K , ранее сформулировал (без доказательства) С.А. Ложкин²³.

Подход, связанный с нахождением структуры минимальных схем, позволил получить новые нижние оценки сложности для линейных функций. Эти оценки описаны в главах 3 и 4.

В главе 3 рассматриваются минимальные схемы для линейных функций в базисе S , состоящем из единственного функционального элемента, реализующего штрих Шеффера (т.е. функцию $x|y = x \& y \oplus 1$). В работе¹² доказано, что $L_S(l_n) = 4n - 4$ и $4n - 4 \leq L_S(\bar{l}_n) \leq 4n - 3$. В настоящей работе найдено точное значение сложности неоднородной линейной функции

²³Ложкин С.А., О структуре минимальных схем в базисе $\{\&, \vee, \neg\}$, реализующих линейную функцию // Труды V Международной конференции „Дискретные модели в теории управляющих систем“ (Ратмино, 26-29 мая 2003 г.). — М.: Издательский отдел факультета ВМиК МГУ имени М.В. Ломоносова, 2003. — С. 50–51.

в базисе S , а также получено описание структуры минимальных схем, реализующих однородную линейную функцию в базисе S . А именно, верны следующие теоремы.

Теорема 5. *Сложность реализации функции \bar{l}_n , $n \in N$, в базисе S составляет $4n - 3$.*

Теорема 6. *Любая минимальная схема в базисе S , реализующая l_n , $n \geq 2$, разбивается на $n - 1$ непересекающихся стандартных блоков, каждый из которых входит в схему правильно.*

Доказываются теоремы 5 и 6 одновременно: показывается, что всякая минимальная схема, реализующая линейную функцию от n переменных (как однородную, так и неоднородную) со сложностью $4n - 4$ разбивается на $n - 1$ непересекающихся стандартных блоков. Из этого утверждения немедленно следует описание структуры минимальных схем, реализующих однородную линейную функцию. С другой стороны, поскольку всякая схема, состоящая из $n - 1$ стандартного блока, реализует однородную линейную функцию, из этого утверждения также следует, что не существует минимальных схем, реализующих неоднородную линейную функцию со сложностью $4n - 4$. Последний факт с применением результатов работы¹² и позволяет получить точное значение сложности неоднородной линейной функции.

Как и в классическом базисе, в базисе Шеффера доказательства теорем не удастся строить с применением исключительно метода забивающих констант: выделяются специальные блоки, на которых метод забивающих констант “не работает”. Для доказательства того, что минимальные схемы не могут содержать специальные блоки, предложен некоторый алгоритм обхода элементов схемы.

Глава 4 посвящена исследованию минимальных схем, реализующих линейные функции в базисе $I = \{x \rightarrow y, \bar{x}\}$. В главе доказываются следующие теоремы.

Теорема 8. *Сложность реализации функции \bar{l}_n , $n \in N$, в базисе I составляет $4n - 3$.*

Теорема 9. *Любая минимальная схема в базисе I , реализующая l_n , $n \geq 2$,*

разбивается на $n - 1$ непересекающихся стандартных блоков, каждый из которых входит в схему правильно.

Теорема 8 усиливает результаты работы¹³, в которой показано, что $L_I(l_n) = 4n - 4$ и $4n - 4 \leq L_I(\bar{l}_n) \leq 4n - 3$. Отметим, что в доказательстве теорем 8 и 9 дополнительные рассуждения, с помощью которых доказывается невозможность существования минимальных схем, содержащих специальные блоки, значительно проще, чем для базисов K и S (хотя эту невозможность по-прежнему не удается доказать при помощи метода забивающих констант). С другой стороны, часть доказательства, использующая метод забивающих констант, заметно сложнее и объемнее, чем для базисов K и S .

В главе 5 показано, как из результатов данной диссертации, а также из результатов работ^{11,12,13} можно получить точные значения сложности линейных функций во всех полных избыточных базисах, состоящих из не более чем двухвходовых элементов.

Автор выражает глубокую благодарность своему научному руководителю доктору физико-математических наук, профессору Николаю Петровичу Редькину за постановку задачи и постоянное внимание к работе. Автор также приносит глубокую благодарность всем сотрудникам кафедры дискретной математики за поддержку и внимание.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

- [1] Комбаров Ю. А. О минимальных схемах для линейных булевых функций // Вестн. Моск. ун-та. Матем. Механ. — 2011. — № 6. — С. 41–44.
- [2] Комбаров Ю. А. О минимальных реализациях линейных булевых функций // Дискретный анализ и исследование операций. — 2012. — **19**, № 3. — С. 39–57.
- [3] Комбаров Ю. А. О минимальных схемах для линейных функций в некоторых базисах // Дискретная математика. — 2013. — **25**, № 1. — С. 33–44.
- [4] Комбаров Ю. А. О сложности реализации линейной булевой функции

в базисе Шеффера // Вестн. Моск. ун-та. Матем. Механ. — 2013. — № 2. — С. 49–53.

- [5] Комбаров Ю. А. О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискретный анализ и исследование операций. — 2013. — **20**, № 4. — С. 65–87.
- [6] Комбаров Ю. А. О сложности реализации линейных булевых функций схемами в базисе „импликация-отрицание“ — М., 2013. — 40 с. — Деп. в ВИНТИ 24.06.2013, № 177-В2013
- [7] Комбаров Ю. А. О минимальных реализациях линейных булевых функций схемами из функциональных элементов в базисе $\{x \rightarrow y, \bar{x} \& y\}$ // Труды VIII международной конференции „Дискретные модели в теории управляющих систем“ (Москва, 6-9 апреля 2009 г.) — Москва, 2009. — С. 145–149.
- [8] Комбаров Ю. А. О минимальных реализациях линейных булевых функций схемами из функциональных элементов в некотором базисе // Проблемы теоретической кибернетики, Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.) — Нижний Новгород, Издательство Нижегородского государственного университета, 2011. — С. 215–218.
- [9] Комбаров Ю. А. О сложности реализации линейных булевых функций в одном базисе // Материалы XI Международного семинара „Дискретная математика и ее приложения“ , посвященного 80-летию со дня рождения академика О.Б.Лупанова (Москва, 18–23 июня 2012 г.) — М.: Изд-во механико-математического факультета МГУ, 2012. — С. 131–133.