ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2012. Том 19, № 3. С. 39–57

УДК 519.95

О МИНИМАЛЬНЫХ РЕАЛИЗАЦИЯХ ЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ *)

Ю. А. Комбаров

Аннотация. Рассматриваются реализации линейных булевых функций схемами из функциональных элементов в классическом базисе (конъюнкция, дизъюнкция и отрицание). Установлено, что все минимальные схемы, реализующие линейные функции в этом базисе, имеют определённую блочную структуру.

Ключевые слова: схема из функциональных элементов, линейная булева функция, минимальная схема, стандартный блок, стандартная редукция.

Введение

Одними из наиболее изученных булевых функций с точки зрения их реализации схемами [3] являются линейные функции вида

$$f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n,$$

где $c_i = 0, 1$ $(i = 0, \ldots, n)$, а $\oplus$ — сложение по модулю два [9]. Важный результат установлен в 1952 г. Кардо [10]: *для реализации линейной булевой функции (существенно зависящей) от n переменных контактной схемой необходимо и достаточно $4n-4$ контакта*. Дальнейшие исследования касались сложности реализации линейных функций схемами из функциональных элементов в различных функционально полных базисах. Под *сложностью реализации* $L(f)$ булевой функции f в том или ином базисе, как правило, понимается наименьшее возможное число функциональных элементов, достаточное для реализации функции f схемой в заданном базисе. Установлено [4], что $L(c \oplus x_1 \oplus \ldots \oplus x_n) = 4n - 4$ в базисе

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 11–01–00508), а также программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

$\{x\&y, x \vee y, \overline{x}\}$ и $L(c \oplus x_1 \oplus \ldots \oplus x_n) = 7n-7$ в базисах $\{x\&y, \overline{x}\}$, $\{x \vee y, \overline{x}\}$ (c — произвольная булева константа). Дальнейшие результаты в этом направлении: $L(x_1 \oplus \ldots \oplus x_n) = 4n - 4$ в базисах $\left\{\overline{x\&y}\right\}$ [5], $\{x \to y, \overline{x}\}$ [6] и $L(x_1 \oplus \ldots \oplus x_n \oplus 1) = 4n - 4$ при чётных n и $L(x_1 \oplus \ldots \oplus x_n) = 4n - 4$ при нечётных n в базисе $\{\overline{x}\&y\}$ [7].

В [4–6] получена сложность реализации линейных функций, но не затронут вопрос о структуре соответствующих минимальных схем. В [1] для любого $c \in \{0, 1\}$ показано, что $L(c \oplus x_1 \oplus \ldots \oplus x_n) = 3n - 3$ в базисе $\{x \to y, \overline{x}\&y\}$, и, кроме того, найдена определённая блочная структура минимальных схем.

1. Основные определения и формулировка результата

Будем рассматривать схемы из функциональных элементов в базисе $\mathfrak{B} = \{x\&y, x \vee y, \overline{x}\}$. Для схемы S через $L(S)$ обозначим число функциональных элементов в S; $L(S)$ будем называть *сложностью схемы* S. Для произвольной булевой функции f положим $L(f) = \min L(S)$, где минимум берётся по всем схемам (в рассматриваемом базисе), реализующим f. Если схема S реализует функцию f и $L(S) = L(f)$, то эту схему будем называть *минимальной* (для рассматриваемой функции f).

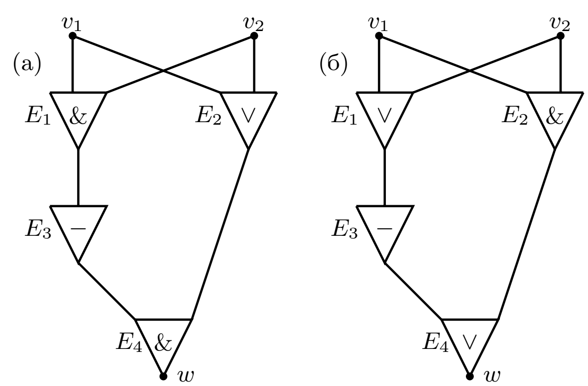

Рис. 1

Схему, изображённую на рис. 1(а), назовём *стандартным блоком первого типа*, а на рис. 1(б) — *стандартным блоком второго типа*. На этом рисунке через v_1 и v_2 обозначены входы блоков, а через w — их выходы (используемые здесь определения схемы, входов и выходов схемы можно найти в [3]). Заметим, что на выходе стандартного блока первого типа реализуется сумма по модулю два функций, поданных на его входы, а на выходе стандартного блока второго типа реализуется отрицание такой суммы.

Будем говорить, что стандартный блок B (первого или второго типа) входит в схему S *правильно*, если выход элемента E_1 (блока B) соединён в схеме S только с входом элемента E_3 (этого блока), а выходы элементов E_2 и E_3 соединены только с входами элемента E_4.

Теорема 1. *Любая минимальная схема S в базисе $\mathfrak{B} = \{x\&y, x\vee y, \overline{x}\}$, реализующая линейную булеву функцию $x_1 \oplus \ldots \oplus x_n \oplus c$, где $n \geqslant 2$, $c \in \{0, 1\}$, разбивается на $n-1$ непересекающихся стандартных блоков, входящих в S правильно.*

Доказывается теорема в предположении, что на входы (модифицированных) схем наряду с переменными $x_1, \ldots, x_n$ можно подавать константы 0 и 1. Нетрудно заметить [4], что утверждение теоремы справедливо и для случая, когда на входы (обычных) схем разрешается подавать только переменные (в приведённой теореме подразумеваются обычные схемы, но всякую обычную схему можно рассматривать и как некий частный случай модифицированной схемы, в которой входы элементов с «константными» входами схемы не соединяются).

2. Вспомогательные определения и утверждения

Стандартный блок B в схеме S будем называть *верхним*, если он правильно входит в схему S и его входы v_1 и v_2 являются двумя различными входами схемы S, с которыми в S соединены только входы соответствующих элементов из B.

Применительно к верхнему блоку B схемы S введём операцию *стандартной редукции*, заключающуюся в том, что один из входов блока B (и схемы S) отождествляется с выходом блока B и оставляется как вход редуцированной схемы S' (получающейся из S), а все остальные вершины (включая второй вход) и все элементы блока B удаляются из S. Тип блока B определяет и тип редукции.

Несложно заметить, что из определения стандартной редукции вытекают следующие утверждения.

Лемма 1. *Если схема S реализует линейную функцию от n переменных и к ней применяется операция стандартной редукции, то редуцированная схема S' реализует линейную функцию от $n-1$ переменных.*

Лемма 2. *Если в редуцированную схему S' правильно входят некоторые стандартные блоки $B_1, \ldots, B_k$, то эти же блоки правильно входят и в исходную схему S.*

Схему, изображённую на рис. 2(а), назовём *специальным блоком первого типа*, а на рис. 2(б) — *специальным блоком второго типа*. Заметим, что обе эти схемы имеют по четыре входа и на рисунке через v_1, v_2 помечены входы блоков, которые будем называть *главными*.

Специальный блок D в схеме S будем называть *верхним*, если его главные входы являются двумя различными входами схемы S, с которыми в S соединены только входы соответствующих элементов из B. Применительно к схемам, реализующим линейные булевы функции и содержащим верхние специальные блоки, введём операцию *специальной редукции*. Пусть схема S реализует линейную функцию от n переменных и содержит верхний специальный блок D (первого или второго типа). Под операцией специальной редукции (соответственно первого или второго типа) будем подразумевать преобразование исходной схемы S, при котором из S удаляются все четыре элемента специального блока D и быть может изменяются соединения остающихся элементов так, что получающаяся из S редуцированная схема S' реализует линейную функцию от $n-1$ переменных. Заметим, что операция специальной редукции первого типа эквивалентна подстановке вместо x_1 нуля, а операция второго типа — подстановке единицы.

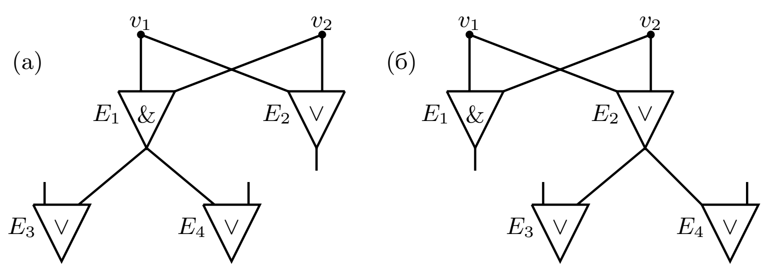

Рис. 2

Лемма 3 (основная). *Всякая минимальная схема в базисе $\mathfrak{B}$, реализующая линейную функцию $x_1 \oplus \ldots \oplus x_n \oplus c$, где $n \geqslant 2$, а $c \in \{0, 1\}$, допускает операцию стандартной редукции хотя бы одного типа или операцию специальной редукции как первого, так и второго типов.*

Далее будет часто использована

Теорема 2 [4]. *Для любых $n \geqslant 2$ и $c \in \{0, 1\}$ справедливо равенство $L(x_1 \oplus \ldots \oplus x_n \oplus c) = 4n - 4$.*

Приведём некоторые определения и обозначения [4, 7]. Пусть на входы некоторой схемы S подаются переменные $x_1, x_2, \ldots, x_n$. Будем говорить, что переменная x_i *забиваема* переменными $x_j, x_k, \ldots, x_l$, если при подаче некоторых булевых констант на входы схемы, отвечающие $x_j, x_k, \ldots, x_l$, реализуемая схемой S (выходная) функция не зависит от x_i.

Забиваемость переменной x_i переменными $x_j, x_k, \ldots, x_l$ (в схеме S) будем обозначать через $S(x_j, x_k, \ldots, x_l \Rightarrow x_i)$ или просто $x_j, x_k, \ldots, x_l \Rightarrow x_i$ (если ясно, какая схема S имеется в виду).

Будем говорить, что переменные $x_i, \ldots, x_k$ *забивают выход элемента* E в схеме S, если при подаче некоторых констант на входы схемы S, отвечающие $x_i, \ldots, x_k$, на выходе элемента E тоже получается константа. Обозначать забиваемость выхода элемента E переменными $x_i, \ldots, x_k$ будем через $x_i, \ldots, x_k \Rightarrow E$.

Введём обозначения:

$x \to E$ ($x \not\to E$) — переменная x подаётся (не подаётся) на вход элемента E;

вход x_i — вход схемы, отвечающий переменной x_i;

$x_i \to E$ ($x_i \not\to E$) — вход x_i подаётся (не подаётся) на вход элемента E;

$E_i \to E_j$ ($E_i \not\to E_j$) — выход элемента E_i подаётся (не подаётся) на вход элемента E_j; если $E_i \to E_j$, то будем говорить, что элемент E_i *предшествует* элементу E_j, а E_j *следует за* E_i;

$E_i \xrightarrow{T} E_j$ ($x_i \xrightarrow{T} E_j$) — выход элемента E_i (вход x_i) подаётся только на вход элемента E_j;

$$\chi(E^o) = \begin{cases} 1, & \text{если } E^o \text{ — дизъюнктор,} \\ 0, & \text{если } E^o \text{ — конъюнктор,} \end{cases}$$

где $o \in \{\&, \vee\}$; константу $\chi(E^o)$ будем называть *забивающей* для элемента E^o.

Как и в [4], будем использовать следующие два свойства схем (в базисе $\mathfrak{B}$), на входы которых разрешается подавать константы.

Свойство 1. *Если на вход какого-либо элемента схемы подаётся булева константа* (0 *или* 1), *то этот элемент можно удалить из схемы, а соединения оставшихся элементов изменить так, что реализуемая схемой функция не изменится.*

Свойство 2. *Если какой-либо (невыходной) элемент схемы реализует булеву константу, то этот элемент можно удалить из схемы, а соединения оставшихся элементов изменить так, что реализуемая схемой функция не изменится.*

Пусть $S_n^{\min}$ — произвольная минимальная схема, реализующая линейную функцию от n переменных ($n \geqslant 2$); для этой схемы выполняются следующие два свойства.

Свойство 3. *Из схемы* $S_n^{\min}$ *нельзя удалить* 5 *элементов и (после любого изменения соединения оставшихся элементов) получить схему, реализующую линейную функцию от* $n-1$ *переменных.*

Свойство 4. *В схеме $S_n^{\min}$ ни одна из переменных не может быть забиваемой другими переменными.*

Третье свойство вытекает из определения минимальной схемы, а четвёртое свойство очевидно.

Пусть v — вход какого-то элемента E схемы S, а w — некоторая вершина этой схемы (т. е. либо вход схемы, либо выход какого-либо её элемента). Будем говорить, что вершина w и вход v *связаны* (в схеме S), если вход v соединён либо с вершиной w, либо с выходом некоторого инвертора E^-, вход которого соединен с w. Кроме того, если вход v соединён с выходом инвертора, вход которого соединён с w, будем говорить, что *между w и v есть инвертор.*

Минимальная схема $S_n^{\min}$ обладает следующим свойством.

Свойство 5. *В $S_n^{\min}$ нет ни одного двухвходового элемента E, оба входа которого связаны с одной и той же вершиной w.*

Действительно, предположим, что оба входа элемента E связаны с вершиной w, в которой реализуется функция φ. Но тогда на выходе элемента E реализована либо функция φ (если оба входа элемента E соединены с w), либо булева константа (если один вход E соединен с w, а второй — с выходом инвертора, подвешенного к w), либо $\overline{\varphi}$ (если оба входа элемента E соединены с выходом подвешенного к w инвертора). В любом случае элемент E, очевидно, можно удалить из схемы $S_n^{\min}$ без изменения реализуемой схемой функции, а это противоречит предположению о минимальности $S_n^{\min}$.

3. Доказательство основной леммы

Пусть задана произвольная минимальная схема $S_n^{\min}$, реализующая линейную функцию $x_1 \oplus \ldots \oplus x_n \oplus c$, где $n \geqslant 2$, а $c \in \{0, 1\}$. Данная схема обладает свойством 5, по которому в $S_n^{\min}$ входы каждого двухвходового элемента связаны с различными вершинами схемы. В зависимости от вида схемы $S_n^{\min}$ рассмотрим всевозможные случаи, представленные на рис. 3 и 6.

Случай 1. Пусть в $S_n^{\min}$ есть вход x_i, связанный с входом ровно одного двухвходового элемента E_1. На второй вход (не связанный с x_i) элемента E_1 подаётся некоторая функция φ, которая с учётом свойства 1 и минимальности схемы $S_n^{\min}$ не может быть константой. Функция φ не зависит от x_i, поскольку $S_n^{\min}$ в рассматриваемом случае не содержит других (отличных от E_1) двухвходовых элементов, связанных с x_i, и в $S_n^{\min}$ нет циклов. Следовательно, при некоторых значениях переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ функция φ принимает значение $\chi(E_1)$; но в таком случае $S_n^{\min}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \Rightarrow x_i)$, а это противоречит свойству 4. Таким образом, рассматриваемый случай невозможен.

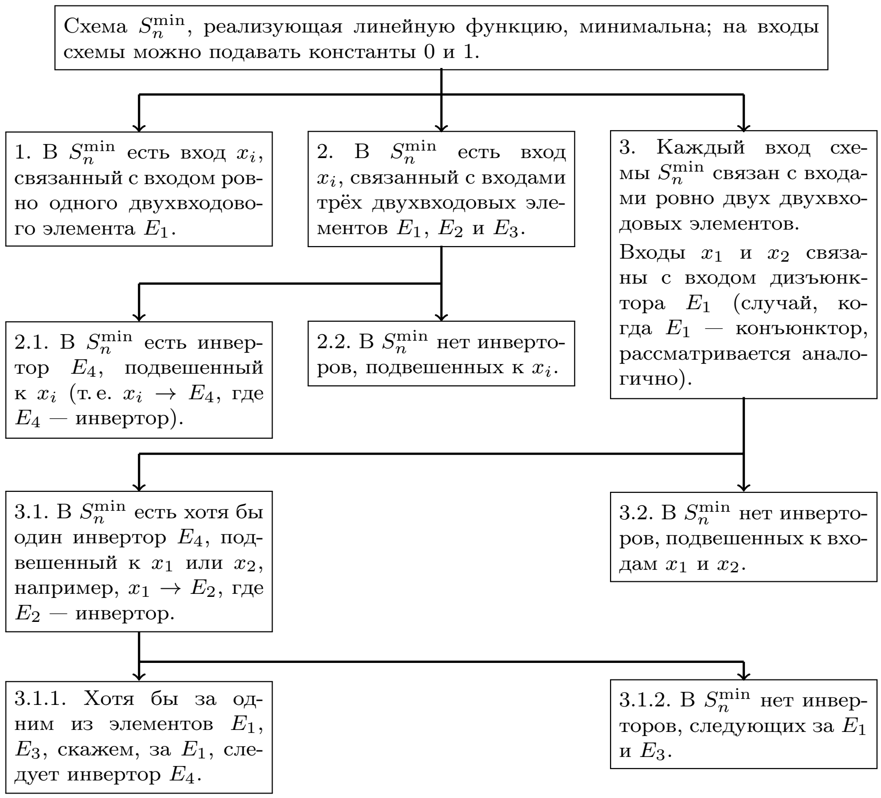

Рис. 3. Разбиение доказательства основной леммы на случаи

Случай 2. Пусть в $S_n^{\min}$ есть вход x_i, связанный с входами трёх двухвходовых элементов E_1, E_2 и E_3. В этом случае ни один из элементов E_1–E_3 не может быть выходным элементом схемы (в противном случае переменная x_i забивала бы остальные переменные) и выход каждого из этих элементов должен подаваться на вход ещё какого-нибудь элемента (иначе схема не будет минимальной).

Случай 2.1. Пусть в $S_n^{\min}$ есть инвертор E_4, подвешенный к x_i. Поскольку ни один из элементов E_1–E_3 не является выходным, в схеме $S_n^{\min}$ найдётся элемент E_5, отличный от E_1–E_4, который следует за одним из элементов E_1–E_3; пусть, например, $E_1 \to E_5$. Положим $x_i \equiv \chi(E_1)$, если $x_i \to E_1$, или $x_i \equiv \overline{\chi}(E_1)$, если $x_i \not\to E_1$, а $E_4 \to E_1$. На входы по крайней мере пяти элементов E_1–E_5 окажутся поданы булевы константы, и эти элементы согласно свойствам 1 и 2 можно удалить и получить схему S', реализующую линейную булеву функцию от $n-1$ переменных, а это противоречит свойству 3. Следовательно, рассматриваемый случай исключается.

Случай 2.2. Пусть в $S_n^{\min}$ нет инверторов, подвешенных к x_i. Среди элементов E_1–E_3 по крайней мере два одинаковых. Без ограничения общности будем считать, что одинаковыми являются элементы E_1, E_2 и каждый из этих элементов реализует дизъюнкцию (случай, когда E_1 и E_2 реализуют конъюнкцию, рассматривается аналогично). Поскольку ни один из элементов E_1–E_3 не может быть выходным элементом схемы, а сама схема $S_n^{\min}$ минимальна, выход каждого из элементов E_1–E_3 соединён в $S_n^{\min}$ с входом какого-то другого элемента.

Как нетрудно заметить, $E_i \not\to E_j$ для любой пары (i, j) различных чисел из множества $\{1, 2, 3\}$ в силу минимальности схемы $S_n^{\min}$. Например, если $E_2 \to E_3$, то на выходе элемента E_3 реализована либо та же самая функция, что и на выходе элемента E_2, либо x_i. При этом появляется возможность удаления элемента E_3, а это противоречит предположению о минимальности $S_n^{\min}$ (аналогично исключаются и другие варианты). Поэтому в $S_n^{\min}$ имеется хотя бы один элемент E_4, отличный от E_1–E_3, который следует за одним из элементов E_1, E_2, например, за E_1 (рис. 4).

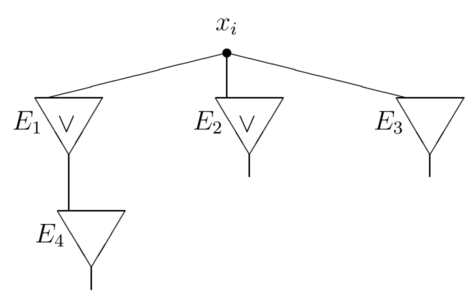

Рис. 4

Если в $S_n^{\min}$ помимо E_4 найдётся и элемент E_5 (отличный от E_1–E_4), следующий за одним из элементов E_1, E_2, то при $x_i \equiv 1$ можно удалить не менее пяти элементов (по свойствам 1 и 2) и получить схему, реализующую линейную функцию от $n-1$ переменной, а это противоречит свойству 3. Будем считать, что в $S_n^{\min}$ нет отличных от E_1–E_4 элементов, следующих за E_1, E_2. В таком случае остаётся предположить, что $E_2 \to E_4$. При $x_i \equiv 1$ на выходе элемента E_4 получим константу 1. Ясно, что элемент E_4 не может быть выходным в схеме $S_n^{\min}$ и за E_4 должен следовать ещё хотя бы один элемент. Если $E_4 \to E_3$, то опять же при $x_i \equiv 1$ на выходах элементов E_1–E_4 получим константу 1, элемент E_3 не может быть выходным в схеме $S_n^{\min}$ и за E_3 должен следовать некоторый элемент E_5. В этом случае из $S_n^{\min}$ снова оказывается возможным удалить пять элементов и получить схему, реализующую линейную функцию от $n-1$ переменных, что снова противоречит свойству 3. Если же $E_4 \not\to E_3$, то за E_4 должен следовать отличный от E_1–E_4 элемент, что опять-таки приводит (как и выше) к противоречию. Таким образом, случай 2.2 исключается.

Случай 3. Пусть каждый вход схемы $S_n^{\min}$ связан с входами ровно двух двухвходовых элементов. При этом в схеме $S_n^{\min}$, очевидно, можно выделить некоторый двухвходовый элемент E_1, связанный с двумя различными входами схемы, скажем, с входами x_1 и x_2. Для определённости считаем, что E_1 — дизъюнктор; случай, когда E_1 — конъюнктор, рассматривается аналогично. В зависимости от наличия инверторов, подвешенных ко входам x_1 и x_2, далее выделяем случаи 3.1 и 3.2.

Случай 3.1. Пусть в $S_n^{\min}$ есть хотя бы один инвертор, подвешенный к x_1 или x_2, например, $x_1 \to E_2$, где E_2 — инвертор. Пусть E_3 — второй двухвходовый элемент в схеме (помимо E_1), связанный с входом x_1. Отвечающая рассматриваемому случаю часть схемы $S_n^{\min}$ изображена на рис. 5 (на рисунке метка $x_1^{\sigma_1}$ для левого входа элемента E_1 означает, что этот вход в случае $\sigma_1 = 1$ соединён с входом x_1 схемы, а в случае $\sigma_1 = 0$ — с выходом инвертора E_2; аналогичный смысл имеют метки $x_2^{\sigma_2}$ и x_1^{β}).

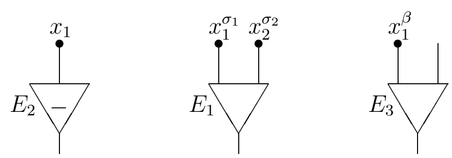

Рис. 5

Случай 3.1.1. Пусть хотя бы за одним из элементов E_1, E_3, скажем, за E_1, следует инвертор E_4. Ни один из элементов E_1, E_4, как нетрудно заметить, не может быть выходным элементом в схеме $S_n^{\min}$. Если хотя бы за одним из элементов E_1, E_4 следует отличный от E_3 элемент E_5, то подадим на вход x_1 такую константу, при которой на левый вход элемента E_1 будет подана забивающая для E_1 константа. В таком случае окажется возможным удалить из $S_n^{\min}$ пять элементов E_1–E_5, что противоречит свойству 3. Случай, когда за E_1 следует только E_4, а за E_4 —

только E_3, исключается из-за минимальности $S_n^{\min}$, поскольку в таком случае функцию, реализуемую на выходе элемента E_3, можно реализовать с использованием двух (а не трёх) элементов.

Случай 3.1.2. Пусть в $S_n^{\min}$ нет инверторов, следующих за E_1, E_3. Если за E_3 следуют два элемента E_4, E_5, то при подаче подходящей константы на вход x_1 снова получаем возможность удалить из $S_n^{\min}$ пять элементов и получить схему, реализующую линейную функцию от $n-1$ переменных, что противоречит свойству 3. Пусть за E_3 следует единственный (двухвходовый) элемент E_4. Далее рассмотрим три случая: $x_2 \not\to E_3, E_4$; $x_2 \to E_3$ и $x_2 \to E_4$.

Случай 3.1.2.1. $x_2 \not\to E_3, E_4$. В этом случае x_2 связан с входом двухвходового элемента E_5, отличного от E_1–E_4. Положим $x_1 \equiv \chi^{\beta}(E_3)$. Тогда на вход E_3 подаётся забивающая константа. На входы элементов E_1, E_2, E_4 также подаются константы. На один вход E_5, скажем, левый, подаётся x_2^{α}, на второй, т. е. правый, — некоторая функция φ от переменных $x_3, \ldots, x_n$. Если φ — не константа, то можно подобрать для $x_3, \ldots, x_n$ такие значения, при подаче которых на входы $x_3, x_4, \ldots, x_n$ схемы $S_n^{\min}$ на правый вход элемента E_5 будет подана забивающая для E_5 константа и значение на выходе схемы $S_n^{\min}$ уже не будет зависеть от x_2. Это противоречит свойству 4 и исключает наше предположение. Если же φ — константа, то можно удалить пять элементов E_1–E_5 и получить схему, реализующую линейную функцию от $n-1$ переменных, что противоречит свойству 3.

Случай 3.1.2.2. $x_2 \to E_3$. Если за E_1 следует отличный от E_4 элемент E_5, то полагая $x_1 \equiv \chi^{\sigma_1}(E_1)$ и рассуждая так же, как и в предыдущем случае, приходим к выводу, что на вход элемента E_4 (отличный от соединённого с выходом элемента E_3) должна подаваться константа, иначе x_2 оказалась бы забиваемой на выходе схемы другими переменными, что противоречит свойству 4. Но если на входы пяти элементов E_1–E_5 подаются константы, то приходим к противоречию со свойством 3.

Предположим, что за E_1 следует только E_4. Если E_4 — такой же элемент (конъюнктор или дизъюнктор), как и один из элементов E_1, E_3, например, E_1, то при $x_1 \equiv \chi^{\sigma_1}(E_1)$ на входы элементов E_1–E_4 будут подаваться константы, элементы E_1, E_4 будут выдавать константу, за элементом E_4 (который в данном случае не может быть выходным) будет следовать отличный от E_1–E_4 элемент E_5 и все пять элементов E_1–E_5 можно удалить из схемы, что противоречит свойству 3.

Предположим, что E_4 отличается от E_1 и E_3; это означает, что элементы E_1, E_3 одинаковые (т. е. по предположению случая 3 они дизъюнкторы). На вход одного из элементов E_1, E_3 должна подаваться переменная x_2, а на вход другого — $\overline{x}_2$; иначе переменная x_1 оказалась бы забиваемой переменной x_2. Это, в свою очередь, означает, что в схеме присутствует инвертор E_5 такой, что $x_2 \to E_5$, и за E_5 следует только один из элементов E_1, E_3, скажем, E_3. При $x_1 \equiv \chi^{\beta}(E_3)$ на входы элементов E_1–E_4 подаются константы и эти элементы можно удалить (свойство 1). Помимо этого можно удалить ещё и E_5, поскольку выход этого элемента связан только с выходом выдающего константу и удаляемого элемента E_3. В итоге получаем противоречие со свойством 3.

Случай 3.1.2.3. $x_2 \to E_4$. Если с выходом элемента E_4 связаны входы хотя бы двух каких-то элементов E_5, E_6, отличных от E_1–E_4, то на вход x_2 подадим константу $\chi(E_4)$. Возможность удаления в этом случае пяти элементов E_1, E_3, E_4, E_5, E_6 (напомним, что за E_3 следует только один элемент E_4, после удаления которого выход элемента E_3 не будет подаваться на входы других элементов схемы и не будет являться выходом схемы) приводит к противоречию со свойством 3.

Допустим, что с выходом E_4 связан вход ровно одного отличного от E_1–E_4 двухвходового элемента E_5 (заметим, что если бы за E_4 следовал инвертор, то в силу минимальности схемы и за этим инвертором следовал бы элемент и с выходом E_4 оказались бы связанными входы двух элементов). При $x_1 \equiv \chi^{\sigma_1}(E_1)$ на вход элемента E_5 (отличный от соединённого с выходом элемента E_4) должна подаваться константа, которая не забивает выход элемента E_5, иначе $x_1, x_3, x_4, \ldots, x_n \Rightarrow x_2$. Положим $x_1 \equiv \chi^{\sigma_1}(E_1)$. Если при этом элемент E_3 реализует константу, то элементы E_1–E_5 можно удалить (по свойствам 1, 2) из $S_n^{\min}$; противоречие со свойством 3. Предположение о том, что E_3 реализует отличную от константы функцию (переменных $x_3, \ldots, x_n$), приводит к противоречию со свойством 4, так как в этом случае переменная x_2 забиваема другими переменными.

Случай 3.2. Пусть в $S_n^{\min}$ нет инверторов, подвешенных к входам x_1 и x_2. Разбиение случая 3.2 на подслучаи представлено на рис. 6.

Случай 3.2.1. Пусть в схеме $S_n^{\min}$ вход, соответствующий переменной x_1, подаётся на вход элемента E_2, а вход, соответствующий x_2, — на вход элемента E_3, отличного от E_2. Этому случаю отвечает рис. 7.

Из условия минимальности $S_n^{\min}$ следует, что $E_1 \not\to E_2, E_3$. Если $E_1 \to E_4, E_5$ (элементы E_4, E_5 отличны от E_1–E_3), то при $x_2 \equiv \chi(E_1)$ на левый вход элемента E_2 должна подаваться константа $\overline{\chi}(E_2)$, иначе $x_2, \ldots, x_n \Rightarrow x_1$; противоречие свойству 4. Но если при $x_2 \equiv \chi(E_1)$ на вход элемента E_2 подаётся константа $\overline{\chi}(E_2)$, то по свойствам 1, 2

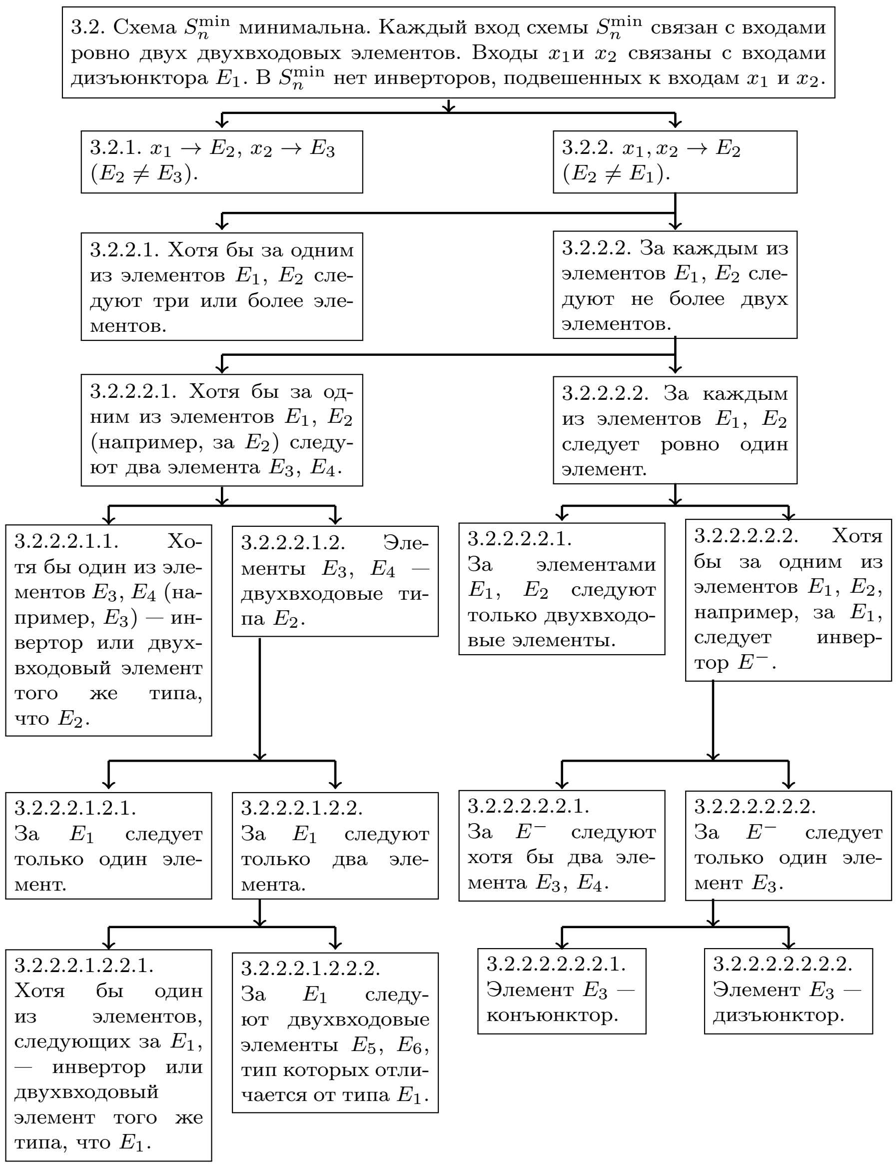

Рис. 6. Разбиение случая 3.2

можно удалить пять элементов E_1–E_5, что противоречит свойству 3. Значит, за E_1 следует только один элемент. Подача переменных, отличных от x_1, x_2, на входы элементов E_2, E_3 привела бы к забиваемости одной из переменных x_1, x_2 остальными переменными, что несовместимо со свойством 4. Остаётся только предположить, что по одному из входов элементов E_2, E_3 соединены с выходами элементов. Поскольку одновременно условия $E_2 \to E_3$ и $E_3 \to E_2$ выполняться не могут (и $E_1 \not\to E_2, E_3$), найдётся элемент E_4, предшествующий одному из элементов E_2, E_3, пусть для определённости $E_4 \to E_2$.

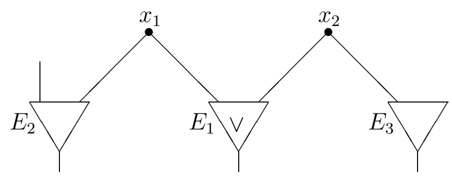

Рис. 7

Предположим, что единственным следующим за E_1 является элемент E_5, отличный от E_4. При $x_2 \equiv \chi(E_1)$ можно удалить элементы E_1 (реализует константу), E_3, E_5 (константа подаётся на входы этих элементов), E_4 (реализует константу $\overline{\chi}(E_2)$, иначе переменная x_1 оказалась бы забиваемой другими переменными) и E_2 (на его вход подаётся константа $\overline{\chi}(E_2)$); противоречие свойству 3.

Остаётся рассмотреть возможность следования за E_1 элемента E_4 (рис. 8).

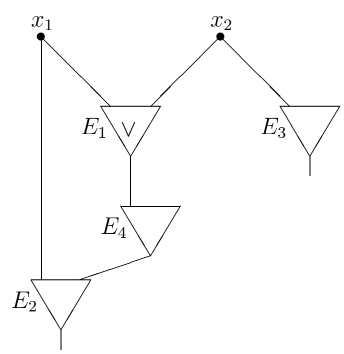

Рис. 8

Если $E_4 \to E_5$ (E_5 отличен от E_1–E_4), то при $x_2 \equiv \chi(E_1)$ элемент E_4 должен выдавать $\overline{\chi}(E_2)$, иначе x_2 окажется забиваемой другими переменными. По свойствам 1 и 2 элементы E_1–E_5 можно удалить, что приведёт к противоречию со свойством 3. Далее рассматриваем возможность следования за E_4 только элементов E_2, E_3.

Если $E_4 \to E_2, E_3$, то найдётся элемент E_5 такой, что $E_2 \to E_5$, и при $x_1 \equiv \chi(E_2)$ на выходе элемента E_4 должно быть $\overline{\chi}(E_3)$, иначе x_2 забиваема остальными переменными. Но тогда можно удалить элементы E_1–E_5; противоречие свойству 3.

Пусть за элементом E_4 следует только элемент E_2. Если $E_2 \to E_5$ (E_5 отличен от E_1–E_4), то при $x_1 \equiv \chi(E_2)$ на вход E_3 должна подаваться константа $\overline{\chi}(E_3)$ и элементы E_1–E_5 можно удалить, что противоречит свойству 3. Если за E_2 следует только E_3, то $x_2 \Rightarrow x_1$; противоречие свойству 4. В итоге приходим к выводу, что случай 3.2.1 исключается.

Случай 3.2.2. Пусть в схеме $S_n^{\min}$ входы x_1 и x_2 подаются на входы двухвходового элемента E_2, отличного от E_1. Заметим, что в этом случае элементы E_1 и E_2 реализуют различные функции (в силу минимальности схемы $S_n^{\min}$).

Случай 3.2.2.1. Пусть хотя бы за одним из элементов E_1, E_2 следуют три или более элементов. Пусть, например, $E_1 \to E_3, E_4, E_5$. В этом случае при $x_1 \equiv \chi(E_1)$ можно удалить пять элементов E_1–E_5, что противоречит свойству 3.

Случай 3.2.2.2. Пусть за каждым из элементов E_1, E_2 следуют не более чем два элемента.

Случай 3.2.2.2.1. Пусть хотя бы за одним из элементов E_1, E_2 (например, за E_2) следуют два элемента E_3, E_4.

Случай 3.2.2.2.1.1. Пусть хотя бы один из элементов E_3, E_4 (например, E_3) — инвертор или двухвходовый элемент того же типа, что E_2 (т. е. конъюнктор, если E_2 является конъюнктором, и дизъюнктор, если E_2 — дизъюнктор). Тогда переменные x_1, x_2 забивают выход элемента E_3, значит, E_3 не может быть выходным элементом схемы (см. свойства 2 и 4) и за ним должны следовать элементы. Если $E_3 \to E_5$ (E_5 отличен от E_1–E_4), то при $x_1 \equiv \chi(E_2)$ появится возможность удаления пяти элементов E_1–E_5, противоречие свойству 3. Если $E_3 \to E_4$, то переменная x_1 забивает выход элемента E_4, а значит, он не является выходным и найдётся элемент E_5 такой, что $E_4 \to E_5$ (E_5 отличен от E_1–E_4), что снова приводит к противоречию.

Случай 3.2.2.2.1.2. Пусть элементы E_3, E_4 — двухвходовые элементы, тип которых не совпадает с типом E_2.

Случай 3.2.2.2.1.2.1. Пусть за E_1 следует только один элемент. Ни один из элементов E_3, E_4 (рис. 9) не может следовать за E_1 (если, например, $E_1 \to E_4$, то на выходе элемента E_4 реализуется $x_1 \& x_2$ или $x_1 \vee x_2$, и схема оказывается не минимальной), следовательно, за E_1 следует некоторый отличный от E_1–E_4 элемент E_5. Если E_5 — двухвходовый элемент, то при $x_1 \equiv \chi(E_2)$ на вход элемента E_5 должна подаваться константа $\overline{\chi}(E_5)$, иначе x_2 забиваема другими переменными; противоречие свойству 2. Но если при $x_1 \equiv \chi(E_2)$ на вход элемента E_5 подаётся константа, то можно удалить элементы E_1–E_5, что противоречит свойству 3, и рассматриваемый случай исключается.

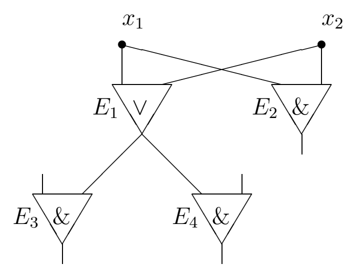

Рис. 9

Предположим, что E_5 — инвертор; очевидно, он не может быть выходным элементом схемы. Если за E_5 следуют два каких-то элемента, то при $x_2 \equiv \chi(E_1)$ можно удалить из схемы пять элементов; противоречие свойству 3. Пусть за E_5 следует только один какой-то элемент E_6. В силу минимальности схемы E_6 — двухвходовый элемент. Если E_6 — отличный от E_3, E_4 элемент, то, как и выше, приходим к выводу, что при $x_1 \equiv \chi(E_2)$ на вход элемента E_6 должна подаваться константа $\overline{\chi}(E_6)$ и возможно удаление пяти элементов, что противоречит свойству 3.

Предположим, что E_6 совпадает, например, с E_4, т. е. $E_5 \to E_4$. Положим $x_1 \equiv \chi(E_2)$ и удалим четыре элемента E_1–E_4. В оставшейся схеме S' переменная x_2 подаётся только на вход инвертора E_5, а на выходе схемы реализована некоторая линейная функция $\varphi(x_2, \ldots, x_n) = x_2 \oplus \ldots \oplus x_n \oplus c$, где $c \in \{0, 1\}$. Удалим теперь из S' инвертор E_5, а все входы других элементов, соединённые в S' с выходом инвертора E_5, соединим с входом x_2. В итоге, как нетрудно заметить, получим некоторую схему S'', реализующую $\overline{\varphi}$ (т. е. линейную функцию от $n-1$ переменных). Всего из исходной схемы S будут удалены пять элементов, что противоречит свойству 3.

Случай 3.2.2.2.1.2.2. Пусть за E_1 следуют два элемента.

Случай 3.2.2.2.1.2.2.1. Пусть хотя бы один из элементов, следующих за E_1, — инвертор или двухвходовый элемент того же типа, что и E_1. Этот случай, как и случай 3.2.2.2.1.1, исключается.

Случай 3.2.2.2.1.2.2.2. Пусть за элементом E_1 следуют двухвходовые элементы E_5, E_6, тип которых отличается от типа E_1. Тогда утверждение леммы выполняется: при $x_1 \equiv \chi(E_2)$ можно удалить специальный блок, содержащий элементы E_1–E_4, а при $x_1 \equiv \chi(E_1)$ можно удалить специальный блок, содержащий элементы E_1, E_2, E_5, E_6, причём эти блоки верхние и имеют различный тип.

Случай 3.2.2.2.2.1. Пусть за элементами E_1, E_2 следуют только двухвходовые элементы. За элементами E_1, E_2 должны следовать различные элементы, иначе схема не минимальна. Пусть для определённости $E_1 \to E_3$, $E_2 \to E_4$. В таком случае на второй вход одного из элементов E_3, E_4, например, на вход E_3, подаётся некоторая функция $\varphi(x_3, \ldots, x_n)$ (в частности, это может быть одна из переменных $x_3, \ldots, x_n$), не зависящая от x_1, x_2 и не равная константе. Положим $x_2 \equiv \chi(E_2)$, а на входы x_3, ..., x_n подадим такие константы $\sigma_3, \ldots, \sigma_n$, при которых $\varphi \equiv \chi(E_3)$. При этом значения на выходах элементов E_2, E_3 не будут зависеть от x_1, и в итоге получим $S_n^{\min}(x_2, \ldots, x_n \Rightarrow x_1)$, что противоречит свойству 4.

Случай 3.2.2.2.2.2. Пусть хотя бы за одним из элементов E_1, E_2, например, за E_1, следует инвертор E^-.

Случай 3.2.2.2.2.2.1. Пусть за E^- следуют хотя бы два элемента E_3 и E_4. Этот случай исключается, поскольку при $x_1 \equiv \chi(E_1)$ можно удалить элементы E_1–E_4, E^-, что противоречит свойству 3.

Случай 3.2.2.2.2.2.2. Пусть за E^- следует только один элемент E_3.

Случай 3.2.2.2.2.2.2.1. Пусть элемент E_3 — конъюнктор. Конъюнктор E_3 не может быть выходным элементом в схеме, и за ним должен следовать какой-то элемент E_4 (заметим, что в силу минимальности схемы $S_n^{\min}$ элемент E_3 не может быть инвертором). При $x_1 \equiv \chi(E_1) \equiv 1$ (напомним, что по предположению случая 3 элемент E_1 — дизъюнктор) можно удалить элементы E_1–E_4, E^-; противоречие свойству 3.

Случай 3.2.2.2.2.2.2.2. Пусть элемент E_3 — дизъюнктор. Предположим, что за E_2 следует какой-то (отличный от E_3) элемент E_4. При $x_1 \equiv \chi(E_2)$ на правый вход элемента E_3 (рис. 10) должна подаваться константа 0, иначе x_1 забиваема другими переменными, что противоречит свойству 4. Удалим элементы E_1–E_4 (на входы которых подаётся константа 0) и получим реализующую некоторую линейную функцию $\varphi(x_2, \ldots, x_n)$ схему S', в которой переменная x_2 подаётся только на вход инвертора E^-. Удалим из S' инвертор E^-, а входы других элементов, соединённые в S' с выходом инвертора E^-, соединим с входом схемы x_2. В итоге получим некоторую схему S'', реализующую $\overline{\varphi}$. Всего из $S_n^{\min}$ удалены пять элементов, что противоречит свойству 3 и исключает рассматриваемый случай.

Остаётся предположить, что выход элемента E_2 соединён только с входом элемента E_3, но в таком случае утверждение леммы выполняется. Лемма 3 доказана.

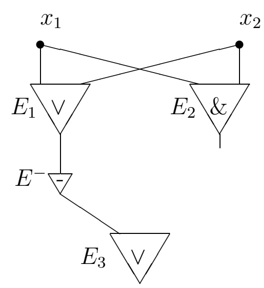

Рис. 10

4. Доказательство теоремы 1

Пусть $S_n^{\min}$ — произвольная минимальная схема, реализующая линейную функцию $x_1 \oplus \ldots \oplus x_n \oplus c$, где $n \geqslant 2$, $c \in \{0,1\}$. По теореме 2 схема $S_n^{\min}$ содержит $4n-4$ элемента. В случае $n=2$ нетрудно убедиться, что $S_2^{\min}$ может быть только стандартным блоком. Ниже будем считать, что $n \geqslant 3$. К схеме $S_n^{\min}$ применим следующую процедуру пошаговой редукции. На i-м шаге, $i = 1, 2, \ldots, n-2$, применим (если это возможно) к схеме $S_{n-i+1}^{\min}$ операцию стандартной редукции (первого или второго типа), в результате которой получится некоторая минимальная схема $S_{n-i}^{\min}$, реализующая линейную булеву функцию от $n-i$ переменных. Если операция стандартной редукции невозможна, то выполняем операцию специальной редукции первого типа и получаем некоторую минимальную схему $S_{n-i}^{\min}$ для линейной функции от $n-i$ переменных. Возможность выполнения указанной процедуры гарантируют основная лемма 3 (проведение операции редукции), лемма 1 и теорема 2 (получение после каждого шага процедуры минимальной схемы, реализующей линейную функцию).

Предположим, что на некоторых шагах описанной процедуры удалялись специальные блоки, и последний специальный блок B удалён при переходе от $S_k^{\min}$ к $S_{k-1}^{\min}$. Поскольку при переходе от $S_k^{\min}$ к $S_{k-1}^{\min}$ удалён специальный блок из четырёх двухвходовых элементов, а далее на каждом шаге удаляли стандартный блок, содержащий ровно три двухвходовых элемента, и в «остатке» получен стандартный блок $S_2^{\min}$, в схеме $S_k^{\min}$ должно быть $3k-2$ двухвходовых функциональных элементов и $k-2$ инверторов. По лемме 3 в схеме $S_k^{\min}$ наряду со специальным блоком B первого типа выделим ещё и специальный блок B' второго типа.

Пусть $R_{k-1}^{\min}$ — схема, которая получается (в результате операции специальной редукции второго типа согласно лемме 3) из $S_k^{\min}$ после удаления блока B'. Схема $R_{k-1}^{\min}$ реализует линейную функцию от $k-1$ переменных, минимальна и содержит $3k-6$ двухвходовых элементов (на четыре элемента меньше $S_k^{\min}$). Используя лемму 3, построим последовательность схем $R_{k-1}^{\min}, \ldots, R_2^{\min}$. При каждом переходе, т. е. при каждой операции редукции, в этой последовательности из схемы удаляются три двухвходовых элемента при стандартной операции и четыре двухвходовых элемента при специальной операции, и если выполняется хотя бы одна операция специальной редукции, то в схеме $R_{k-1}^{\min}$ должно быть более чем $3k-6$ двухвходовых элементов. Но $R_{k-1}^{\min}$ содержит ровно $3k-6$ двухвходовых элементов, следовательно, при переходе от $R_{k-1}^{\min}$ к $R_{k-2}^{\min}$, от $R_{k-2}^{\min}$ к $R_{k-3}^{\min}$ и т. д. удалялись только стандартные блоки (и в «остатке» получается стандартный блок $R_2^{\min}$).

Предположим, что в схеме $S_{k-1}^{\min}$ содержится h стандартных блоков первого типа и $k-2-h$ стандартных блоков второго типа. Тогда число конъюнкторов в ней равно $h+k-2$. Это означает, что в $S_k^{\min}$ содержится $h+k-1$ конъюнкторов, а в $R_{k-1}^{\min}$ — $h+k-4$ конъюнкторов. С другой стороны, если схема $R_{k-1}^{\min}$ содержит, скажем, h' стандартных блоков первого типа, то в ней $h'+k-2$ конъюнкторов. Получаем $h+k-4=h'+k-2$, откуда $h'=h-2$. Последнее равенство означает, что число стандартных блоков второго типа (реализующих $x \oplus y \oplus 1$, т. е. эквивалентность) в схемах $S_{k-1}^{\min}$ и $R_{k-1}^{\min}$ отличается на 2, поэтому эти схемы реализуют одну и ту же линейную функцию. Вместе с тем при удалении из $S_k^{\min}$ блока B на некоторый вход схемы $S_k^{\min}$ подаётся константа 0, а при удалении из $S_k^{\min}$ блока B' на тот же самый вход подаётся константа 1. В таком случае схемы $S_{k-1}^{\min}$ и $R_{k-1}^{\min}$ должны реализовывать различные функции. Получаем противоречие, исключающее наше исходное предположение о вхождении в процедуру хотя бы одной операции специальной редукции. Если же на каждом шаге процедуры удаляется стандартный блок, то в этом случае утверждение теоремы вытекает из леммы 2. Теорема 1 доказана.

Замечание. После написания этой работы автору стали известны тезисы доклада С. А. Ложкина [2], содержащие формулировки утверждений, аналогичных теореме 1 из настоящей работы, но без доказательств.

В заключение приношу глубокую благодарность своему научному руководителю профессору Н. П. Редькину.

ЛИТЕРАТУРА

1. **Комбаров Ю. А.** О минимальных реализациях линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x} \& y\}$ // Тр. VIII междунар. конф. «Дискретные модели в теории управляющих систем» (Москва, 6–9 апреля 2009 г.). — М.: МАКС Пресс, 2009. — С. 145–149.
2. **Ложкин С. А.** О структуре минимальных схем из функциональных элементов в базисе $\{\&, \vee, \neg\}$, реализующих линейную функцию // Тр. V междунар. конф. «Дискретные модели в теории управляющих систем» (Ратмино, 26–29 мая 2003 г.). — М.: Изд. отд. фак. ВМиК МГУ им. М. В. Ломоносова, 2003. — С. 50.
3. **Лупанов О. Б.** Асимптотические оценки сложности управляемых систем. — М.: МГУ, 1984. — 136 с.
4. **Редькин Н. П.** Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — № 23. — С. 83–101.
5. **Редькин Н. П.** О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — № 6. — С. 31–38.
6. **Редькин Н. П.** О минимальных и асимптотически минимальных схемах для некоторых индивидуальных булевых функций // Мат. IX междунар. семинара «Дискретная математика и её приложения», посвящённого 75-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2007 г.). — М.: Изд-во мех.-мат. фак. МГУ, 2007. — С. 11–19.
7. **Редькин Н. П.** О минимальной реализации двоичного сумматора // Проблемы кибернетики. — 1981. — № 38. — С. 181–216.
8. **Шкребела И. С.** О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$ // Дискрет. математика. — 2003. — Т. 15, № 4. — С. 100–112.
9. **Яблонский С. В.** Введение в дискретную математику. — М.: Наука, 1986. — 384 с.
10. **Cardot C.** Quelques résultats sur l'application de l'algèbre de Boole á la synthèse des circuits a relais // Ann. Telecomm. — 1952. — Vol. 7, N 2. — P. 75–84.

Комбаров Юрий Анатольевич
e-mail: yuri.kombarov@gmail.com

Статья поступила
28 июня 2011 г.

Переработанный вариант —
18 августа 2011 г.