ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2015. Том 22, № 5. С. 71–85

УДК 519.714 DOI: 10.17377/daio.2015.22.481

ДОСТАТОЧНЫЕ УСЛОВИЯ ЛОКАЛЬНОЙ БЕСПОВТОРНОСТИ МИНИМАЛЬНЫХ π-СХЕМ, РЕАЛИЗУЮЩИХ ЛИНЕЙНЫЕ БУЛЕВЫ ФУНКЦИИ

К. Л. Рычков[1]

[1]Институт математики им. С. Л. Соболева,
пр. Коптюга, 4, 630090 Новосибирск, Россия
e-mail: rychkov@math.nsc.ru

Аннотация. Сформулированы достаточные условия локальной бесповторности минимальных π-схем, реализующих линейные булевы функции. Выполнение этих условий приводит к описанию классов минимальных π-схем, реализующих линейные булевы функции, существенно зависящие от n переменных. Ил. 2, библиогр. 12.

Ключевые слова: сложность формул, π-схема, нижняя оценка сложности.

Введение

В [8] С. В. Яблонским для линейных булевых функций, существенно зависящих от n переменных, приведён алгоритм построения параллельно-последовательных контактных схем (π-схем). В [5] В. М. Храпченко показал, что при $n = 2^k,\ k = 0, 1, 2, \ldots$, построенные по этому алгоритму π-схемы являются минимальными. Кроме того, в [2] установлено, что при указанных значениях n в некотором вполне определённом смысле этими π-схемами исчерпываются все минимальные π-схемы, реализующие линейные булевы функции, существенно зависящие от n переменных. В силу этого возникает гипотеза, состоящая в том, что та же картина должна сохраняться и в случае произвольного натурального n. В настоящей статье делается попытка найти подход к доказательству этой гипотезы. При некоторых предположениях, в том числе очень сильном предположении о минимальности π-схем Яблонского, даётся положительное решение поставленной задачи.

Более точно, цель статьи заключается в том, чтобы для произвольного натурального n сформулировать некоторую задачу о разбиении рёбер n-мерного единичного куба, положительное решение которой приводит к описанию класса минимальных π-схем, реализующих линейные булевы функции, существенно зависящие от n переменных. Описание состоит в следующем: любая минимальная π-схема, реализующая одну из указанных функций, с точностью до перестановки подсхем совпадает с некоторой π-схемой Яблонского. Как отмечено выше, в [2] такое описание получено для классов минимальных π-схем, реализующих линейные булевы функции, существенно зависящие от $2^k,\ k = 0, 1, 2, \dots$, переменных.

Существуют две линейные булевы функции, существенно зависящие от n переменных $x_1, \dots, x_n$:

$$\Phi_n^1(x_1, \dots, x_n) = x_1 + \dots + x_n \pmod 2,$$

$$\Phi_n^0(x_1, \dots, x_n) = x_1 + \dots + x_n + 1 \pmod 2.$$

Назовём *π-схемами Яблонского* π-схемы, построенные для функций Φ_n^1, Φ_n^0 по несколько обобщённому алгоритму С. В. Яблонского [8].

Определим класс π-схем Яблонского. Обозначим его через Y. Подклассы класса Y, состоящие из π-схем, реализующих функции $\Phi_n^1,\ \Phi_n^0$, обозначим через Y_n^1, Y_n^0 соответственно. Будем использовать общепринятое обозначение

$$x_i^\delta = \begin{cases} x_i & \text{при } \delta = 1, \\ \overline{x}_i & \text{при } \delta = 0, \end{cases}$$

где x_i — произвольная переменная из множества $X = \{x_1, x_2, \dots\}$ булевых переменных.

Пусть $n = 1$. По определению любая π-схема, состоящая из одного контакта, помеченного $x_i^1,\ x_i \in X$, принадлежит Y_1^1; любая π-схема, состоящая из одного контакта, помеченного $x_i^0,\ x_i \in X$, принадлежит Y_1^0. Других π-схем в $Y_1^1,\ Y_1^0$ нет.

Очевидно, что π-схемы из класса Y_1^1 реализуют функции $\Phi_1^1(x_i)$, $x_i \in X$; π-схемы из класса Y_1^0 реализуют функции $\Phi_1^0(x_i),\ x_i \in X$.

Пусть $n = 2^k + \rho,\ k \geqslant 1,\ 0 \leqslant \rho < 2^k$, и для всех $m < n$ классы $Y_m^1,\ Y_m^0$ уже определены. Представим число n всеми возможными способами в виде суммы

$$n = p + q$$

двух чисел p и q таких, что $2^{k-1} \leqslant p,\ q \leqslant 2^k$.

Через $S_p^1,\ S_p^0,\ S_q^1,\ S_q^0$ обозначим произвольные π-схемы из классов $Y_p^1,\ Y_p^0,\ Y_q^1,\ Y_q^0$, которые реализуют соответственно функции

$$\Phi_p^1(x_1, \dots, x_p), \quad \Phi_p^0(x_1, \dots, x_p), \quad \Phi_q^1(x_{p+1}, \dots, x_n), \quad \Phi_q^0(x_{p+1}, \dots, x_n).$$

По определению классу Y_n^1 принадлежат π-схемы, собранные из π-схем S_p^1, S_p^0, S_q^1, S_q^0 так, как это показано на рис. 1.

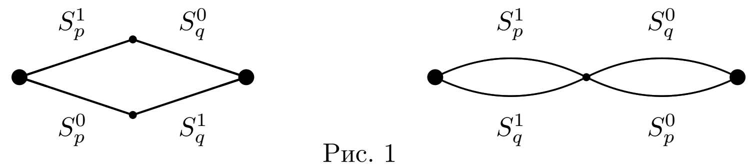

Рис. 1

Кроме того, классу Y_n^1 принадлежат π-схемы, полученные из этих π-схем заменой (без отождествления) переменных $x_1, \ldots, x_n$ произвольными переменными $x_{i_1}, \ldots, x_{i_n} \in X$. Других π-схем в Y_n^1 нет.

Очевидно, что π-схемы из Y_n^1 реализуют функции $\Phi_n^1(x_{i_1}, \ldots, x_{i_n})$, $x_{i_1}, \ldots, x_{i_n} \in X$.

По определению классу Y_n^0 принадлежат π-схемы, собранные из π-схем S_p^1, S_p^0, S_q^1, S_q^0 так, как это показано на рис. 2.

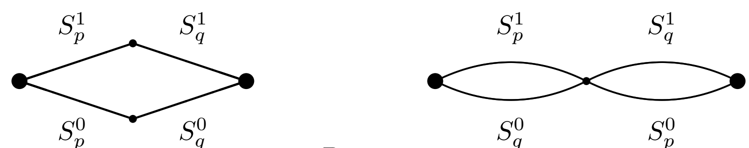

Рис. 2

Кроме того, классу Y_n^0 принадлежат π-схемы, полученные из этих π-схем заменой (без отождествления) переменных $x_1, \ldots, x_n$ произвольными переменными $x_{i_1}, \ldots, x_{i_n} \in X$. Других π-схем в Y_n^0 нет.

Очевидно, что π-схемы из Y_n^0 реализуют функции $\Phi_n^0(x_{i_1}, \ldots, x_{i_n})$, $x_{i_1}, \ldots, x_{i_n} \in X$.

Пусть $Y_n = Y_n^1 \cup Y_n^0$, $n = 1, 2, \ldots$. По определению $Y = \bigcup\limits_{n=1}^{\infty} Y_n$.

Определим понятие подсхемы π-схемы S. *Подсхемой* произвольной *контактной схемы* называется любой подграф этой схемы. При этом полюсами подсхемы считаются те из принадлежащих этой подсхеме вершин, которые являются или полюсами самой схемы, или концами контактов схемы, не принадлежащих этой подсхеме. *Подсхемой π-схемы S* называем двухполюсную подсхему контактной схемы S. Очевидно, что любая подсхема π-схемы S является π-схемой.

Пусть некоторая подсхема P π-схемы S является последовательным соединением π-схем P_1, P_2. Переставим местами P_1, P_2 в подсхеме P. Полученную из S в результате этой перестановки π-схему обозначим через T. Говорим, что *π-схема T* (а также любая ей изоморфная π-схема) *получена из S транспозицией подсхем.* Будем говорить, что *π-схема A совпадает с π-схемой S с точностью до перестановки подсхем*, если A может быть получена из S в результате конечной последовательности транспозиций подсхем.

Через U обозначим класс всех π-схем, которые с точностью до перестановки подсхем совпадают с некоторой π-схемой из Y. Через $U_n,\ n = 1, 2, \dots$, обозначим класс всех π-схем, которые с точностью до перестановки подсхем совпадают с некоторой π-схемой из Y_n.

Сложностью $L(S)$ π-схемы S называется число контактов в S. Если π-схема S имеет наименьшую сложность среди всех π-схем, реализующих ту же функцию что и S, то она называется *минимальной π-схемой. Сложностью $L_\pi(f)$ булевой функции f* называется сложность минимальной π-схемы для f.

Очевидно, что из всякой π-схемы для функции $\Phi_n^1(x_1, \dots, x_n)$ немедленно получается π-схема для функции $\Phi_n^0(x_1, \dots, x_n)$ с тем же числом контактов и наоборот. Поэтому справедливо равенство

$$L_\pi\bigl(\Phi_n^1\bigr) = L_\pi\bigl(\Phi_n^0\bigr).$$

Величину $L_\pi\bigl(\Phi_n^1\bigr)$ обозначим через λ_n.

Через $Q_n,\ n = 1, 2, \dots$, обозначим класс всех минимальных π-схем, реализующих функции $\Phi_n^1,\ \Phi_n^0$.

Индукцией по n нетрудно показать [2, 8], что все π-схемы из класса U_n имеют одинаковую сложность, и эта сложность равна

$$n^2 + n(n - 2^{\lfloor \log_2 n \rfloor}) - 2(n - 2^{\lfloor \log_2 n \rfloor})^2.$$

В [3–5] получены следующие нижние оценки величины λ_n:

$$\lambda_n \geqslant \begin{cases} n^2 & \text{при } n = 2^k, \\ n^2 + 1 & \text{при } n \ne 2^k, \\ n^2 + 2 & \text{при чётном } n \ne 2^k, \\ n^2 + 3 & \text{при нечётном } n \geqslant 5. \end{cases} \tag{1}$$

Кроме того, в [4, 7] доказано, что $\lambda_6 \geqslant 40$.

Из этих оценок следует, что при $n = 2^k,\ k = 0, 1, \dots$, и при $n = 3, 5, 6, 7$ имеет место равенство

$$\lambda_n = n^2 + n(n - 2^{\lfloor \log_2 n \rfloor}) - 2(n - 2^{\lfloor \log_2 n \rfloor})^2.$$

Вследствие этого справедливы включения

$$U_{2^k} \subseteq Q_{2^k},\ k = 0, 1, \dots, \quad U_3 \subseteq Q_3, \quad U_5 \subseteq Q_5, \quad U_6 \subseteq Q_6, \quad U_7 \subseteq Q_7.$$

Как было отмечено в начале статьи, классами U_{2^k}, $k = 0, 1, \ldots$, исчерпываются все минимальные π-схемы, реализующие линейные булевы функции, существенно зависящие от 2^k переменных [2]. Поэтому весьма правдоподобной представляется гипотеза о том, что при любом $n \geqslant 1$ справедливо равенство $U_n = Q_n$.

Определим понятие локально бесповторной π-схемы. *Цепью π-схемы* называется простая (без самопересечений) цепь в этой π-схеме, соединяющая её полюсы. *Тупиковым сечением π-схемы* называется минимальное по включению множество контактов π-схемы, имеющее хотя бы один общий контакт с каждой цепью π-схемы. Цепь π-схемы называется *бесповторной*, если приписанные контактам этой цепи символы x_i^δ не повторяются. Точно так же тупиковое сечение π-схемы называется *бесповторным*, если приписанные контактам этого тупикового сечения символы x_i^δ не повторяются. Пусть $f(x_1, \ldots, x_n)$ — функция проводимости π-схемы S. Говорим, что контакт π-схемы S *замкнут на наборе* $(\alpha_1, \ldots, \alpha_n)$ значений переменных $x_1, \ldots, x_n$, если этому контакту приписан символ $x_i^{\alpha_i}$, $1 \leqslant i \leqslant n$. Если контакту приписан символ $x_i^{\overline{\alpha}_i}$, $1 \leqslant i \leqslant n$, то говорим, что этот контакт *разомкнут на наборе* $(\alpha_1, \ldots, \alpha_n)$. Будем говорить, что *цепь π-схемы S замыкает S на наборе* $(\alpha_1, \ldots, \alpha_n)$, если все контакты цепи замкнуты на этом наборе. Точно так же будем говорить, что тупиковое сечение π-схемы *S размыкает S на наборе* $(\alpha_1, \ldots, \alpha_n)$, если все контакты тупикового сечения разомкнуты на этом наборе. Если для каждого $(\beta_1, \ldots, \beta_n) \in f^{-1}(1)$ найдётся бесповторная цепь π-схемы S, замыкающая S на наборе $(\beta_1, \ldots, \beta_n)$, и для каждого $(\alpha_1, \ldots, \alpha_n) \in f^{-1}(0)$ найдётся бесповторное тупиковое сечение π-схемы S, размыкающее S на наборе $(\alpha_1, \ldots, \alpha_n)$, то π-схема S называется *локально бесповторной*.

Нетрудно проверить, что все π-схемы из класса Y (а значит, и из U) локально бесповторны.

Через A_n, $n = 1, 2, \ldots$, обозначим класс всех локально бесповторных π-схем, реализующих функции Φ_n^1, Φ_n^0. Пусть $A = \bigcup\limits_{n=1}^{\infty} A_n$.

Если $S \in A$ и S имеет наименьшую сложность среди всех π-схем из A, реализующих ту же функцию что и S, то π-схема S называется *минимальной в классе A*.

В [2] показано, что класс всех π-схем, минимальных в классе A, совпадает с U. Поэтому чтобы для произвольного n доказать равенство $U_n = Q_n$, достаточно доказать включение $Q_n \subseteq A_n$.

Основным результатом настоящей статьи является формулировка достаточных условий для этого включения. Данная формулировка не зависит от π-схем, она дана в терминах некоторых специальных разбиений рёбер n-мерного единичного куба.

1. Разбиения рёбер куба B^n, порождённые π-схемами, реализующими булевы функции Φ_n^1 и Φ_n^0

Пусть B^n — множество вершин n-мерного единичного куба. *Гранью* куба B^n называется множество

$$B_{i_1,\dots,i_k}^{n,\delta_1,\dots,\delta_k} = \{(\alpha_1,\dots,\alpha_n) \in B^n \mid \alpha_{i_1} = \delta_1,\dots,\alpha_{i_k} = \delta_k\}.$$

Множество $I\big(B_{i_1,\dots,i_k}^{n,\delta_1,\dots,\delta_k}\big) = \{1,\dots,n\} \setminus \{i_1,\dots,i_k\}$ называется *множеством образующих грани*, число $n-k$ — *размерностью грани*. Если $\delta_1 + \ldots + \delta_k = 0 \pmod 2$, то грань $B_{i_1,\dots,i_k}^{n,\delta_1,\dots,\delta_k}$ называется *чётной*, если $\delta_1 + \ldots + \delta_k = 1 \pmod 2$, то — *нечётной*.

Грань размерности 1 называется *ребром куба* B^n. Если для ребра r куба B^n выполнено равенство $I(r) = \{i\}$, то говорят, что r *имеет направление* i. Очевидно, что любое ребро состоит из двух вершин куба B^n, эти вершины называются *концами ребра*.

Элементы множеств

$$N^0 = \{(\alpha_1,\dots,\alpha_n) \in B^n \mid \alpha_1 + \cdots + \alpha_n = 0 \pmod 2\},$$

$$N^1 = \{(\beta_1,\dots,\beta_n) \in B^n \mid \beta_1 + \cdots + \beta_n = 1 \pmod 2\}$$

назовём *чётными* и *нечётными вершинами* куба B^n соответственно. Элементы множества $N^0 \times N^1$ назовём (0-1)-*парами куба* B^n.

Множество вида $A^0 \times A^1$, $A^0 \subseteq N^0$, $A^1 \subseteq N^1$, назовём *замкнутым подмножеством множества* $N^0 \times N^1$. Для произвольного подмножества M множества $N^0 \times N^1$ через $\widehat{M}$ обозначим замыкание M, т. е. минимальное по включению замкнутое подмножество $N^0 \times N^1$, содержащее M.

Расстояние Хемминга между вершинами $\alpha = (\alpha_1,\dots,\alpha_n)$ и $\beta = (\beta_1,\dots,\beta_n)$ куба B^n обозначим через $\rho(\alpha,\beta)$.

Рёбра куба B^n ориентируем следующим образом: чётную вершину ребра будем считать начальной, нечётную — конечной. Введением такой ориентации мы фактически отождествили множество рёбер куба B^n с множеством

$$R = \{(\alpha,\beta) \in N^0 \times N^1 \mid \rho(\alpha,\beta) = 1\},$$

множество нечётных рёбер направления i куба B^n — с множеством

$$R_i^0 = \{(\alpha,\beta) \in R \mid \alpha_i = 1,\ \beta_i = 0\},$$

множество чётных рёбер направления i куба B^n — с множеством

$$R_i^1 = \{(\alpha, \beta) \in R \mid \alpha_i = 0,\ \beta_i = 1\}.$$

Элементы множества R будем называть (0-1)-*рёбрами* куба B^n. Элементы множеств $R_i^0,\ R_i^1,\ R_i = R_i^0 \cup R_i^1,\ \ i = 1, \ldots, n,$ — *отрицательными, положительными* и просто (0-1)-*рёбрами направления* i куба B^n.

Вследствие этого отождествления слова (0-1)-рёбра и рёбра (куба B^n) будем использовать как синонимы.

Разбиением множества P называется множество $T = \{M_1, \ldots, M_L\}$ непустых попарно не пересекающихся подмножеств множества P такое, что $M_1 \cup \cdots \cup M_L = P$. При этом множества $M_1, \ldots, M_L$ называются *блоками разбиения* T.

Разбиение T множества R (0-1)-рёбер куба B^n назовём *однородным*, если для каждого $M \in T$ найдутся $i \in \{1, \ldots, n\}$, $\delta \in \{0, 1\}$ такие, что $M \subseteq R_i^\delta$ (другими словами, если блоки разбиения T состоят из (0-1)-рёбер одного направления и одного знака).

Однородное разбиение $T = \{M_1, \ldots, M_L\}$ множества R назовём *правильным*, если множества $\widehat{M}_1, \ldots, \widehat{M}_L$ попарно не пересекаются.

Пусть S — произвольная π-схема, реализующая линейную булеву функцию $f(x_1, \ldots, x_n)$, равную $\Phi_n^1(x_1, \ldots, x_n)$ или $\Phi_n^0(x_1, \ldots, x_n)$. Через $K(S)$ обозначим множество контактов π-схемы S, через $K_i^\delta(S)$ — множество контактов π-схемы S, помеченных x_i^δ.

Через $h : R \to K(S)$ обозначим отображение Храпченко для π-схемы S. Это отображение впервые рассмотрено В. М. Храпченко в [5], строится оно по следующим правилам.

В случае $f = \Phi_n^1$ каждому набору $(\alpha_1, \ldots, \alpha_n) \in N^0$ поставим в соответствие какое-нибудь одно тупиковое сечение π-схемы S, размыкающее S на этом наборе; каждому набору $(\beta_1, \ldots, \beta_n) \in N^1$ поставим в соответствие какую-нибудь одну цепь π-схемы S, замыкающую S на этом наборе. В силу равенств $N^0 = f^{-1}(0),\ N^1 = f^{-1}(1)$ такие тупиковое сечение и цепь найдутся.

В случае $f = \Phi_n^0$ каждому набору $(\beta_1, \ldots, \beta_n) \in N^1$ поставим в соответствие какое-нибудь одно тупиковое сечение π-схемы S, размыкающее S на этом наборе; каждому набору $(\alpha_1, \ldots, \alpha_n) \in N^0$ поставим в соответствие какую-нибудь одну цепь π-схемы S, замыкающую S на этом наборе. В силу равенств $N^1 = f^{-1}(0),\ N^0 = f^{-1}(1)$ такое тупиковое сечение и такая цепь найдутся.

Известно [5], что каждые цепь и тупиковое сечение любой π-схемы имеют ровно один общий контакт (это утверждение легко доказывается индукцией по сложности схемы). По определению отображение h каждому (0-1)-ребру $((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) \in R$ ставит в соответствие тот единственный контакт $k \in K(S)$, который является общим для тупикового сечения и цепи, соответствующих наборам $(\alpha_1, \ldots, \alpha_n)$ и $(\beta_1, \ldots, \beta_n)$.

Отображение $H : N^0 \times N^1 \to K(S)$, которое не только каждому (0-1)-ребру, но и каждой (0-1)-паре $((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) \in N^0 \times N^1$ ставит в соответствие контакт $k \in K(S)$, общий для соответствующих тупикового сечения и цепи, назовём *естественным расширением отображения Храпченко* h.

Разбиение $T = \{h^{-1}(k) \mid k \in K(S),\ h^{-1}(k) \neq \varnothing\}$ множества R будем называть *разбиением, порождённым π-схемой* S.

Заметим, что $|T| \leqslant L(S)$. Кроме того, отображение Храпченко для данной π-схемы S, вообще говоря, не единственно. Вследствие этого не единственным может быть и порождённое S разбиение T.

Лемма 1. *Для произвольной π-схемы S, реализующей линейную булеву функцию, существенно зависящую от n переменных, любое порождённое S разбиение рёбер куба B^n является правильным.*

Доказательство. Рассмотрим произвольную π-схему S, реализующую линейную булеву функцию $f(x_1, \ldots, x_n)$, равную $\Phi_n^1(x_1, \ldots, x_n)$ или $\Phi_n^0(x_1, \ldots, x_n)$. Пусть T — порождённое S разбиение множества R и h — такое отображение Храпченко для S, что выполнено равенство $T = \{h^{-1}(k) \mid k \in K(S),\ h^{-1}(k) \neq \varnothing\}$.

Непосредственно из определения отображения h следует, что в случае $f = \Phi_n^1$ при $k \in K_i^\delta(S)$ справедливо включение $h^{-1}(k) \subseteq R_i^\delta$; в случае $f = \Phi_n^0$ при $k \in K_i^\delta(S)$ — включение $h^{-1}(k) \subseteq R_i^{\overline{\delta}}$. Это означает, что разбиение T однородное.

Чтобы доказать, что T правильное, осталось показать, что множества $\widehat{h^{-1}(k)},\ k \in K(S)$, попарно не пересекаются. Пусть $H : N^0 \times N^1 \to K(S)$ — естественное расширение h. Из определения отображения H следует, что множества $H^{-1}(k),\ k \in K(S)$, являются замкнутыми подмножествами множества $N^0 \times N^1$. Поэтому справедлива система включений $\widehat{h^{-1}(k)} \subseteq H^{-1}(k),\ k \in K(S)$. В силу этих включений из того, что множества $H^{-1}(k),\ k \in K(S)$, попарно не пересекаются, следует, что множества $\widehat{h^{-1}(k)}$, $k \in K(S)$, попарно не пересекаются. Лемма 1 доказана.

Правильное разбиение рёбер куба B^n назовём *минимальным*, если оно имеет наименьшую мощность среди всех правильных разбиений множества R.

Мощность минимального правильного разбиения рёбер куба B^n обозначим через μ_n.

Теорема 1. *Для любого $n \geqslant 1$ справедливо неравенство $\mu_n \leqslant \lambda_n$.*

Доказательство. Теорема 1 является непосредственным следствием леммы 1.

Заметим, что теорема 1 хотя и не явно, но фактически является результатом статьи В. М. Храпченко [5]. Приведённый в этой статье метод получения нижних оценок сложности π-схем в дальнейшем неоднократно переосмысливался и модифицировался [1, 6, 9–12], в том числе и самим автором метода [6]. Теорема 1 также является одним из вариантов такого переосмысления.

2. Достаточные условия локальной бесповторности

Правильное разбиение $T = \{M_1, \dots, M_L\}$ множества R назовём *совершенным*, если выполнено равенство

$$\widehat{M_1} \cup \dots \cup \widehat{M_L} = N^0 \times N^1.$$

Теорема 2. *Пусть S — минимальная π-схема, реализующая линейную булеву функцию, существенно зависящую от n переменных, и T — порождённое S разбиение рёбер куба B^n. Тогда из совершенности T следует локальная бесповторность S.*

Доказательство. Рассмотрим произвольную π-схему S, реализующую линейную булеву функцию $f(x_1, \dots, x_n)$, равную $\Phi_n^1(x_1, \dots, x_n)$, случай $f = \Phi_n^0$ рассматривается аналогично. Пусть T — порождённое S разбиение множества R и h — отображение Храпченко для S такое, что $T = \{h^{-1}(k) \mid k \in K(S),\ h^{-1}(k) \neq \varnothing\}$. Тупиковые сечения и цепи π-схемы S, которые поставлены в соответствие наборам $(\alpha_1, \dots, \alpha_n) \in N^0$ и $(\beta_1, \dots, \beta_n) \in N^1$ в процессе построения отображения h, назовём *выделенными*. Пусть H — естественное расширение отображения h.

Чтобы доказать теорему 2, сначала покажем, что из совершенности T и минимальности S следует система соотношений

$$\widehat{h^{-1}(k)} = H^{-1}(k) \neq \varnothing, \quad k \in K(S).$$

Далее, опираясь на эти соотношения, покажем, что выделенные цепи и тупиковые сечения бесповторны. Этим теорема 2 будет доказана.

Лемма 2. *Из совершенности разбиения T следует система равенств*

$$\widehat{h^{-1}(k)} = H^{-1}(k), \quad k \in K(S).$$

Доказательство. Как отмечено в доказательстве леммы 1, множества $H^{-1}(k),\ k \in K(S)$, являются замкнутыми подмножествами множества $N^0 \times N^1$. Поэтому $\widehat{h^{-1}(k)} \subseteq H^{-1}(k),\ k \in K(S)$. Равенства $\widehat{h^{-1}(k)} = H^{-1}(k),\ k \in K(S)$, следуют из этих включений и того факта, что наборы множеств

$$\{\widehat{h^{-1}(k)} \mid k \in K(S),\ \widehat{h^{-1}(k)} \neq \varnothing\}, \quad \{H^{-1}(k) \mid k \in K(S),\ H^{-1}(k) \neq \varnothing\}$$

являются разбиениями множества $N^0 \times N^1$ (для первого набора это верно в силу совершенности разбиения T, для второго — по определению отображения H). Лемма 2 доказана.

Лемма 3. *Из минимальности π-схемы S следует система неравенств*

$$H^{-1}(k) \neq \varnothing, \quad k \in K(S).$$

Доказательство. Предположим, напротив, что для некоторого контакта $k \in K(S)$ имеет место равенство $H^{-1}(k) = \varnothing$. Чтобы прийти к противоречию, покажем, что S не минимальна.

Равенство $H^{-1}(k) = \varnothing$ означает, что либо все выделенные тупиковые сечения не содержат k, либо все выделенные цепи не содержат k. Рассмотрим первый случай (выделенные тупиковые сечения не содержат k), второй случай рассматривается аналогично.

Рассмотрим множество $C(S)$ всех цепей π-схемы S. Пусть E — произвольное подмножество множества контактов $K(S)$. Преобразуем элементы множества $C(S)$ следующим образом: каждый контакт цепи $c \in C(S)$, если он принадлежит E, замкнём накоротко (т. е. отождествим концы этого контакта, а сам контакт удалим из c). Множество таким образом преобразованных цепей назовём *E-образом множества $C(S)$*.

Заметим, что если для тупикового сечения t π-схемы S справедливо $t \cap E = \varnothing$, то множество t имеет общий контакт с каждой преобразованной цепью и является минимальным по включению среди всех таких множеств (другими словами, t является тупиковым сечением для E-образа множества $C(S)$).

Через a, b обозначим концы контакта k. Будем говорить, что *контакт e* (или *вершина p*) *π-схемы S лежит между вершинами a, b*, если существует проходящая через a, b цепь π-схемы S такая, что контакт e (вершина p) лежит между вершинами a, b на этой цепи.

Через P обозначим подсхему π-схемы S, которая состоит из всех вершин и контактов S, лежащих между a, b. Ясно, что P — это π-схема с полюсами a, b. Она либо состоит из одного контакта k, либо является параллельным соединением k с некоторой π-схемой Q.

Заметим, что выделенные тупиковые сечения π-схемы S не имеют общих с P контактов (это следует из того, что они не содержат k и являются минимальными по включению сечениями π-схемы S).

Через S' обозначим π-схему, которая получается из S после замыкания накоротко контакта k. Более точно, S' получается из S в результате отождествления вершин a, b и удаления подсхемы P. Через $K(P)$ обозначим множество контактов π-схемы P. Очевидно, что множество $C(S')$ цепей π-схемы S' является $K(P)$-образом множества $C(S)$. Поэтому все выделенные тупиковые сечения π-схемы S являются тупиковыми сечениями π-схемы S'.

Через $f'(x_1, \dots, x_n)$ обозначим функцию проводимости π-схемы S'. Очевидно, что $f'(\delta_1, \dots, \delta_n) \geqslant f(\delta_1, \dots, \delta_n)$ для любого набора $(\delta_1, \dots, \delta_n)$ из B^n. Из того, что выделенные тупиковые сечения π-схемы S являются тупиковыми сечениями π-схемы S', следует, что $f'(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n) = 0$ при $(\alpha_1, \dots, \alpha_n) \in N^0 = f^{-1}(0)$. Поэтому $f' = f$. Схема S' имеет меньше контактов чем S, следовательно, S не минимальна. Лемма 3 доказана.

Докажем, что выделенные цепи π-схемы S бесповторны (бесповторность выделенных тупиковых сечений доказывается аналогично). Предположим противное. Пусть для некоторого $(\beta_1, \dots, \beta_n) \in N^1$ поставленная в соответствие этому набору выделенная цепь c не является бесповторной. Это означает, что для некоторого $i \in \{1, \dots, n\}$ найдутся два различных контакта k_1, k_2 цепи c, помеченные символом $x_i^{\beta_i}$. Из определения отображения h, следует, что

$$h^{-1}(k_1) \subseteq R_i, \quad h^{-1}(k_2) \subseteq R_i, \quad h^{-1}(k_1) \cap h^{-1}(k_2) = \varnothing.$$

Чтобы прийти к противоречию, покажем, что $h^{-1}(k_1) \cap h^{-1}(k_2) \neq \varnothing$.

Через e обозначим (0-1)-ребро направления i, инцидентное вершине $\beta = (\beta_1, \dots, \beta_n)$ куба B^n. Покажем, что $e \in h^{-1}(k_1) \cap h^{-1}(k_2)$.

В силу минимальности π-схемы S из леммы 3 следует $H^{-1}(k_1) \neq \varnothing$ и $H^{-1}(k_2) \neq \varnothing$. Поэтому существуют $\alpha, \gamma \in N^0$ такие, что $(\alpha, \beta) \in H^{-1}(k_1)$, $(\gamma, \beta) \in H^{-1}(k_2)$. В силу совершенности разбиения T из леммы 2 вытекает, что $(\alpha, \beta) \in \widehat{h^{-1}(k_1)}$ и $(\gamma, \beta) \in \widehat{h^{-1}(k_2)}$. Последние включения возможны только в том случае, если в $h^{-1}(k_1)$ есть (0-1)-ребро, инцидентное вершине β, и в $h^{-1}(k_2)$ есть (0-1)-ребро, инцидентное вершине β. Поскольку $h^{-1}(k_1) \subseteq R_i$ и $h^{-1}(k_2) \subseteq R_i$, это означает, что $e \in h^{-1}(k_1)$ и $e \in h^{-1}(k_2)$. Полученное противоречие показывает, что наше предположение неверно, значит, π-схема S локально бесповторна. Теорема 2 доказана.

Непосредственно из теорем 1, 2 следует

Теорема 3. *Для любого $n \geqslant 1$ справедливо утверждение: если $\mu_n = n^2 + n(n - 2^{\lfloor \log_2 n \rfloor}) - 2(n - 2^{\lfloor \log_2 n \rfloor})^2$ и все минимальные правильные разбиения рёбер куба B^n совершенны, то $Q_n \subseteq A_n$.*

Заметим, что нижние оценки (1) величины λ_n, приведённые в [3–5], фактически получены для величины μ_n. Вследствие этого при $n = 3, 5, 7$ имеет место равенство

$$\mu_n = \lambda_n = n^2 + n(n - 2^{\lfloor \log_2 n \rfloor}) - 2(n - 2^{\lfloor \log_2 n \rfloor})^2.$$

Поэтому в случае $n = 3, 5, 7$ теорему 3 можно переформулировать следующим образом.

Теорема 4. *При $n = 3, 5, 7$ справедливо утверждение: если все минимальные правильные разбиения рёбер куба B^n совершенны, то справедливо включение $Q_n \subseteq A_n$.*

ЛИТЕРАТУРА

1. **Рычков К. Л.** Модификация метода В. М. Храпченко и применение её к оценкам сложности П-схем для кодовых функций // Дискрет. анализ. Вып. 42. 1985. С. 91–98.
2. **Рычков К. Л.** О минимальных π-схемах для линейных булевых функций // Дискрет. анализ. Вып. 51. 1991. С. 84–104.
3. **Рычков К. Л.** О нижних оценках сложности параллельно-последовательных контактных схем, реализующих линейные булевы функции // Сиб. журн. исслед. операций. 1994. Т. 1, № 4. С. 33–52.
4. **Рычков К. Л.** О нижних оценках формульной сложности линейной булевой функции // Сиб. электрон. мат. изв. 2014. Т. 11. С. 165–184.
5. **Храпченко В. М.** О сложности реализации линейной функции в классе П-схем // Мат. заметки. 1971. Т. 9, № 1. С. 35–40.
6. **Храпченко В. М.** Об одном методе получения нижних оценок сложности П-схем // Мат. заметки. 1971. Т. 10, № 1. С. 83–92.
7. **Черухин Д. Ю.** К вопросу о логическом представлении счётчика чётности // Неформальная наука. 2009. № 2. С. 14–23.
8. **Яблонский С. В.** Реализация линейной функции в классе П-схем // Докл. АН СССР. 1954. Т. 94, № 5. С. 805–806.
9. **Håstad J.** The shrinkage exponent of de Morgan formulas is 2 // SIAM J. Comput. 1998. Vol. 27, Mo. 1. P. 48–64.
10. **Karchmer M., Wigderson A.** Monotone circuits for connectivity require super-logarithmics depth // SIAM J. Discrete Math. 1990. Vol. 3, No. 2. P. 255–265.

11. **Razborov A.** Applications of matrix methods to the theory of lower bounds in computational complexity // Combinatorica. 1990. Vol. 10, No. 1. P. 81–93.
12. **Wegener I.** The complexity of Boolean functions. Chichester: Wiley, 1987. 458 p.

Рычков Константин Леонидович

Статья поступила
16 марта 2015 г.
Исправленный вариант —
23 июля 2015 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
September–October 2015. Volume 22, No. 5. P. 71–85

UDC 519.714 DOI: 10.17377/daio.2015.22.481

SUFFICIENT CONDITIONS FOR THE MINIMAL π-SCHEMES FOR LINEAR BOOLEAN FUNCTIONS TO BE LOCALLY NON-REPEATING

K. L. Rychkov[1]
[1]Sobolev Institute of Mathematics,
4 Koptyug Ave., 630090 Novosibirsk, Russia
e-mail: rychkov@math.nsc.ru

Abstract. We formulate sufficient conditions for the minimal π-schemes for linear Boolean functions to be locally non-repeating. The validity of these conditions gives a description of the classes of all minimal π-schemes for linear Boolean functions which depend essentially on n variables. Ill. 2, bibliogr. 12.

Keywords: formula size, π-scheme, lower bound on the complexity.

REFERENCES

1. **K. L. Rychkov,** A modification of Khrapchenko's method and its application to estimation of complexity of π-schemes for code functions, in *Metody diskretnogo analiza v teorii grafov i skhem* (Methods of Discrete Analysis in Theory of Graphs and Schemes), Vol. 42, pp. 91–98, Izd. Inst. Mat., Novosibirsk, 1985.
2. **K. L. Rychkov,** On minimal π-schemes for linear Boolean functions, in *Metody diskretnogo analiza v sinteze realizatsii bulevykh funktsii* (Methods of Discrete Analysis in Synthesis of Schemes for Boolean Functions), Vol. 51, pp. 84–104, Izd. Inst. Mat., Novosibirsk, 1991. Translated in *Sib. Adv. Math.,* **3**, No. 3, 172–185, 1993.
3. **K. L. Rychkov,** On the lower bounds for the complexity of serial-parallel contact circuits realizing linear Boolean functions, *Sib. Zh. Issled. Oper.,* **1**, No. 4, 33–52, 1994. Translated in A. D. Korshunov, ed., *Discrete Analysis and Operation Research,* pp. 217–234, Kluwer Acad. Publ., Dordrecht, 1996 (Math. Its Appl., Vol. 355).
4. **K. L. Rychkov,** Lower bounds on the formula complexity of a linear Boolean function, *Sib. Elektron. Mat. Izv.,* **11**, 165–184, 2014.
5. **V. M. Khrapchenko,** Complexity of the realization of a linear function in the class of Π-circuits, *Mat. Zametki,* **9**, No. 1, 35–40, 1971. Translated in *Math. Notes Acad. Sci. USSR,* **9**, No. 1, 21–23, 1971.

6. **V. M. Khrapchenko,** A method of determining lower bounds for the complexity of P-schemes, *Mat. Zametki,* **10**, No. 1, 83–92, 1971. Translated in *Math. Notes Acad. Sci. USSR,* **10**, No. 1, 474–479, 1971.
7. **D. Yu. Cherukhin,** To the question of a logical representation for the parity counter, *Neform. Nauka,* No. 2, 14–23, 2009.
8. **S. V. Yablonskii**, Realization of a linear function in the class of Π-circuits, *Dokl. Akad. Nauk SSSR, Nov. Ser.,* **94**, No. 5, 805–806, 1954.
9. **J. Håstad,** The shrinkage exponent of de Morgan formulas is 2, *SIAM J. Comput.,* **27**, No. 1, 48–64, 1998.
10. **M. Karchmer** and **A. Wigderson,** Monotone circuits for connectivity require super-logarithmic depth, *SIAM J. Discrete Math.,* **3**, No. 2, 255–265, 1990.
11. **A. A. Razborov,** Applications of matrix methods to the theory of lower bounds in computational complexity, *Combinatorica,* **10**, No. 1, 81–93, 1990.
12. **I. Wegener,** *The Complexity of Boolean Functions,* Wiley, Chichester, UK, 1987.

Konstantin L. Rychkov

Received
16 March 2015
Revised
23 July 2015