СИБИРСКИЙ ЖУРНАЛ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ
Октябрь – декабрь 1994. Том 1, № 4, 33–52

УДК 519.714

О НИЖНИХ ОЦЕНКАХ СЛОЖНОСТИ ПАРАЛЛЕЛЬНО-ПОСЛЕДОВАТЕЛЬНЫХ КОНТАКТНЫХ СХЕМ, РЕАЛИЗУЮЩИХ ЛИНЕЙНЫЕ БУЛЕВЫ ФУНКЦИИ*)

К. Л. Рычков

Известно [1], что в любой параллельно-последовательной контактной схеме (иначе π-схеме), реализующей линейную булеву функцию, существенно зависящую от n переменных, содержится не менее n^2 контактов. В настоящей статье эта оценка усиливается следующим образом: при любом нечетном $n \geqslant 5$ число контактов в каждой такой схеме не меньше n^2+3, а при n четном, но не равном степени 2, число контактов не меньше n^2+2.

Пусть $f(\widetilde{x})$ — отличная от константы булева функция, заданная на множестве вершин n-мерного единичного куба B^n. Функции $f(\widetilde{x})$ сопоставим следующие множества:

N^0 — совокупность вершин из B^n, на которых $f(\widetilde{x})=0$;
N^1 — совокупность вершин из B^n, на которых $f(\widetilde{x})=1$;
R — совокупность пар вершин $(\widetilde{\alpha},\widetilde{\beta})$ из B^n таких, что $\widetilde{\alpha}\in N^0$, $\widetilde{\beta}\in N^1$, $\sum\limits_{i=1}^{n}|\alpha_i-\beta_i|=1$.

Сложностью π-схемы S называется величина $L(S)$, равная числу контактов в S. *Сложностью функции f в классе π-схем* называется величина $L_\pi(f)=\min L(S)$, где минимум берется по всем π-схемам S, реализующим функцию f.

Пусть S — π-схема, реализующая функцию $f(\widetilde{x})$. Все контакты этой схемы занумеруем числами от 1 до L. В. М. Храпченко [1] предложил следующий подход к получению нижних оценок сложности π-схем. Рассматривается некоторое специальное соответствие между множеством R и множеством контактов схемы S. С этим соответствием связывается вектор $\widetilde{a}=(a_1,\ldots,a_L)$, где a_j — мощность полного прообраза контакта с номером j, $1\leqslant j\leqslant L$. В. М. Храпченко показал,

---

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-011-16009).

что

$$\sum_{j=1}^{L} a_j = |R|, \quad \sum_{j=1}^{L} a_j^2 \leqslant |N^0|\,|N^1|.$$

Эти соотношения позволили доказать неравенство

$$L \geqslant \frac{|R|^2}{|N^0|\,|N^1|},$$

из которого непосредственно вытекает нижняя оценка сложности линейной функции $\Phi_n = x_1 + \ldots + x_n (\mathrm{mod}\, 2)$:

$$L_\pi(\Phi_n) \geqslant n^2.$$

В статье используются следующие обозначения:

$J(x_i)$ — множество номеров, присвоенных контактам переменной x_i, $1 \leqslant i \leqslant n$;

$J(\overline{x}_j)$ — множество номеров, присвоенных контактам переменной $\overline{x}_i$, $1 \leqslant i \leqslant n$.

В настоящей работе показано, что в случае линейной функции Φ_n для вектора $\widetilde{a}$ при любом i, $1 \leqslant i \leqslant n$, выполнены соотношения

$$\sum_{k \in J(x_i)} a_k = \sum_{l \in J(\overline{x}_i)} a_l = \frac{|R|}{2n}, \tag{1}$$

$$\sum_{j=1}^{L} a_j^2 + \left| \sum_{k \in J(x_i)} a_k^2 - \sum_{l \in J(\overline{x}_i)} a_l^2 \right| \leqslant |N^0|\,|N^1|. \tag{2}$$

На основе формул (1), (2) усилена нижняя оценка из [1]. Эта оценка при $n = 5$ и $n = 7$ совпадает с верхней оценкой из [2]:

$$L_\pi(\Phi_n) \leqslant n^2 + \rho n - 2\rho^2,$$

где $\rho = \rho(n)$ находится из соотношений $n = 2^k + \rho$, $0 \leqslant \rho < 2^k$.

Соотношения (1), (2) доказываются в § 1. В § 2 вводятся специальные частично упорядоченные множества и устанавливаются некоторые свойства функций, которые используются в § 3 при доказательстве основного результата статьи.

§ 1. Усиление соотношений Храпченко

Пусть $f(\widetilde{x})$ — булева функция, заданная на множестве вершин n-мерного единичного куба B^n. Элементы множества $N^0 \times N^1$ функции $f(\widetilde{x})$ назовем (0-1)-*парами*, а элементы множества R — (0-1)-*ребрами*.

Пусть $\widetilde{\delta} = (\delta_1, \ldots, \delta_n) \in N^0$, $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_n) \in N^1$. Будем говорить, что (0-1)-*пара* $(\widetilde{\delta}, \widetilde{\sigma})$ *имеет ориентацию* i, если $\delta_i = 0$, $\sigma_i = 1$, и *ориентацию* $\bar{i}$, если $\delta_i = 1$, $\sigma_i = 0$. Вообще говоря, (0-1)-пара может иметь несколько ориентаций. Ясно, что (0-1)-пара имеет ровно одну ориентацию только в том случае, когда эта пара является (0-1)-ребром.

Две (0-1)-пары из $N^0 \times N^1$ назовем *одинаково ориентированными*, если множества их ориентаций совпадают. Будем говорить, что подмножество P множества $N^0 \times N^1$ *имеет ориентацию* i (соответственно $\bar{i}$), если каждая (0-1)-пара из P имеет ориентацию i (соответственно $\bar{i}$).

Пусть S — π-схема, реализующая функцию $f(\widetilde{x})$. Множество контактов схемы S обозначим через $E(S)$.

Множество $C \subseteq E(S)$ называется *цепью в* S, если все элементы множества C в графе схемы S образуют простую цепь, соединяющую полюса схемы. Множество всех цепей в S обозначим через $Q(S)$.

Множество $H \subseteq E(S)$ называется *сечением в* S, если $C \cap H \neq \varnothing$ для каждой цепи $C \in Q(S)$. Сечение H в S называется *тупиковым*, если H минимально по включению среди всех сечений в S. Множество всех тупиковых сечений в S обозначим через $T(S)$.

Функцию $\chi_0 \colon N^0 \to T(S)$ назовем *функцией выбора сечения в* S, если область определения χ_0 есть все множество N^0 и для каждого $\widetilde{\delta} \in N^0$ все контакты тупикового сечения $\chi_0(\widetilde{\delta})$ разомкнуты на $\widetilde{\delta}$. Функцию $\chi_1 \colon N^1 \to Q(S)$ назовем *функцией выбора цепи в* S, если область определения χ_1 есть все множество N^1 и для каждого $\widetilde{\sigma} \in N^1$ все контакты цепи $\chi_1(\widetilde{\sigma})$ замкнуты на $\widetilde{\sigma}$. Очевидно, что такие функции χ_0, χ_1 существуют.

Пусть χ_0 — функция выбора сечения в S, χ_1 — функция выбора цепи в S. Следуя [1], с помощью функций χ_0, χ_1 определим соответствие между множеством всех (0-1)-пар $N^0 \times N^1$ и множеством контактов $E(S)$. По определению каждой (0-1)-паре $(\widetilde{\delta}, \widetilde{\sigma})$ соответствуют те и только те контакты из $E(S)$, которые принадлежат множеству $\chi_0(\widetilde{\delta}) \cap \chi_1(\widetilde{\sigma})$. Это соответствие обозначим через $\chi_0 \cap \chi_1$.

В [3] было показано, что в любой π-схеме каждая цепь и произвольное тупиковое сечение имеют ровно один общий контакт. Поэтому в случае π-схем соответствие $\chi_0 \cap \chi_1$ является однозначным отображением множества $N^0 \times N^1$ в множество $E(S)$ с областью определения $N^0 \times N^1$.

Лемма 1. *Пусть $f(x_1,\dots,x_n)$ — отличная от константы булева функция; S — π-схема, реализующая функцию f; χ_0 и χ_1 — функции выбора сечения и цепи в S; $P_1,\dots,P_L$ — полные прообразы при отображении $\chi_0\cap\chi_1$ контактов с номерами $1,\dots,L$ соответственно. Тогда справедливы следующие утверждения.*

1. *Множества $P_1,\dots,P_L$ являются декартовыми произведениями.*
2. *При каждом i, $1\leqslant i\leqslant n$, множества P_k, $k\in J(x_i)$, имеют ориентацию i, а множества P_l, $l\in J(\overline{x}_i)$, — ориентацию $\overline{i}$.*

Доказательство. 1. Пусть e — контакт из $E(S)$ и j — номер этого контакта. Если множество P_j состоит не более чем из одного элемента, то P_j, очевидно, является декартовым произведением. Предположим, что P_j содержит не менее двух элементов. Пусть $(\widetilde{\delta},\widetilde{\sigma})$, $(\widetilde{\alpha},\widetilde{\beta})$ — две произвольные (0-1)-пары из P_j. Покажем, что (0,1)-пары $(\widetilde{\delta},\widetilde{\beta})$, $(\widetilde{\alpha},\widetilde{\sigma})$ также принадлежат P_j. Действительно, из определения отображения $\chi_0\cap\chi_1$ следует, что

$$\chi_0(\widetilde{\delta})\cap\chi_1(\widetilde{\sigma})=\{e\},\qquad \chi_0(\widetilde{\alpha})\cap\chi_1(\widetilde{\beta})=\{e\}.$$

Поэтому

$$\chi_0(\widetilde{\delta})\cap\chi(\widetilde{\beta})=\{e\},\qquad \chi_0(\widetilde{\alpha})\cap\chi_1(\widetilde{\sigma})=\{e\},$$

и, значит, $(\widetilde{\delta},\widetilde{\beta})\in P_j$, $(\widetilde{\alpha},\widetilde{\sigma})\in P_j$. Ввиду произвольности выбора (0-1)-пар $(\widetilde{\delta},\widetilde{\sigma})$, $(\widetilde{\alpha},\widetilde{\beta})$ множество P_j есть декартово произведение, т. е. справедливость утверждения 1 установлена.

2. Пусть e — контакт из $E(S)$ и j — номер этого контакта. Предположим, что $j\in J(x_i)$ для некоторого i, $1\leqslant i\leqslant n$, т. е. e — контакт переменной x_i (случай переменной $\overline{x}_i$ рассматривается аналогично). Пусть $(\widetilde{\delta},\widetilde{\sigma})$ — (0-1)-пара из P_j. По определению функции χ_0 все контакты тупикового сечения $\chi_0(\widetilde{\delta})$ разомкнуты на $\widetilde{\delta}$. В частности, разомкнут контакт e, поэтому $\delta_i=0$. По определению функции χ_1 все контакты цепи $\chi_1(\widetilde{\sigma})$ замкнуты на $\widetilde{\sigma}$. В частности, замкнут контакт e, поэтому $\sigma_i=1$. Следовательно, (0-1)-пара $(\widetilde{\delta},\widetilde{\sigma})$ имеет ориентацию i. Поскольку (0-1)-пара $(\widetilde{\delta},\widetilde{\sigma})$ выбрана из P_j произвольно, множество P_j имеет ориентацию i. Лемма 1 доказана.

Обозначим через $(\chi_0\cap\chi_1)|_R$ сужение отображения $\chi_0\cap\chi_1$ на множество R. Вектор $\widetilde{a}=(a_1,\dots,a_L)$ будем называть *вектором отображения* $(\chi_0\cap\chi_1)|_R$, если при любом j, $1\leqslant j\leqslant L$, величина a_j равна мощности полного прообраза контакта с номером j при отображении $(\chi_0\cap\chi_1)|_R$.

Теорема 1. *Пусть f — линейная булева функция, существенно зависящая от переменных $x_1,\dots,x_n$; $n\geqslant 2$; S — π-схема, реализующая функцию f; χ_0 и χ_1 — функции выбора сечения и цепи в S;*

$\widetilde{a} = (a_1, \dots, a_n)$ — вектор отображения $(\chi_0 \cap \chi_1)|_R$. Тогда при любом i, $1 \leqslant i \leqslant n$, справедливы соотношения (1), (2).

Доказательство. Убедимся в справедливости соотношения (1). Пусть $r_1, \dots, r_L$ — полные прообразы контактов с номерами $1, \dots, L$ соответственно при отображении $(\chi_0 \cap \chi_1)|_R$. Поскольку $(\chi_0 \cap \chi_1)|_R$ — однозначное отображение с областью определения R, множества $r_1, \dots, r_L$ попарно не пересекаются и верно равенство

$$\bigcup_{j=1}^{L} r_j = R.$$

Обозначим через $R(i)$ (соответственно $R(\bar{i})$), $1 \leqslant i \leqslant n$, множество всех (0-1)-ребер из R с ориентацией i (соответственно $\bar{i}$). Легко проверить, что если $n \geqslant 2$, то при любом i, $1 \leqslant i \leqslant n$, выполнены равенства

$$|R(i)| = |R(\bar{i})| = \frac{|R|}{2n}.$$

Далее, в силу утверждения 2 леммы 1 при любом i, $1 \leqslant i \leqslant n$, справедливы включения

$$\bigcup_{k \in J(x_i)} r_k \subseteq R(i), \qquad \bigcup_{l \in J(\overline{x}_i)} r_l \subseteq R(\bar{i}).$$

Поскольку каждое (0-1)-ребро имеет только одну ориентацию, при любом i, $1 \leqslant i \leqslant n$, справедливы также обратные включения. Поэтому при любом i, $1 \leqslant i \leqslant n$, имеем

$$\bigcup_{k \in J(x_i)} r_k = R(i), \qquad \bigcup_{l \in J(\overline{x}_i)} r_l = R(\bar{i}),$$

т. е. справедливо соотношение (1).

Убедимся в справедливости соотношения (2). Для этого каждому множеству r_j, $1 \leqslant j \leqslant L$, сопоставим два множества r_j^0, r_j^1 такие, что r_j^0 — множество нулевых концов всех (0-1)-ребер из r_j и r_j^1 — множество единичных концов всех (0-1)-ребер из r_j. В силу утверждения 2 леммы 1 любое непустое множество r_j, $1 \leqslant j \leqslant L$, состоит из одинаково ориентированных (0-1)-ребер. Поэтому при любом j, $1 \leqslant j \leqslant L$, имеем

$$|r_j^0| = |r_j^1| = |r_j| = a_j.$$

Пусть, как и выше, $P_1, \dots, P_L$ — полные прообразы контактов с номерами $1, \dots, L$ соответственно при отображении $\chi_0 \cap \chi_1$. Очевидно,

что множества $P_1, \ldots, P_L$ не пересекаются и $\bigcup\limits_{j=1}^{L} P_j = N^0 \times N^1$. Поскольку $r_j \subseteq P_j$, $1 \leqslant j \leqslant L$, и в силу утверждения 1 леммы 1 множества $P_1, \ldots, P_L$ являются декартовыми произведениями, при любом j, $1 \leqslant j \leqslant L$, имеем $r_j^0 \times r_j^1 \subseteq P_j$. Поэтому множества $r_1^0 \times r_1^1$, $r_2^0 \times r_2^1, \ldots$, $r_L^0 \times r_L^1$ попарно не пересекаются и

$$\bigcup_{j=1}^{L} (r_j^0 \times r_j^1) \subseteq N^0 \times N^1.$$

Пусть $D = (N^0 \times N^1) \backslash \Big(\bigcup\limits_{j=1}^{L} (r_j^0 \times r_j^1) \Big)$. Тогда

$$\Big(\bigcup_{j=1}^{L} (r_j^0 \times r_j^1) \Big) \cup D = N^0 \times N^1, \tag{3}$$

$$\sum_{j=1}^{L} |r_j^0 \times r_j^1| + |D| = |N^0 \times N^1|. \tag{4}$$

Поскольку $|r_j^0 \times r_j^1| = a_j^2$ при любом j, $1 \leqslant j \leqslant L$, из (4) следует равенство

$$\sum_{j=1}^{L} a_j^2 + |D| = |N^0|\,|N^1|.$$

Таким образом, для завершения доказательства (2) осталось показать, что при любом i, $1 \leqslant i \leqslant n$, выполнено неравенство

$$|D| \geqslant \Big| \sum_{k \in J(x_i)} a_k^2 - \sum_{l \in J(\overline{x}_i)} a_l^2 \Big|. \tag{5}$$

Убедимся в справедливости (5). При фиксированном i, $1 \leqslant i \leqslant n$, множество N^0 разобьем на подмножества $N_{\bar{i}}^0$, N_i^0, где

$$N_{\bar{i}}^0 = \{\widetilde{\delta} \in N^0 \mid \delta_i = 0\}, \qquad N_i^0 = \{\widetilde{\delta} \in N^0 \mid \delta_i = 1\},$$

и множество N^1 — на подмножества $N_{\bar{i}}^1$, N_i^1, где

$$N_{\bar{i}}^1 = \{\widetilde{\sigma} \in N^1 \mid \sigma_i = 0\}, \qquad N_i^1 = \{\widetilde{\sigma} \in N^1 \mid \sigma_i = 1\}.$$

Ясно, что множества $N^0_{\bar{i}} \times N^1_i$, $N^0_i \times N^1_{\bar{i}}$, $N^0_i \times N^1_i$, $N^0_{\bar{i}} \times N^1_{\bar{i}}$ попарно не пересекаются и их объединение совпадает с множеством $N^0 \times N^1$. Очевидно, что $N^0_{\bar{i}} \times N^1_i$ есть множество всех (0-1)-пар, имеющих ориентацию i; $N^0_i \times N^1_{\bar{i}}$ — множество всех (0-1)-пар, имеющих ориентацию $\bar{i}$.

Введем обозначения:

$$D(i) = D \cap (N^0_{\bar{i}} \times N^1_i), \quad D(\bar{i}) = D \cap (N^0_i \times N^1_{\bar{i}}),$$

d, $d(i)$, $d(\bar{i})$ — мощности множеств D, $D(i)$, $D(\bar{i})$ соответственно. Поскольку $D(i) \subseteq D$, $D(\bar{i}) \subseteq D$, имеем

$$d \geqslant |d(i) - d(\bar{i})|.$$

Поэтому для доказательства неравенства (5) достаточно показать, что

$$d(\bar{i}) - d(i) = \sum_{k \in J(x_i)} a_k^2 - \sum_{l \in J(\bar{x}_i)} a_l^2.$$

Для этого рассмотрим равенство (3). Множества, находящиеся в левой и правой частях этого равенства, пересечем с множеством $N^0_{\bar{i}} \times N^1_i$. Поскольку множества в левой части равенства (3) попарно не пересекаются, имеем

$$\sum_{j \in \{1,\dots,L\} \setminus (J(x_i) \cup J(\bar{x}_i))} |(r_j^0 \times r_j^1) \cap (N^0_{\bar{i}} \times N^1_i)| + \sum_{k \in J(x_i)} |(r_k^0 \times r_k^1) \cap (N^0_{\bar{i}} \times N^1_i)| + \sum_{l \in J(\bar{x}_i)} |(r_l^0 \times r_l^1) \cap (N^0_{\bar{i}} \times N^1_i)| + |D(i)| = |N^0_{\bar{i}} \times N^1_i|. \quad (6)$$

Множества, находящиеся в левой и правой частях равенства (3), пересечем с множеством $N^0_i \times N^1_{\bar{i}}$. В результате получим

$$\sum_{j \in \{1,\dots,L\} \setminus (J(x_i) \cup J(\bar{x}_i))} |r_j^0 \times r_j^1 \cap (N^0_i \times N^1_{\bar{i}})| + \sum_{k \in J(x_i)} |(r_k^0 \times r_k^1) \cap (N^0_i \times N^1_{\bar{i}})| + \sum_{l \in J(\bar{x}_i)} |(r_l^0 \times r_l^1) \cap (N^0_i \times N^1_{\bar{i}})| + |D(\bar{i})| = |N^0_i \times N^1_{\bar{i}}|. \quad (7)$$

В силу утверждения 2 леммы 1 при любых $k \in J(x_i)$, $l \in J(\bar{x}_i)$, $j \in \{1, \dots, L\} \setminus (J(x_i) \cup J(\bar{x}_i))$ справедливы включения

$$r_k^0 \times r_k^1 \subseteq N^0_{\bar{i}} \times N^1_i, \qquad r_l^0 \times r_l^1 \subseteq N^0_i \times N^1_{\bar{i}},$$
$$r_j \subseteq (N^0_i \times N^1_i) \cup (N^0_{\bar{i}} \times N^1_{\bar{i}}).$$

Поэтому при тех же k, l, j имеем

$$|(r_k^0 \times r_k^1) \cap (N_{\bar{i}}^0 \times N_i^1)| = a_k^2, \qquad |(r_k^0 \times r_k^1) \cap (N_i^0 \times N_{\bar{i}}^1)| = 0,$$

$$|(r_l^0 \times r_l^1) \cap (N_{\bar{i}}^0 \times N_i^1)| = 0, \qquad |(r_l^0 \times r_l^1) \cap (N_i^0 \times N_{\bar{i}}^1)| = a_l^2,$$

$$|(r_j^0 \times r_j^1) \cap (N_{\bar{i}}^0 \times N_i^1)| = |(r_j^0 \times r_j^1) \cap (N_i^0 \times N_{\bar{i}}^1)|.$$

Учитывая соотношение $|N_{\bar{i}}^0 \times N_i^1| = |N_i^0 \times N_{\bar{i}}^1|$, приравняем левые части равенств (6), (7) и выполним необходимые сокращения. В результате получим равенство

$$\sum_{k \in J(x_i)} a_k^2 + d(i) = \sum_{l \in J(\overline{x}_i)} a_l^2 + d(\bar{i}),$$

из которого ввиду произвола в выборе i следует (2). Теорема 1 доказана.

§ 2. Свойства специальных функций на частично упорядоченном множестве

Пусть n, L — целые числа такие, что $n \geqslant 2$, $L \geqslant 2n$. Через $\widetilde{\mathfrak{T}}_L^{2n}$ обозначим множество целочисленных векторов $\widetilde{\tau} = (\tau_1, \ldots, \tau_{2n})$ таких, что $\tau_1 \geqslant \tau_2 \geqslant \ldots \geqslant \tau_{2n} > 0$, $\tau_1 + \tau_2 + \ldots + \tau_{2n} = L$. На множестве $\widetilde{\mathfrak{T}}_L^{2n}$ определим двухместное отношение $\succ$ следующим образом: если $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$, то $\widetilde{\alpha} \succ \widetilde{\beta}$ тогда и только тогда, когда выполнена система неравенств

$$\begin{aligned}
&\alpha_1 \geqslant \beta_1, \\
&\alpha_1 + \alpha_2 \geqslant \beta_1 + \beta_2, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\alpha_1 + \alpha_2 + \ldots + \alpha_{2n-1} \geqslant \beta_1 + \beta_2 + \ldots + \beta_{2n-1}.
\end{aligned}$$

Ясно, что отношение $\succ$ есть частичный порядок на множестве $\widetilde{\mathfrak{T}}_L^{2n}$. Будем говорить, что *вектор* $\widetilde{\alpha} \in \widetilde{\mathfrak{T}}_L^{2n}$ *получается из вектора* $\widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ *переносом единицы*, если существуют j, i такие, что $1 \leqslant j, i \leqslant 2n$, $j < i$ и $\alpha_j = \beta_j + 1$, $\alpha_i = \beta_i - 1$, $\alpha_l = \beta_l$ при $l \neq j, i$. При этом будем говорить, что *единица переносится из слоя* β_i *в слой* $\beta_j + 1$. Следовательно, единица всегда переносится из рассматриваемого слоя в более высокий слой, и наивысший слой, в который может быть перенесена единица, есть слой $\beta_1 + 1$.

Замечание 1. Легко проверить, что для любых различных векторов $\widetilde{\alpha}$, $\widetilde{\beta}$ из множества $\widetilde{\mathfrak{T}}_L^{2n}$ справедливо следующее утверждение: *$\widetilde{\alpha} \succ \widetilde{\beta}$ тогда и только тогда, когда существует последовательность векторов $\widetilde{\tau}_1, \widetilde{\tau}_2, \ldots, \widetilde{\tau}_k$ из $\widetilde{\mathfrak{T}}_L^{2n}$ такая, что $\widetilde{\tau}_1 = \widetilde{\beta}$, $\widetilde{\tau}_k = \widetilde{\alpha}$, а при любом j, $1 \leqslant j \leqslant k-1$, вектор $\widetilde{\tau}_{j+1}$ получается из вектора $\widetilde{\tau}_j$ переносом единицы.*

Через $\widetilde{\mu}$ обозначим вектор из множества $\widetilde{\mathfrak{T}}_L^{2n}$ вида

$$\widetilde{\mu} = (\underbrace{\lfloor L/2n \rfloor + 1, \ldots, \lfloor L/2n \rfloor + 1}_{a}, \underbrace{\lfloor L/2n \rfloor, \ldots, \lfloor L/2n \rfloor}_{b}),$$

где $a = L - 2n\lfloor L/2n \rfloor$, $b = 2n - a$. Легко проверить, что вектор $\widetilde{\mu}$ является наименьшим в частично упорядоченном множестве $\langle \widetilde{\mathfrak{T}}_L^{2n}, \succ \rangle$. Если $L - 2n\lfloor L/2n \rfloor \geqslant 2$, то через $\widetilde{\nu}$ обозначим вектор из множества $\widetilde{\mathfrak{T}}_L^{2n}$ вида

$$\widetilde{\nu} = (\lfloor L/2n \rfloor + 2, \underbrace{\lfloor L/2n \rfloor + 1, \ldots, \lfloor L/2n \rfloor + 1}_{a}, \underbrace{\lfloor L/2n \rfloor, \ldots, \lfloor L/2n \rfloor}_{b}),$$

где $a = L - 2n\lfloor L/2n \rfloor - 2$, $b = 2n - (a+1)$. Ясно, что вектор $\widetilde{\nu}$ получается из вектора $\widetilde{\mu}$ переносом единицы из слоя μ_1 в слой $\mu_1 + 1$.

Будем говорить, что *функция $\lambda(\widetilde{\tau})$ возрастает (не убывает) на частично упорядоченном множестве* $\langle \widetilde{\mathfrak{T}}_L^{2n}, \succ \rangle$, если $\lambda(\widetilde{\alpha}) > \lambda(\widetilde{\beta})$ ($\lambda(\widetilde{\alpha}) \geqslant \lambda(\widetilde{\beta})$) для любых различных векторов $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ таких, что $\widetilde{\alpha} \succ \widetilde{\beta}$.

На множестве $\widetilde{\mathfrak{T}}_L^{2n}$ определим функции

$$\lambda_1(\widetilde{\tau}) = \sum_{i=1}^{2n} \frac{1}{\tau_i}, \quad \lambda_2(\widetilde{\tau}) = \lambda_1(\widetilde{\tau}) + \frac{1}{\tau_1 - 1} - \frac{1}{\tau_1}.$$

Лемма 2. *Пусть n, L — целые числа такие, что $n \geqslant 2$, $L \geqslant 2n$. Тогда справедливы следующие утверждения.*

1. *Функция $\lambda_1(\widetilde{\tau})$ возрастает на частично упорядоченном множестве $\langle \widetilde{\mathfrak{T}}_L^{2n}, \succ \rangle$.*
2. *Функция $\lambda_2(\widetilde{\tau})$ не убывает на частично упорядоченном множестве $\langle \widetilde{\mathfrak{T}}_L^{2n}, \succ \rangle$.*

Для любых различных векторов $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ таких, что $\widetilde{\alpha} \succ \widetilde{\beta}$, равенство $\lambda_2(\widetilde{\alpha}) = \lambda_2(\widetilde{\beta})$ выполнено тогда и только тогда, когда $\widetilde{\alpha}$ получается из $\widetilde{\beta}$ переносом единицы из слоя β_1 в слой $\beta_1 + 1$.

Доказательство. Ввиду замечания 1 для доказательства утверждения 1 достаточно показать, что операция переноса единицы увеличивает значение функции $\lambda_1(\widetilde{\tau})$. Пусть вектор $\widetilde{\alpha} \in \widetilde{\mathfrak{T}}_L^{2n}$ получается из вектора $\widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ переносом единицы, а числа j, i $(1 \leqslant j < i \leqslant 2n)$ таковы, что $\alpha_j = \beta_j + 1$, $\alpha_i = \beta_i - 1$. Тогда

$$\lambda_1(\widetilde{\alpha}) = \lambda_1(\widetilde{\beta}) + \frac{1}{\alpha_j} + \frac{1}{\alpha_i} - \frac{1}{\beta_j} - \frac{1}{\beta_i}.$$

Поскольку $\beta_j \geqslant \beta_i$, $\beta_i - 1 = \alpha_i > 0$, имеем

$$\frac{1}{\alpha_j} + \frac{1}{\alpha_i} - \frac{1}{\beta_j} - \frac{1}{\beta_i} = \left(\frac{1}{\alpha_i} - \frac{1}{\beta_i}\right) - \left(\frac{1}{\beta_j} - \frac{1}{\alpha_j}\right) = \left(\frac{1}{\beta_i - 1} - \frac{1}{\beta_i}\right) - \left(\frac{1}{\beta_j} - \frac{1}{\beta_j + 1}\right)$$
$$= \sum_{p=\beta_i-1}^{\beta_j-1} \left(\left(\frac{1}{p} - \frac{1}{p+1}\right) - \left(\frac{1}{p+1} - \frac{1}{p+2}\right)\right) = \sum_{p=\beta_i-1}^{\beta_j-1} \frac{2}{p(p+1)(p+2)} > 0.$$

Поэтому $\lambda_1(\widetilde{\alpha}) > \lambda_1(\widetilde{\beta})$, т. е. справедливо утверждение 1 леммы 2.

В силу замечания 1 для доказательства утверждения 2 достаточно убедиться в истинности следующего утверждения. Пусть вектор $\widetilde{\alpha} \in \widetilde{\mathfrak{T}}_L^{2n}$ получается из вектора $\widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ переносом единицы. Тогда если единица переносится из слоя β_1 в слой $\beta_1 + 1$, то $\lambda_2(\widetilde{\alpha}) = \lambda_2(\widetilde{\beta})$, в противном случае $\lambda_2(\widetilde{\alpha}) > \lambda_2(\widetilde{\beta})$. Убедимся в справедливости этого утверждения. Пусть вектор $\widetilde{\alpha} \in \widetilde{\mathfrak{T}}_L^{2n}$ получается из вектора $\widetilde{\beta} \in \widetilde{\mathfrak{T}}_L^{2n}$ переносом единицы и числа j, i $(1 \leqslant j < i \leqslant 2n)$ таковы, что $\alpha_j = \beta_j + 1$, $\alpha_i = \beta_i - 1$. Тогда

$$\lambda_2(\widetilde{\alpha}) = \lambda_2(\widetilde{\beta}) + \frac{1}{\alpha_j} + \frac{1}{\alpha_i} - \frac{1}{\beta_j} - \frac{1}{\beta_i} + \left(\frac{1}{\alpha_1 - 1} - \frac{1}{\alpha_1}\right) - \left(\frac{1}{\beta_1 - 1} - \frac{1}{\beta_1}\right)$$
$$= \lambda_2(\widetilde{\beta}) + \sum_{p=\beta_i-1}^{\beta_j-1} \frac{2}{p(p+1)(p+2)} - \left(\left(\frac{1}{\beta_1 - 1} - \frac{1}{\beta_1}\right) - \left(\frac{1}{\alpha_1 - 1} - \frac{1}{\alpha_1}\right)\right).$$

Предположим, что единица переносится из слоя β_1 в слой $\beta_1 + 1$. Это означает, что $\alpha_1 = \beta_1 + 1$, $j = 1$, $\beta_i = \beta_1$. Поэтому

$$\sum_{p=\beta_i-1}^{\beta_j-1} \frac{2}{p(p+1)(p+2)} = \frac{2}{(\beta_1 - 1)\beta_1(\beta_1 + 1)},$$

$$\left(\frac{1}{\beta_1-1}-\frac{1}{\beta_1}\right)-\left(\frac{1}{\alpha_1-1}-\frac{1}{\alpha_1}\right)=\frac{2}{(\beta_1-1)\beta_1(\beta_1+1)}.$$

Следовательно, $\lambda_2(\widetilde{\alpha})=\lambda_2(\widetilde{\beta})$.

Предположим противное, т. е. единица переносится в слой β_1+1 из слоя, отличного от слоя β_1, либо в слой, отличный от слоя β_1+1.

Пусть единица переносится в слой β_1+1 из слоя, отличного от слоя β_1. Это означает, что $\alpha_1=\beta_1+1$, $j=1$, $\beta_i<\beta_1$. Поэтому

$$\sum_{p=\beta_i-1}^{\beta_j-1}\frac{2}{p(p+1)(p+2)}>\frac{2}{(\beta_1-1)\beta_1(\beta_1+1)},$$

$$\left(\frac{1}{\beta_1-1}-\frac{1}{\beta_1}\right)-\left(\frac{1}{\alpha_1-1}-\frac{1}{\alpha_1}\right)=\frac{2}{(\beta_1-1)\beta_1(\beta_1+1)}.$$

Следовательно, $\lambda_2(\widetilde{\alpha})>\lambda_2(\widetilde{\beta})$.

Пусть единица переносится в слой, отличный от слоя β_1+1. Это означает, что $\alpha_1=\beta_1$. Поэтому

$$\sum_{p=\beta_i-1}^{\beta_j-1}\frac{2}{p(p+1)(p+2)}>0,\quad \left(\frac{1}{\beta_1-1}-\frac{1}{\beta_1}\right)-\left(\frac{1}{\alpha_1-1}-\frac{1}{\alpha_1}\right)=0.$$

Следовательно, $\lambda_2(\widetilde{\alpha})>\lambda_2(\widetilde{\beta})$. Лемма 2 доказана.

§ 3. Доказательство нижних оценок

Пусть n, L — целые числа такие, что $n\geqslant 2$, $L\geqslant 2n$. Обозначим через V_n^L множество векторов $\widetilde{a}=(a_1,\dots,a_L)$ с вещественными неотрицательными координатами такими, что $\sum\limits_{j=1}^{L}a_j=2^{n-1}n$ и через T_L^{2n} множество всех упорядоченных разбиений $\widetilde{t}=(t_1,\dots,t_n,\overline{t}_1,\dots,\overline{t}_n)$ множества $\{1,\dots,L\}$ на $2n$ непустых подмножества $t_1,\dots,t_n$; $\overline{t}_1,\dots,\overline{t}_n$.

Разбиение $\widetilde{t}\in T_L^{2n}$ называется *правильным разбиением координат вектора* $\widetilde{a}\in V_n^L$, если при любом i, $1\leqslant i\leqslant n$, справедливо соотношение

$$\sum_{k\in t_i}a_k=\sum_{l\in\overline{t}_i}a_l=2^{n-2}.$$

Обозначим через $T_L^{2n}(\widetilde{a})$ множество всех правильных разбиений координат вектора $\widetilde{a}\in V_n^L$. Пусть

$$A_n^L=\{\widetilde{a}\in V_n^L\mid T_L^{2n}(\widetilde{a})\neq\varnothing\}.$$

Каждой паре $(\widetilde{a},\widetilde{t})$, где $a \in A_n^L$, $\widetilde{t} \in T_L^{2n}(\widetilde{a})$, сопоставим величину

$$\varphi(\widetilde{a},\widetilde{t}) = \max_{1\leqslant i\leqslant n}\left|\sum_{k\in t_i} a_k^2 - \sum_{l\in \bar{t}_i} a_l^2\right|.$$

На множестве A_n^L определим функцию

$$\varphi(\widetilde{a}) = \min_{\widetilde{t}\in T_L^{2n}(\widetilde{a})} \varphi(\widetilde{a},\widetilde{t}),$$

а на множестве V_n^L — функцию

$$\|\widetilde{a}\|^2 = \sum_{j=1}^{L} a_j^2.$$

Введем обозначение $X_n^L = \{\widetilde{a} \in A_n^L \mid \|\widetilde{a}\|^2 + \varphi(\widetilde{a}) \leqslant (2^{n-1})^2\}$. Из теоремы 1 следует, что в случае линейной булевой функции n переменных вектор отображения $(\chi_0 \cap \chi_1)\,|_R$ принадлежит некоторому множеству X_n^L.

Пусть $\widetilde{t} \in T_L^{2n}$, $\widetilde{\tau} \in \widetilde{\mathfrak{T}}_L^{2n}$. Будем говорить, что *разбиение* $\widetilde{t}$ *имеет тип* $\widetilde{\tau}$, если $\widetilde{\tau}$ можно получить перестановкой координат из вектора $(|t_1|,\dots,|t_n|,|\bar{t}_1|,\dots,|\bar{t}_n|)$. Каждому разбиению $\widetilde{t} \in T_L^{2n}$ сопоставим вектор $\widetilde{m}(\widetilde{t}) \in A_n^L$, заданный следующей системой равенств:

$$\begin{aligned} m_k(\widetilde{t}) &= 2^{n-2}/|t_i|, \quad k \in t_i,\ 1 \leqslant i \leqslant n,\\ m_l(\widetilde{t}) &= 2^{n-2}/|\bar{t}_i|, \quad l \in \bar{t}_i,\ 1 \leqslant i \leqslant n. \end{aligned}$$

Из определения вектора $\widetilde{m}(\widetilde{t})$ следует, что $\widetilde{t}$ является правильным разбиением координат вектора $\widetilde{m}(\widetilde{t})$ и если для некоторого $\widetilde{a} \in A_n^L$ разбиение $\widetilde{t}$ является правильным разбиением координат вектора $\widetilde{a}$, то $\|\widetilde{m}(\widetilde{t})\|^2 \leqslant \|\widetilde{a}\|^2$.

Обозначим через $M_n^L\widetilde{\mu}$ множество всех векторов из A_n^L, которые можно получить перестановкой координат из вектора

$$\widetilde{u} = \Bigg(\underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor + 1},\dots,\frac{2^{n-2}}{\lfloor L/2n\rfloor + 1}}_{a},\ \underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor},\dots,\frac{2^{n-2}}{\lfloor L/2n\rfloor}}_{b}\Bigg),$$

где $a = (L - 2n\lfloor L/2n\rfloor)(\lfloor L/2n\rfloor + 1)$, $b = (2n - (L - 2n\lfloor L/2n\rfloor))\lfloor L/2n\rfloor$.

Лемма 3. *Для любого вектора* $\widetilde{a}$ *из* A_n^L *справедливо неравенство*

$$\|\widetilde{a}\|^2 \geqslant 2^{2n-4}\left(\frac{L-2n\lfloor L/2n\rfloor}{\lfloor L/2n\rfloor+1}+\frac{2n-(L-2n\lfloor L/2n\rfloor)}{\lfloor L/2n\rfloor}\right), \tag{8}$$

причем равенство достигается тогда и только тогда, когда $\widetilde{a}\in M_n^L\widetilde{\mu}$.

Доказательство. Пусть вектор $\widetilde{\mu}$ является наименьшим элементом в частично упорядоченном множестве $\langle\widetilde{\mathfrak{T}}_L^{2n},\succ\rangle$. Непосредственно проверяется, что выражение в правой части неравенства (8) равно $2^{2n-4}\lambda_1(\widetilde{\mu})$. Пусть $\widetilde{a}$ — вектор из A_n^L; $\widetilde{t}$ — разбиение из $T_L^{2n}(\widetilde{a})$; $\tau\in\widetilde{\mathfrak{T}}_L^{2n}$ — тип разбиения $\widetilde{t}$;

$$\varepsilon_i=\sum_{k\in t_i}a_k^2-\sum_{k\in t_i}m_k^2(\widetilde{t}),\qquad \overline{\varepsilon}_i=\sum_{l\in\overline{t}_i}a_l^2-\sum_{l\in\overline{t}_i}m_l^2(\widetilde{t}),$$

где $1\leqslant i\leqslant n$. Тогда

$$\|\widetilde{a}\|^2=\|\widetilde{m}(\widetilde{t})\|^2+\sum_{i=1}^{n}(\varepsilon_i+\overline{\varepsilon}_i)=2^{2n-4}\lambda_1(\widetilde{\tau})+\sum_{i=1}^{n}(\varepsilon_i+\overline{\varepsilon}_i). \tag{9}$$

В свою очередь, в силу леммы 2 имеем $\lambda_1(\widetilde{\tau})\geqslant\lambda_1(\widetilde{\mu})$. Поэтому справедливо неравенство $\|\widetilde{a}\|^2\geqslant 2^{2n-4}\lambda_1(\widetilde{\mu})$. Таким образом, неравенство (8) доказано.

Непосредственно проверяется, что $\|\widetilde{u}\|^2=2^{2n-4}\lambda_1(\widetilde{\mu})$. Поэтому на любом векторе из $M_n^L\widetilde{\mu}$ неравенство (8) обращается в равенство.

Предположим, что на некотором векторе $\widetilde{a}\in A_n^L$ в (8) достигается равенство. Пусть $\widetilde{t}$ — правильное разбиение координат вектора $\widetilde{a}$. Рассмотрим равенство (9). Поскольку $\|\widetilde{a}\|^2=2^{2n-4}\lambda_1(\widetilde{\mu})$, из леммы 2 следует, что разбиение $\widetilde{t}$ имеет тип $\widetilde{\mu}$, а $\varepsilon_i=\overline{\varepsilon}_i=0$, $1\leqslant i\leqslant n$. Поэтому вектор $\widetilde{a}$ совпадает с вектором $\widetilde{m}(\widetilde{t})$ и его можно получить перестановкой координат из вектора $\widetilde{u}$, т. е. $\widetilde{a}\in M_n^L\widetilde{\mu}$. Лемма 3 доказана.

Лемма 4. *Пусть* n, L *— целые числа такие, что* $n\geqslant 2$, $L\geqslant 2n$, L *нечетно,* $\widetilde{t}$ *— разбиение из множества* T_L^{2n}, $\widetilde{\tau}\in\widetilde{\mathfrak{T}}_L^{2n}$ *— тип разбиения* $\widetilde{t}$. *Тогда*

$$\varphi(\widetilde{m}(\widetilde{t}),\widetilde{t})\geqslant 2^{2n-4}\left(\frac{1}{\tau_1-1}-\frac{1}{\tau_1}\right).$$

Доказательство. Обозначим через q произвольное значение i такое, что выражение

$$\left|\sum_{k\in t_i}m_k^2(\widetilde{t})-\sum_{l\in\overline{t}_i}m_l^2(\widetilde{t})\right|$$

как функция от i, $1 \leqslant i \leqslant n$, принимает максимальное значение. Поскольку число L нечетно, среди множеств $t_1, \dots, t_n, \overline{t}_1, \dots, \overline{t}_n$ нечетную мощность имеет нечетное число множеств. Поэтому имеется номер j, $1 \leqslant j \leqslant n$, такой, что числа $|t_j|$, $|\overline{t}_j|$ имеют разную четность. Следовательно, при таком j справедливо неравенство

$$\left|\sum_{k\in t_j} m_k^2(\widetilde{t}) - \sum_{l\in \overline{t}_j} m_l^2(\widetilde{t})\right| > 0.$$

Поэтому $\varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) > 0$, следовательно, $|t_q| \neq |\overline{t}_q|$. Без ограничения общности считаем, что $|t_q| > |\overline{t}_q|$. Тогда

$$\begin{aligned}\varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) = \left|\sum_{k\in t_q} m_k^2(\widetilde{t}) - \sum_{l\in \overline{t}_q} m_l^2(\widetilde{t})\right| &= 2^{2n-4}\left(\frac{1}{|\overline{t}_q|} - \frac{1}{|t_q|}\right)\\ &= 2^{2n-4} \sum_{p=|\overline{t}_q|+1}^{|t_q|} \left(\frac{1}{p-1} - \frac{1}{p}\right)\\ &\geqslant 2^{2n-4}\left(\frac{1}{\tau_1 - 1} - \frac{1}{\tau_1}\right).\end{aligned}$$

Лемма 4 доказана.

Пусть $L - 2n\lfloor L/2n\rfloor \geqslant 1$. Обозначим через $\overline{M}_n^L\widetilde{\mu}$ множество векторов из A_n^L, которые можно получить перестановкой координат из вектора вида

$$\Bigl(c_1, \dots, c_{\lfloor L/2n\rfloor+1}, \underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor+1}, \dots, \frac{2^{n-2}}{\lfloor L/2n\rfloor+1}}_{a}, \underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor}, \dots, \frac{2^{n-2}}{\lfloor L/2n\rfloor}}_{b}\Bigr),$$

где $a = (L - 2n\lfloor L/2n\rfloor - 1)(\lfloor L/2n\rfloor + 1)$, $b = (2n - (L - 2n\lfloor L/2n\rfloor))\lfloor L/2n\rfloor$, $c_1, \dots, c_{\lfloor L/2n\rfloor+1}$ — вещественные неотрицательные числа,

$$\sum_{i=1}^{\lfloor L/2n\rfloor+1} c_i = 2^{n-2}, \qquad \sum_{i=1}^{\lfloor L/2n\rfloor+1} c_i^2 \leqslant \frac{2^{2n-4}}{\lfloor L/2n\rfloor}.$$

Пусть $L - 2n\lfloor L/2n\rfloor \geqslant 3$. Обозначим через $\overline{M}_n^L\widetilde{\nu}$ множество всех векторов из A_n^L, которые можно получить перестановкой координат из вектора вида

$$\Bigl(c_1, \dots, c_{\lfloor L/2n\rfloor+2}, \underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor+1}, \dots, \frac{2^{n-2}}{\lfloor L/2n\rfloor+1}}_{a}, \underbrace{\frac{2^{n-2}}{\lfloor L/2n\rfloor}, \dots, \frac{2^{n-2}}{\lfloor L/2n\rfloor}}_{b}\Bigr),$$

где $a = (L-2n\lfloor L/2n\rfloor-2)(\lfloor L/2n\rfloor+1)$, $b = (2n-(L-2n\lfloor L/2n\rfloor)+1)\lfloor L/2n\rfloor$, $c_1, \dots, c_{\lfloor L/2n\rfloor+2}$ — вещественные неотрицательные числа,

$$\sum_{i=1}^{\lfloor L/2n\rfloor+2} c_i = 2^{n-2}, \qquad \sum_{i=1}^{\lfloor L/2n\rfloor+2} c_i^2 \leqslant \frac{2^{2n-4}}{\lfloor L/2n\rfloor+1}.$$

Лемма 5. *Пусть n, L — целые числа такие, что $n \geqslant 2$, $L \geqslant 2n$, L нечетно. Тогда для любого вектора $\widetilde{a}$ из A_n^L справедливо неравенство*

$$\|\widetilde{a}\|^2 + \varphi(\widetilde{a}) \geqslant 2^{2n-4}\left(\frac{L-2n\lfloor L/2n\rfloor-1}{\lfloor L/2n\rfloor+1} + \frac{2n-(L-2n\lfloor L/2n\rfloor)+1}{\lfloor L/2n\rfloor}\right). \qquad (10)$$

Если $L - 2n\lfloor L/2n\rfloor \leqslant 2$, то в (10) достигается равенство тогда и только тогда, когда $\widetilde{a} \in \overline{M}_n^L\widetilde{\mu}$.

Если $L - 2n\lfloor L/2n\rfloor \geqslant 3$, то в (10) достигается равенство тогда и только тогда, когда $\widetilde{a} \in \overline{M}_n^L\widetilde{\mu} \cup \overline{M}_n^L\widetilde{\nu}$.

Доказательство. Пусть вектор $\widetilde{\mu}$ является наименьшим элементом в частично упорядоченном множестве $\langle\widetilde{\mathfrak{T}}_L^{2n}, \succ\rangle$. Непосредственно проверяется, что выражение в правой части неравенства (10) равно $2^{2n-4}\lambda_2(\widetilde{\mu})$. Пусть $\widetilde{a}$ — вектор из A_n^L; $\widetilde{t}$ — разбиение из T_L^{2n}; $\widetilde{\tau} \in \widetilde{\mathfrak{T}}_L^{2n}$ — тип разбиения $\widetilde{t}$ и при любом i, $1 \leqslant i \leqslant n$,

$$\varepsilon_i = \sum_{k\in t_i} a_k^2 - \sum_{k\in t_i} m_k^2(\widetilde{t}), \quad \overline{\varepsilon}_i = \sum_{l\in \overline{t}_i} a_l^2 - \sum_{l\in \overline{t}_i} m_l^2(\widetilde{t}).$$

Ясно, что при любом i, $1 \leqslant i \leqslant n$, справедливы соотношения

$$\varepsilon_i \geqslant 0, \quad \overline{\varepsilon}_i \geqslant 0, \quad \|\widetilde{a}\|^2 = \|\widetilde{m}(\widetilde{t})\|^2 + \sum_{i=1}^{n}(\varepsilon_i + \overline{\varepsilon}_i).$$

Обозначим через q произвольное значение i, $1 \leqslant i \leqslant n$, такое, что выражение

$$\left|\sum_{k\in t_i} m_k^2(\widetilde{t}) - \sum_{l\in \overline{t}_i} m_l^2(\widetilde{t})\right|$$

как функция от i принимает максимальное значение. Тогда

$$\varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) = \left|\sum_{k\in t_q} m_k^2(\widetilde{t}) - \sum_{l\in \overline{t}_q} m_l^2(\widetilde{t})\right|,$$

$$\varphi(\widetilde{a}, \widetilde{t}) \geqslant \left|\sum_{k\in t_q} m_k^2(\widetilde{t}) + \varepsilon_q - \sum_{l\in \overline{t}_q} m_l^2(\widetilde{t}) - \overline{\varepsilon}_q\right|, \qquad (11)$$

откуда используя равенство $\|\widetilde{m}(\widetilde{t})\|^2 = 2^{2n-4}\lambda_1(\widetilde{\tau})$ и неравенства

$$\varphi(\widetilde{m}(\widetilde{t}),\widetilde{t}) \geqslant 2^{2n-4}\left(\frac{1}{\tau_1 - 1} + \frac{1}{\tau_1}\right), \quad \lambda_2(\widetilde{\tau}) \geqslant \lambda_2(\widetilde{\mu})$$

(первое неравенство справедливо по лемме 4, второе — по лемме 2), получаем

$$\begin{aligned}
\|\widetilde{a}\|^2 + \varphi(\widetilde{a},\widetilde{t}) &\geqslant \|\widetilde{m}(\widetilde{t})\|^2 + \sum_{i=1}^{n}(\varepsilon_i + \overline{\varepsilon}_i) \\
&\quad + \left|\sum_{k\in t_q} m_k^2(\widetilde{t}) + \varepsilon_q - \sum_{l\in \overline{t}_q} m_l^2(\widetilde{t}) - \overline{\varepsilon}_q\right| \\
&\geqslant \|\widetilde{m}(\widetilde{t})\|^2 + \varphi(\widetilde{m}(\widetilde{t}),\widetilde{t}) + \sum_{i=1}^{n}(\varepsilon_i + \overline{\varepsilon}_i) - |\varepsilon_q - \overline{\varepsilon}_q| \\
&\geqslant 2^{2n-4}\lambda_2(\widetilde{\tau}) \geqslant 2^{2n-4}\lambda_2(\widetilde{\mu}). \qquad (12)
\end{aligned}$$

Поскольку разбиение $\widetilde{t}$ из $T_L^{2n}(\widetilde{a})$ выбрано произвольно, неравенство (10) доказано.

Предположим, что для некоторого вектора $\widetilde{a} \in A_n^L$ неравенство (10) обращается в равенство. Пусть разбиение $\widetilde{t} \in T_L^{2n}(\widetilde{a})$ такое, что $\varphi(\widetilde{a},\widetilde{t}) = \varphi(\widetilde{a})$. Из неравенств (12) и леммы 2 следует, что если $L - 2n\lfloor L/2n\rfloor = 1$, то разбиение $\widetilde{t}$ имеет тип $\widetilde{\mu}$; если $L - 2n\lfloor L/2n\rfloor \geqslant 2$, то разбиение $\widetilde{t}$ имеет либо тип $\widetilde{\mu}$, либо тип $\widetilde{\nu}$ ($\widetilde{\nu}$ — вектор, полученный из вектора $\widetilde{\mu}$ переносом единицы из слоя μ_1 в слой $\mu_1 + 1$). Покажем, что в случае $L - 2n\lfloor L/2n\rfloor = 2$ разбиение $\widetilde{t}$ не может иметь тип $\widetilde{\nu}$. Действительно, если в этом случае разбиение $\widetilde{t}$ имеет тип $\widetilde{\nu}$, то

$$\varphi(\widetilde{m}(\widetilde{t}),\widetilde{t}) = 2^{2n-4}\left(\frac{1}{\nu_1 - 2} - \frac{1}{\nu_1}\right) > 2^{2n-4}\left(\frac{1}{\nu_1 - 1} - \frac{1}{\nu_1}\right).$$

Поэтому из (12) вытекает, что

$$\|\widetilde{a}\|^2 + \varphi(\widetilde{a},\widetilde{t}) > 2^{2n-4}\lambda_2(\widetilde{\nu}) = 2^{2n-4}\lambda_2(\widetilde{\mu}).$$

Это противоречит тому, что на векторе $\widetilde{a}$ неравенство (10) обращается в равенство.

Пусть разбиение $\widetilde{t}$ имеет тип $\widetilde{\mu}$. Докажем, что в этом случае вектор $\widetilde{a}$ принадлежит множеству $\overline{M}_n^L\widetilde{\mu}$. В силу леммы 4 имеем $\varphi(\widetilde{m}(\widetilde{t}),\widetilde{t}) > 0$, поэтому $|t_q| \neq |\overline{t}_q|$. Без ограничения общности считаем, что $|t_q| > |\overline{t}_q|$. В таком случае для доказательства включения $\widetilde{a} \in \overline{M}_n^L\widetilde{\mu}$ достаточно

показать, что координаты вектора $\widetilde{a}$ и разбиение $\widetilde{t}$ удовлетворяют следующим условиям:

$$a_k = m_k(\widetilde{t}) \text{ при } k \in t_i,\ 1 \leqslant i \leqslant n,\ i \neq q; \tag{13}$$

$$a_l = m_l(\widetilde{t}) \text{ при } l \in \bar{t}_i,\ 1 \leqslant i \leqslant n; \tag{14}$$

$$\sum_{k \in t_q} a_k^2 \leqslant \frac{2^{2n-4}}{\lfloor L/2n \rfloor}; \tag{15}$$

$$|t_q| = \lfloor L/2n \rfloor + 1. \tag{16}$$

Действительно, поскольку разбиение $\widetilde{t}$ имеет тип $\widetilde{\mu}$, имеем

$$|t_q| = \lfloor L/2n \rfloor + 1, \qquad |\bar{t}_q| = \lfloor L/2n \rfloor.$$

Поэтому верно (16). Поскольку $\|\widetilde{a}\|^2 + \varphi(\widetilde{a}, \widetilde{t}) = 2^{2n-4}\lambda_2(\widetilde{\mu})$, из (12) следует, что на векторе $\widetilde{a}$ неравенство (11) обращается в равенство и все ε_i, $\bar{\varepsilon}_i$ $(1 \leqslant i \leqslant n)$, за исключением либо ε_q, либо $\bar{\varepsilon}_q$, равны нулю. Покажем, что $\bar{\varepsilon}_q = 0$. Действительно, в противном случае $\varepsilon_q = 0$, и из (11) вытекает, что

$$\varphi(\widetilde{a}, \widetilde{t}) = \sum_{l \in \bar{t}_q} m_l^2(\widetilde{t}) - \sum_{k \in t_q} m_k^2(\widetilde{t}) + \bar{\varepsilon}_q > \varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}).$$

Но согласно (12) последнее соотношение противоречит равенству $\|\widetilde{a}\|^2 + \varphi(\widetilde{a}, \widetilde{t}) = 2^{2n-4}\lambda_2(\widetilde{\mu})$. Поэтому $\bar{\varepsilon}_q = 0$. Следовательно, равенства (13), (14) доказаны.

Покажем, что выполнено неравенство (15). Действительно, в противном случае имеем

$$\varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) - \varepsilon_q = \sum_{l \in \bar{t}_q} m_l^2(\widetilde{t}) - \Big(\sum_{k \in t_q} m_k^2(\widetilde{t}) + \varepsilon_q\Big) = \frac{2^{2n-4}}{\lfloor L/2n \rfloor} - \sum_{k \in t_q} a_k^2 < 0.$$

Поэтому $\varepsilon_q > \varphi(\widetilde{m}(\widetilde{t}), \widetilde{t})$. Следовательно, из (11) вытекает равенство $\varphi(\widetilde{a}, \widetilde{t}) = \varepsilon_q - \varphi(\widetilde{m}(\widetilde{t}), \widetilde{t})$. Таким образом,

$$\begin{aligned} \|\widetilde{a}\|^2 + \varphi(\widetilde{a}, \widetilde{t}) &= \|\widetilde{m}(\widetilde{t})\|^2 + \varepsilon_q + \varepsilon_q - \varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) \\ &> \|\widetilde{m}(\widetilde{t})\|^2 + \varphi(\widetilde{m}(\widetilde{t}), \widetilde{t}) \geqslant 2^{2n-4}\lambda_2(\widetilde{\mu}), \end{aligned}$$

что противоречит равенству $\|\widetilde{a}\| + \varphi(\widetilde{a}, \widetilde{t}) = 2^{2n-4}\lambda_2(\widetilde{\mu})$. Отсюда следует справедливость (15). Итак, доказано, что если $\widetilde{t}$ имеет тип $\widetilde{\mu}$, то вектор $\widetilde{a}$ принадлежит множеству $\overline{M}_n^L \widetilde{\mu}$.

Пусть верно неравенство $L-2n\lfloor L/2n\rfloor \geqslant 3$ и разбиение $\widetilde{t}$ имеет тип $\widetilde{\nu}$. Докажем, что в этом случае $\widetilde{a}\in \overline{M}_n^L\widetilde{\nu}$. Для этого достаточно показать, что вектор $\widetilde{a}$ и разбиение $\widetilde{t}$ удовлетворяют следующим условиям:

$$a_k = m_k(\widetilde{t}) \ \text{при } k\in t_i,\ 1\leqslant i\leqslant n,\ i\neq q;$$
$$a_l = m_l(\widetilde{t}) \ \text{при } l\in \overline{t}_i,\ 1\leqslant i\leqslant n;$$

$$\sum_{k\in t_q} a_k^2 \leqslant \frac{2^{2n-4}}{\lfloor L/2n\rfloor+1},\quad |t_q| = \lfloor L/2n\rfloor + 2.$$

Справедливость этого утверждения устанавливается так же, как и в случае, когда $\widetilde{t}$ имеет тип $\widetilde{\mu}$ с той лишь разницей, что в данном случае $|t_q| = \lfloor L/2n\rfloor + 2$, $|\overline{t}_q| = \lfloor L/2n\rfloor + 1$. Покажем, что последние равенства выполнены. Действительно, в противном случае либо $|t_q| = \lfloor L/2n\rfloor + 2$ и $|\overline{t}_q| = \lfloor L/2n\rfloor$, либо $|t_q| = \lfloor L/2n\rfloor + 1$ и $|\overline{t}_q| = \lfloor L/2n\rfloor$. Непосредственно проверяется, что в обоих случаях справедливо неравенство

$$\varphi(\widetilde{m}(\widetilde{t}),\widetilde{t}) > 2^{2n-4}\left(\frac{1}{\nu_1-1}-\frac{1}{\nu_1}\right),$$

из которого ввиду (12) получаем неравенство

$$\|\widetilde{a}\|^2 + \varphi(\widetilde{a},\widetilde{t}) > 2^{2n-4}\lambda_2(\widetilde{\mu}),$$

которое противоречит предположению, что на векторе $\widetilde{a}$ неравенство (10) обращается в равенство. Следовательно, если $L-2n\lfloor L/2n\rfloor \geqslant 3$ и разбиение $\widetilde{t}$ имеет тип $\widetilde{\nu}$, то $\widetilde{a}\in \overline{M}_n^L\widetilde{\nu}$.

Непосредственно проверяется, что на любом векторе из $\overline{M}_n^L\widetilde{\mu}$ неравенство (10) обращается в равенство; если $L-2n\lfloor L/2n\rfloor \geqslant 3$, то на любом векторе из $\overline{M}_n^L\widetilde{\nu}$ неравенство (10) обращается в равенство. Лемма 5 доказана.

Теорема 2. *Пусть Φ_n — линейная булева функция, существенно зависящая от n переменных. Тогда*

$$L_\pi(\Phi_n) \geqslant n^2+2,\quad \text{если } n \text{ четно},\quad n\neq 2^k;$$
$$L_\pi(\Phi_n) \geqslant n^2+3,\quad \text{если } n \text{ нечетно},\quad n\geqslant 5.$$

Доказательство. Пусть S — π-схема, реализующая Φ_n, а все контакты схемы S занумерованы числами от 1 до L. Поскольку согласно [1] $L_\pi(\Phi_n)\geqslant n^2$, верно неравенство $L\geqslant n^2$. Пусть χ_0 и χ_1 — функции выбора сечения и цепи в S. Из теоремы 1 следует, что вектор отображения $(\chi_0\cap\chi_1)|_R$ принадлежит множеству X_n^L. Поэтому

для доказательства теоремы 2 достаточно убедиться в справедливости следующих утверждений.

1. *Если n четно и $n \neq 2^k$, то либо множества $X_n^{n^2}$, $X_n^{n^2+1}$ пустые, либо каждый вектор из этих множеств имеет хотя бы одну нецелую координату.*

2. *Если n нечетно и $n \geqslant 5$, то либо множества $X_n^{n^2}$, $X_n^{n^2+1}$, $X_n^{n^2+2}$ пустые, либо каждый вектор из этих множеств имеет хотя бы одну нецелую координату.*

Для произвольного натурального числа n, $n \neq 2^k$, имеем $X_n^{n^2} \subseteq V_n^{n^2}$, где V_n^L определено в начале § 3. Обозначим через $\widetilde{v}$ вектор из множества $V_n^{n^2}$, все координаты которого одинаковы и равны $\frac{2^{n-1}}{n}$. Поскольку $n \neq 2^k$, число $\frac{2^{n-1}}{n}$ нецелое. Очевидно, что для любого вектора $\widetilde{w} \in V_n^{n^2}$, $\widetilde{w} \neq \widetilde{v}$, имеем $||\widetilde{w}||^2 > ||\widetilde{v}||^2 = (2^{n-1})^2$. Поэтому множество $X_n^{n^2}$ либо пусто, либо состоит из единственного вектора $\widetilde{v}$, все координаты которого нецелые.

Пусть n четно и $n \neq 2^k$. Из леммы 5 следует, что $X_n^{n^2+1} = \overline{M}_n^{n^2+1}\widetilde{\mu}$ и любой вектор из множества $\overline{M}_n^{n^2+1}\widetilde{\mu}$ имеет координату, равную $2^{n-2}/\lfloor(n^2+1)/2n\rfloor$. При рассматриваемом n число $\lfloor(n^2+1)/2n\rfloor = n/2$ отлично от степени двойки. Поэтому любой вектор из $X_n^{n^2+1}$ имеет хотя бы одну нецелую координату. Тем самым справедливость утверждения 1 установлена.

Пусть n нечетно и $n \geqslant 5$. Из леммы 3 вытекает, что $X_n^{n^2+1} \subseteq M_n^{n^2+1}\widetilde{\mu}$ и любой вектор из $M_n^{n^2+1}\widetilde{\mu}$ имеет хотя бы одну координату, равную $2^{n-2}/\lfloor(n^2+1)/2n\rfloor + 1)$, и хотя бы одну координату, равную $2^{n-2}/\lfloor(n^2+1)/2n\rfloor$. Далее, из леммы 5 следует, что $X_n^{n^2+2} = \overline{M}_n^{n^2+2}\widetilde{\mu} \cup \overline{M}_n^{n^2+2}\widetilde{\nu}$ и любой вектор из $\overline{M}_n^{n^2+2}\widetilde{\mu} \cup \overline{M}_n^{n^2+2}\widetilde{\nu}$ имеет хотя бы одну координату, равную $2^{n-2}/(\lfloor(n^2+2)/2n\rfloor+1)$, и хотя бы одну координату, равную $2^{n-2}/(\lfloor(n^2+2)/2n\rfloor)$. Поскольку при $n \geqslant 5$ по крайней мере одно из чисел

$$\lfloor(n^2+1)/2n\rfloor + 1 = \lfloor(n^2+2)/2n\rfloor + 1 = \frac{n-1}{2} + 1,$$

$$\lfloor(n^2+1)/2n\rfloor = \lfloor(n^2+2)/2n\rfloor = \frac{n-1}{2}$$

отлично от 2^k, либо множества $X_n^{n^2+1}$, $X_n^{n^2+2}$ пусты, либо каждый вектор из этих множеств имеет по крайней мере одну нецелую координату, т. е. справедливо утверждение 2. Теорема 2 доказана.

ЛИТЕРАТУРА

1. **Храпченко В. М.** Об одном методе получения нижних оценок сложности π-схем // Мат. заметки. 1971. Т. 10, № 1. С. 83–92.
2. **Яблонский С. В.** Реализация линейной функции в классе π-схем // Докл. АН СССР. 1954. Т. 94, № 5. С. 805–806.
3. **Храпченко В. М.** О сложности реализации линейной функции в классе π-схем // Мат. заметки. 1971. Т. 9, № 1. С. 35–40.

Адрес автора:

РОССИЯ,
630090, Новосибирск,
Университетский пр., 4,
Институт математики СО РАН

Статья поступила
26 сентября 1994 г.