ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2012. Том 19, № 3. С. 3–12

УДК 519.714

ФОРМУЛЬНАЯ СЛОЖНОСТЬ ТЕРНАРНОЙ ЛИНЕЙНОЙ ФУНКЦИИ *)

С. В. Августинович, Ю. Л. Васильев, К. Л. Рычков

Аннотация. Установлено, что сложность реализации в классе обобщённых (троичных) π-схем троичного счётчика кратности 3, зависящего от трёх переменных, равна 18.

Ключевые слова: сложность, обобщённая π-схема, тернарная линейная функция.

Под *q-ичной параллельно-последовательной контактной схемой* (*π-схемой*) понимается обычная (двоичная) π-схема, контактам которой приписаны символы x_i^δ, $i = 1, \ldots, n$, $\delta = 0, 1, \ldots, q-1$. При этом x_i^δ — не булева переменная или её отрицание, а функция от x_i, определённая на $B_q = \{0, 1, \ldots, q-1\}$ и принимающая значения из $\{0, 1\}$. Значение функции x_i^δ равно 1, если $x_i = \delta$, и равно 0, если $x_i \neq \delta$. Для определённых таким образом переменных естественно ввести операции дизъюнкции и конъюнкции. Поэтому любой обобщённой π-схеме будет соответствовать формула, сложность которой определяется числом вхождений в неё переменных.

Функция $f : B_q^n \to \{0, 1\}$ проводимости q-ичной π-схемы определяется по аналогии с двоичным случаем: по определению q-ичная π-схема реализует функцию $f(x_1, \ldots, x_n) = \bigvee\limits_C K_C$, где дизъюнкция берётся по всем простым (без самопересечений) цепям, соединяющим полюсы схемы, а K_C — это конъюнкция всех функций $x_{i_1}^{\delta_1}, \ldots, x_{i_k}^{\delta_k}$, приписанных контактам цепи C. Как и в двоичном случае, говорим, что контакт, помеченный x_i^δ, *замкнут на наборе* $(\alpha_1, \ldots, \alpha_n) \in B_q^n$, если $\alpha_i = \delta$, и разомкнут в противном случае.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 09–01–00528 и 10–01–00424–а), целевой программы СО РАН на 2012–2014 гг. (интеграционный проект № 14), а также ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 14.740.11.0362).

Сложностью $L(S)$ *q-ичной π-схемы* S называется число контактов в S. *Сложностью* $L_\pi(f)$ *функции* $f : B_q^n \to \{0,1\}$ в классе π-схем называется $\min\limits_S L(S)$, где минимум берётся по всем q-ичным π-схемам, реализующим f. На множестве B_q^n определим следующую функцию (линейную функцию, существенно зависящую от всех своих переменных):

$$\varphi_q(x_1,\ldots,x_n) = \begin{cases} 1, & \text{если } x_1+\ldots+x_n = 0 \pmod q, \\ 0 & \text{в противном случае.} \end{cases}$$

В [4] установлено, что при $q \geqslant 2$, $n \geqslant 3$

$$L_\pi(\varphi_q(x_1,\ldots,x_n)) \geqslant \begin{cases} \max\left\{2qn-q,\ \dfrac{q^n n^2}{q^n-(q-1)^n-(-1)^n(q-1)}\right\} \\ \hfill \text{при } n = 1 \pmod q, \\ \max\left\{2qn-q,\ \dfrac{q^n n^2}{q^n-(q-1)^n+(-1)^n}\right\} \\ \hfill \text{при } n \neq 1 \pmod q. \end{cases}$$

В частности, $L_\pi(\varphi_3(x_1,x_2,x_3)) \geqslant 15$ при $q=n=3$.

Результатом настоящей работы является точное значение сложности функции $\varphi_3(x_1,x_2,x_3)$.

Теорема 1. *Для функции* $\varphi_3(x_1,x_2,x_3)$ *справедливо равенство*

$$L_\pi(\varphi_3(x_1,x_2,x_3)) = 18.$$

Доказательство. Через $(\pi_1(\delta),\pi_2(\delta),\pi_3(\delta))$, $\delta = 0,1,2$, обозначим циклический сдвиг вектора $(0,1,2)$ на δ позиций вправо.

Нетрудно проверить, что троичная π-схема, соответствующая формуле

$$\Bigl(\bigwedge_{\delta=0,1,2}\bigl(x_1^\delta \vee x_2^\delta \vee x_3^\delta\bigr)\Bigr)\bigvee\Bigl(\bigwedge_{\delta=0,1,2}\bigl(x_1^{\pi_1(\delta)} \vee x_2^{\pi_2(\delta)} \vee x_3^{\pi_3(\delta)}\bigr)\Bigr),$$

имеет сложность 18 и реализует функцию $\varphi_3(x_1,x_2,x_3)$. Следовательно, справедливо неравенство

$$L_\pi(\varphi_3(x_1,x_2,x_3)) \leqslant 18.$$

Докажем, что $L_\pi(\varphi_3(x_1,x_2,x_3)) \geqslant 18$. Доказательство опирается на подход В. М. Храпченко к получению нижних оценок сложности π-схем [1–6], основная идея которого сформулирована в лемме 1.

Пусть $f(x_1, \ldots, x_n)$ — произвольная функция, заданная на B_q^n, значения которой принадлежат $\{0, 1\}$,

$$N_0(f(x_1, \ldots, x_n)) = \bigl\{(\alpha_1, \ldots, \alpha_n) \in B_q^n \;\mid\; f(\alpha_1, \ldots, \alpha_n) = 0\bigr\},$$

$$N_1(f(x_1, \ldots, x_n)) = \bigl\{(\beta_1, \ldots, \beta_n) \in B_q^n \;\mid\; f(\beta_1, \ldots, \beta_n) = 1\bigr\}.$$

Для произвольной π-схемы S множество её контактов будем обозначать через $K(S)$.

Лемма 1. *Для произвольных непостоянной функции $f : B_q^n \to \{0, 1\}$ и реализующей её q-ичной π-схемы S существует отображение*

$$H : N_0(f(x_1, \ldots, x_n)) \times N_1(f(x_1, \ldots, x_n)) \to K(S),$$

удовлетворяющее условию: если произвольный контакт $k \in K(S)$ помечен символом x_i^δ, то $H^{-1}(k) = A \times B$, где A — подмножество $N_0\bigl(x_i^\delta \vee f(x_1, \ldots, x_n)\bigr)$, B — подмножество $N_1\bigl(x_i^\delta \wedge f(x_1, \ldots, x_n)\bigr)$.

Доказательство. Пусть S — произвольная q-ичная π-схема, реализующая функцию $f(x_1, \ldots, x_n)$.

Цепью π-схемы S называется простая цепь в S, соединяющая полюсы схемы. *Тупиковым сечением* π-схемы S называется минимальное по включению множество контактов этой схемы, имеющее общий контакт с каждой цепью схемы. Индукцией по сложности π-схемы нетрудно доказать, что каждая цепь и каждое тупиковое сечение π-схемы S имеют ровно один общий контакт [5].

Отображение $H : N_0(f(x_1, \ldots, x_n)) \times N_1(f(x_1, \ldots, x_n)) \to K(S)$ определим следующим образом. Заметим, что для каждого набора $(\alpha_1, \ldots, \alpha_n)$ из $N_0(f(x_1, \ldots, x_n))$ найдётся тупиковое сечение π-схемы S, все контакты которого разомкнуты на этом наборе. Поставим это сечение в соответствие с $(\alpha_1, \ldots, \alpha_n)$. Точно так же для каждого набора $(\beta_1, \ldots, \beta_n)$ из $N_1(f(x_1, \ldots, x_n))$ найдётся цепь π-схемы S, все контакты которой замкнуты на этом наборе. Поставим эту цепь в соответствие с $(\beta_1, \ldots, \beta_n)$.

По определению отображение

$$H : N_0(f(x_1, \ldots, x_n)) \times N_1(f(x_1, \ldots, x_n)) \to K(S)$$

каждой паре наборов

$$((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) \in N_0(f(x_1, \ldots, x_n)) \times N_1(f(x_1, \ldots, x_n))$$

ставит в соответствие тот единственный контакт π-схемы S, который является общим для тупикового сечения, соответствующего $(\alpha_1, \ldots, \alpha_n)$, и цепи, соответствующей $(\beta_1, \ldots, \beta_n)$.

Покажем, что отображение H удовлетворяет условию леммы. Пусть $k \in K(S)$ — произвольный контакт π-схемы S, и пусть x_i^δ — метка контакта k. Обозначим множество наборов $(\alpha_1, \ldots, \alpha_n) \in N_0(f(x_1, \ldots, x_n))$ таких, что соответствующие им тупиковые сечения π-схемы S содержат контакт k, через A. Через B обозначим множество таких наборов $(\beta_1, \ldots, \beta_n) \in N_1(f(x_1, \ldots, x_n))$, что соответствующие этим наборам цепи π-схемы S содержат контакт k. Ясно, что $H^{-1}(k) = A \times B$. Включение $A \subseteq N_0\big(x_i^\delta \vee f(x_1, \ldots, x_n)\big)$ следует из того, что контакт k разомкнут на каждом наборе $(\alpha_1, \ldots, \alpha_n) \in A$. Включение $B \subseteq N_1\big(x_i^\delta \wedge f(x_1, \ldots, x_n)\big)$ следует из того, что на каждом наборе $(\beta_1, \ldots, \beta_n) \in B$ контакт k замкнут. Лемма 1 доказана.

Пусть S — произвольная π-схема, реализующая функцию $\varphi_3(x_1, x_2, x_3)$. Докажем, что $L(S) \geqslant 18$. Для этого рассмотрим отображение

$$H : N_0(\varphi_3(x_1, x_2, x_3)) \times N_1(\varphi_3(x_1, x_2, x_3)) \to K(S),$$

существование которого утверждает лемма 1.

Пусть

$$A_1 = \big\{\overline{\alpha} = (\alpha_1, \alpha_2, \alpha_3) \in B_3^3 \mid \alpha_1 + \alpha_2 + \alpha_3 = 1 \ (\mathrm{mod}\, 3)\big\},$$

$$A_0 = \big\{\overline{\beta} = (\beta_1, \beta_2, \beta_3) \in B_3^3 \mid \beta_1 + \beta_2 + \beta_3 = 0 \ (\mathrm{mod}\, 3)\big\}.$$

Отметим, что

$$A_1 \subseteq N_0(\varphi_3(x_1, x_2, x_3)), \quad A_0 = N_1(\varphi_3(x_1, x_2, x_3)).$$

Множество B_3^3 будем рассматривать как векторное пространство над полем $GF(3)$. Введём следующие обозначения:

$$\overline{e}^1 = (1, 0, 0), \quad \overline{e}^2 = (0, 1, 0), \quad \overline{e}^3 = (0, 0, 1);$$

$$R_i = \{(\overline{\alpha}, \overline{\beta}) \in A_1 \times A_0 \mid \overline{\alpha} - \overline{\beta} = \overline{e}^i\}, \quad i = 1, 2, 3;$$

$$R_i^\delta = \{(\overline{\alpha}, \overline{\beta}) \in R_i \mid \beta_i = \delta\}, \quad i = 1, 2, 3, \ \delta = 0, 1, 2;$$

$$R = R_1 \cup R_2 \cup R_3.$$

Рассмотрим также отображение $h : R \to K(S)$, являющееся сужением отображения H на множество R.

Заметим, что если контакт $k \in K(S)$ помечен x_i^δ, $i \in \{1, 2, 3\}$, $\delta \in \{0, 1, 2\}$, то $h^{-1}(k) \subseteq R_i^\delta$. Это следует из того, что в силу леммы 1

$$h^{-1}(k) \subseteq H^{-1}(k) \subseteq N_0\big(x_i^\delta \vee \varphi_3(x_1, x_2, x_3)\big) \times N_1\big(x_i^\delta \wedge \varphi_3(x_1, x_2, x_3)\big).$$

Поэтому $|h^{-1}(k)| \leqslant |R_i^\delta| = 3$.

Пусть
$$y_i = |\{\ k \in K(S) \mid |h^{-1}(k)| = i\ \}|, \quad i = 1, 2, 3.$$
Неравенство $L(S) \geqslant 18$ является следствием очевидного неравенства
$$L(S) \geqslant y_1 + y_2$$
и следующей системы соотношений:
$$\begin{cases} y_1 + 2y_2 + 3y_3 = 27, \\ y_2 + 3y_3 \leqslant 9. \end{cases}$$
Равенство $y_1 + 2y_2 + 3y_3 = 27$ вытекает из очевидных равенств
$$y_1 + 2y_2 + 3y_3 = |R|, \quad |R| = 27.$$
Докажем, что $y_2 + 3y_3 \leqslant 9$. Для каждого $i \in Z$ определим вектор $\overline{e}^i \in B_3^3$, отображение $C_i : A_1 \times A_0 \to A_1 \times A_0$ и множество $D_i \subseteq A_1 \times A_0$ по следующим правилам:
$$\overline{e}^i = \begin{cases} \overline{e}^1, & \text{если } i = 1 \pmod 3, \\ \overline{e}^2, & \text{если } i = 2 \pmod 3, \\ \overline{e}^3, & \text{если } i = 3 \pmod 3; \end{cases}$$
$$C_i((\overline{\alpha}, \overline{\beta})) = (\overline{\beta} + \overline{e}^i,\ \overline{\alpha} - \overline{e}^i), \qquad (\overline{\alpha}, \overline{\beta}) \in A_1 \times A_0;$$
$$D_i = \{(\overline{\alpha}, \overline{\beta}) \in A_1 \times A_0 \mid \overline{\alpha} - \overline{\beta} = 2\overline{e}^i + \overline{e}^{i+1} + \overline{e}^{i+2}\}.$$
Отметим, что, если $i = j \pmod 3$, то $C_i \equiv C_j$, $D_i = D_j$. Заметим также, что $|D_1| = |D_2| = |D_3| = 9$, множества D_1, D_2, D_3 попарно не пересекаются и для любого $d \in D_1$ имеют место включения $C_3(d) \in D_2$, $C_2(d) \in D_3$.

Определим множество T, элементами которого являются следующие девять трёхэлементных подмножеств множества $D_1 \cup D_2 \cup D_3$:
$$T = \{\{d,\ C_3(d),\ C_2(d)\} \mid d \in D_1\}.$$

Множество $M \subseteq A_1 \times A_0$ будем называть *независимым*, если для любых двух пар $(\overline{\alpha}, \overline{\beta}), (\overline{\gamma}, \overline{\lambda}) \in M$ из неравенства $(\overline{\alpha}, \overline{\beta}) \neq (\overline{\gamma}, \overline{\lambda})$ следует, что $\overline{\alpha} \neq \overline{\gamma}$ и $\overline{\beta} \neq \overline{\lambda}$.

Для $M \subseteq A_1 \times A_0$ обозначим
$$\widehat{M} = \{\overline{\alpha} \in A_1 \mid \exists \overline{\alpha}' \in A_0\, (\overline{\alpha}, \overline{\alpha}') \in M\} \times \{\overline{\beta} \in A_0 \mid \exists \overline{\beta}' \in A_1\, (\overline{\beta}', \overline{\beta}) \in M\}.$$
Множество $\widehat{M}$ будем называть *замыканием множества* M.

Заметим, что каждое множество R_i^δ (а также каждое его подмножество), $i = 1,2,3$, $\delta = 0,1,2$, является независимым. Кроме того, для любого независимого множества M справедливо равенство $|\widehat{M}| = |M|^2$.

Каждому контакту $k \in K(S)$ поставим в соответствие подмножество

$$T(k) = \{t \in T \mid \widehat{h}^{-1}(k) \cap t \neq \varnothing\}$$

множества T. Покажем, что система подмножеств $T(k)$, $k \in K(S)$, множества T обладает свойствами, сформулированными в леммах 2 и 3.

Лемма 2. *Множества $T(k)$, $k \in K(S)$, попарно не пересекаются.*

Лемма 3. *Для каждого $k \in K(S)$ справедливо равенство*

$$|T(k)| = \frac{|h^{-1}(k)|^2 - |h^{-1}(k)|}{2}.$$

Следующие соотношения являются очевидными следствиями лемм 2 и 3:

$$\sum_{k \in K(S)} |T(k)| \leqslant |T|,$$

$$|T(k)| = \begin{cases} 0, & \text{если } |h^{-1}(k)| = 1, \\ 1, & \text{если } |h^{-1}(k)| = 2, \\ 3, & \text{если } |h^{-1}(k)| = 3, \end{cases} \qquad k \in K(S).$$

Неравенство $y_2 + 3y_3 \leqslant 9$ непосредственно вытекает из этих соотношений.

Доказательства лемм 2 и 3 опираются на леммы 4–6.

Множество M называется *разбиением множества* D, если каждый элемент M есть некоторое подмножество D, элементы M попарно не пересекаются и $\bigcup\limits_{m \in M} m = D$.

Для каждого $k \in K(S)$ определим множество

$$T'(k) = \{\widehat{h}^{-1}(k) \cap t \mid t \in T(k)\}.$$

Лемма 4. *Множество T является разбиением множества $D_1 \cup D_2 \cup D_3$.*

Лемма 5. *Для любых $k \in K(S)$ и $t \in T(k)$ имеет место равенство $|\widehat{h}^{-1}(k) \cap t| = 2$.*

Лемма 6. *Для любого $k \in K(S)$ множество $T'(k)$ является разбиением множества $\widehat{h}^{-1}(k) \setminus h^{-1}(k)$.*

В свою очередь, доказательства лемм 4–6 основаны на свойствах отображений C_i, $i \in Z$, множеств D_i, $i \in Z$, и множества T, сформулированных в леммах 7–12.

Лемма 7. *Пусть контакт k из $K(S)$ помечен x_i^δ, $i \in \{1,2,3\}$, $\delta \in \{0,1,2\}$. Тогда для любого $d \in A_1 \times A_0$ из включения $d \in \widehat{h}^{-1}(k)$ следует включение $C_i(d) \in \widehat{h}^{-1}(k)$.*

Доказательство. Пусть $d = (\overline{\alpha}, \overline{\beta}) \in \widehat{h}^{-1}(k)$. Определение замыкания множества влечёт существование таких $\overline{\beta}' \in A_1$ и $\overline{\alpha}' \in A_0$, что выполнены включения $(\overline{\beta}', \overline{\beta}) \in h^{-1}(k)$ и $(\overline{\alpha}, \overline{\alpha}') \in h^{-1}(k)$. Из этих включений следует также, что $(\overline{\beta}', \overline{\alpha}') \in \widehat{h}^{-1}(k)$. Покажем, что $(\overline{\beta}', \overline{\alpha}') = C_i((\overline{\alpha}, \overline{\beta}))$. Действительно, из леммы 1 вытекает (как показано выше), что $h^{-1}(k) \subseteq R_i^\delta \subseteq R_i$, поэтому выполнены равенства $\overline{\beta}' = \overline{\beta} + \overline{e}^i$ и $\overline{\alpha}' = \overline{\alpha} - \overline{e}^i$. Лемма 7 доказана.

Лемма 8. *Для любых $i \in Z$ и $d \in A_1 \times A_0$ справедливо равенство $C_i(C_i(d)) = d$.*

Лемма 9. *Для любых $i \in Z$ и $d \in D_i$ имеют место равенства*

$$C_{i+2}(C_i(C_{i+1}(d))) = d, \quad C_{i+1}(C_i(C_{i+2}(d))) = d.$$

Лемма 10. *Для любых $i \in Z$ и $d \in D_i$ справедливы включения $C_{i+2}(d) \in D_{i+1}$, $C_{i+1}(d) \in D_{i+2}$.*

Справедливость лемм 8–10 непосредственно вытекает из определения отображений C_i, $i \in Z$, и множеств D_i, $i \in Z$.

Лемма 11. *Для любых $i \in Z$ и $d \in D_i$ справедливо включение $\{d, C_{i+2}(d), C_{i+1}(d)\} \in T$.*

Доказательство. Указанное включение следует из определения множества T и следующих утверждений.

При $i = 1 \pmod 3$ выполнены соотношения

$$d \in D_i = D_1, \quad C_{i+2}(d) = C_3(d), \quad C_{i+1}(d) = C_2(d).$$

При $i = 2 \pmod 3$ имеют место соотношения

$$C_{i+1}(d) \in D_{i+2} = D_1 \quad \text{(лемма 10)},$$

$$d = C_{i+1}(C_{i+1}(d)) = C_3(C_{i+1}(d)) \quad \text{(лемма 8)},$$

$$C_{i+2}(d) = C_i(C_{i+1}(d)) = C_2(C_{i+1}(d)) \quad \text{(леммы 9, 8)}.$$

При $i = 3 \pmod 3$ справедливы соотношения

$$C_{i+2}(d) \in D_{i+1} = D_1 \quad \text{(лемма 10)},$$

$$C_{i+1}(d) = C_i(C_{i+2}(d)) = C_3(C_{i+2}(d)) \quad \text{(леммы 9, 8)},$$
$$d = C_{i+2}(C_{i+2}(d)) = C_2(C_{i+2}(d)) \quad \text{(лемма 8)}.$$

Лемма 11 доказана.

Лемма 12. *Для любых $i \in \{1,2,3\}$, $\delta \in \{0,1,2\}$ и $M \subseteq R_i^\delta$ верны соотношения*

$$\widehat{R}_i^\delta \subseteq R_i^\delta \cup D_{i+1} \cup D_{i+2}, \quad \widehat{M} \setminus M \subseteq D_{i+1} \cup D_{i+2}.$$

Доказательство. Заметим, что для любых $i \in \{1,2,3\}$ и $\delta \in \{0,1,2\}$ имеет место равенство

$$\widehat{R}_i^\delta = \{\overline{\alpha} \in A_1 \mid \alpha_i = \delta + 1\} \times \{\overline{\beta} \in A_0 \mid \beta_i = \delta\}.$$

Поэтому для любого $(\overline{\alpha}, \overline{\beta}) \in \widehat{R}_i^\delta$ выполнено одно из следующих трёх равенств:

$$\overline{\alpha} - \overline{\beta} = \overline{e}^i, \quad \overline{\alpha} - \overline{\beta} = \overline{e}^i + 2\overline{e}^{i+1} + \overline{e}^{i+2}, \quad \overline{\alpha} - \overline{\beta} = \overline{e}^i + \overline{e}^{i+1} + 2\overline{e}^{i+2}.$$

В первом случае $(\overline{\alpha}, \overline{\beta}) \in R_i^\delta$, во втором — $(\overline{\alpha}, \overline{\beta}) \in D_{i+1}$, в третьем — $(\overline{\alpha}, \overline{\beta}) \in D_{i+2}$. Первое соотношение доказано.

Пусть $(\overline{\alpha}, \overline{\beta}) \in \widehat{M} \setminus M$. Тогда из включения $M \subseteq R_i^\delta \subseteq R_i$ и определения множества $\widehat{M}$ следует, что $(\overline{\alpha},\ \overline{\alpha} - \overline{e}^i) \in M$ и $(\overline{\beta} + \overline{e}^i,\ \overline{\beta}) \in M$. Из этих включений и из того, что $(\overline{\alpha}, \overline{\beta}) \notin M$, вытекает, что $\overline{\alpha} - \overline{\beta} \neq \overline{e}^i$. Поэтому $(\overline{\alpha}, \overline{\beta}) \notin R_i^\delta$. Тем самым $(\overline{\alpha}, \overline{\beta}) \in D_{i+1} \cup D_{i+2}$. Второе соотношение и лемма 2 доказаны.

Доказательство леммы 4. В силу леммы 11 имеем

$$\bigcup_{t \in T} t = D_1 \cup D_2 \cup D_3.$$

Поэтому из равенства $\sum\limits_{t \in T} |t| = 27 = |D_1 \cup D_2 \cup D_3|$ следует, что элементы множества T попарно не пересекаются. Таким образом, множество T является разбиением множества $D_1 \cup D_2 \cup D_3$. Лемма 4 доказана.

Доказательство леммы 5. Пусть контакт $k \in K(S)$ помечен x_j^δ, $j \in \{1,2,3\}$, $\delta \in \{0,1,2\}$, и пусть $t \in T(k)$. Тогда $h^{-1}(k) \subseteq R_j^\delta$ в силу леммы 1. Поэтому из леммы 12 следует, что $\widehat{h}^{-1}(k) \subseteq R_j^\delta \cup D_{j+1} \cup D_{j+2}$. Учитывая, что $R \cap (D_1 \cup D_2 \cup D_3) = \varnothing$ и $t \subseteq D_1 \cup D_2 \cup D_3$, имеем

$$\widehat{h}^{-1}(k) \cap t \subseteq D_{j+1} \cup D_{j+2}, \quad (\widehat{h}^{-1}(k) \cap t) \cap D_j = \varnothing.$$

Из определения $T(k)$ вытекает, что $\widehat{h}^{-1}(k) \cap t \neq \varnothing$. Через d обозначим произвольный элемент множества $\widehat{h}^{-1}(k) \cap t$. Возможны два случая: $d \in D_{j+1}$ и $d \in D_{j+2}$.

Случай 1: $d \in D_{j+1}$. В силу лемм 4 и 11 справедливо равенство $t = \{d, C_{j+3}(d), C_{j+2}(d)\}$. Покажем, что $\widehat{h}^{-1}(k) \cap t = \{d, C_{j+3}(d)\}$. Действительно, $C_{j+3}(d) = C_j(d) \in \widehat{h}^{-1}(k) \cap t$ в силу леммы 7. Из леммы 10 следует, что $C_{j+2}(d) \in D_{j+3} = D_j$. Поэтому $C_{j+2}(d) \notin \widehat{h}^{-1}(k) \cap t$.

Случай 2: $d \in D_{j+2}$. Ввиду лемм 4 и 11 справедливо равенство $t = \{d, C_{j+4}(d), C_{j+3}(d)\}$. Покажем, что $\widehat{h}^{-1}(k) \cap t = \{d,\ C_{j+3}(d)\}$. Действительно, $C_{j+4}(d) \in D_{j+3} = D_j$ в силу леммы 10. Поэтому $C_{j+4}(d) \notin \widehat{h}^{-1}(k) \cap t$. Из леммы 7 следует, что $C_{j+3}(d) = C_j(d) \in \widehat{h}^{-1}(k) \cap t$. Лемма 5 доказана.

Доказательство леммы 6. Пусть k — произвольный контакт из множества $K(S)$. Из леммы 4 следует, что $T'(k)$ является разбиением множества $\widehat{h}^{-1}(k) \cap (D_1 \cup D_2 \cup D_3)$. Для завершения доказательства леммы 6 осталось показать, что

$$\widehat{h}^{-1}(k) \cap (D_1 \cup D_2 \cup D_3) = \widehat{h}^{-1}(k) \setminus h^{-1}(k).$$

Пусть контакт $k \in K(S)$ помечен $x_i^\delta,\ i \in \{1,2,3\},\ \delta \in \{0,1,2\}$. В силу леммы 1 имеем $h^{-1}(k) \subseteq R_i^\delta \subseteq R$. Поэтому $R \cap (D_1 \cup D_2 \cup D_3) = \varnothing$ влечёт включение

$$\widehat{h}^{-1}(k) \cap (D_1 \cup D_2 \cup D_3) \subseteq \widehat{h}^{-1}(k) \setminus h^{-1}(k).$$

Ввиду леммы 12 из $h^{-1}(k) \subseteq R_i^\delta$ следует, что

$$\widehat{h}^{-1}(k) \setminus h^{-1}(k) \subseteq D_1 \cup D_2 \cup D_3.$$

Поэтому справедливо включение

$$\widehat{h}^{-1}(k) \cap (D_1 \cup D_2 \cup D_3) \supseteq \widehat{h}^{-1}(k) \setminus h^{-1}(k).$$

Лемма 6 доказана.

Доказательство леммы 2. Предположим, напротив, что для контактов $k_1, k_2 \in K(S),\ k_1 \neq k_2$, справедливо $T(k_1) \cap T(k_2) \neq \varnothing$. Пусть t — произвольный элемент множества $T(k_1) \cap T(k_2)$. Из леммы 5 следует, что $|\widehat{h}^{-1}(k_1) \cap t| = 2$ и $|\widehat{h}^{-1}(k_2) \cap t| = 2$. Поскольку $|t| = 3$, существует такой элемент $d \in t$, что $d \in \widehat{h}^{-1}(k_1) \cap \widehat{h}^{-1}(k_2)$. Но в силу леммы 1 справедливы включения $\widehat{h}^{-1}(k_1) \subseteq H^{-1}(k_1)$ и $\widehat{h}^{-1}(k_2) \subseteq H^{-1}(k_2)$. Так как

$H^{-1}(k_1) \cap H^{-1}(k_2) = \varnothing$, то и $\widehat{h}^{-1}(k_1) \cap \widehat{h}^{-1}(k_2) = \varnothing$. Полученное противоречие показывает, что наше предположение неверно. Лемма 2 доказана.

Доказательство леммы 3. Из лемм 5 и 6 следует, что для любого $k \in K(S)$ справедливо равенство

$$|T'(k)| = \frac{|\widehat{h}^{-1}(k) \setminus h^{-1}(k)|}{2} = \frac{|h^{-1}(k)|^2 - |h^{-1}(k)|}{2}.$$

Для завершения доказательства осталось заметить, что $|T(k)| = |T'(k)|$. Лемма 3 и теорема 1 доказаны.

ЛИТЕРАТУРА

1. **Рычков К. Л.** Модификация метода В. М. Храпченко и применение её к оценкам сложности π-схем для кодовых функций // Дискрет. анализ. Вып. 42. — 1985. — С. 91–98.
2. **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.
3. **Рычков К. Л.** О сложности обобщённых контактных схем // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 5. — С. 78–87.
4. **Рычков К. Л.** Нижняя оценка сложности реализации в классе π-схем q-ичного счётчика кратности q // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 6. — С. 68–76.
5. **Храпченко В. М.** О сложности реализации линейной функции в классе π-схем // Мат. заметки. — 1971. — Т. 9, № 1. — С. 35–40.
6. **Храпченко В. М.** Об одном методе получения нижних оценок сложности π-схем // Мат. заметки. — 1971. — Т. 10, № 1. — С. 83–92.

Августинович Сергей Владимирович,
e-mail: avgust@math.nsc.ru
Васильев Юрий Леонидович
e-mail: vas@math.nsc.ru
Рычков Константин Леонидович,
e-mail: rychkov@math.nsc.ru

Статья поступила
11 июля 2011 г.

Переработанный вариант —
30 ноября 2011 г.