ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Ноябрь—декабрь 2010. Том 17, № 6. С. 68–76

УДК 519.714

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ РЕАЛИЗАЦИИ В КЛАССЕ π-СХЕМ q-ИЧНОГО СЧЁТЧИКА КРАТНОСТИ q [*)]

К. Л. Рычков

Аннотация. Рассматривается обобщение понятия параллельно-последовательной контактной схемы (π-схемы) на случай, когда переменные, приписанные контактам, могут принимать не два, как в булевом случае, а большее число значений. При этом проводимость контакта по-прежнему остаётся двузначной (контакт либо замкнут, либо разомкнут). Получена нижняя оценка сложности таких схем, реализующих q-ичный счётчик кратности q, т. е. функцию $\varphi_q : \{0, 1, \ldots, q-1\}^n \to \{0, 1\}$, которая равна 1, если сумма значений её переменных кратна q.

Ключевые слова: булева функция, контактная схема, сложность схем.

Под *q-ичной параллельно-последовательной контактной схемой* (*π-схемой*) понимается обычная (двоичная) π-схема, контактам которой приписаны символы x_i^δ, $i = 1, \ldots, n$; $\delta = 0, 1, \ldots, q-1$. Но при этом символ x_i^δ мы понимаем не как булеву переменную или её отрицание, а как функцию одной переменной x_i, определённую на множестве $B_q = \{0, 1, \ldots, q-1\}$ и принимающую значения из множества $\{0, 1\}$. Значение функции x_i^δ равно 1, если $x_i = \delta$, и равно 0, если $x_i \neq \delta$.

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 08–01–00671 и 09–01–00528).

© 2010 **Рычков К. Л.**

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.

Заметим, что при $q \geqslant 3$ в отличие от двоичного случая сложность функции $f : B_q^n \to \{0,1\}$ может отличаться от сложности её отрицания $\overline{f}$. Так сложность функции x_i^δ равна 1, а сложность её отрицания $\overline{x_i^\delta} = x_i^0 \vee \ldots \vee x_i^{\delta-1} \vee x_i^{\delta+1} \vee \ldots \vee x_i^{q-1}$ равна $q-1$. При этом, очевидно, имеет место неравенство $L_\pi(f) \geqslant \frac{1}{q-1} L_\pi(\overline{f})$. Действительно, если S — минимальная q-ичная π-схема, реализующая функцию f, и F — соответствующая S формула, то «навесив» на F отрицание, «опустив» его по законам де Моргана до переменных и заменив все $\overline{x_i^\delta}$ на $x_i^0 \vee \ldots \vee x_i^{\delta-1} \vee x_i^{\delta+1} \vee \ldots \vee x_i^{q-1}$, получим формулу, а значит, и некоторую π-схему S' для $\overline{f}$. При этом, очевидно, выполнены соотношения

$$L_\pi(f) = L(S) = \frac{1}{q-1} L(S') \geqslant \frac{1}{q-1} L_\pi(\overline{f}).$$

На множестве B_q^n определим следующую функцию:

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

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

$$L_\pi(\overline{\varphi_q}(x_1, \ldots, x_n)) \geqslant \max\left\{\frac{qn\log q}{2},\ (q-1)n^2\right\}.$$

Это неравенство в силу сделанного замечания влечёт нижнюю оценку сложности функции $\varphi_q(x_1, \ldots, x_n)$:

$$L_\pi(\varphi_q(x_1, \ldots, x_n)) \geqslant \max\left\{\frac{qn\log q}{2(q-1)},\quad n^2\right\}.$$

Результатом настоящей работы является теорема, улучшающая эту нижнюю оценку сложности.

Теорема. *Для любых натуральных* $q, n,\ q \geqslant 2, n \geqslant 3$, *справедливы следующие неравенства*:

$$L_\pi(\varphi_q(x_1, \ldots, x_n)) \geqslant \max\left\{2qn - q,\quad \frac{q^n n^2}{q^n - (q-1)^n - (-1)^n(q-1)}\right\}$$
$$\text{при } n = 1 \pmod q;$$

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

При доказательстве теоремы используется подход В. М. Храпченко получения нижних оценок сложности π-схем [1–3, 5, 6], основную идею которого можно сформулировать в виде леммы.

Пусть $f(x_1,\ldots,x_n)$ — произвольная функция, заданная на множестве B_q^n, значения которой принадлежат множеству $\{0,1\}$. Обозначим множество наборов $(\alpha_1,\ldots,\alpha_n) \in B_q^n$ таких, что $f(\alpha_1,\ldots,\alpha_n)=0$, через $N_0(f(x_1,\ldots,x_n))$. Через $N_1(f(x_1,\ldots,x_n))$ обозначим множество таких наборов $(\beta_1,\ldots,\beta_n) \in B_q^n$, что $f(\beta_1,\ldots,\beta_n)=1$. Для произвольной π-схемы S множество контактов S будем обозначать через $K(S)$.

Лемма. *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 следующему условию: если контакт $k \in K(S)$ помечен символом x_i^δ, то

$$H^{-1}(k) = A \times B,$$

где A — некоторое подмножество множества $N_0\big(x_i^\delta \vee (f(x_1,\ldots,x_n))\big)$, B — некоторое подмножество множества $N_1\big(x_i^\delta \wedge f(x_1,\ldots,x_n)\big)$.

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 такое минимальное по включению множество контактов этой схемы, которое имеет общий контакт с каждой цепью схемы. Индукцией по сложности π-схемы нетрудно доказать, что каждые цепь и 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

$$(\alpha_1,\ldots,\alpha_n) \in N_0(f(x_1,\ldots,x_n))$$

найдётся тупиковое сечение π-схемы S, все контакты которого разомкнуты на этом наборе. Каждому набору $(\alpha_1,\ldots,\alpha_n) \in N_0(f(x_1,\ldots,x_n))$ поставим в соответствие какое-нибудь одно такое тупиковое сечение.

Точно так же для каждого набора $(\beta_1, \ldots, \beta_n) \in N_1(f(x_1, \ldots, x_n))$ найдётся цепь π-схемы S, все контакты которой замкнуты на этом наборе. Каждому набору $(\beta_1, \ldots, \beta_n) \in N_1(f(x_1, \ldots, x_n))$ поставим в соответствие какую-нибудь одну такую цепь.

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 набору $(\alpha_1, \ldots, \alpha_n)$, и цепи, соответствующей набору $(\beta_1, \ldots, \beta_n)$.

Покажем, что отображение H удовлетворяет условию леммы. Пусть $k \in K(S)$ — произвольный контакт π-схемы S, 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 этим наборам 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 контакт k замкнут на каждом наборе $(\beta_1, \ldots, \beta_n)$ из B. Лемма доказана.

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

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

— отображение, существование которого утверждает лемма.

Пусть

$$A_l = \big\{\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in B_q^n \mid \alpha_1 + \ldots + \alpha_n = l \pmod q\big\}, \quad l = 0, 1, \ldots, q-1.$$

Отметим, что

$$A_1 \subseteq N_0(\varphi_q(x_1, \ldots, x_n)), \quad A_0 = N_1(\varphi_q(x_1, \ldots, x_n)).$$

Через $A_{i,l}^\delta$, $i = 1, \ldots, n$, $\delta, l = 0, 1, \ldots, q-1$, обозначим множество $\{\overline{\alpha} \in A_l \mid \alpha_i = \delta\}$.

Множество пар $(\overline{\alpha}, \overline{\beta}) = ((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) \in A_1 \times A_0$ таких, что наборы $\overline{\alpha}$ и $\overline{\beta}$ различаются ровно в одном разряде, обозначим через R.

Через $h_1 : R \to K(S)$ обозначим сужение отображения H на множество R.

Пусть $R_i^\delta = \{(\overline{\alpha}, \overline{\beta}) \in R \mid \alpha_i \neq \beta_i,\ \beta_i = \delta\}$, $i = 1, \ldots, n$, $\delta = 1, \ldots, q-1$.

Пусть $D \subseteq N_0(\varphi_q(x_1, \ldots, x_n)) \times N_1(\varphi_q(x_1, \ldots, x_n))$. Через $\widehat{D}$ обозначим множество $D_0 \times D_1 \subseteq N_0(\varphi_q(x_1, \ldots, x_n)) \times N_1(\varphi_q(x_1, \ldots, x_n))$ такое, что

$$D_0 = \{\overline{\alpha} \in N_0(\varphi_q(x_1, \ldots, x_n)) \mid \exists \overline{\beta} \in N_1(\varphi_q(x_1, \ldots, x_n)) \ \ (\overline{\alpha}, \overline{\beta}) \in D\},$$

$$D_1 = \{\overline{\beta} \in N_1(\varphi_q(x_1, \ldots, x_n)) \mid \exists \overline{\alpha} \in N_0(\varphi_q(x_1, \ldots, x_n)) \ \ (\overline{\alpha}, \overline{\beta}) \in D\}.$$

Заметим, что для множеств R_i^δ, $i = 1, \ldots, n$, $\delta = 0, 1, \ldots, q-1$, справедливы равенства

$$\widehat{R_i^\delta} = A_{i,1}^{\delta+1} \times A_{i,0}^{\delta}, \quad i = 1, \ldots, n,\ \delta = 0, 1, \ldots, q-1,$$

здесь подразумевается, что при $\delta = q-1$ имеют место равенства $A_{i,1}^{\delta+1} = A_{i,1}^{0}$, $i = 1, \ldots, n$. Из этих равенств следует, что если $q \geqslant 2$, $n \geqslant 3$, то при $i \neq j$ для любых $\delta, \sigma \in \{0, 1, \ldots, q-1\}$ справедливо

$$\widehat{R_i^\delta} \cap \widehat{R_j^\sigma} \neq \varnothing.$$

Множество $D \subseteq N_0(\varphi_q(x_1, \ldots, x_n)) \times N_1(\varphi_q(x_1, \ldots, x_n))$ будем называть *независимым*, если для любых двух пар $(\overline{\alpha}, \overline{\beta}), (\overline{\gamma}, \overline{\lambda}) \in D$ из того, что $(\overline{\alpha}, \overline{\beta}) \neq (\overline{\gamma}, \overline{\lambda})$, следует, что $\overline{\alpha} \neq \overline{\gamma}$ и $\overline{\beta} \neq \overline{\lambda}$.

Заметим, что если D — независимое множество, то справедливо равенство $|\widehat{D}| = |D|^2$. Кроме того, R_i^δ, $i = 1, \ldots, n$, $\delta = 0, 1, \ldots, q-1$, являются независимыми множествами.

Докажем неравенство $L(S) \geqslant 2qn - q$. Оно непосредственно вытекает из следующих двух утверждений.

(i) Для каждых $i \in \{1, \ldots, n\}$ и $\delta \in \{0, 1, \ldots, q-1\}$ в π-схеме S найдётся хотя бы один контакт, помеченный символом x_i^δ.

(ii) Если для некоторых $i \in \{1, \ldots, n\}$ и $\delta \in \{0, 1, \ldots, q-1\}$ в π-схеме S имеется ровно один контакт, помеченный символом x_i^δ, то для каждых $j \in \{1, \ldots, n\} \backslash \{i\}$ и $\sigma \in \{0, 1, \ldots, q-1\}$ в π-схеме S найдётся не менее двух контактов, помеченных символом x_j^σ.

Докажем (i). Рассмотрим произвольный контакт $k \in K(S)$. Пусть x_i^δ — метка этого контакта. Тогда из леммы следует, что

$$h_1^{-1}(k) \subseteq H^{-1}(k) \subseteq N_0\big(x_i^\delta \vee (f(x_1, \ldots, x_n))\big) \times N_1\big(x_i^\delta \wedge f(x_1, \ldots, x_n)\big).$$

Поэтому справедливо включение $h_1^{-1}(k) \subseteq R_i^\delta$. Поскольку множества R_i^δ, $i = 1, \dots, n$, $\delta = 0, 1, \dots, q-1$, непустые, попарно не пересекаются и

$$\bigcup_{i=1}^{n} \bigcup_{\delta=0}^{q-1} R_i^\delta = R,$$

из этого включения следует, что для любых i, δ в π-схеме S найдётся контакт, помеченный символом x_i^δ.

Докажем (ii). Предположим противное, т. е. для некоторых $i, j \in \{1, \dots, n\}$, $i \neq j$, и $\delta, \sigma \in \{0, 1, \dots, q-1\}$ имеется ровно один контакт $k_1 \in K(S)$, помеченный символом x_i^δ, и ровно один контакт $k_2 \in K(S)$, помеченный символом x_j^σ. Тогда $h_1^{-1}(k_1) = R_i^\delta$, $h_2^{-1}(k_1) = R_j^\sigma$. Кроме того, из леммы следует, что $\widehat{h_1^{-1}(k_1)} \subseteq H^{-1}(k_1)$ и $\widehat{h_1^{-1}(k_2)} \subseteq H^{-1}(k_2)$. Поэтому

$$\widehat{h_1^{-1}(k_1)} \cap \widehat{h_1^{-1}(k_2)} \subseteq H^{-1}(k_1) \cap H^{-1}(k_2) = \varnothing.$$

Но это противоречит тому, что $\widehat{R_i^\delta} \cap \widehat{R_j^\sigma} \neq \varnothing$.

Докажем, что

$$L(S) \geqslant \frac{q^n n^2}{q^n - (q-1)^n + (-1)^n (q-1)} \text{ при } n = 1 (\mathrm{mod}\ q),$$

$$L(S) \geqslant \frac{q^n n^2}{q^n - (q-1)^n + (-1)^n} \text{ при } n \neq 1 (\mathrm{mod}\ q).$$

Учитывая, что множества R_i^δ, $i = 1, \dots, n$, $\delta = 0, 1, \dots, q-1$, являются независимыми и для каждого контакта $k \in K(S)$ найдутся такие i, δ, что $h_1^{-1}(k) \subseteq R_i^\delta$, имеем

$$\sum_{k \in K(S)} \left| h_1^{-1}(k) \right|^2 = \sum_{k \in K(S)} \left| \widehat{h_1^{-1}(k)} \right|.$$

Учитывая, что в силу леммы для каждого контакта $k \in K(S)$ справедливо включение $\widehat{h_1^{-1}(k)} \subseteq H^{-1}(k)$ и множества $H^{-1}(k)$, $k \in K(S)$, попарно не пересекаются, имеем

$$\sum_{k \in K(S)} \left| \widehat{h_1^{-1}(k)} \right| \leqslant \left| \bigcup_{i=1}^{n} \bigcup_{\delta=0}^{q-1} \widehat{R_i^\delta} \right|.$$

Далее, учитывая очевидное равенство

$$\sum_{k\in K(S)} \left|h_1^{-1}(k)\right| = |R|$$

и частный случай неравенства Коши — Буняковского

$$\Big(\sum_{k\in K(S)} \left|h_1^{-1}(k)\right|\Big)^2 \leqslant |K(S)| \sum_{k\in K(S)} \left|h_1^{-1}(k)\right|^2,$$

как следствие имеем

$$L(S) = |K(S)| \geqslant \frac{|R|^2}{\left|\bigcup\limits_{i=1}^{n}\bigcup\limits_{\delta=0}^{q-1}\widehat{R_i^{\delta}}\right|}.$$

Нетрудно посчитать, что $|R| = q^{n-1}n$. Для вычисления мощности множества $\bigcup\limits_{i=1}^{n}\bigcup\limits_{\delta=0}^{q-1}\widehat{R_i^{\delta}}$ воспользуемся формулой включения–исключения [4]

$$\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{k=1}^{n}(-1)^{k-1}\sum_{1\leqslant j_1<\ldots<j_k\leqslant n}|X_{j_1}\cap\ldots\cap X_{j_k}|.$$

Получим

$$\left|\bigcup_{i=1}^{n}\bigcup_{\delta=0}^{q-1}\widehat{R_i^{\delta}}\right| = \left|\bigcup_{i=1}^{n}\bigcup_{\delta=0}^{q-1}\left(A_{i,1}^{\delta+1}\times A_{i,0}^{\delta}\right)\right| = \left|\bigcup_{\overline{\alpha}\in A_0}\bigcup_{i=1}^{n}\left(A_{i,1}^{\alpha_i+1}\times\{\overline{\alpha}\}\right)\right|$$

$$= \sum_{\overline{\alpha}\in A_0}\left|\bigcup_{i=1}^{n} A_{i,1}^{\alpha_i+1}\right| = \sum_{\overline{\alpha}\in A_0}\ \sum_{k=1}^{n}(-1)^{k-1}\sum_{1\leqslant j_1<\ldots<j_k\leqslant n}\left|A_{j_1,1}^{\alpha_{j_1}+1}\cap\ldots\cap A_{j_k,1}^{\alpha_{j_k}+1}\right|$$

$$= |A_0|\ \sum_{k=1}^{n}(-1)^{k-1}\sum_{1\leqslant j_1<\ldots<j_k\leqslant n}\left|A_{j_1,1}^{1}\cap\ldots\cap A_{j_k,1}^{1}\right|.$$

Заметим, что $\left|A_{j_1,1}^{1}\cap\ldots\cap A_{j_k,1}^{1}\right| = q^{n-k-1}$, $k = 1,\ldots,n-1$. Кроме того, $\left|A_{1,1}^{1}\cap\ldots\cap A_{n,1}^{1}\right| = 1$ при $n = 1(\mathrm{mod}\ q)$ и $\left|A_{1,1}^{1}\cap\ldots\cap A_{n,1}^{1}\right| = 0$ при $n \neq 1(\mathrm{mod}\ q)$.

Таким образом, при $n = 1 (\mathrm{mod}\ q)$ имеем

$$\left|\bigcup_{i=1}^{n}\bigcup_{\delta=0}^{q-1}\widehat{R_i^\delta}\right| = q^{n-1}\left(\sum_{k=1}^{n-1}(-1)^{k-1}\binom{n}{k}q^{n-k-1} + (-1)^{n-1}\right)$$
$$= q^{n-1}\,\frac{q^n - \sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}q^{n-k} + (-1)^n - (-1)^n q}{q}$$
$$= q^{n-2}(q^n - (q-1)^n - (-1)^n(q-1)).$$

Следовательно,

$$L(S) \geqslant \frac{q^n n^2}{q^n - (q-1)^n - (-1)^n(q-1)}.$$

При $n \neq 1 (\mathrm{mod}\ q)$ имеем

$$\left|\bigcup_{i=1}^{n}\bigcup_{\delta=0}^{q-1}\widehat{R_i^\delta}\right| = q^{n-1}\sum_{k=1}^{n-1}(-1)^{k-1}\binom{n}{k}q^{n-k-1}$$
$$= q^{n-1}\,\frac{q^n - \sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}q^{n-k} + (-1)^n}{q} = q^{n-2}(q^n - (q-1)^n + (-1)^n).$$

Тем самым

$$L(S) \geqslant \frac{q^n n^2}{q^n - (q-1)^n + (-1)^n}.$$

Теорема доказана.

ЛИТЕРАТУРА

1. **Рычков К. Л.** Модификация метода В. М. Храпченко и применение её к оценкам сложности π-схем для кодовых функций // Дискрет. анализ. — 1985. — Вып. 42. — 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. **Сачков В. Н.** Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982. — 384 с.

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.

Рычков Константин Леонидович,
e-mail: rychkov@math.nsc.ru

Статья поступила
26 июня 2010 г.