МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

# ТРУДЫ
# XI МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
# «ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва и Подмосковье
26–29 мая 2023 г.

MAKS PRESS

Москва – 2023

УДК 510.5+519.71
ББК 22.12:22.18
Д48

https://elibrary.ru/oqmbbq

Отв. ред. С.А. Ложкин, Д.С. Романов, В.В. Подымов

Д48 **Дискретные модели в теории управляющих систем** : XI международная конференция, Москва и Подмосковье, 26–29 мая 2023 г. : Труды / Отв. ред. С.А. Ложкин, Д.С. Романов, В.В. Подымов. – М.: МАКС Пресс, 2023. – 130 с.
ISBN 978-5-317-07114-1
https://doi.org/10.29003/m3789.978-5-317-07114-1

В сборнике представлены труды Одиннадцатой международной конференции «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 26–29 мая 2023 г.). Тематика конференции включает следующие направления: дискретные функциональные системы, свойства дискретных функций, синтез и сложность управляющих систем, надежность, контроль и диагностика управляющих систем, автоматы, теория графов, комбинаторика, теория кодирования, математические методы защиты информации, теория распознавания образов, математическая теория интеллектуальных систем, прикладная математическая логика.

*Ключевые слова:* дискретные функциональные системы, дискретные функции, синтез и сложность управляющих систем, надежность управляющих систем, контроль и диагностика управляющих систем, автоматы, теория графов, комбинаторика, теория кодирования, математические методы защиты информации, распознавание образов, интеллектуальные системы, прикладная математическая логика.

УДК 510.5+519.71
ББК 22.12:22.18

**ISBN 978-5-317-07114-1**

# Содержание

# Quantum search for a given substring in a text based on hashing technique

**Ablayev Farid, Ablayev Marat, Salikhova Nailya**

Kazan Federal University, e-mail: fablayev@gmail.com, mablayev@gmail.com, nailyasalikhova66@gmail.com

**Problem, notable results, definitions.** The paper considers the problem of finding a given substring in a text.

Given a binary sequence *string*, $N$ is a length of *string*: $string = b_1 \dots b_N$. Given a binary sequence $w$, $m$ is a length of $w$, $m < N$. It is required to find the index of the occurrence of the substring $w$ in the text *string*. Namely, it is required to find an index $k$ such that $w = b_k \dots b_{k+m-1}$ is true for *string* and $w$.

We denote by $T(string)$ the *sequence* of all substrings of length $m$ of the text *string*. Namely, for $n = N + 1 - m$ the sequence $T(string)$ is composed of all substrings $w_k$ of length $m$ of *string*.

$$T(string) = \{w_0, \dots, w_{n-1}\},$$

where $w_k = b_{k+1} \dots b_{k+m}$ for $0 \le k \le n-1$.

The known Knuth-Morris-Pratt's [1] classical algorithm (1977) solves the problem in linear time $QSize(n, m) = O(m + n)$.

In the early 2000s, a quantum algorithm $A$ [2] for searching for a given substring in a text was presented. It returns one of the indexes of the occurrence of the searching substring. The probability $Er^A(n, m)$ of getting the correct answer is strictly greater than $1/2$. The time complexity $QSize^A(n, m)$ of an algorithm is

$$QSize^A(n, m) = O(\sqrt{n} \log \sqrt{\frac{n}{m}} \log m + \sqrt{m} \log^2 m)$$

The algorithm requires

$$S^A(n, m) = O(\log n + m)$$

qubits for working.

**Our contribution.** We propose a quantum algorithm $\mathcal{A}2$ that searches for a substring in the text a) with a high probability of obtaining the correct result and b) with the same quadratic time acceleration compared to the classical one, but c) allows to reduce exponentially (compared to the [2] algorithm) the number of qubits relative to the substring length $m$, namely, the algorithm needs $S^{\mathcal{A}2}(n, m) = O(\log n + \log m)$ qubits for its work.

The $\mathcal{A}2$ algorithm is constructed for the case when it is known in advance that the required substring occurs exactly once in the text. Such a case was considered

by L. Grover in his paper [3], which laid the foundation for research in the field of quantum search.

**Algorithm $\mathcal{A}2$.** A binary string (substring) $w$ of length $m$ will also be considered a number, $0 \leq w \leq 2^m - 1$. We denote by $Set(string)$ the *set* (dictionary of text *string*) of all distinct subwords of length $m$ in *string*. Recall that $T(string)$ is a *sequence* of words of length $m$ formed from *string*. It is clear that $|Set(string)| \leq |T(string)|$.

$P = \{p_1, \ldots, p_d\}$ will denote the set of the first $d$ primes, where $d = d(n, m) = cnm$, for the integer $c \geq 3$.

— The first stage of the algorithm is the classic one: a prime number $p$ is chosen equiprobably from the set $P$.

— Second stage (preparation of the quantum state):
for the number $v \in \{0, \ldots, 2^m - 1\}$ and $p \in P$ we denote by $r(v)_p$ the remainder of $v/p$. Then $v = c_1 p + r(v)_p$, for some $c_1$. By

$$T_p(string) = \{r(w_0)_p, \ldots, r(w_{n-1})_p\}$$

we denote the sequence of words (here the remainders $r(w_j)_p$ are already considered as binary words) formed from *string*.
$T_p(string)$ generates a quantum state:

$$|string, p\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |k\rangle \otimes |r(w_k)_p\rangle \otimes |1\rangle$$

— The third stage (quantum) of the algorithm: Algorithm $\mathcal{A}1$ [4] is applied to the state $|string, p\rangle$ and the search word $r(w)_p$. As a result of measuring the first $\log n$ qubits, the number $j \in \{0, \ldots, n-1\}$ will be obtained, which is given as an answer and declared as the desired index of the word $w_j$ such that $w_j = w$.

**Theorem 1.** *For an arbitrary integer $c \geq 3$*

$$Er^{\mathcal{A}2}(string, w)) \leq \frac{1}{c} + \frac{1}{n},$$
$$QSize^{\mathcal{A}2}(n, m) = O(\sqrt{n} \log (mn)),$$
$$S^{\mathcal{A}2}(n, m) \leq O(\log n + \log m).$$

**Generalization: Universal Hashing Technique for Quantum Search.** The family $\mathcal{F} = \{f_1, \ldots, f_d\}$ of functions $f : \{0,1\}^m \to \{0,1\}^l$ for $l < m$ is called a universal family of hash functions (the set $\{0,1\}^m$ is the function domain $f$) [5] if for some $\epsilon \in [0, 1]$ and for an arbitrary pair $v, w \in \{0,1\}^m$

$$\frac{|F_{v,w}|}{|\mathcal{F}|} \leq \epsilon,$$

where $F_{w,v} = \{f \in \mathcal{F} : f(v) = f(w)\}$.

Universal family $\mathcal{F} = \{f_1, \ldots, f_d\}$ of hash functions $f : \{0,1\}^m \to \{0,1\}^l$ for $n \leq 2^m$ and $\epsilon \in [0,1]$ will be called a *strongly* $(n,\epsilon)$*-universal family of hash functions* if for each $n$-subset $Set = \{v_1, \ldots, v_n\}$ of the set $\{0,1\}^m$ and an arbitrary word $w \in \{0,1\}^m$

$$\frac{|F_{Set,w}|}{|\mathcal{F}|} \leq \epsilon,$$

where $F_{Set,w} = \bigcup_{v \in Set} F_{v,w}$.

An example of a strongly $(n,\epsilon)$-universal family of hash functions for the set $Set = T(string)$ and $w$ is the set $\mathcal{F} = \{f_1, \ldots, f_d\}$, where the $f_j$ functions are defined by the $j$-th prime number $p_j$ as follows: $f_j(w) = r(w)_{p_j}$ (the word $w$ is assumed to be an integer $w \in \{0, \ldots, 2^m - 1\}$), and $r(w)_{p_j}$ is the (represented as a word) remainder $r$ of the $w$ divided by a prime $p_j$.

For the constant $c \geq 3$, for $d = cnm$ the set $\mathcal{F} = \{f_1, \ldots, f_d\}$ is strongly $(n, 1/c)$-universal family of hash functions for each of the sets $Set \subseteq \{0,1\}^m$ of cardinality $n$ and each word $w \in \{0,1\}^m$.

Our research on the development of the technique of quantum search in databases based on hashing continues.

The study was funded by a Russian Science Foundation's grant (Project No. 19-19-00656).

## References

[1] Knuth D. E., Morris J. H. Jr., Pratt V. R. Fast pattern matching in strings // SIAM Journal on Computing. 1977. Vol. 6, № 2. P. 323–350.

[2] Ramesh H., Vinay V. String matching in O(n+m) quantum time // Journal of Discrete Algorithms. 2003. Vol. 1, № 1. P. 103–110.

[3] Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 1996. P. 212–219.

[4] Аблаев М. Ф., Салихова Н. М. Квантовый поиск заданной подстроки в тексте на основе техники хеширования // Ученые записки Казанского университета. Серия Физико-математические науки. 2020. Т. 162. № 3. С. 241–258.

[5] Carter J. L., Wegman M. N. Universal classes of hash functions // Journal of Computer and System Sciences. 1979. Vol. 18, № 2. P. 143–154.

# Nonlinearity of vectorial functions over finite fields with given differential uniformity

**Ryabov Vladimir**

NP "GST", e-mail: 4vryabov@gmail.com

Let $\mathbf{F}_q$ denote a finite field of $q$ elements, where $q = p^m$, $p$ is a prime number, $m$ is a natural number, and $\mathbf{F}_q^n$ is an $n$-dimensional vector space over the field $\mathbf{F}_q$, where $n$ is a natural number. Denote by $P_q^{n,k}$ the set of mappings from the $n$-dimensional space $\mathbf{F}_q^n$ to the $k$-dimensional space $\mathbf{F}_q^k$. In what follows, such mappings will be called vectorial functions. The subset of vectorial functions from $P_q^{n,k}$ formed by homomorphisms of the Abelian group of the space $\mathbf{F}_q^n$ into the Abelian group of the space $\mathbf{F}_q^k$ with a shift of the space $\mathbf{F}_q^k$ is denoted by $G_q^{n,k}$.

Any vectorial function is uniquely determined by an ordered set of its coordinate functions. In turn, each coordinate function can be represented by a polynomial over the field $\mathbf{F}_q$. For a vectorial function $F$, its algebraic degree of nonlinearity $deg\ F$ is defined as the maximum degree of the polynomials of its coordinate functions. When condition $deg\ F \leqslant 1$ is satisfied, the mapping $F$ is called affine. Denote by $A_q^{n,k}$ the subset of affine mappings from $P_q^{n,k}$. There is an inclusion $A_q^{n,k} \subseteq G_q^{n,k}$, which becomes an equality in the case of a simple field.

One of the characteristics of a vectorial function is differential spectrum. This spectrum is formed by the cardinalities of subsets of arguments for which the directional derivative satisfies the condition $D_\alpha F(x) = F(x \oplus \alpha) \ominus F(x) = \beta$, where $\alpha \in \mathbf{F}_q^n \backslash 0$, $\beta \in \mathbf{F}_q^k$, $\oplus$ is the addition operation in $\mathbf{F}_q^n$, and $\ominus$ is the subtraction operation in $\mathbf{F}_q^k$. An important indicator of the differential spectrum is the value

$$\triangle_F = \max_{\alpha \in \mathbf{F}_q^n \backslash 0,\ \beta \in \mathbf{F}_q^k} card\ \{x \mid D_\alpha F(x) = \beta\}, \tag{1}$$

From (1) it follows that the bounds are valid: $q^{n-k} \leqslant \triangle_F \leqslant q^n$. The upper bound is reached, in particular, for $F \in G_q^{n,k}$, and the lower bound is reached for the so-called perfect nonlinear (PN) functions.

**Definition 1.** *A vectorial function $F \in P_q^{n,k}$ for which the inequality $\triangle_F \leqslant \delta$ holds is called* differentially $\delta$-uniform [1].

For $k = n$, in the case of a field of odd characteristic, the PN functions are differentially 1-uniform. In the case of a field of even characteristic, all elements of the differential spectrum are even and, accordingly, $\triangle_F \geqslant 2$. In this case, differentially 2-uniform functions were called almost perfect nonlinear (APN) functions.

To determine the nonlinearity of a vectorial function $F \in P_q^{n,k}$, here we use the classical Hamming distance in the space of values of all mappings from $P_q^{n,k}$, represented as $\mathbf{F}_{q^k}^{q^n}$. Denote it by $\rho$, and introduce two indicators, namely:

$$NG_F = \min_{G \in G_q^{n,k}} \rho(F, G) \tag{2}$$

and

$$NA_F = \min_{A \in A_q^{n,k}} \rho(F, A). \tag{3}$$

From (2), (3) and the inclusion $A_q^{n,k} \subseteq G_q^{n,k}$, the inequality $NG_F \leqslant NA_F$ follows.

In article [2], the indicator $NA_F$ was called the second type of nonlinearity of vectorial Boolean functions. This nonlinearity, which characterizes the best affine approximation of a vectorial function, plays an important role in various applications of discrete mathematics and mathematical cybernetics [2, 3, 4]. With this in mind, by analogy with works [3, 4], let's give the following definition.

**Definition 2.** *For the vectorial function $F \in P_q^{n,k}$ the indicator $NA_F$ given by formula* (3) *is called* the nonlinearity.

The best lower bound on the nonlinearity of differentially $\delta$-uniform vectorial Boolean functions $F \in P_2^{n,k}$ of the form

$$NA_F \geqslant 2^n - \sqrt{(\delta + 1)2^n - \delta} \tag{4}$$

was obtained in article [5]. In the case of an arbitrary field, we prove the theorem.

**Theorem 1.** *If a vectorial function $F \in P_q^{n,k}$ is differentially $\delta$-uniform, then the following inequality holds:*

$$NG_F \geqslant q^n - \sqrt{\delta \cdot q^n - (\delta - 2^{-2})} - 2^{-1}. \tag{5}$$

*Proof.* Let's prove by contradiction, assuming that the following inequality is true $NG_F < q^n - \sqrt{\delta \cdot q^n - (\delta - 2^{-2})} - 2^{-1}$.

Consider the case of a field of odd characteristic. From relation (2), it follows that there is a mapping $G \in G_q^{n,k}$ that coincides with $F$ in $q^n - NG_F$ arguments. Let $\mathbf{C}_{F,G} = \{x \in \mathbf{F}_q^n \mid F(x) = G(x)\}$ and $C_{F,G} = card\ \mathbf{C}_{F,G}$. From the above assumption it follows that $C_{F,G} > \sqrt{\delta \cdot q^n - (\delta - 2^{-2})} + 2^{-1}$. In turn, the number of ordered pairs of elements from $\mathbf{C}_{F,G}$ satisfies the inequality $C_{F,G}(C_{F,G} - 1) > \delta \cdot (q^n - 1)$. Consequently, among all possible nonzero differences of vectors from $\mathbf{C}_{F,G}$, there are necessarily $\delta + 1$ identical ones. Let $x''_1 \ominus x'_1 = \cdots = x''_{\delta+1} \ominus x'_{\delta+1} = \alpha \neq 0$. All the vectors to be subtracted are pairwise distinct, because otherwise we would get completely matching pairs in the chain.

It remains to note that since $F$ coincides with $G$ on the set $\mathbf{C}_{F,G}$, the equalities hold: $F(x'_1 \oplus \alpha) \ominus F(x'_1) = G(x'_1 \oplus \alpha) \ominus G(x'_1)$, ... , $F(x'_{\delta+1} \oplus \alpha) \ominus F(x'_{\delta+1}) = G(x'_{\delta+1} \oplus \alpha) \ominus G(x'_{\delta+1})$, which contradicts the condition of differential $\delta$-uniformity.

In the case of a field of even characteristic, the proof is similar. Taking into account the coincidence of addition and subtraction operations, one should consider unordered pairs on the set of coincidences $F$ and $G$, the number of which is found by the formula for the number of combinations. □

**Corollary 1.** *The nonlinearity of a differentially $\delta$-uniform vectorial function $F \in P_q^{n,k}$ satisfies the inequality*

$$NA_F \geqslant q^n - \sqrt{\delta \cdot q^n - (\delta - 2^{-2})} - 2^{-1}. \tag{6}$$

For $k = n$, based on (5) and (6), we obtain the lower bounds on the indicators $NG_F$ and $NA_F$ for the PN and APN functions of the form $q^n - \sqrt{q^n - 3 \cdot 2^{-2}} - 2^{-1}$ and $q^n - \sqrt{2 \cdot q^n - 7 \cdot 2^{-2}} - 2^{-1}$, respectively. In the Boolean case, the lower bound (6) is better than the bound (4) from [5].

In work [3], an upper bound on the nonlinearity of the vectorial function $F \in P_q^{n,k}$ of the following form was obtained:

$$NA_F \leqslant (q^k - 1)q^{n-k} - q^{n/2-k}. \tag{7}$$

In the Boolean case, under condition $k > n - \log_2(n+1) + \log_2(1 + 2^{-n/2})$, the best upper bound of the form $2^n - n - 1$, presented in [5], takes place. Using arguments similar to [5], we can obtain the following statement.

**Statement 1.** *The nonlinearity of a mapping $F \in P_q^{n,k}$ satisfies the inequality*

$$NA_F \leqslant q^n - n - 1. \tag{8}$$

Combining (7) and (8) we obtain a universal upper bound on nonlinearity of the form $NA_F \leqslant \min\{(q^k - 1)q^{n-k} - q^{n/2-k},\ q^n - n - 1\}$.

**Remark.** *For small values of the parameter $\delta$, the bounds (6) and (8) define a rather narrow range for the values of the nonlinearity. The complexity of calculating $NA_F$ is $O(q^{kn+k+n})$ of additive operations in the field $\mathbf{F}_{q^k}$, while for $\triangle_F$ it is only $O(q^{2n})$. Thus, it becomes possible to draw conclusions about the behavior of the nonlinearity, significantly reducing the amount of calculations.*

## References

[1] Nyberg K. Differentially uniform mappings for cryptography // EUROCRYPT 1993. Lecture Notes in Computer Science. 1994. Vol. 765. P. 55–64.

[2] Liu J., Mesnager S., Chen L. On the nonlinearity of the second type of multi-output Boolean functions // Cryptography and Communications. 2017. Vol. 9, Iss. 1. P. 345–361.

[3] Рябов В. Г. О приближении векторных функций над конечными полями и их ограничений на линейные многообразия аффинными аналогами // Дискретная математика. 2022. Т. 34, № 2. С. 83–105.

[4] Рябов В. Г. К вопросу о приближении векторных функций над конечными полями аффинными аналогами // Математические вопросы криптографии. 2022. Т. 13, № 4. С. 125–146.

[5] Carlet C. Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions // IEEE Transactions on Information Theory. 2021. Vol. 67, iss. 12. P. 8325–8334.

# Анализ амплитудной формы квантовой хеш-функции

**Аблаев Фарид Мансурович, Васильев Александр Валерьевич**

Казанский федеральный университет,
Казанский физико-технический институт им. Е.К. Завойского, e-mail: fablayev@gmail.com, vav.kpfu@gmail.com

Основные свойства квантового криптографического хеширования были сформулированы нами в [1], а позднее в статье [2] произведен более детальный анализ взаимного влияния свойств однонаправленности и устойчивости к коллизиям и предложено более общее определение квантовой $(\delta, \varepsilon)$-устойчивой хеш-функции. Для полноты приведем здесь это определение в краткой форме.

**Определение 1.** *Пусть $\delta \in (0, 1]$ и $\varepsilon \in [0, 1)$. Для конечного множества $\mathbb{X}$ и множества ($\mathcal{H}^K$ квантовых состояний назовем отображение $\psi : \mathbb{X} \to \mathcal{H}^K$ квантовой $(\delta, \varepsilon)$-устойчивой хеш-функцией, если она обладает следующими свойствами:*

— *$\delta$-односторонность, т.е.*

$$\frac{K}{|\mathbb{X}|} \leq \delta,$$

— *$\varepsilon$-устойчивостью к коллизиям, т.е. для любой пары различных входных значений $x_1, x_2$*

$$|\langle \psi(x_1) | \psi(x_2) \rangle| \leq \varepsilon.$$

Другими словами, квантовая функция $\psi$ переводит входное значение $x \in \mathbb{X}$ в квантовое состояние $|\psi(x)\rangle$ размерности $K$. Основными свойствами такой функции являются устойчивость к инвертированию (также называемая «односторонностью» или «однонаправленностью»), которая обеспечивает малую

вероятность «извлечения» входной информации из квантового состояния, а также устойчивость к квантовым коллизиям, которая означает возможность с высокой вероятностью различать несовпадающие значения квантовой хеш-функции (квантовые хеш-коды).

### Множества с малым отклонением

Следующее понятие было введено в рассмотрение в теории групп в начале 1990-ых [3], а позднее обобщено в ряде работ (см., например, [4], [5]).

**Определение 2.** *Множество $B \subseteq \mathbb{Z}_q$ называется множеством с $\varepsilon$-отклонением ($\varepsilon$-biased) для $\mathbb{Z}_q$, если для любого $a \neq 0$ выполняется*

$$\frac{1}{|B|}\left|\sum_{b\in B} e^{i\frac{2\pi ab}{q}}\right| \leq \varepsilon.$$

Введение понятия множества с $\varepsilon$-отклонением сопровождалось предложением конструкции множества с $\varepsilon$-отклонением малой мощности и демонстрацией ряда приложений, в которых такие конструкции находят применение.

Целый ряд конструкций множеств $B$ с $\varepsilon$-отклонением с мощностями близкими к минимальным $O((\log q)/\varepsilon^2)$ предложено в работе [4] и последующих исследованиях. Возможность построения хороших квантовых хеш-функций является еще одним приложением малых по мощностям множеств с $\varepsilon$-отклонением.

### Квантовая хеш-функция в амплитудной форме

В данном разделе мы рассматриваем квантовую хеш-функцию, описанную нами в [1], а также применяем для ее построения множества с малым отклонением.

Пусть $\mathbb{X} = \mathbb{Z}_q$, $q = 2^n$. Для множества $B \subseteq \mathbb{Z}_q$, $B = \{b_i : b_i \in \mathbb{Z}_q\}$ квантовую функцию

$$_B : \mathbb{Z}_q \to \mathcal{H}^K,$$

где $K = 2^s$, $s = \log|B| + 1$, определим следующим образом. Для $w \in \mathbb{Z}_q$ полагаем

$$|\psi_B(w)\rangle = \frac{1}{\sqrt{|B|}} \sum_{i=0}^{|B|-1} |i\rangle \left(\cos\frac{2\pi b_i w}{q}|0\rangle + \sin\frac{2\pi b_i w}{q}|1\rangle\right).$$

**Теорема 1.** *Для $q > 2$, для $\varepsilon > 0$, для множества $B_\varepsilon = \{b_0, \ldots, b_{T-1}\}$ с $\varepsilon$-отклонением с $T = O\left(\frac{\log q}{\varepsilon^2}\right)$, для $s = \log T + 1 = O(\log(n) + \log(1/\varepsilon^2))$ функция*

$$\psi_{B_\varepsilon} : \mathbb{Z}_q \to \mathcal{H}^{2^s},$$

$$|\psi_{B_\varepsilon}(w)\rangle = \frac{1}{\sqrt{T}} \sum_{i=0}^{T-1} |i\rangle \left( \cos \frac{2\pi b_i w}{q} |0\rangle + \sin \frac{2\pi b_i w}{q} |1\rangle \right)$$

*является квантовой $(\delta, \varepsilon)$-устойчивой хеш-функцией с $\delta = O(c \log q/(q\varepsilon^2))$.*

*Доказательство.* Как нами было показано ранее [1], вероятность квантовых коллизий определяется величиной

$$|\langle \psi_{B_\varepsilon}(x_1) | \psi_{B_\varepsilon}(x_2) \rangle| = \frac{1}{T} \left| \sum_{j=0}^{T-1} \cos \frac{2\pi b_j (x_2 - x_1)}{q} \right|.$$

В соответствии с формулой Эйлера $\cos(2\pi b_j(x_2 - x_1)/q)$ — есть вещественная часть комплекснозначного числа $\exp(2\pi i b_j(x_2 - x_1)q)$, т.е.

$$\cos \frac{2\pi b_j (x_2 - x_1)}{q} = Re \left( e^{\frac{2\pi i b_j (x_2 - x_1)}{q}} \right).$$

Следовательно, для $|\langle \psi_{B_\varepsilon}(x_1) | \psi_{B_\varepsilon}(x_2) \rangle|$ справедлива следующая оценка:

$$\frac{1}{T} \left| \sum_{j=0}^{T-1} \cos \frac{2\pi b_j (x_2 - x_1)}{q} \right| = \frac{1}{T} \left| \sum_{j=0}^{T-1} Re \left( e^{\frac{2\pi i b_j (x_2 - x_1)}{q}} \right) \right| \leq \frac{1}{T} \left| \sum_{j=0}^{T-1} e^{\frac{2\pi i b_j (x_2 - x_1)}{q}} \right| \leq \varepsilon,$$

т.к. $B_\varepsilon$ — множество с $\varepsilon$-отклонением и $(x_2 - x_1) \neq 0$.

Далее, заметим, что по построению $\delta \leq 2|B_\varepsilon|/q = 2T/q$. Согласно [5]) мощность $T$ множества $B_\varepsilon$ может быть равна $c \log q/\varepsilon^2$ для некоторой константы $c$. Получаем, что $\delta \leq c \log q/(q\varepsilon^2)$. □

**Обсуждение.** Из теоремы 1 имеем, что для произвольного $\varepsilon > 0$ (начиная с некоторого $q$) предлагаемая конструкция квантовой хеш-функции $\psi_{B_\varepsilon}$ на основе множества $B_\varepsilon$ с $\varepsilon$-отклонением достаточно хороша. А именно, $\psi_{B_\varepsilon}$ является $\varepsilon$-устойчивой к коллизиям и является $\delta$-односторонней. Для произвольного $\varepsilon \in (0, 1)$, начиная с некоторого $q$, вероятность $\delta$ обращения функции $\psi_{B_\varepsilon}$ может быть сколь угодно малой.

**Благодарности.** Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации (тема No AAAA-A19-119011790156-3).

Список литературы

[1] Ablayev F. M., Vasiliev A. V. Cryptographic quantum hashing // Laser Physics Letters. 2014. V. 11, No. 2. P. 025202.

[2] Ablayev F., Ablayev M., Vasiliev A. On the balanced quantum hashing // Journal of Physics: Conference Series. 2016. V. 681, No. 1. P. 012019.

[3] Naor J., Naor M. Small-bias Probability Spaces: Efficient Constructions and Applications // Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing. 1990. P. 213–223.

[4] Ben-Aroya A., Ta-Shma A. Constructing Small-Bias Sets from Algebraic-Geometric Codes // FOCS '09: Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science. 2009. P. 191–197.

[5] Chen S., Moore C., Russell A. Small-Bias Sets for Nonabelian Groups // APPROX 2013, RANDOM 2013. Lecture Notes in Computer Science. 2013. V. 8096. P. 436–451.

# Описание интервала замкнутых классов $Int(S \cap T_0 \cap T_1)$ в частичной двузначной логике

**Алексеев Валерий Борисович**

МГУ имени М. В. Ломоносова, e-mail: vbalekseev@rambler.ru

Пусть $E_k = \{0, 1, \ldots, k-1\}$, $E_k^n = \{(a_1, a_2, \ldots, a_n) \mid \forall i(a_i \in E_k)\}$ и $\infty$ трактуется как неопределенность. Множество всех функций $f : E_k^n \to E_k$ ($f : E_k^n \to E_k \cup \{\infty\}$), ($n = 1, 2, \ldots$) с операцией суперпозиции называют $k$-значной логикой $P_k$ (соответственно, частичной $k$-значной логикой $P_k^*$).

Пусть $A$ — произвольный клон в $P_k$, то есть замкнутый класс, содержащий все селекторные функции. Ранее многими авторами изучался интервал $\mathcal{I}(A)$, который состоит из всех замкнутых классов в $P_k^*$, пересечение которых с $P_k$ есть в точности $A$. После долгих исследований в 2017 году была установлена мощность интервалов $\mathcal{I}(A)$ для всех клонов $A$ булевых функций [1].

Автором в [2] предложено изучать более узкие интервалы $Int(A)$, для описания которых удается по-новому использовать предикаты. Через $Int(A)$ будем обозначать множество всех замкнутых классов в $P_k^*$, содержащих $A$ и состоящих только из функций, доопределимых до какой-нибудь функции из $A$ [2]. Мощность и описание интервалов $Int(A)$ для некоторых клонов $A$ в $P_k$ представлены в работах [2-5]. В частности, из [5] и [3] следует, что семейство

$Int(A)$ в $P_2^*$ бесконечно для любого клона $A \subseteq L$, где $L$ — класс линейных булевых функций. Точная мощность $Int(L)$ пока не известна.

В докладе представлено полное описание интервала $Int(S \cap T_0 \cap T_1)$ в $P_2^*$, где $S$ — класс самодвойственных булевых функций, а $T_0$ и $T_1$ — классы булевых функций, сохраняющих 0 и 1 соответственно. Установлено, что в этом интервале содержится ровно 91 замкнутый класс.

Пусть $Pr(k)$ — множество всех предикатов на $E_k$ (то есть функций, принимающих только значения 0 и 1) от любого числа переменных. Пусть $A \subseteq P_k$, $K \subseteq Pr(k)$. Через $[K]_A$ будем обозначать замыкание множества предикатов $K$ относительно следующих операций над предикатами: 1) произвольное переименование переменных; 2) добавление и изъятие фиктивных переменных; 3) конъюнкция предикатов; 4) подстановка в предикат функций из $A$ вместо некоторых переменных.

Множество всех предикатов $1(x_1, \ldots, x_n) \equiv 1$ от любого числа переменных будем обозначать $\{1\}$. Через $Z(A)$ будем обозначать семейство всех подмножеств $K$ в $Pr(k)$, содержащих $\{1\}$ и таких, что $[K]_A = K$.

Пусть $f(x_1, \ldots, x_n) \in P_k^*$, $R(x_1, \ldots, x_n) \in Pr(k)$. Тогда через $f/R$ мы будем обозначать следующую функцию $h(x_1, \ldots, x_n) \in P_k^*$:

$$h(x_1, \ldots, x_n) = \begin{cases} f(x_1, \ldots, x_n), & \text{если } R(x_1, \ldots, x_n) = 1, \\ \infty, & \text{если } R(x_1, \ldots, x_n) = 0. \end{cases}$$

Пусть $A \subseteq P_k$, $K \subseteq Pr(k)$. Тогда положим

$$A/K = \{g \in P_k^* | \exists f \in A, \exists R \in K (g = f/R)\}.$$

Автором в [3] доказано следующее утверждение, которое сводит изучение интервала $Int(A)$ к изучению $Z(A)$.

**Теорема 1.** *Если $A$ — клон в $P_k$, то $Int(A)$ состоит из всех классов $A/K$, где $K$ пробегает все классы предикатов из $Z(A)$. При этом $A/K_1 \subset A/K_2$ тогда и только тогда, когда $K_1 \subset K_2$.*

Пусть $K_1, K_2 \subseteq Pr(k)$. Тогда положим $K_1 \cdot K_2 = \{R_1 \cdot R_2 | R_1 \in K_1, R_2 \in K_2\}$. Здесь под умножением предикатов понимается их конъюнкция. Введенная операция на семействе всех подмножеств предикатов коммутативна и ассоциативна, а также дистрибутивна относительно объединения подмножеств предикатов по любому сомножителю. Следовательно, семейство всех подмножеств предикатов с операциями объединения и умножения подмножеств образует коммутативное полукольцо.

Множество всех предикатов $0(x_1, \ldots, x_n) \equiv 0$ от любого числа переменных будем обозначать $\{0\}$. Очевидно, что $\{0\} \cdot K = \{0\}$ и $\{1\} \cdot K = K$ для любого

подмножества предикатов $K$. Можно рассматривать и произведение бесконечного числа классов, имея в виду объединение всех конечных произведений этих классов.

Класс $K$ из $Z(A)$ будем называть базисным классом для $Z(A)$, если существует такой предикат $R \in Pr(k)$, что $[R \cup \{1\}]_A = K$. Для описания $Z(A)$ мы используем следующее утверждение [4].

**Теорема 2.** *Пусть $A \subseteq P_k$. Тогда семейство $Z(A)$ состоит в точности из всех произведений (возможно бесконечных) базисных классов для $Z(A)$.*

Введем в множестве $Pr(2)$ всех предикатов на $E_2$ следующие классы предикатов: $A$ — класс всех четных предикатов, то есть, предикатов, принимающих на любых двух противоположных наборах одинаковые значения; $B$ — класс всех предикатов, у которых на каждой паре противоположных наборов хотя бы одно значение равно 0; $C$ — класс всех предикатов $Pr(2)$. Если $X$ — один из классов $A$, $B$ или $C$ и $a, b \in \{0, 1\}$, то положим

$$X_{ab} = \{p(x_1, x_2, \ldots, x_n) \in X \mid p(0, \ldots, 0) = a, p(1, \ldots, 1) = b\}.$$

**Теорема 3.** *Базисными классами для $Z(S \cap T_0 \cap T_1)$ являются только следующие 11 классов предикатов: $\{1\}, \{1\} \cup \{0\}, \{1\} \cup A_{00}, A_{11}, \{1\} \cup B_{00}, \{1\} \cup B_{01}, \{1\} \cup B_{10}, \{1\} \cup C_{00}, \{1\} \cup C_{01}, \{1\} \cup C_{10}, C_{11}$.*

Введем семейства классов предикатов $\mathcal{D}_{00} = \{\emptyset, \{0\}, A_{00}, B_{00}, A_{00} \cup B_{00}, C_{00}\}$, $\mathcal{D}_{01} = \{\emptyset, B_{01}, C_{01}\}$, $\mathcal{D}_{10} = \{\emptyset, B_{10}, C_{10}\}$, $\mathcal{D}_{11} = \{\{1\}, A_{11}, C_{11}\}$.

**Теорема 4.** *Семейство $Z(S \cap T_0 \cap T_1)$ содержит ровно 91 класс предикатов. Все они имеют вид: $X_{00} \cup X_{01} \cup X_{10} \cup X_{11}$, где $X_{00} \in \mathcal{D}_{00}$, $X_{01} \in \mathcal{D}_{01}$, $X_{10} \in \mathcal{D}_{10}$, $X_{11} \in \mathcal{D}_{11}$. При этом:*

*1) если $X_{00} \in \{\emptyset, \{0\}\}$, то либо $X_{01} = \emptyset$, либо $X_{10} = \emptyset$ (30 классов);*

*2) если $X_{00} = A_{00}$, то $X_{01} = \emptyset$, $X_{10} = \emptyset$, $X_{11} \in \{\{1\}, A_{11}\}$ (2 класса);*

*3) если $X_{00} = B_{00}$, то либо $X_{01} \neq C_{01}$, либо $X_{10} \neq C_{10}$ (24 класса);*

*4) если $X_{00} = A_{00} \cup B_{00}$, то $X_{01} \neq C_{01}$, $X_{10} \neq C_{10}$, $X_{11} \neq C_{11}$ (8 классов);*

*5) если $X_{00} = C_{00}$, то нет других ограничений (27 классов).*

Теорема 4 вместе с теоремой 1 дают полное описание $Int(S \cap T_0 \cap T_1)$.

**Теорема 5.** *В частичной двузначной логике $P_2^*$ имеется ровно 91 замкнутый класс функций, содержащий все функции из $S \cap T_0 \cap T_1$ и состоящий только из функций, доопределимых до какой-нибудь функции из $S \cap T_0 \cap T_1$. Это классы вида $(S \cap T_0 \cap T_1)/K$, где $K$ пробегает все классы предикатов из теоремы 4.*

Список литературы

[1] A solution to a problem of D. Lau: Complete classification of intervals in the lattice of partial Boolean clones / M. Couceiro, L. Haddad, K. Schoelzel, T. Waldhauser // J. Mult.-Valued Logic Soft Comput. 2017. V. 28. P. 47–58.

[2] Алексеев В. Б. О замкнутых классах в частичной $k$-значной логике, содержащих все полиномы // Дискретная математика. 2021. Т. 33, вып. 2. С. 6–19.

[3] Alekseev V. B. On some intervals of partial clones // J. Mult.-Valued Logic Soft Comput. 2022. V. 38. P. 3–22.

[4] Алексеев В. Б., Миронов М. И. Некоторые свойства интервала $Int$ в частичной $k$-значной логике // Материаалы XIV Международного семинара «Дискретная математика и ее приложения» им. академика О. Б. Лупанова (Москва, 20-25 июня 2022 г.). М. : ИПМ им. М. В. Келдыша РАН, 2022. С. 118–121. https://keldysh.ru/dms.

[5] Алексеев В. Б., Вороненко А. А. О некоторых замкнутых классах в частичной двузначной логике // Дискретная математика. 1994. Т. 6, вып. 4. С. 58–79.

# Использование методов алгебры при решении задач теории графов

**Андреева Татьяна Владимировна**[1], **Трофимов Яков Георгиевич**[2]

[1] МГТУ им. Н. Э. Баумана, e-mail: t-v-andreeva@mail.ru

[2] РУТ (МИИТ), e-mail: j.trofimov@outlook.com

В работе рассмотрен подход к решению задачи построения кратчайших путей и задачи построения гамильтоновых циклов в ориентированном графе, основанный на понятиях и методах теории полуколец.

**Основные понятия алгебры.** Алгебра $\mathcal{S} = \big(S; +, \cdot, \mathbf{0}, \mathbf{1}\big)$ называется полукольцом, если удовлетворяет следующим аксиомам:

1) $a + (b + c) = (a + b) + c$,
2) $a + b = b + a$,
3) $\mathbf{0} + a = a$,
4) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
5) $\mathbf{1} \cdot a = a \cdot \mathbf{1} = a$,
6) $a \cdot (b + c) = a \cdot b + a \cdot c$,
7) $(b + c) \cdot a = b \cdot a + c \cdot a$,
8) $\mathbf{0} \cdot a = a \cdot \mathbf{0} = \mathbf{0}$.

Полукольцо называется идемпотентным, если $a + a = a$ для любого $a$.

Полукольцо $\mathcal{S}$ называется полукольцом Конвея [1], если в нем определена унарная операция $*$ и выполняются тождества

9) $(a + b)^* = (a^* b)^* b^*$,
10) $(ab)^* = \mathbf{1} + a(ba)^* b$.

В полных полукольцах [1] операция $*$, называемая итерацией, обычно опреде-

ляется по формуле (Клини)

$$a^* = \mathbf{1} + \sum_{n \geq 1} a^n.$$

В полукольце Конвея рассмотрим уравнение $x = a \cdot x + b$. Известно [1], что одним из его решений является $x = a^* \cdot b$.

Обозначим через $M_n(S)$ множество всех квадратных матриц порядка $n$, элементы которых принадлежат множеству $S$. Если $\mathcal{S}$ является полукольцом Конвея, то и $\mathcal{M}_n(S) = \big(M_n(S); +, \cdot, \mathbb{O}_n, \mathbb{I}_n\big)$ с естественными операциями сложения и умножения матриц также является полукольцом Конвея [1].

**Разметка орграфа в полукольце.** Пусть $G = (V, E)$ — ориентированный граф (орграф), $V = \{v_1, v_2, \ldots, v_n\}$, $E \subseteq V^2$, $(v_i, v_i) \notin E$ для всех $i = 1, \ldots, n$.

Маршрут в орграфе $G$ — это последовательность вершин $v_{i_0}, v_{i_1}, \ldots, v_{i_m}$, где $(v_{i_k}, v_{i_{k+1}}) \in E$ для всех $k = 0, 1, \ldots, m-1$. Будем называть его $[v_{i_0}, v_{i_m}]$-маршрутом и обозначать $v_{i_0} \to v_{i_1} \to \ldots \to v_{i_m}$. Число $m$ называется длиной маршрута. Произвольную вершину графа будем считать маршрутом длины 0.

Пусть задана функция $\delta : E \to S$ разметки ребер орграфа $G$. Матрица меток $C(G)$ определяется следующим образом:

$$c_{ij} = \begin{cases} \delta\big((v_i, v_j)\big), & \text{если } (v_i, v_j) \in E, \\ \mathbf{0} & \text{иначе.} \end{cases}$$

В полукольце $\mathcal{S}$ метку маршрута $P = v_{i_0} \to v_{i_1} \to \ldots \to v_{i_m}$ определяют как

$$\delta(P) = \prod_{k=0}^{m-1} \delta\big((v_{i_k}, v_{i_{k+1}})\big).$$

Если $P$ — маршрут длины 0, полагают $\delta(P) = \mathbf{1}$. Имеет место [2]

**Утверждение 1.** *При $l \geq 0$ элемент $c_{ij}^{(l)}$ матрицы $C^l(G)$ равен сумме меток всех $[v_i, v_j]$-маршрутов длины $l$ в орграфе $G$.*

Здесь предполагается, что если между вершинами $v_i, v_j$ орграфа $G$ не существует маршрута, то соответствующий элемент матрицы равен $\mathbf{0}$.

В полукольце Конвея $\mathcal{M}_n\big(S\big)$ справедливо

**Утверждение 2.** *Элемент $c_{ij}^{(*)}$ матрицы $C^*(G)$ равен сумме меток всех $[v_i, v_j]$-маршрутов конечной длины в орграфе $G$.*

**Описание подхода.** Пусть $R(A)$ — множество всех регулярных языков в алфавите $A = \{a_1, a_2, \ldots, a_n\}$ [3].

Рассмотрим алгебру $(2^{A^*}; +, \cdot, \emptyset, \lambda)$, где «+» обозначает операцию объединения, «$\cdot$» — операцию произведения языков, $\lambda$ — пустое слово. Эта алгебра и ее подалгебра $\mathcal{R}(A) = \big(R(A); +, \cdot, \emptyset, \lambda\big)$ являются идемпотентными полукольцами Конвея.

Для орграфа $G = (V, E)$ определим [4] функцию $\delta : E \to R(A)$. Положим $\delta\big((v_i, v_k)\big) = a_k$. Из утверждения 2 вытекает, что элемент $c_{ik}^{(*)}$ матрицы $C^*$ является языком, состоящим из меток всех $[v_i, v_k]$-маршрутов конечной длины. Более того, по определению, каждое слово из языка $c_{ik}^{(*)}$ однозначно определяет некоторый $[v_i, v_k]$-маршрут.

**Утверждение 3.** *Если язык $c_{ii}^{(*)}$ содержит слово, являющееся перестановкой всех букв алфавита $A$, то оно соответствует гамильтонову циклу.*

**Утверждение 4.** *При $i \neq k$ в языке $c_{ik}^{(*)}$ слово наименьшей длины соответствует кратчайшему $[v_i, v_k]$-маршруту.*

Матрица $C^*$ является решением матричного уравнения $X = C \cdot X + \mathbb{I}_n$. Через $\vec{e}_{(k)}$ обозначим $k$-й столбец матрицы $\mathbb{I}_n$. Тогда векторное уравнение

$$\vec{x} = C \cdot \vec{x} + \vec{e}_{(k)} \tag{1}$$

имеет единственное решение [3, 5], которое является $k$-м столбцом матрицы $C^*$. Поскольку операция сложения идемпотентна, сумма всех столбцов матрицы $C^*$ является решением уравнения

$$\vec{x} = C \cdot \vec{x} + \sum_{k=1}^{n} \vec{e}_{(k)}. \tag{2}$$

Чтобы найти матрицу $C^*$, достаточно [5] решить уравнение (2).

Уравнения (1) и (2) можно рассматривать как системы линейных (аффинных) уравнений. Для их решения можно применять метод исключения неизвестных [3].

В работах [5, 6] описан метод решения задач о кратчайших путях (маршрутах) и о гамильтоновых циклах в орграфах. Показано, что при решении систем уравнений можно переходить не к эквивалентным системам, а к системам, имеющим более простой вид, без потери искомых решений.

**Задача о кратчайших путях.** 1) Чтобы построить все кратчайшие пути в орграфе $G$ между парой заданных вершин $v_i$ и $v_k$, достаточно рассмотреть систему уравнений (1) и найти значение неизвестной $x_i$.

2) Чтобы построить все кратчайшие пути между заданной вершиной $v_i$ и всеми остальными вершинами, достаточно рассмотреть систему (2) и найти значение неизвестной $x_i$.
3) Для построения всех кратчайших путей между всеми парами вершин орграфа необходимо найти значения всех неизвестных в системе (2).

**Задача о гамильтоновых циклах.** Чтобы построить все гамильтоновы циклы в орграфе $G$, достаточно рассмотреть систему (1) при $k = 1$ и найти значение неизвестной $x_1$.

## Список литературы

[1] Ésik Z, Kuich W. Inductive *-Semirings // Theoretical computer science. 2004. Vol. 324, issue 1. P. 3–33.

[2] Белоусов А. И., Ткачев С. Б. Дискретная математика: Учеб. для вузов / Под ред. В. С. Зарубина, А. П. Крищенко. 7-е изд. М. : Изд. МГТУ им. Н.Э. Баумана, 2021. 703 с.

[3] Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Т. 1. М. : Мир, 1978. 613 с.

[4] Кристофидес Н. Теория графов. Алгоритмический подход: Пер. с англ. М. : Мир, 1978. 432 с.

[5] Андреева Т. В., Трофимов Я. Г. Применение полуколец при решении задачи построения кратчайших путей в графе в научно-исследовательской работе // Modern European Researches. 2023. Т. 1. № 1. С. 6–17.

[6] Андреева Т. В., Трофимов Я. Г. Использование методов алгебры при решении задач теории графов в научно-исследовательской работе // Modern European Researches. 2022. Т. 1. № 3. С. 6–16.

# О функциях Шеннона длин тестов относительно локальных константных неисправностей на входах схем

**Антюфеев Григорий Валерьевич, Романов Дмитрий Сергеевич**
МГУ имени М. В. Ломоносова, e-mail: grigoriy.rus@gmail.com, romanov@cs.msu.ru

Пусть $E_2 = \{0, 1\}$, $E_2^n = \{(\alpha_1, \ldots, \alpha_n) \,|\, \alpha_i \in E_2, i = \overline{1, n}\}$. Через $P_2(n)$ будем обозначать множество всех булевых функций вида $f(x_1, \ldots, x_n)$ (иначе: $f(\tilde{x}^n)$), то есть $P_2(n) = \{f(\tilde{x}^n) \,|\, f : E_2^n \to E_2\}$.

Допустим, на логическую схему (для определенности — на схему из функциональных элементов над полным базисом $B$) $S$, реализовывавшую булеву функцию $f(x_1, \ldots, x_n)$, мог до момента исследования подействовать источник неисправностей $U$, способный преобразовать схему $S$ в любую схему из

конечного содержащего исходную схему $S$ множества $H$ схем (традиционно такое множество $H$ схем восстанавливается однозначно по исходной схеме и описанию источника неисправностей полным перебором). Обычно предполагается, что источник неисправностей не вносит в схемы новые входы и выходы (то есть как сама схема $S$, так и любая схема, полученная из нее действием источника неисправностей $U$, имеют один и тот же набор входных переменных $(x_1, \ldots, x_n)$ и один выход). Тестовое исследование схемы заключается в анализе выходных значений, возникающих как реакция схемы на подачу на входы схемы входных наборов (то есть наборов значений входных переменных).

Множество $T$ входных наборов называется *проверяющим тестом* для схемы $S$ относительно источника неисправностей $U$ тогда и только тогда, когда для любой схемы $S'$ из множества $H$ справедливо: если $S'$ реализует некоторую булеву функцию $g(x_1, x_2, \ldots, x_n)$, не равную $f(x_1, x_2, \ldots, x_n)$, то найдется набор $\tilde{\alpha}$ из $T$ такой, что $f(\tilde{\alpha}) \neq g(\tilde{\alpha})$. Множество $T$ входных наборов называется *диагностическим тестом* для схемы $S$ относительно источника неисправностей $U$ тогда и только тогда, когда для любых двух схем $S_1$, $S_2$ из множества $H$ справедливо: если $S_1$ и $S_2$ реализуют неравные булевы функции $g'(x_1, x_2, \ldots, x_n)$ и $g''(x_1, x_2, \ldots, x_n)$ соответственно, то найдется набор $\tilde{\alpha}$ из $T$ такой, что $g'(\tilde{\alpha}) \neq g''(\tilde{\alpha})$. Число наборов в тесте $T$ называется длиной теста и обозначается $L(T)$. Тест минимальной длины называется минимальным. Длина минимального проверяющего (диагностического) теста для схемы $S$ относительно источника неисправностей $U$ обозначается через $L^{\mathrm{dt}}(U, S)$ ($L^{\mathrm{dn}}(U, S)$). Под длиной проверяющего (диагностического) теста для булевой функции $f$ относительно источника неисправностей $U$ понимается величина $L^{\mathrm{dt}}(U, f)$ (соответственно $L^{\mathrm{dn}}(U, f)$), равная минимуму по всем реализующим $f$ схемам из функциональных элементов $S$ над базисом $B$ величин $L^{\mathrm{dt}}(U, S)$ (соответственно $L^{\mathrm{dn}}(U, S)$). *Функцией Шеннона длины проверяющего (диагностического) теста относительно источника неисправностей* $U$ называется величина

$$L^{\mathrm{dt}}(U, n) = \max_{f \in P_2(n)} L^{\mathrm{dt}}(U, f) \text{ (соответственно } L^{\mathrm{dn}}(U, n) = \max_{f \in P_2(n)} L^{\mathrm{dn}}(U, f)).$$

Неисправности на входах схем действуют одинаково вне зависимости от реализующей функцию схемы, так что схемная реализация функции для таких неисправностей не имеет значения, важна лишь сама функция. Константные неисправности на входах схем, фактически, заключаются в подстановках произвольных булевых констант вместо переменных в булевых функциях. Константные неисправности являются классическим и, в ряде случаев, модельным классом неисправностей. В обозначениях источников константных неисправностей на входах схем будем придерживаться следующих правил. Буква $P$ показывает, что это — источник неиправностей на входах схем. Верхний индекс ‘c’ (‘lc’) указывает на произвольные константные неисправности (соответственно локальные произвольные константные неисправности, при

которых константы подставляются только вместо подряд идущих переменных) на входах схем. Верхний индекс '0' ('1') указывает на однотипные константные неисправности типа «ноль» (соответственно типа «один») на входах схем. Нижний индекс '$k$' (соответственно '$= k$') означает, что количество забитых константами переменных не больше $k$ (соответственно в точности равно $k$); отсутствие нижнего индекса символизирует произвольность числа забитых константами переменных.

Приведем обзор известных оценок функций Шеннона длин тестов относительно константных неисправностей на входах схем. Если не оговорено иное, то приведенные оценки справедливы при всех целых положительных $n$. $L^{\mathrm{dt}}(P^{\mathrm{c}}, n) \leq 2n - 4$ для $n \geq 5$ (К. Д. Вейсс [8]). $L^{\mathrm{dt}}(P^{\mathrm{c}}, n) = L^{\mathrm{dt}}(P^{\mathrm{c}}_1, n) = 2n - 2t + 1$, если $n = k^{t-1} + t$, и $L^{\mathrm{dt}}(P^{\mathrm{c}}, n) = L^{\mathrm{dt}}(P^{\mathrm{c}}_1, n) = 2n - 2t$, если $k^{t-1} + t < n \leq k^t + t$, при $k = 2$, $n \geq 136$ (В. Н. Носков [3]). Последний результат был обобщен Г. Р. Погосяном [5] на $k$-значный случай при всех $k \geq 2$ и $n \geq 1$. $L^{\mathrm{dn}}(P^{\mathrm{c}}_1, n) = 2n$ (В. Н. Носков [4]). $\log_2 L^{\mathrm{dn}}(P^{\mathrm{c}}_k, n) = k \log_2(n/k) \cdot (1 + o(1))$ при $n \to \infty$ и $k = o(n)$; $2^{\lfloor \frac{n}{2} \rfloor} - 1 \leq \leq L^{\mathrm{dn}}(P^{\mathrm{c}}, n) \leq 4(n+1)^3 \cdot 2^{0{,}773n}$, причем нижняя оценка только заявлена, а доказывается более слабая нижняя оценка для однотипных константных неисправностей (В. Н. Носков [2]). $L^{\mathrm{dn}}(P^{\mathrm{c}}, n) \geq 2^{n/2}$ при четных $n$, $L^{\mathrm{dn}}(P^{\mathrm{c}}, n) \geq \left\lfloor \frac{2\sqrt{2}}{3} \cdot 2^{n/2} \right\rfloor$ при нечетных $n$; $L^{\mathrm{dn}}(P^0, n) = L^{\mathrm{dn}}(P^1, n) > \frac{2^{n/2} \cdot \sqrt[4]{n}}{2\sqrt{n + 0{,}5 \log_2 n + 2}}$ (К. А. Попков [6]). $L^{\mathrm{dn}}(P^{\mathrm{c}}, n) \geq 2^{\lfloor n/2 \rfloor + 1} \cdot (1 + o(1))$; $\log_2 L^{\mathrm{dn}}(P^{\mathrm{lc}}_{=k}, n) = k \cdot (1 + o(1))$ при $n \to \infty$, $k = k(n) \to \infty$, $2 \leq k \leq n/2$ и $\log_2 n = o(k)$ (авторы [1, 7]).

В настоящей работе авторами продолжено исследование функций Шеннона длин тестов относительно локальных константных неисправностей фиксированной кратности на входах схем. Имеют место следующие утверждения.

**Теорема 1.** *Пусть $n$ и $k$ — целые положительные, $2 \leq k \leq n$. Тогда имеют место неравенства*

$$2 \cdot \left( \left\lfloor \frac{2 \cdot \left( n - \left\lceil \log_2 \left\lfloor \frac{2n}{k+1} \right\rfloor \right\rceil \right)}{k+1} \right\rfloor - 2 \right) \leq L^{\mathrm{dt}}(P^{\mathrm{lc}}_{=k}, n) \leq 4 \cdot \left\lceil \frac{n+2}{k+1} \right\rceil - 4.$$

**Теорема 2.** *Пусть $n$ и $k$ — целые положительные, $c > 1$ — действительная константа, $2 \leq k \leq \frac{n}{2c}$. Тогда имеют место неравенства*

$$(n - 2k + 3 - \lceil \log_2(n - k + 1) \rceil) \cdot 2^{k-2} - 1 \leq L^{\mathrm{dg}}(P^{\mathrm{lc}}_{=k}, n) \leq (n - k + 1) \cdot 2^k.$$

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной

математики по соглашению № 075-15-2022-284. Публикация полной версии статьи планируется в журнале «Математические заметки».

Список литературы

[1] Антюфеев Г. В., Романов Д. С. Об оценках функции Шеннона длины диагностического теста при локальных константных неисправностях на входах схем // Вопросы радиоэлектроники. Серия ЭВТ. 2016. Вып. 7. С. 49–51.

[2] Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. Новосибирск: ИМ СО АН СССР. 1974. Вып. 26. С. 72–83.

[3] Носков В. Н. О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. Новосибирск: ИМ СО АН СССР. 1975. Вып. 27. С. 23–51.

[4] Носков В. Н. О длинах минимальных единичных диагностических тестов, контролирующих работу входов логических схем // Методы дискретного анализа в синтезе управляющих систем. Новосибирск: ИМ СО АН СССР. 1978. Вып. 32. С. 40–51.

[5] Погосян Г. Р. О сложности тестов, контролирующих работу входов логических схем. М.: ВЦ АН СССР, 1982.

[6] Попков К. А.. Нижние оценки длин полных диагностических тестов для схем и входов схем // Прикладная дискретная математика. 2016. № 4(34). С. 65–73.

[7] Antyufeev G. V., Romanov D. S. Tests with stuck-at and shift faults on circuit inputs // Computational Mathematics and Modeling. 2020. Vol. 31, iss. 4. P. 494–500.

[8] Weiss C. D. Bound of the length of terminal stuck-fault tests // IEEE Transactions on Computers. 1972. Vol. C-21, iss. 3. P. 305–309.

# О конфигурации паросочетаний графа и многограннике паросочетаний

**Болотников Алексей Игоревич**

МГУ имени М. В. Ломоносова, e-mail: bolotnikov-94@mail.ru

## Введение

Для любой конфигурации гиперплоскостей можно построить частично упорядченное множество пересечений его гиперплоскостей. С использованием функции Мёбиуса такого частично упорядоченного множества можно далее определить характеристический многочлен конфигурации гиперплоскостей.

С помощью характеристического многочлена конфигурации гиперплоскостей можно посчитать число регионов конфигурации [1]. Данный результат использовался, в частности, в одном из доказательств теоремы Стенли [2] о хроматическом многочлене графа и числе ациклических ориентаций графа.

В работе [3] задача о максимальном паросочетании для произвольного графа была представлена как задача линейного программирования. В рамках этого представления был построен многогранник паросочетаний, вершины которого соответствуют паросочетаниям исходного графа. С линейным программированием также тесно связано понятие LP-ориентаций [4].

Доклад посвящен свойствам конфигурации паросочетаний графа. В докладе будет построено взаимно-однозначное соответствие между регионами конфигурации паросочетаний и LP-ориентациями многогранника паросочетаний. Также будут рассказаны результаты о характеристическом многочлене конфигурации паросочетаний некоторых семейств графов.

## Основные определения

**Определение.** *Конфигурация гиперплоскостей — конечное множество гиперплоскостей в некотором векторном пространстве.*

**Определение.** *Регион конфигурации — связная компонента дополнения к объединению гиперплоскостей конфигурации.*

**Определение.** *Для произвольной конфигурации гиперплоскостей A следующим образом определяется частично упорядоченное множество L(A): элементы L(A) — всевозможные непустые пересечения гиперплоскостей конфигурации, частичный порядок $\leq$ таков:*

$$x \leq y \Leftrightarrow x \supseteq y.$$

**Определение.** *Характеристический многочлен пучка A определяется следующей формулой:*

$$\chi_A(t) = \sum_{x \in L(A)} \mu([0, x]) t^{dim(x)},$$

*где $\mu$ — функция Мёбиуса частично упорядоченного множества L(A).*

**Определение.** *Пусть G(V,E), |E|=n, — граф без петель и кратных ребер. Рассмотрим в пространстве $R^n$ следующие гиперплоскости: для любой последовательности ребер $(e_1, e_2, e_3, \ldots, e_k)$, образующей простой незамкнутый путь или простой цикл четной длины в графе G, берем гиперплоскость*

$$x_1 - x_2 + x_3 - \cdots + (-1)^{k-1} x_k = 0.$$

*Все такие гиперплоскости образуют некоторую конфигурацию гиперплоскостей. Данную конфигурацию гиперплоскостей назовем конфигурацией паросочетаний графа и обозначим MA(G).*

**Основные результаты**

**Теорема.** *Пусть G(V,E), |E|=n - граф без петель и кратных ребер. Выберем произвольный регион пучка $MA(G)$ и выберем два вектора из этого региона. Для каждого вектора рассмотрим задачу о максимальном паросочетании в графе G с этим вектором в качестве вектора весов на ребрах. Эти две задачи имеют одно и то же единственное решение, т. е. для обоих векторов одно и то же паросочетание, и только оно, будет иметь наибольший вес. Кроме того, $MA(G)$ как множество гиперплоскостей является подмножеством любой конфигурации, обладающей этим свойством.*

**Теорема.** *Пусть $G_1$, $G_2$ — графы без петель, кратных ребер и изолированных вершин, и $MA(G_1) = MA(G_2)$. Тогда $G_1$ и $G_2$ изоморфны, за исключением случая, когда один из графов содержит компоненту связности, изоморфную $K_3$, а другой — компоненту, изоморфную $K_{1,3}$.*

**Теорема.** *Пусть $G(V, E), |E| = n,$ — граф без петель и кратных ребер, $P(G)$ — многогранник паросочетаний G. Пусть $L(P(G))$ — множество LP-ориентаций многогранника $P(G)$. Определим отображение $F : L(P(G)) \to 2^{R^n}$ следующим образом. Для любой LP-ориентации O*

$$F(O) = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n \mid f(x_1, x_2, \ldots, x_n) =$$

$$= \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n \text{ индуцирует } O\}.$$

*Пусть $RG(MA(G))$ — множество регионов пучка паросочетаний графа G, а именно $RG(MA(G)) = \{R_1, R_2, \ldots, R_n\}$. Тогда:*

1. *$\forall O \in L(P(G))$ $F(O)$ является регионом $MA(G)$, то есть*

$$F(O) \in RG(MA(G)),$$

   *так что F можно рассматривать как отображение из $L(P(G))$ в $RG(MA(G))$.*

2. *$F : L(P(G)) \to RG(MA(G))$ является биекцией.*

**Теорема.** *Пусть G — граф без петель, кратных ребер и изолированных вершин, $G_1, G_2, \ldots, G_k$ — его компоненты связности. Тогда*

$$\chi_{MA(G)}(t) = \chi_{MA(G_1)}(t) \cdot \chi_{MA(G_2)}(t) \cdot \ldots \cdot \chi_{MA(G_k)}(t).$$

**Теорема.** *Пусть $G$ — дерево. Тогда*

$$\chi_{MA(G)}(t) = (t-1)(t-2)\dots(t-n).$$

**Теорема.** *Пусть $G_1$, $G_2$ — графы без петель и кратных ребер, причем существуют подграфы $H_1 \subset G_1, T_1 \subset G_1, H_2 \subset G_2, T_2 \subset G_2$ такие, что:*

1) $G_1 = H_1 \cup T_1, G_2 = H_2 \cup T_2$;
2) $H_1 \cap T_1 = \{u\}, H_2 \cap T_2 = \{v\}$, *где $u$ — вершина в $G_1$, $v$ — вершина в $G_2$;*
3) *существует изоморфизм из $H_1$ в $H_2$, переводящий $u$ в $v$;*
4) *$T_1$ и $T_2$ — деревья с одинаковым ненулевым количеством ребер.*

*Тогда $\chi_{MA(G_1)} = \chi_{MA(G_2)}$.*

**Теорема.** *Пусть $G$ — граф, состоящий из одного простого цикла, $n$ — количество ребер в $G$. Тогда:*

1. $\chi_{MA(G)} = (t-1)(t-n)^{n-1}$, *если $n$ — четное.*
2. $\chi_{MA(G)} = (t-1)(t-3)(t-5)\dots(t-(2k-1))\dots(t-(2n-3))(t-(n-1))$, *если $n$ — нечетное.*

## Список литературы

[1] Zaslavsky T. Facing up to Arrangements: Face-Count Formulas for Partitions of Space by Hyperplanes. Memoirs of the American Mathematical Society. 1975. Vol. 1. 102 p.

[2] Greene C., Zaslavsky T. On the interpretation of Whitney numbers through arrangements of hyperplanes, zonotopes, non-Radon partitions, and orientations of graphs // Transactions of the American Mathematical Society. 1983. Vol. 280, issue 1. P. 97–126.

[3] Edmonds J. Maximum matching and a polyhedron with 0,1-vertices // Journal of Research of the National Bureau of Standards. Section B "Mathematics and Mathematical Physics". 1965. Vol. 69B. P. 125–130.

[4] Holt F., Klee V. A proof of the strict monotone 4-step conjecture // Contemporary Mathematics. 1999. Vol. 223. P. 201–216.

# О сложности синтеза плоских автоматных схем, реализующих некоторые классы автоматных функций

**Воротников Алексей Сергеевич**

Кафедра МАТиС механико-математического факультета МГУ имени М. В. Ломоносова, e-mail: vorotnikov.lexa@yandex.ru

Впервые понятие схемы из клеточных элементов, далее так же называемой плоской схемой, было введено в работе Кравцова С. С. [1]. В работах [2, 3]

Калачев Г. В. показал, что порядок потенциала и переключательной мощности плоской схемы, реализующей булеву функцию от $n$ переменных, составляет $2^{n/2}$.

В данной работе мы будем опираться на определение, введённое автором в работе [4]. Поскольку ниже мы рассмотрим плоские автоматные схемы со входами, нам придётся рассматривать иные меры мощности.

Состоянием схемы $K$ на такте $t$ при подаче на вход строки $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ длины $l$ назовём вектор $s_K(\alpha, t) := (g_1(t), \ldots, g_h(t))$. Величину $c_K(t) := |s_K(\alpha, t) \oplus s_K(\alpha, t+1)|$ назовём *затратой энергии на переключение схемы* с такта $t$ на $t+1$.

*Переключательной мощностью* схемы $K$ на последовательности $\alpha$, назовём $W(K, \alpha) = \dfrac{1}{l} \sum\limits_{t=0}^{l-1} c_K(t, \alpha)$. *Переключательной мощностью* схемы $K$ на последовательностях длины $s$, назовём $W(K, s) = \dfrac{1}{2^s} \sum\limits_{\alpha \in E^s} W(K, \alpha)$.

*Переключательной мощностью* автомата $A$ на последовательностях длины $s$ назовём величину $W(A, s) = = \min\limits_{A_K = A} W(K, s)$, где $A_K$ — автомат, реализуемый схемой $K$.

Функцией Шеннона для переключательной мощности автоматов из класса $\mathcal{A}$ на последовательностях длины $s$ назовём $W(\mathcal{A}, s) = \max\limits_{A \in \mathcal{A}} W(A, s)$.

Рассмотрим множество бинарных корневых ориентированных от корня деревьев на $n$ вершинах $D(n)$ с минимальным путём от корня к листу длиной не меньше $\log_2 n$. Листьями ниже будем называть листья графов из $D(n)$.

Определим множество $\Gamma$ по индукции:

1. Граф $g \in D(n)$. Тогда $(g, V(g), R) \in \Gamma$, где $V(g) = \{(v, 2) \mid v$ — лист $g\}$, $R$ — корень $g$.
2. Если $(g, V^\star, R)$ принадлежит $\Gamma$, $g = (V, E)$ — граф, то разрешены следующие две операции:
   (a) Пусть граф $g' = (V', E') \in D(n)$, причём $V \cap V' = \varnothing$, $g_1 = (V \cup V', E \cup E' \cup \{(v, r)\})$, где $(v, i) \in V^\star$, причём $i > 0$ , $r \in R$. Положим $V_1^\star = (V^\star \setminus \{(v, i)\}) \cup \{(v, i-1)\} \cup V(g')$, пусть $r$ — корень $g'$, тогда $R_1 = R \cup \{r\}$, $(g_1, V_1^\star, R_1)$ принадлежит $\Gamma$.
   (b) Пусть граф $g_1 = (V, E \cup \{v, r\})$, где $(v, i) \in V^\star$, причём $i > 0$, $r \in R$. Положим $V_1^\star = (V^\star \setminus \{(v, i)\}) \cup \{(v, i-1)\}$, тогда $(g_1, V_1^\star, R)$ принадлежит $\Gamma$.

Определим $\Gamma(2^n)$.

$$\Gamma(2^n) = \{(g, V^\star, R) \mid (g, V^\star, R) \in \Gamma, g = (V, E), |V| = 2^n\}.$$

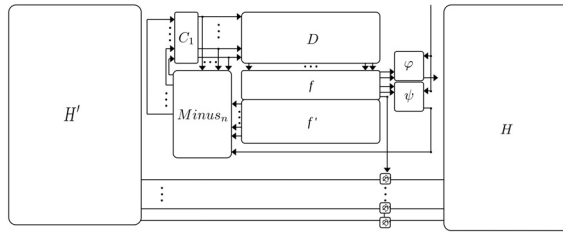


Рис. 1: Схематичное изображение плоской схемы, реализующей автомат из класса $\mathbb{A}\left(2^n, \frac{2^n}{n^{2/3}}\right)$

Определим $\Gamma(2^n, s)$. Пусть $(g, V^\star, R)$ принадлежит $\Gamma(2^n)$. После выполнения всех возможных операций 2b получим множество $\gamma_0(g, V^\star, R)$.

$\gamma(g, V^\star, R) = \{(g, V^\star, R) \mid (g', V'^\star, R') \in \gamma_0(g, V^\star, R), \forall (v, i) \in V'^\star i < 2\}$

$$\Gamma(2^n, s) = \{(g', V'^\star, R') \mid (g', V'^\star, R') \in \gamma(g, V^\star, R); (g, V^\star, R) \in \Gamma; \sum_{(v,i)\in V'^\star} i \leqslant s\}$$

Иными словами это множество графов, составленных из деревьев из $D(n)$, причём деревья связаны не более чем $s$ рёбрами, а из каждой вершины выходит хотя бы одно ребро.

Наконец, определим множество диаграмм Мура автоматов $\mathbb{A}(2^n, s)$.

1. Возьмём произвольный $(g, V^\star, R) \in \Gamma(2^n, s)$ такой, что из любой вершины выходит минимум одно ребро.
2. Нагрузим рёбра графа $g$. Если из вершины выходит только одно ребро, то нагрузим его символом $(0, 1)$, если два ребра, то одно — символом 0, другое — 1.
3. Выберем произвольную вершину и отметим её как начальную.
4. Нагрузим каждую вершину одним из символов $\{0, 1, x, \bar{x}\}$.

**Теорема 1.** *Функция Шеннона переключательной мощности плоских автоматных схем для класса* $\mathbb{A}(2^n, s)$ *по порядку не больше* $\max\left(\frac{2^{n/2}}{\log_2 n}, \frac{\sqrt{sn}}{\log_2 n}\right)$.

При доказательстве теоремы используется подсхема схемы $H$, построенной в работе [4]. Она применяется для хранения деревьев (обозначена на рисунке 1 через $H'$). Аналогичная схема, обозначенная на рисунке 1 через $H$, используется для хранения данных о переходе от дерева к дереву. Очереди $f$ и $f'$ хранят данные о текущем дереве, счётчик $C_1$ содержит информацию о номере текущего состояния, а оператор $Minus_n$ позволяет переключаться между состояниями внутри дерева.

Список литературы

[1] Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. 1967. Т. 9. С. 99–102.

[2] Калачев Г. В. Порядок мощности плоских схем, реализующих булевы функции // Дискретная математика. 2014. Т. 26, вып. 1. С. 49–74.

[3] Калачев Г. В. Нижние оценки мощности плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. Теория и приложения. 2014. Т. 18, вып. 2. С. 279–322.

[4] Воротников А. С. Верхние оценки переключательной мощности плоских схем, реализующих автономные автоматные функции // Интеллектуальные системы. Теория и приложения. 2021. Т. 25, вып. 4. С. 96–99.

# О сложности вычисления функции «Перемешанное неравенство» в классических и квантовых недетерминированных OBDD

**Гайнутдинова Аида Фаритовна**

Казанский федеральный университет, e-mail: aida.ksu@gmail.com

Ветвящаяся программа (BP — Branching Program) — известная модель для представления булевых функций. Определяется как ориентированный ациклический граф, финальные вершины которого помечены 1 и 0 (принимающие и отвергающие вершины), внутренние вершины помечены булевскими переменными из множества $X = \{x_1, \ldots, x_n\}$ и имеют по два исходящих ребра с пометками 0 и 1. Вычисление на входном наборе $\tilde{\sigma} \in \{0,1\}^n$ начинается из выделенной начальной вершины. Из каждой вершины, помеченной $x_j$, осуществляется переход по 0-ребру или по 1-ребру в соответствии со значением $\sigma_j$. Значение функции $f(\tilde{\sigma})$ — это значение достигнутой финальной вершины.

BP называется *один раз читающей*, если на любом вычислительном пути каждая переменная считывается не более одного раза. BP называется *уровневой*, если её вершины могут быть разбиты на уровни $0, 1, \ldots$ так, что $\forall i$ рёбра из вершин уровня $i$ ведут только в вершины уровня $(i+1)$. Уровневая BP называется *забывающей*, если во всех вершинах одного уровня считывается одна и та же переменная. *OBDD* (Ordered Binary Decision Diagram) — это уровневая забывающая один раз читающая BP.

*Ширина* $Width(P)$ OBDD $P$ — это максимальное число вершин на уровне.

Недетерминированная OBDD (NOBDD) допускает переходы из вершины текущего уровня в более чем одну вершину последующего уровня. NOBDD $P$ принимает вход $\tilde{\sigma} \Leftrightarrow$ существует вычислительный путь, соответствующий $\tilde{\sigma}$, завершающийся в принимающей вершине.

Квантовая OBDD (QOBDD) функционирует согласно законам квантовой механики и использует эффект квантового параллелизма. Пусть $QS$ — квантовая система с устойчивыми состояниями из множества $S$ ($|S| = d$). Чистое состояние $QS$ описывается в виде суперпозиции устойчивых состояний. Суперпозиция — это вектор нормы 1, элемент Гильбертова пространства $\mathcal{H}^d$, где $\forall\ s \in S$ сопоставлен единичный вектор, обозначаемый $|s\rangle$. Суперпозиция представляется в виде $|\psi\rangle = \sum_{s\in S} z_s|s\rangle$, где $z_s$ — комплексное число и $\sum_{s\in S}|z_s|^2 = 1$. Унитарная эволюция (изменение состояния $QS$ за определенный период времени) описывается унитарной матрицей $U$. Матрица $U$ унитарна, если $U\,U^\dagger = I$. Ортогональное измерение $QS$ описывается системой операторов $\mathcal{O} = \{P_1, \ldots, P_t\}$, действующих в $\mathcal{H}^d$ таких, что $P_i = P_i^\dagger$, $P_i^2 = P_i$, $P_iP_j = \mathbf{0}$, $\sum_{i=1}^t P_i = I$ ($i, j = 1, \ldots, t$, $i \neq j$, $t \leq d$). Если $|\psi\rangle$ — состояние $QS$ до измерения, то результатом измерения является одно из значений из множества $\{1, \ldots, t\}$. При этом: 1) $p_k = ||P_k|\psi\rangle||^2$ — вероятность того, что исходом измерения является значение $k$; 2) $|\psi'\rangle = \frac{P_k|\psi\rangle}{||P_k|\psi\rangle||}$ — состояние квантовой системы после измерения, результатом которого является значение $k$.

QOBDD $Q$ ширины $d$ и длины $l$ (использующая промежуточные измерения) определяется как

$$Q = \big(|\psi(0)\rangle, R, M, \mathcal{O}_{final}\big),$$

где $|\psi(0)\rangle$ — начальная суперпозиция; $R$ — последовательность (длины $l$) $d$-мерных унитарных преобразований $QS$ с $d$ устойчивыми состояниями:

$$R = \{\langle j_i, U_i^1(0), \ldots, U_i^{t_{i-1}}(0), U_i^1(1), \ldots, U_i^{t_{i-1}}(1)\rangle\}_{i=1}^l,$$

где $U_i^k(\sigma)$, $i = 1, \ldots, l$, $k = 1, \ldots, t_{i-1}$, $\sigma \in \{0, 1\}$ — унитарные матрицы, задающие преобразования на шаге $i$ при условии, что результат измерения шаге $i-1$ равен $k$ и значение входной переменной равно $\sigma$ ($t_{i-1}$ равно числу исходов измерения, при отсутствии измерения на предыдущем шаге $t_{i-1} = 1$); $M$ — последовательность операций промежуточного измерения $QS$:

$$M = \{\mathcal{O}_1, \ldots, \mathcal{O}_{l-1}\},$$

где $\mathcal{O}_i = \{P_1^i, \ldots, P_{t_i}^i\}$ ($i = 1, \ldots, l-1$) — система операторов, задающая измерение на $i$-м шаге (если $\mathcal{O}_i = \{I\}$, это означает, что на шаге $i$ измерение не применяется); $\mathcal{O}_{final} = \{P_{accept}, P_{reject}\}$ — система операторов, задающих финальное измерение с исходами $accept$ и $reject$, соответственно.

QOBDD $Q$ обрабатывает вход $\tilde{\sigma} = \sigma_1 \ldots \sigma_n \in \{0, 1\}^n$ следующим образом. $Q$ начинает работу в суперпозиции $|\psi(0)\rangle$ с вероятностью 1. Пусть на текущем шаге $Q$ находится в состоянии $|\psi\rangle$ с вероятностью $p$ и $k$ — результат измерения. Тогда на следующем $j$-ом шаге работы:

1. $Q$ считывает очередной символ $\sigma$ входного слова $\tilde{\sigma} \in \Sigma^n$, определяемый последовательностью $R$ преобразований программы, и преобразует текущую суперпозицию $|\psi\rangle$ в суперпозицию $|\psi'\rangle = U_j^k(\sigma)|\psi\rangle$.

2. Если $j < l$ и на шаге $j$ используется измерение, $Q$ измеряет суперпозицию $|\psi'\rangle$. Результатом является значение $k' \in \{1, \ldots, t_j\}$ с вероятностью $p_{k'} = ||P^j_{k'}|\psi'\rangle||^2$.

3. После измерения $|\psi'\rangle$ преобразуется в конфигурацию $|\psi''\rangle = \frac{P^j_{k'}|\psi'\rangle}{||P^j_{k'}|\psi'\rangle||}$.

После считывания входного набора производится финальное измерение. Если исход измерения *accept*, вход принимается, в противном случае — отвергается. $Q$ недетерминированно вычисляет функцию $f$ тогда и только тогда, когда вероятность завершить вычисление в состоянии *accept* положительна.

Известно, что порядок считывания переменных может существенным образом влиять на сложность. Так, функция "Равенство" ($EQ_{2n}(x, y) = 1 \Leftrightarrow x = y$, $x, y \in \{0,1\}^n$), вычислима OBDD ширины 3 при использовании порядка считывания $x_1, y_1, \ldots, x_n, y_n$ и требует ширины $\Omega(2^n)$ при использовании естественного порядка считывания переменных. Очевидно, что для симметрических булевых функций сложность не зависит от порядка считывания переменных, однако ширина OBDD для таких функций не более чем линейна. Для устранения зависимости сложности от порядка считывания используют различные техники построения функций. Например:

1. Сдвиги. Входной набор разделяется на две части: первая часть определяет величину циклического сдвига, который применяется к индексам второй части набора для получения окончательного порядка следования битов, от которых зависит функция.
2. Перестановки. Входной набор разделяется на две части: одна часть содержит значение перестановки, которая применяется к индексам второй части набора для получения окончательного порядка битов в последовательности, от которой зависит функция.
3. Указание принадлежности: определенные биты набора используются для явного указания, к какой части входной последовательности принадлежат соответствующие им значащие биты входа.

Функция "Перемешанное равенство" $NEQS_n$ [1] определяется на основе функции "Неравенство" ($NEQ_n(x) = 1 \Leftrightarrow x_1 \ldots\ x_{n/2} \neq x_{n/2+1} \ldots\ x_n$, $n$ — четно) с использованием приема 3). Пусть $x_1 \ldots x_n$ — переменные, от которых зависит функция, $n$ кратно 4. По входному набору $\tilde{\sigma} \in \{0,1\}^n$ формируются битовые последовательности $\alpha$, $\beta$: если $\sigma_{2i-1} = 0$, то бит $\sigma_{2i}$ дописывается к $\alpha$, в противном случае $\sigma_{2i}$ дописывается к $\beta$. Функция $NEQS_n = 1 \Leftrightarrow \alpha \neq \beta$.

В работе [1] доказан следующий результат:

**Утверждение 1.** *Функция $NEQS_n$ вычислима NOBDD ширины $O(n^4 \log n)$.*

В данной работе мы улучшаем эту оценку.

**Утверждение 2.** *Функция $NEQS_n$ вычислима NOBDD ширины $\frac{9}{8}n^2 + 3n + 3$.*

Для полноты изложения приведем нижнюю оценку.

**Утверждение 3.** *Для любого порядка считывания переменных ширина NOBDD, вычисляющей функцию $NEQS_n$, не менее $n/4$.*

Известно, что квантовые алгоритмы обладают ограничениями: унитарные преобразования являются обратимыми. Использование промежуточного измерения помогает справиться с этой проблемой.

**Утверждение 4.** *Функция $NEQS_n$ вычислима недетерминированной QOBDD, использующей промежуточные измерения, ширины $2n + 8$.*

## Список литературы

[1] Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Lobachevskii Journal of Mathematics. 2016. № 37. P. 670–682.

# Критерии правильности семейства функций

**Галатенко Алексей Владимирович, Носов Валентин Александрович, Панкратьев Антон Евгеньевич, Царегородцев Кирилл Денисович**
МГУ имени М. В. Ломоносова, e-mail: agalat@msu.ru, vnosov40@mail.ru, apankrat@intsys.msu.ru, kirill94_12@mail.ru

Правильные семейства функций, введенные В. А. Носовым в работе [1], являются удобным средством для задания больших параметрических классов перестановок, квазигрупп и $n$-квазигрупп [2, 3]. Оказалось, что в булевом случае существуют естественным образом определенные биекции между правильными семействами функций, булевыми сетями с наследственно единственной неподвижной точкой и одностоковыми ориентациями булева куба. Мы представим эквивалентные определения правильности, сформулированные в терминах различных моделей, покажем, что при переходе к логикам более высокой значности биективное соответствие между моделями не сохраняется, и обсудим свойство правильности в логиках значности больше 2.

### Критерии правильности в булевом случае

Пусть $n \in \mathbb{N}$. Обозначим множество всех $n$-местных булевых функций через $P_2^n$, множество всех двоичных наборов длины $n$ — через $E_2^n$.

**Определение 1.** *Семейство $(f_1, \ldots, f_n)$, $f_i \in P_2^n$, $i = 1, \ldots, n$, называется правильным, если для любых $\alpha, \beta \in E_2^n$, $\alpha \neq \beta$, найдется индекс $j$, такой что $\alpha_j \neq \beta_j$, но $f_j(\alpha) = f_j(\beta)$.*

**Определение 2.** *Семейство* $(f_1, \ldots, f_n)$, $f_i \in P_2^n$, $i = 1, \ldots, n$, *называется булевой сетью размера* $n$.

В работе [4] Томас предложил использовать булевы сети как модель набора генов: единица означает, что ген экспрессирует, ноль — что не экспрессирует, а функции задают правила регуляции. При анализе активности генов особую роль играют неподвижные точки булевой сети, то есть стабильные состояния. В работе [5] было введено понятие булевой сети с наследственно единственной неподвижной точкой (хотя само явление изучалось и в более ранних работах [6, 7]).

**Определение 3.** *Булева сеть* $G = (g_1, \ldots, g_{n-k})$ *является подсетью булевой сети* $F = (f_1, \ldots, f_n)$, *если существуют индексы* $1 \leq i_1 < \ldots < i_k \leq n$ *и константы* $a_1, \ldots, a_k \in E_2$, *такие что* $G$ *получается из* $F$ *подстановкой* $a_j$ *вместо* $x_{i_j}$ *и исключением функций с номерами* $i_1, \ldots, i_k$. *Для удобства будем считать, что сама сеть является своей подсетью.*

**Определение 4.** *Булева сеть* $F$ *является сетью с наследственно единственной неподвижной точкой, если для любой ее подсети* $G = (g_1, \ldots, g_k)$ *существует единственный набор* $\alpha \in E_2^k$, *такой что* $g_i(\alpha) = \alpha_i$, $i = 1, \ldots, k$.

**Определение 5.** *Пусть* $F = (f_1, \ldots, f_n)$ — *булева сеть. Наборы* $\alpha, \beta \in E_2^n$, $\alpha \neq \beta$, *называются зеркальными для* $F$, *если для любого индекса* $i$, *такого что* $\alpha_i \neq \beta_i$, *выполнено равенство* $f_i(\alpha) \oplus \alpha_i = f_i(\beta) \oplus \beta_i$.

**Теорема 1** ([6]). *Булева сеть является сетью с наследственно единственной неподвижной точкой тогда и только тогда, когда для нее не существует зеркальных наборов.*

**Следствие 1.** *Булева сеть является сетью с наследственно единственной неподвижной точкой тогда и только тогда, когда она является правильным семейством.*

Тождественность двух объектов позволяет переносить результаты, идеи и технические приемы из одной области в другую. В частности, следующее утверждение является обобщением теоремы 8 из работы [7], "переведенной" на язык правильных семейств.

**Теорема 2.** *Семейство является правильным тогда и только тогда, когда оно не содержит подсети, состоящей из самодвойственных функций.*

Булевой сети $(f_1, \ldots, f_n)$ можно поставить в соответствие асинхронный граф состояний $\Gamma$. Вершинами $\Gamma$ являются всевозможные наборы из $E_2^n$, множество ориентированных ребер задается как

$$\{\alpha \to \alpha \oplus e_i \mid i \in \{1, \ldots, n\}, f_i(\alpha) \neq \alpha_i\}, \tag{1}$$

где $e_i$ — набор с единственной единицей в позиции $i$, а сложение производится покомпонентно. В случае, если одноименная переменная фиктивна для каждой функции $f_i$ (это заведомо так для правильных семейств), можно считать, что граф Г получен из булева куба введением ориентаций на ребрах. Заметим, что соотношение (1) может быть прочитано и справа налево, что дает возможность восстановить по ориентации ребер куба булеву сеть. В дальнейшем мы будем отождествлять булев куб и граф Г.

В работе [8] в контексте решения задач оптимизации был выделен класс ориентаций ребер булева куба с единственным стоком (Unique Sink Orientation, USO).

**Определение 6.** *Граф* Г *обладает свойством USO, если в каждой грани булева куба (произвольной размерности) существует единственная вершина, являющаяся стоком.*

Из определения следует, что семейство является правильным тогда и только тогда, когда ему соответствует USO-ориентация. Благодаря этому появляется возможность при исследовании правильных семейств булевых функций пользоваться результатами из области USO-ориентаций, в частности, оценками мощности множества правильных семейств, методами порождения, утверждениями о сложности распознавания.

### Случай $k$-значной логики

При переходе от булева случая к случаю $k$-значной логики при $k > 2$ ситуация существенно усложняется. Неочевидно, как в этом случае определять свойство одностоковости ориентаций. Наличие наследственно единственной неподвижной точки становится необходимым, но не достаточным условием правильности. Критериальным свойством правильности является существование и единственность неподвижной точки у самого семейства и всех его “перекодировок”. Тем не менее, ряд результатов для булева случая удается обобщить на произвольное $k$ (например, методы порождения и утверждения о сложности).

## Список литературы

[1] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. 1998. Т. 3, № 3–4. С. 269–280.

[2] Носов В. А. Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. 1999. Т. 4, № 3–4. С. 307–320.

[3] О порождении $n$-квазигрупп с помощью правильных семейств функций / А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев // Дискретная математика. 2023. Т. 35, № 1. С. 35–53.

[4] Thomas R. Boolean formalization of genetic control circuits // Theoretical Biology. 1973. V. 42, issue 3. C. 563–585.

[5] Ruet P. Local cycles and dynamical properties of Boolean networks // Mathematical Structures in Computer Science. 2016. V. 26, issue 4. P. 702–718.

[6] Ruet P. Geometric characterization of hereditarily bijective Boolean networks // Cellular Automata. ACRI 2014. Lecture Notes in Computer Science, V. 8751. P. 536–545.

[7] Richard A. Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks // Theoretical Computer Science. 2015. V. 583. P. 1–26.

[8] Stickney A., Watson L. Digraph models of Bard-type algorithms for the linear complementarity problem // Mathematics of Operations Research. 1978. V. 3, No. 4. P. 322–333.

# О сложности задачи о доминирующем множестве для некоторых наследственных классов графов, порожденных запретами с не более чем 6 вершинами

**Дахно Григорий Сергеевич**

НИУ ВШЭ, Нижний Новгород, e-mail: dahnogrigory@yandex.ru

В настоящей работе рассматриваются только *обыкновенные графы*, т. е. неориентированные графы без петель и кратных ребер. Класс обыкновенных графов называется *наследственным*, если он замкнут относительно изоморфизма и удаления вершин. Каждый наследственный класс $\mathcal{X}$ определяется множеством $\mathcal{Y}$ своих *минимальных запрещенных порожденных подграфов*, т. е. минимальных относительно удаления вершин графов, не принадлежащих $\mathcal{X}$, это принято записывать так: $\mathcal{X} = Free(\mathcal{Y})$. Если наследственный класс задается конечным множеством своих минимальных запрещенных порожденных подграфов, то он называется *конечно определенным*.

Пусть $\Pi$ — какая-нибудь $\mathbb{NP}$-полная задача на графах. Наследственный класс с полиномиально разрешимой задачей $\Pi$ называется $\Pi$-*простым*. Наследственный класс, для которого задача $\Pi$ является $\mathbb{NP}$-полной, называется $\Pi$-*сложным*.

Наследственный класс $\mathcal{X}$ называется $\Pi$-*предельным*, если существует такая бесконечная последовательность $\mathcal{X}_1 \supseteq \mathcal{X}_2 \supseteq \dots$ из $\Pi$-сложных классов графов, что $\mathcal{X} = \bigcap\limits_{i=1}^{\infty} \mathcal{X}_i$. Минимальный по включению $\Pi$-предельный класс называется $\Pi$-*граничным*. Понятие граничного класса графов было введено

В. Е. Алексеевым в работе [1]. Значение этого понятия раскрывает следующая теорема (см. работы [1, 2]):

**Теорема 1.** *Пусть $\mathcal{X}$ — произвольный конечно определенный класс. Если $\mathcal{X}$ содержит какой-нибудь* П*-предельный класс, то он является* П*-сложным. Если $\mathcal{X}$ не содержит никакой* П*-граничный класс, то он не является* П*-сложным, иначе $\mathbb{P} = \mathbb{NP}$.*

Стоит заметить, что доказательство любого известного утверждения о том, что тот или иной класс является П-граничным, всегда использует предположение $\mathbb{P} \neq \mathbb{NP}$. Поэтому далее, говоря о граничности тех или иных классов, мы везде неявно предполагаем, что $\mathbb{P} \neq \mathbb{NP}$.

*Доминирующим множеством* графа $G = (V, E)$ называется такое подмножество $D \subseteq V$, что каждая вершина из $V \setminus D$ имеет соседа в $D$. Минимальное по мощности доминирующее множество называется *наименьшим*. Мощность наименьшего доминирующего множества графа $G$ называется его *числом доминирования* и обозначается через $\gamma(G)$. *Задача о доминирующем множестве* (кратко, *задача ДМ*) для заданных графа $G$ и числа $k$ состоит в том, чтобы проверить, выполняется ли неравенство $\gamma(G) \leq k$ или нет.

К сожалению, на настоящее время не получено полного описания совокупности ДМ-граничных классов. Тем не менее, иногда известных ДМ-граничных классов оказывается достаточно для получения полных классификаций сложности задачи ДМ в некоторых подсемействах семейства конечно определенных классов, см. работы [3, 4]. Настоящая работа продолжает работы [3, 4], в которых была получена полная сложностная дихотомия для задачи ДМ и всех наследственных классов, определяемых 5-вершинными запрещенными порожденными подграфами. В них фигурируют три класса графов $\mathcal{T}, \mathcal{D}, \mathcal{Q}$.

Класс $\mathcal{T}$ определяется как множество лесов, каждая компонента связности которых имеет не более чем три листа. Класс $\mathcal{D}$ в точности состоит из графов, являющихся реберными к графам класса $\mathcal{T}$. Класс $\mathcal{Q}$ определяется как множество порожденных подграфов (не обязательно собственных) в графах $Q(G)$, где $G \in \mathcal{T}, V(Q(G)) = V(G) \cup E(G)$ и

$$E(Q(G)) = \{xy : x, y \in V(G), x \neq y\} \cup$$
$$\{xe : x \in V(G), e \in E(G) \text{ и в графе } G \text{ вершина } x \text{ инцидентна ребру } e\}.$$

В данной работе рассматриваются два семейства, образованных классами вида $\mathcal{X}_1 = Free(\{P_5\} \cup \mathcal{Y})$ и $\mathcal{X}_2 = Free(\{fork\} \cup \mathcal{Y})$, где $\mathcal{Y}$ состоит из графов, каждый не более чем с 6 вершинами. Через $P_5$ обозначается порожденный путь на 5 вершинах, а через $fork$ обозначается результат добавления вершины к порожденному пути на 4 вершинах и ребра между добавленной вершиной и второй вершиной этого пути. Основные результаты доклада сформулированы ниже:

**Теорема 2.** *Пусть $\mathcal{Y}$ — произвольное множество графов, каждый из которых имеет не более шести вершин. Положим $\mathcal{X} = Free(\{P_5\} \cup \mathcal{Y})$. Тогда класс $\mathcal{X}$ является ДМ-сложным, если $\mathcal{Q} \subseteq \mathcal{X}$, а иначе он является ДМ-простым.*

**Теорема 3.** *Пусть $\mathcal{Y}$ — произвольное множество графов, каждый из которых имеет не более шести вершин. Положим $\mathcal{X} = Free(\{fork\} \cup \mathcal{Y})$. Тогда класс $\mathcal{X}$ является ДМ-сложным, если $\mathcal{D} \subseteq \mathcal{X}$, а иначе он является ДМ-простым.*

Теоремы 2 и 3 дают полные классификации сложности задачи ДМ в подсемействах семейства наследственных классов графов, образованных запрещенными порожденными фрагментами, каждый не более чем с 6 вершинами.

Автор выражает благодарность профессору Малышеву Д. С. за постановку задачи и внимание к работе.

Список литературы

[1] Alekseev V. E. On easy and hard hereditary classes of graphs with respect to the independent set problem // Discrete Applied Mathematics. 2004. V. 132. No 1–3. P. 17–26.

[2] NP-hard graph problems and boundary classes of graphs / V. E. Alekseev, R. Boliac, D. V. Korobitsyn, V. V. Lozin // Theoretical Computer Science. 2007. V. 389. No 1–2. P. 219–236.

[3] Malyshev D. S. A complexity dichotomy and a new boundary class for the dominating set problem // Journal of Combinatorial Optimization. 2016. V. 203. P. 226–243.

[4] Malyshev D. S. A dichotomy for the dominating set problem for classes defined by small forbidden induced subgraphs // Discrete Applied Mathematics. 2016. V. 203. P. 117–126.

[5] Földes S., Hammer P. Split graphs having Dilworth number two // Canadian Journal of Mathematics. 1977. V. 29. №. 3. P. 666–672.

# Автоматный анализ некоторых графов на выполнение свойства быть графом-кактусом

**Демидова Анна Андреевна**

Механико-математический факультет МГУ имени М. В. Ломоносова, e-mail: anna.dem98@mail.ru

Графом-кактусом является связный граф, в котором любое ребро принадлежит не более чем одному циклу, или любые два цикла могут иметь не более одной общей вершины. Графы этого класса могут использоваться для визуализации, индексации и дальнейшего сравнения геномов [1], в теории

коммуникационных сетей [2], а также в других областях. Обзор работ по обходам лабиринтов автоматами представлен в [3], а результаты из области автоматов, осуществляющих обход графов, описаны в [4].

Разница в функционировании автомата в лабиринтах и на графах заключается в том, что в первом случае в распоряжении автомата есть компас [5].

Обозначим через G класс всех связных плоских неориентированных простых графов. В данной работе сформулированы результаты исследования способностей автомата с 6 красками по определению того, является ли граф из класса G графом-кактусом.

**Теорема 1.** *Существует автомат $A_c$ с 6 красками, который сможет установить, является ли произвольный граф из класса G кактусом.*

До начала обхода все рёбра графа окрашены в серый цвет, и впоследствии автомат перекрашивает их — возможно, неоднократно. По умолчанию используется чёрная краска. Автомат устанавливает наличие цикла в ситуации, когда он только что покрасил некоторое ребро в чёрный цвет и определил, что текущей вершине инцидентно ещё одно не серое ребро [6].

Поскольку обход графа по умолчанию осуществляется по правилу левой руки, автомат до установления наличия цикла обходит подграфы, имеющие общие вершины с обнаруженным циклом и лежащие только в одной из граней, на которые этот цикл разбивает плоскость. Эти подграфы будем называть левыми ветвлениями. Единственное левое ветвление, обход которого мог быть не закончен к моменту обнаружения цикла, является первым — тем, из которого автомат попал на цикл.

После обнаружения цикла автомат должен обойти не посещённые ранее подграфы, имеющие общие вершины с обнаруженным циклом. Подграфы, лежащие в грани, которая ранее во время обхода не затрагивалась, будем называть правыми ветвлениями. В соответствии с леммой 1 для произвольного цикла наличие другого цикла, имеющего с ним общую цепочку рёбер, может быть впоследствии установлено только в них. Для обхода правых ветвлений автомат должен поменять направление движения по правилу левой руки на противоположное первоначальному.

**Лемма 1.** *Допустим, что автомат при обходе графа установил наличие цикла, у которого есть общие рёбра с другими циклами графа. Тогда эти новые циклы могут лежать только в правых ветвлениях только что обнаруженного цикла.*

Перед обходом очередного правого ветвления автомат должен поставить в текущей вершине цикла «галочку», состоящую из двух рёбер (см. рис. 1).

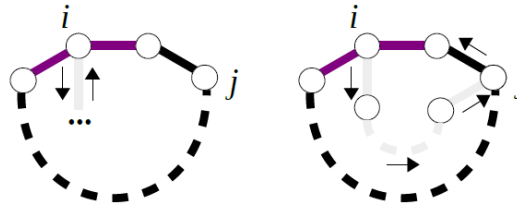


Рис. 1: Примеры обхода правых ветвлений цикла

Первая «галочка» на произвольном цикле состоит из последнего ребра, перекрашенного в чёрный цвет перед обнаружением цикла, и первого не серого ребра справа. Для остальных «галочек» в силу изменения направления движения необходимо будет выбирать уже первое не серое слева. Для первой «галочки» на первом обнаруженном цикле автомат использует красный цвет — в дальнейшем возвращение из первого левого ветвления этого цикла к данной паре рёбер будет означать окончание обхода графа-кактуса. При постановке всех остальных «галочек» автомат использует фиолетовый цвет. Кроме того, после постановки первой «галочки» на произвольном цикле автомат также должен перекрасить первое левое ребро в первом ветвлении обнаруженного цикла в определённый цвет в зависимости от его текущего цвета: чёрное ребро становится синим, фиолетовое — голубым, а серое или красное ребро цвет не меняет. Чёрные и фиолетовые рёбра перекрашиваются в разные цвета для того, чтобы при возвращении в этот подграф после завершения обхода правых ветвлений цикла можно было перекрасить это ребро обратно в соответствующий цвет.

Автомат устанавливает, что граф не является кактусом, в следующих ситуациях:

1. Автомат обнаруживает новый цикл и тут же видит ровно одно фиолетовое или красное ребро.
2. Автомат обнаруживает новый цикл, и ему негде ставить второе ребро первой «галочки», поскольку первое не серое ребро справа не является чёрным.
3. Автомат обнаруживает новый цикл, пытается поставить на нём первую «галочку», но устанавливает, что на этом цикле уже есть по крайней мере одно фиолетовое ребро.
4. Автомат ошибочно устанавливает, что очередная «галочка» является последней на некотором цикле, если при постановке фиолетового ребра первое не серое ребро слева не является чёрным, но при дальнейшем проходе по этому ребру оказывается, на самом деле цикл не был докрашен.

Автор выражает благодарность профессору Э. Э. Гасанову за постановку задачи.

Список литературы

[1] Cactus graphs for genome comparisons / B. Paten, M. Diekhans, D. Earl, J. St. John, J. Ma, B. Suh, D. Haussler // Journal of Computational Biology. 2011. Vol. 18, Iss. 3. P. 469–481.

[2] Zmazek B., Zerovnik J. Estimating the traffic on weighted cactus networks in linear time // Ninth International Conference on Information Visualisation (IV'05). 2005. P. 111–127.

[3] Кудрявцев В. Б., Килибарда Г., Ушчумлич Ш. Системы автоматов в лабиринтах // Интеллектуальные системы. 2006. Т. 10, №. 1–4. С. 449–562.

[4] Okhotin A. Graph-Walking automata: from whence they come, and whither they are bound // Implementation and Application of Automata: 24th International Conference, CIAA 2019, Košice, Slovakia, July 22–25, 2019, Proceedings 24. Springer International Publishing, 2019. P. 10–29.

[5] Blum M., Kozen D. On the power of the compass (or, why mazes are easier to search than graphs) // 19th Annual Symposium on Foundations of Computer Science (sfcs 1978). IEEE Computer Society, 1978. P. 132–142.

[6] Демидова А. А. Автоматный анализ свойств графа быть деревом и псевдодеревом // Интеллектуальные системы. Теория и приложения. 2021. Т. 25, № 2. С. 111–127.

# О сохранении неоднозначности алфавитного кодирования при автоматных неисправностях

**Дергач Пётр Сергеевич**

МГУ имени М. В. Ломоносова, e-mail: dergachpes@mail.ru

## Введение

Текст статьи является тезисами к докладу с тем же названием, подготовленному к XI Международной конференции «Дискретные модели в теории управляющих систем». В нём исследуется задача о классификации поведения автоматных языков в двухэлементном алфавите относительно сохранения свойства неоднозначности алфавитного кодирования под действием ряда неисправностей. А именно, в данной работе рассмотрены единичные неисправности искажения выходного значения на ребре. Показано, что любой регулярный язык, обладающий свойством неоднозначности относительного некоторого кодирования, может сохранить данное свойство при какой-то единичной неисправности выходного значения.

**Ключевые слова:** конечный автомат, алфавитное кодирование, единичная неисправность.

## Определения и результаты

Понятия конечного автомата, регулярного языка, диаграммы Мура и алфавитного кодирования считаются общеизвестными и здесь не приводятся. Желающие могут с ними ознакомиться в работах [1, 2].

Пусть $A$ – двухэлементный алфавит. Всюду далее будем считать, что $A = E_2 = \{0, 1\}$.

Конечную непустую последовательность слов в алфавите $A$ называем *словом.*

Слово $\alpha$ называем *измельчением* слова $\beta$, если $\beta = \alpha^n$ для некоторого натурального $n$.

Пару слов в алфавите $A$ называем *соизмеримыми,* если у них есть общее изммельчение.

Для диаграммы Мура с входным и выходным множеством $\{0, 1\}$ называем *единичной неисправностью выхода* искажение выходного значения (с 0 на 1 или наоборот) в одной из стрелок диаграммы.

Говорим, что *алфавитное кодирование неоднозначно на регулярном языке* $P \subseteq A^*$, если найдется пара различных слов в этом языке с одинаковым кодом. Также в этом случае говорим, что $P$ обладает свойством неоднозначности алфавитного кодирования на $f$.

Для произвольной диаграммы Мура с входным и выходным алфавитом $E_2$, задающей регулярный язык $P$, и произвольного алфавитного кодирования $f$, неоднозначного на $P$, говорим, что *диаграмма неоднозначна на* $f$. Также говорим, что *диаграмма слабо устойчива на* $f$, если найдется единичная неисправность выхода диаграммы такая, что новый регулярный язык по прежнему будет обладать свойством неодназначности на $f$.

**Теорема.** *Любая диаграмма Мура с входным и выходным алфавитом* $E_2$, *неоднозначная на* $f$, *является слабо устойчивой.*

## Вспомогательные результаты

**Лемма 1.** *Если алфавитное кодирование из* $E_2$ *в* $E_2$ *неоднозначно на некотором* $P \subseteq E_2^*$, *то элементарные коды* $f(0), f(1)$ *соизмеримы.*

Приводим краткую идею доказательства. Лемма доказывается индукцией по сумме длин элементарных кодов. В базе эта сумма равна 2 и эти элементарные коды обязаны совпадать. А в переходе рассматривается пара слов из

$P$ с общим кодом и первые два различных элементарных кода, с которых начинается расхождение декодирования этого кода. Более длинный элементарный код $\alpha$ обязан содержать в себе более короткий элементарный код $\beta$ в качестве префикса. И происходит замена $\alpha = \beta\alpha'$. К новой склейке из $\beta$ и $\alpha'$ применяется утверждение индукции.

**Лемма 2.** *Если $f(0) = 0^k$, $f(1) = 0^m$ для некоторых натуральных $k, m$ и в регулярном языке $P \subseteq E_2^*$ для некоторого $\gamma \in E_2^*$ есть пара несоизмерых слов $\alpha, \beta$ таких, что $\gamma\alpha^*, \gamma\beta^* \subseteq P$, то $f$ неоднозначно на $P$.*

Приводим краткую идею доказательства. Достаточно заметить, что общий префикс никак не влияет на однозначность или неоднозначность, поэтому можно рассматривать сразу множества $\alpha^*, \beta^*$. И если $f(\alpha) = 0^x$, $f(\beta) = 0^y$, то в этих множествах лежат слова $\alpha^y$ $\beta^x$ с общим кодом. И эти слова различны, так как иначе из леммы 1 мы получили бы соизмеримость $\alpha$ и $\beta$.

## Доказательство теоремы

Ввиду ограниченного объема тезисов приводим здесь лишь краткую схему доказательства.

Если хотя бы на одной из стрелок диаграммы выходная пометка равна 0, то мы можем изменить ее на 1, расширив распознаваемый диаграммой язык и тем самым сохранив свойство неоднозначности на $f$. Поэтому далее считаем, что все выходные значения на стрелках равны 1.

На начальное состояние диаграммы подается последовательность из 0. В какой-то момент состояния начнут повторяться и произойдет зацикливание с вершиной в некотором состоянии – обозначим его через $q$. Из $q$ начинаем подавать последовательность из 1. Если мы в какой-то момент посетим встречавшиеся до этого при подаче 0 состояния, то процесс заканчивается, так как мы смогли найти две петли, проходящие через $q$. Одна из петель полностью состоит из 1, а в другой есть хотя бы один 0. Значит, циклы по петлям несоизмеримы, и мы можем применить лемму 2 и вывести отсюда, что для сохранения неоднозначности достаточно не менять пометку на двух ребрах, которые лежат в наших петлях и входят в $q$. А это можно сделать, поскольку даже для случая с диаграммой Мура, имеющей всего пару ребер, утверждение теоремы верно. В самом деле, такая диаграмма состоит только из одной вершины и распознает язык $\{0, 1\}^*$; можно изменить значение на стрелке с входным значением 0, и в новом языке по-прежнему будет пара слов с общим кодом, так как этот язык содержит все слова, заканчивающиеся на 1. В частности, $0^*1$ и $1^*1$ – наличие склейки здесь очевидно. Если в диаграмме больше двух ребер, то утверждение тем более очевидно, ведь можно изменить выходное значение на каком-нибудь третьем ребре.

Разберем теперь основной случай, когда подача 1 не привела нас к посещению ранее пройденных состояний при подаче по 0. Это означает, что произошло зацикливание по 1 и образовалась новая петля. Из основного узла этой петли мы снова подадим последовательность из 0 и опять разберем два случая – мы зашли в какое-то из ранее посещенных на предыдущих этапах состояние (и тогда в дело снова вступает лемма 2 с накруткой по паре несоизмеримых петель) либо мы образовали новую петлю. В последнем случае процесс продолжается уже для новой петли. Рано или поздно новые петли образовываться перестанут, так как состояний в диаграмме конечно. Таким образом, мы все равно найдем пару пересекающихся петель и сможем применить к ним утверждение леммы 2. Теорема доказана.

## Список литературы

[1] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.

[2] Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986.

# Границы полноты и избегаемости множеств запрещённых слов и геометрия контуров графов перекрытия слов

**Евдокимов Александр Андреевич**

Институт математики им. С.Л. Соболева СО РАН, г. Новосибирск, e-mail: evdok@math.nsc.ru

Множество $S$ слов (запретов) в алфавите $A$ называется полным (или блокирующим), если любая бесконечная последовательность букв из $A$ не свободна от $S$, то есть содержит в качестве своего подслова хотя бы одно слово из $S$ [1, 2]. Аналогично определяется полнота $S$ по отношению к любому бесконечному множеству $M$ слов и $\omega$-слов (так принято называть слова бесконечной длины). $S$ полное для $M$ если $P(\omega) \cap S \neq \emptyset$ для любого $\omega$-слова из $M$, где $P(\omega)$ — множество всех подслов в $\omega$ [3]. $S$ полное для $M$ может не быть полным для $A^*$. Например $S = \{0^i, 1^i\}$ для $i > 1$ полное для $M = \{0^\infty, 1^\infty\}$, но не полно для $< 0, 1 >^*$, так как $\omega = (0, 1)^\infty \in \widehat{S}$, то есть $\omega$ свободно от $S$.

Говорят, что $M$ замкнуто, если $P(\omega) \subset M$ для любого $\omega \in M$. Легко видеть, что выполнены обычные свойства оператора замыкания.

**Теорема.** *Для любого замкнутого $M$ и произвольного $S$ справедливо:*

*a) $\widehat{S}$-замкнутое множество меры 0;*

*b) существует $\omega$-слово, такое, что $P(\omega) \subset M$;*

*c) $S$ полное для $M$ тогда и только тогда, когда $\widehat{S} \cap M$-конечное множество;*

*d*) *во всяком бесконечном $S$,полном для $M$, существует конечное $S' \subset S$ полное для $M$;*

*e*) *существует $S$ полное для $M$ такое, что для любого конечного $S' \subset S$ множество $S \setminus S'$ также полно для $M$.*

Заметим, что без свойства замкнутости множества $M$ теорема неверна.

Работа выполнена в рамках государственного задания ИМ СО РАН (проект № FWNF-2022-0018).

Список литературы

[1] Евдокимов А. А. Алгоритм распознавания полноты множества слов и динамика запретов // ПДМ. Приложение. 2016. № 9. С. 10–12.

[2] Evdokimov A. A., Kitaev S. V. Crucial words and the complexity of some extremal problems for sets of prohibited words // J. Comb. Theory. Ser. A. 2004. V. 105. P. 273–289.

# Точные алгоритмы для задачи составления расписаний с предписаниями работ на одной машине

**Захарова Юлия Викторовна**

Институт математики им. С.Л. Соболева СО РАН, e-mail: kovalenko@ofim.oscsbras.ru

## Введение

Исследуются задачи составления расписаний с предписаниями работ на одной машине. Для каждой позиции в очередности выполнения на машине задано подмножество работ, которые здесь могут выполняться. Такие условия возникают ввиду переналадок оборудования, маршрутизации машин, структурных ограничений и других факторов в многопроцессорных компьютерных и производственных системах [2, 3]. Для решения представленного класса задач в случае мощности каждого предписания не превосходящей двух предлагается два точных подхода и их приближенные варианты. Первый подход основан на переборе допустимых решений путем формирования совершенных паросочетаний в специальном двудольном графе [1]. Второй подход основан на моделях целочисленного программирования [2, 5], по разному учитывающих специфику предписаний работ в позициях машины. Оценивается применимость подходов при различных целевых критериях.

## Постановка задачи

Рассмотрим задачи составления расписаний на перестановках с предписаниями работ. Имеется множество работ $\mathcal{J}$, $|\mathcal{J}| = n$, которые необходимо выполнить

на одной машине. Прерывания выполнения работ запрещаются. Для машины задан набор позиций $N = \{1, \ldots, n\}$, где могут размещаться работы. Пусть $X^i$ есть подмножество работ, которые могут выполняться в позиции $i \in N$. Это и есть предписания работ в позициях перестановок машины. Требуется назначить работы в позиции машины с учетом предписаний так, чтобы полиномиально вычислимый регуляный критерий $F(\cdot)$ имел минимальное значение.

Числовые параметры задач:
$d_j$ — директивный срок работы $j$;
$r_j$ — момент поступления работы $j$;
$p_j$ — длительность работы $j$, $j \in \mathcal{J}$.

Обозначим через $C_j$ момент окончания работы $j \in \mathcal{J}$, тогда
$T_j = \max\{0; C_j - d_j\}$ — запаздывание для работы $j$;
$L_j = C_j - d_j$ — временное смещение для работы $j$;
$U_j = 0$, если $C_j \le d_j$, и $U_j = 1$, если $C_j > d_j$.
Рассматриваемые задачи составления расписаний на одной машине с дополнительным условием на предписания работ в позициях вершин:
$1|r_j, X^i| \sum_j C_j$;
$1|r_j, d_j, X^i| L_{\max} = \max_j\{L_j\}$;
$1|r_j, d_j, X^i| \sum_j U_j$;
$1|r_j, d_j, X^i| \sum_j T_j$.

Такие задачи возникают в случае технологических предписаний на производстве или в многопроцессорных компьютерных системах, когда на очередность выполнения работ влияют наладка оборудования, рабочие смены, структурные ограничения и другие факторы [2, 3, 5]. Также большую роль указанные задачи играют в эволюционных алгоритмах, где в операторе скрещивания решается задача оптимальной рекомбинации [3, 4], сформулированная с учетом свойства передачи генов [6].

### Алгоритм переборного типа

В данном разделе предлагается алгоритм переборного типа для варианта задачи, когда каждое предписание содержит не более двух элементов (работ). Построим двудольный граф $G = (N, \mathcal{J}, U)$ с подмножествами вершин $N$, $\mathcal{J}$ (соответствующим позициям и работам) и множеством ребер $U = \{\{i, j\} : i \in N,\ j \in X^i\}$. Всякому совершенному паросочетанию $w = \{\{1, j^1\}, \ldots, \{n, j^n\}\}$ графа $G$ можно поставить в соответствие перестановку $\pi = (j^1, \ldots, j^n)$ и наоборот.

Покажем, каким образом могут быть найдены все совершенные паросочетания двудольного графа $G$. Ребра, принадлежащие всем совершенным паросочетаниям графа $G$, будем называть *особыми*. Максимальные связные

подграфы графа $G$, содержащие не менее двух ребер, соответсвуют *циклам*. Пусть через $nc(G)$ обозначено число циклов в $G$. Особые ребра и циклы могут быть найдены за линейное время с помощью метода «поиск в глубину».

Циклы графа $G$ содержат по два совершенных паросочетания и не включают в себя особых ребер. Следовательно, всякое совершенное паросочетание в графе $G$ взаимно однозначно определяется набором совершенных паросочетаний в циклах и совокупностью особых ребер.

В результате задача составления расписаний с предписаниями вершин на одной машине может быть решена следующим образом. Формируем двудольный граф $G$, указанной ранее структуры. Вычисляем особые ребра, циклы и максимальные паросочетания в них. Перебираем совершенные паросочетания $w$ в графе $G$ (формируя их из максимальных паросочетаний в циклах и особых ребер), ставя им в соотвествие перестановки $\pi$ и вычисляя значение целевой функции $F(\pi)$. В результате находим требуемую перестановку $\pi^* \in \Pi$. Вычислительная сложность алгоритма равна $O(2^{nc(G)}T(F))$, где $nc(G) \leq \lfloor \frac{n}{2} \rfloor$, $T(F)$ — время вычисления целевой функции $F(\cdot)$ для перестановки $\pi \in \Pi$.

Как показано в [4], «почти все» системы предписаний имеют число циклов $nc(G) \leq \frac{\ln(n)}{\ln(2)}$, то есть соответствующая задача составления расписаний имеет не более $n$ допустимых решений. Опишем приведенный результат более подробно.

**Определение** ([1]). *Двудольный граф $G = (N, \mathcal{J}, U)$ будем называть «хорошим», если для него выполняется неравенство $nc(G) \leq \frac{\ln(n)}{\ln(2)}$.*

Обозначим через $\bar{\Re}_n$ множество предписаний с $n$ элементами, которые соответствуют «хорошим» двудольным графам $G$, а через $\Re_n$ — множество всех возможных предписаний с $n$ элементами. Используя результаты из [1, 4] получаем следующее утверждение.

**Теорема.** $|\bar{\Re}_n|/|\Re_n| \longrightarrow 1$ *при* $n \to \infty$.

Согласно известной терминологии (см., например, [1]), это означает, что «почти все» предписания задают задачу с не более чем $n$ допустимыми решениями, которая разрешима за время $O(nT(F))$.

В качестве приближенных аналогов предлагаются различные модификации, где просматривается не все множество допустимых решений, а случайные подмножества, построенные различными способами.

Отметим, что при предписаниях произвольной мощности допустимая перестановка работ может быть найдена за полиномиальное время посредством решения задачи о назначениях.

**Модель целочисленного линейного программирования**

Предлагается модель целочисленного линейного программирования, основанная на представлении решений с учетом назначения работ в позиции машины [2, 5].

Введем следующие переменные:

$$x_{ij} = \begin{cases} 1, & \text{если работа } j \text{ выполняется в позиции } i, \\ 0 & \text{в противном случае, } i = 1, \ldots, n,\ j \in X^i; \end{cases}$$

$C_i \geq 0$ — момент завершения работы в позиции $i$.

Обозначим через $Y^j$ подмножество позиций, в которых может выполняться работа $j \in \mathcal{J}$.

Ограничения модели записываются следующим образом:

$$\sum_{j \in X^i} x_{ij} = 1,\ i \in N, \tag{1}$$

$$\sum_{i \in Y^j} x_{ij} = 1,\ j \in \mathcal{J}, \tag{2}$$

$$C_i \geq C_{i-1} + \sum_{j \in X^i} x_{ij} p_j,\ i = 2, \ldots, n, \tag{3}$$

$$C_i \geq \sum_{j \in X^i} x_{ij} r_j + \sum_{j \in X^i} x_{ij} p_j,\ i \in N, \tag{4}$$

$$C_i \geq 0,\ i \in N, \tag{5}$$

$$x_{ij} \in \{0, 1\},\ i \in N,\ j \in X^i. \tag{6}$$

Ограничения (1)–(2) гарантируют, что каждая позиция содержит одну работу и каждая работа выполняется ровно в одной позиции. Ограничение (3) задает усвловие, что момент окончания в позиции $i$ должен быть не меньше, чем момент окончания в предшествуюшей позиции плюс длительность работы в позиции $i$. Условие (4) позволяет учесть моменты поступления работ при вычислении моментов окончания в позициях. Ограничения (5)–(6) задают область определения переменных.

Критерии формулируются так:
суммарное время завершения

$$\sum C_i = \sum_{i=1}^{n} C_i \to \min,$$

максимальное временное смещение

$$L_{\max} \to \min,$$

$$L_{\max} \geq C_i - \sum_{j \in X^i} x_{ij} d_j,\ i \in N,$$

суммарное запаздывание

$$\sum T_i = \sum_{i=1}^{n} T_i \to \min,$$

$$T_i \geq 0,\ T_i \geq C_i - \sum_{j \in X^i} x_{ij} d_j,\ i \in N,$$

число запаздывающих работ

$$\sum U_i = \sum_{i=1}^{n} U_i \to \min,$$

$$C_i \leq \sum_{j \in X^i} x_{ij} d_j + U_i \cdot BigM,\ U_i \in \{0, 1\},\ i \in N.$$

Здесь через $BigM$ обозначена достаточно большая константа.

Заметим, что представленная модель имеет $n \leq \sum_{i=1}^{n} |X^i| \leq 2n$ булевых переменных и $n$ непрерывных переменных при $|X^i| \leq 2,\ i \in N$. Однако модель может использоваться при любых системах предписаний. В литературе для задач теории расписаний также известны модели, основанные на свойстве смежности (например, [2]), но такие модели плохо адаптируются к задачам с предписаниями работ в позициях.

Для случая $|X^i| \leq 2,\ i = 1, \ldots, n$, с помощью предварительных расчетов на основе вычисления циклов и особых ребер в специальном двудольном графе из предыдущего раздела можно построить модель с меньшим числом переменных и ограничений, в частности содержащую $nc(\bar{G}) \leq \lfloor \frac{n}{2} \rfloor$ булевых переменных.

Исследование выполнено за счет гранта Российского научного фонда N 22-71-10015, https://rscf.ru/project/22-71-10015/.

## Список литературы

[1] Сердюков А. И. О задаче коммивояжера при наличии запретов // Управляемые системы. 1978. Вып. 17. С. 80–86.

[2] Blazewicz J., Dror M., Weglarz J. Mathematical programming formulations for machine scheduling: A survey // European Journal of Operational Research. 1991. Vol. 51, No 3. P. 283–300.

[3] Eremeev A., Kovalenko Y. Optimal recombination in genetic algorithms for combinatorial optimization problems. Part II // Yugoslav Journal of Operations Research. 2014. Vol. 24, No 2. P. 165–186.

[4] Eremeev A., Kovalenko Y. On solving travelling salesman problem with vertex requisitions // Yugoslav Journal of Operations Research. 2017. Vol. 27, No 4. P. 415–426.

[5] Floudas C. A., Lin X. Mixed integer linear programming in process scheduling: Modeling, algorithms, and applications // Annals of Operations Research. 2005. Vol. 139. P. 131–162.

[6] Radcliffe N. The algebra of genetic algorithms // Annals of Mathematics and Artificial Intelligence. 1994. Vol. 10, No 4. P. 339–384.

# Оптимизация квантового метода отпечатков для квантового вычислителя специфической архитектуры

**Зиннатуллин Илнар Гумарович, Хадиев Камиль Равилевич, Хадиева Алия Ихсановна**

Казанский федеральный университет, e-mail: galaxys4a@gmail.com, kamilhadi@gmail.com, AlIHadieva@kpfu.ru

В этой работе мы рассматриваем оптимизацию квантовой схемы для реализации метода квантовых отпечатков из работы [1]. Подразумевается, что схема запускается на квантовом процессоре определённой архитектуры. В данном случае под архитектурой понимается взаимосвязь кубитов. Это накладывает определенные ограничения, например, на непосредственное применение CNOT-гейта к произвольной паре кубит. Мы покажем, как решается эта проблема. Оптимизацию будем производить по числу CNOT-гейтов.

**Квантовый метод отпечатков.** Пусть $f(x_1, \ldots, x_n)$ — булева функция, а $g(x_1, \ldots, x_n)$ — характеристический многочлен над $\mathbb{Z}_m$ для функции $f$ такой, что для $x \in \{0, 1\}^n$ $g(x) = 0$, тогда и только тогда, когда $f(x) = 1$. Пусть $\delta > 0$, $t = O(\delta^{-1} \log n)$ и $K = \{k_1, \ldots, k_t \mid k_i \in \mathbb{Z}_m\}$ — набор параметров, удовлетворяющий условию $\frac{1}{t^2} \left(\sum_{i=1}^{t} \cos \frac{2\pi k_i b}{m}\right)^2 < \delta$ для всех $b \not\equiv 0 (\mod m)$.

Для $x$ квантовый отпечаток $|\psi(x)\rangle$ формируется следующим образом:

$$|\psi(x)\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \left( \cos \frac{2\pi k_i g(x)}{m} |0\rangle + \sin \frac{2\pi k_i g(x)}{m} |1\rangle \right).$$

Число используемых кубит зависит от $t$. Пусть $t = 8$. Рассмотрим квантовую схему (рис. 1) для реализации квантового метода отпечатков. Гейт

$R_y^i$ осуществляет поворот на угол $\alpha_i = \frac{4\pi k_i g(x)}{m}$ вокруг оси $y$. Схема на рис. 1 является uniformly-controlled поворотом [2].

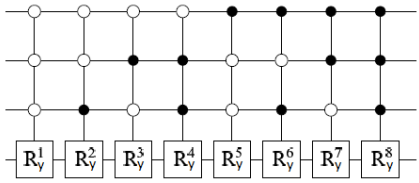


Рис. 1: Квантовая схема для случая $t = 8$

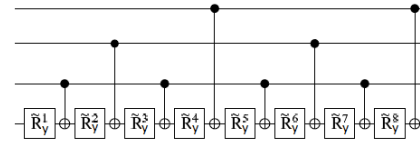


Рис. 2: Декомпозиция uniformly-controlled поворота для $t = 8$

**Декомпозиция uniformly-controlled поворотов.** В работе [2] приводится метод декомпозиции $(t+1)$-кубитного uniformly-controlled поворота в эквивалентную схему из $2^t$ однокубитных поворотов и $2^t$ CNOT-гейтов. На рис. 2 представлена декомпозиция нашей схемы. Гейт $\tilde{R}_y^i$ осуществляет поворот на некоторый угол $\beta_i$ вокруг оси $y$. Связь между углами определяется уравнением $M^k\alpha = \beta$, где $M_{ij}^k = (-1)^{(b_{i-1}\cdot\gamma_{j-1})}$, $b_{i-1}$ — двоичное представление числа $i-1$, $\gamma_{j-1}$ — $(j-1)$-ое кодовое слово Грея, $(b_{i-1}\cdot\gamma_{j-1})$ — скалярное произведение векторов $b_{i-1}$ и $\gamma_{j-1}$.

**Оптимизация квантовой схемы для определенной архитектуры.** В данной работе мы рассматриваем квантовые процессоры, предоставляемые компанией IBM. Каждый процессор характеризуется числом кубит и графом, задающим топологию, иллюстрирующим связи между кубитами. Мы используем стратегию nearest-neighbor декомпозиции [3]. Идея оптимизации схемы заключается в выборе наиболее выгодного положения (индекса) для целевого кубита. Перебирая позицию целевого кубита, считаем общее число CNOT-гейтов и делаем вывод, где целесообразнее всего его расположить.

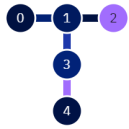


Рис. 3: Архитектура 5-кубитного процессора типа Falcon r4T


Рис. 4: Архитектура 5-кубитного процессора типа Falcon r5.11L

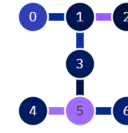


Рис. 5: Архитектура 7-кубитного процессора типа Falcon r5.11H

Были выбраны квантовые вычислители, архитектуры которых представлены на рис. 3–5. Для данных квантовых машин была реализована программа

на фреймворке qiskit [4], демонстрирующая работоспособность метода и работающая на эмуляторе реального квантового вычислителя. На рис. 6 приведена квантовая схема для реализации оператора в случае, когда мы рассматриваем архитектуру Falcon r4T и 1-м целевой кубит.

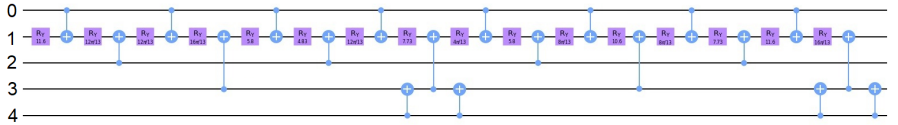


Рис. 6: Квантовая схема для реализации оператора в случае, когда мы рассматриваем архитектуру Falcon r4T и 1-м целевой кубит

| Индекс | CNOT-гейты |
|---|---|
| 0 | 48 |
| 1 | 20 |
| 2 | 52 |
| 3 | 28 |
| 4 | 44 |

Табл. 1: Результаты для вычислителя типа Falcon r4T

| Индекс | CNOT-гейты |
|---|---|
| 0 | 68 |
| 1 | 40 |
| 2 | 28 |
| 3 | 28 |
| 4 | 44 |

Табл. 2: Результаты для вычислителя типа Falcon r5.11L

| Индекс | CNOT-гейты |
|---|---|
| 0 | 324 |
| 1 | 200 |
| 2 | 332 |
| 3 | 124 |
| 4 | 156 |
| 5 | 92 |
| 6 | 156 |

Табл. 3: Результаты для вычислителя типа Falcon r5.11H

С результатами вычислительного эксперимента можно ознакомиться в табл. 1–3. Таким образом, мы можем сделать следующие выводы: для процессоров типа Falcon r4T наиболее оптимально взять в качестве целевого кубит с индексом 1, для процессоров типа Falcon r5.11L — кубит с индексом 2 или 3, а для процессоров типа Falcon r5.11H — кубит с индексом 5. Используя эти данные, можно сделать переиндексацию кубитов: целевой кубит получает индекс 0, а индексы остальных задаются в зависимости от расстояния от целевого кубита. Отметим, что таких вариантов может быть несколько. На рис. 7–9 изображены возможные варианты переиндексации кубитов.

Работа выполнена за счёт средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 0671-2020-0065.

## Список литературы

[1] Ablayev F. M., Vasiliev A. V. Algorithms for quantum branching programs based on fingerprinting // Electronic Proceedings in Theoretical Computer Science 9. 2009. P. 1–11.

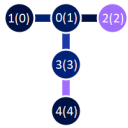


Рис. 7: Переиндексация для Falcon r4T


Рис. 8: Переиндексация для Falcon r5.11L

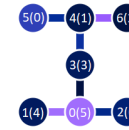


Рис. 9: Переиндексация для Falcon r5.11H

[2] Quantum circuits for general multiqubit gates / M. Möttönen, J. J. Vartiainen, V. Bergholm, M. M. Salomaa // Physical Review Letters. 2004. V. 93, No 13. P. 130502.

[3] Quantum circuits with uniformly controlled one-qubit gates / V. Bergholm, J. J. Vartiainen, M. Möttönen, M. M. Salomaa // Physical Review A. 2005. V. 71, No 5. P. 052330.

[4] Qiskit SDK : official site. URL: `https://qiskit.org/` (дата обращения: 01.12.2023).

# О математических моделях и структурных графах теории механизмов

**Ковалёв Михаил Дмитриевич**

Кафедра дискретной математики механико-математического факультета МГУ имени М. В. Ломоносова, e-mail: `mkov@rambler.ru`

## Введение

В теории механизмов существует направление, занимающееся их структурным анализом. Исходными понятиями являются инженерные понятия звена, кинематической пары и кинематической цепи. Звеном механизма называют его часть, которую можно считать абсолютно твёрдым телом. Кинематическая пара — это соединение двух звеньев, допускающее движение одного звена относительно другого. Далее мы будем рассматривать лишь узкий класс механизмов, а именно, плоские механизмы с вращательными парами. Вращательная пара (шарнир) допускает вращение одного звена, которое мы можем мыслить как фигуру в плоскости, относительно смежного ему звена. Кинематической цепью называют позволяющее передавать движение соединение звеньев кинематическими парами.

Понятие кинематической цепи хорошо работало при анализе применяющихся на практике несложных механизмов. Однако, для анализа строения сложных механизмов начало использоваться понятие графа. Традиционно, это граф Г, получаемый сопоставлением звеньям механизма вершин, а кинематическим парам — рёбер [1, 2, 3]. Однако оказалось, что уже в случае

плоских механизмов с совмещёнными шарнирами граф Γ не несёт полной информации о строении.

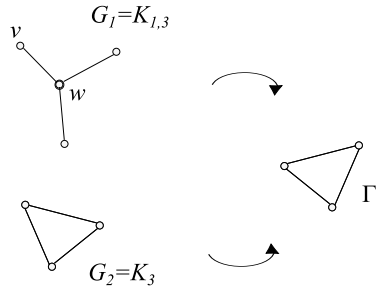


Рис. 1: Механизму с совмещённым шарниром $w$, то есть надетыми на одну ось тремя звеньями, и недеформируемому треугольнику, изображённым слева, отвечает один и тот же граф Γ

Поэтому предпринимаются попытки [1, 2] видоизменить граф Γ. Однако, эти попытки проводятся без привязки структурного графа к чётко определённой математической модели механизма. Так в работе [1] в качестве примера структурного графа механизма приводится модифицированный граф $\Gamma'$, могущий содержать петли и кратные рёбра. Но петля в $\Gamma'$ означает соединение звена кинематической парой с самим собой, чего не бывает в реальных механизмах. Двойное ребро в случае плоского шарнирного механизма влечёт жёсткое соединение по существу в одно звено двух звеньев.

Чтобы примение теорию графов к анализу строения механизмов наполнилось содержанием, необходимо структурный граф соотносить математической модели механизма. Мы определим две модели плоских механизмов с вращательными парами и проанализируем описание их строения различными графами. Также будет сформулирован один важный для приложений вопрос.

### Шарнирно-рычажные механизмы

Это плоские конструкции, составленные из прямолинейных жёстких стержней (*рычагов*), соединённых шарнирами в их концах. Если в шарнире соединены лишь два рычага, — то этому шарниру отвечает обычная вращательная пара. Мы называем такой шарнир *1-шарниром*. Если в шарнире соединены $k > 2$ рычагов, то это так называемый совмещённый шарнир с одним общим центром вращения для всех $k$ рычагов. Его мы назовём $(k-1)$-*шарниром*. В этом шарнире каждый из $k$ рычагов допускает проворачивание, независимое от остальных рычагов. Если же конец рычага не соединён ни с каким другим рычагом, то в нём нет кинематической пары, и мы его называем *0-шарниром*.

Так на рисунке 1 шарнир $v$ есть 0-шарнир, а шарнир $w$ — 2-шарнир. В теории механизмов обычно рассматривают закреплённые в плоскости (стойке) конструкции. Закрепление производится шарнирами, также допускающими полное проворачивание. В закреплённом шарнире непременно имеется хотя бы одна кинематическая пара.

Исследование структуры шарнирно-рычажных конструкций естественным образом сводится [4] к исследованию графа $G$, вершины которого отвечают шарнирам, а рёбра — рычагам конструкции. Граф $G$ мы считаем связным без петель и кратных рёбер. Более того, при наличии закреплённых шарниров, порождённый свободными шарнирами подграф графа $G$ также считаем связным. Это условие налагается, чтобы не считать одним механизмом кинематически не связанные между собой устройства. И, естественно, в $G$ нет рёбер, соединяющих вершины, отвечающие закреплённым шарнирам. Исследование же кинематики сводится к исследованию множества решений системы уравнений, накладывающих условия на расстояния между шарнирами. Эту систему удобно записать в виде квадратных уравнений:

$$(x_i - x_j)^2 + (y_i - y_j)^2 = d_{ij}, \tag{1}$$

где $(x_i, y_i)$ — декартовы координаты $i$-го шарнира $p_i$, а $d_{ij}$ — квадрат длины рычага, несущего на концах шарниры $p_i$ и $p_j$. При наличии закрепления, конфигурационное пространство механизма есть компонента связности положительной размерности множества решений этой системы. Компонентам связности нулевой размерности, то есть состоящим из одной точки, отвечают шарнирные фермы. В нашей модели допускается пересечение различных рычагов и совпадение положений несмежных шарниров.

Как показывает пример рисунка 1, описание структуры шарнирно-рычажной конструкции графом $G$ не равносильно её описанию графом Γ. Конструкция с графом $G = K_{1,3}$ при закреплении одного их её рычагов становится механизмом с двумя степенями свободы, тогда как конструкция с графом $G = K_3$ становится фермой. В случае незакреплённых конструкций граф Γ является рёберным или смежностным графом по отношению к $G$. Известна следующая теорема [5].

**Теорема 1.** *Пусть $G$ и $G_1$ — связные графы, у которых рёберные графы изоморфны. Графы $G$ и $G_1$ изоморфны всегда, кроме случая, когда один из них $K_3$, а другой $K_{1,3}$.*

Следующие утверждения непосредственно вытекают из этой теоремы [6].

**Утверждение 1.** *Если в графе $G$ связной незакреплённой шарнирно-рычажной конструкции более четырёх вершин, то он восстанавливается по графу Γ с точностью до переобозначения вершин.*

**Утверждение 2.** *В случае отсутствия совмещённых шарниров описание строения связной незакреплённой шарнирно-рычажной конструкции графом* $\Gamma$ *равносильно её описанию графом* $G$.

**Утверждение 3.** *Описание структуры связных закреплённых шарнирно-рычажных конструкций графом* $\Gamma$ *равносильно описанию их графом* $G$*, за исключением случаев, когда* $G$ *есть граф с одной закреплённой вершиной и двумя, исходящими из неё рёбрами, либо* $G$ *есть граф с двумя закреплёнными и одной свободной вершинами.*

### Модель 2. Плоские механизмы с вращательными парами.

Рассмотрим теперь плоские конструкции, составленные из связанных возможно совмещёнными шарнирами абсолютно твёрдых звеньев произвольной формы. Одно звено может содержать произвольное натуральное число пар. В этой модели мы также считаем конструкцию кинематически связанной, и допускаем возможность пересечения различных звеньев. Однако, не имеет смысла считать два звена связанными двумя различными вращательными парами. Ибо в этом случае они составят одно абсолютно твёрдое звено. Таким образом, конструкции этой модели можно сопоставить граф $\Gamma$ без кратных рёбер и, естественно, без петель. Подчеркнём, что если придерживаться нашей терминологии, то такие конструкции могут содержать $k$-шарниры с $k \geq 1$, но не содержат 0-шарниров. Каждой такой конструкции $\mathcal{K}^*$ можно сопоставить, возможно, неединственную наследующую её кинематические свойства шарнирно-рычажную конструкцию $\mathcal{K}$. При этом сопоставлении $k$-кратным ($k \geq 1$) шарнирам $\mathcal{K}^*$ отвечают не менее, чем $k$-шарниры конструкции $\mathcal{K}$, имеющие те же положения в плоскости. Звенья конструкции $\mathcal{K}^*$ мы заменяем рычагами конструкции $\mathcal{K}$, соединяющими эти шарниры так, чтобы сохранить определённость расположения шарниров в звеньях $\mathcal{K}^*$ не вводя лишних рычагов (рис. 2). Если имеется звено лишь с одним шарниром, то мы ему сопоставляем рычаг, несущий кроме этого шарнира дополнительный 0-шарнир. Если в $\mathcal{K}^*$ все звенья, содержат не более трёх шарниров, то такое сопоставление однозначно. В противном случае, конструкции $\mathcal{K}^*$ отвечает конечное число конструкций $\mathcal{K}$, и их графов $G$, которые мы будем считать эквивалентными в смысле представимости ими конструкции $\mathcal{K}^*$. В самом деле, каждая из конструкций $\mathcal{K}$ имеет те же кинематические свойства, что и конструкция $\mathcal{K}^*$. Пусть $\mathbf{G}$ — совокупность графов $G$, сопоставляемых конструкции $\mathcal{K}^*$.

Имеет место следующее утверждение.

**Утверждение 4.** *Описание структуры связных плоских конструкций с вращательными парами, но без совмещённых шарниров, графом* $\Gamma$ *равносильно её описанию произвольным графом* $G \in \mathbf{G}$.

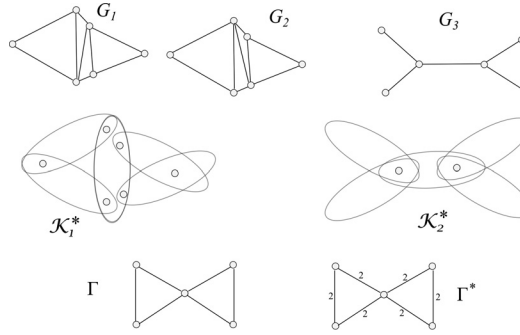


Рис. 2: Изображены две незакреплённые пятизвенные плоские конструкции $\mathcal{K}_1^*$ и $\mathcal{K}_2^*$, составленные из овальных звеньев. Конструкция $\mathcal{K}_1^*$ с простыми шарнирами неизгибаема. Конструкция $\mathcal{K}_2^*$ с совмещёнными шарнирами изгибаема с четырьмя степенями подвижности. Конструкции $\mathcal{K}_1^*$ отвечают шесть эквивалентных графов $G_i$, два из которых $G_1$ и $G_2$ изображены. Конструкции $\mathcal{K}_2^*$ отвечает неэквивалентный графам $G_1$ и $G_2$ граф $G_3$. Но обеим конструкциям отвечает один и тот же граф Γ. Сохранить сведения о совмещённых щарнирах позволяет взвешенный граф $\Gamma^*$, на рёбрах которого проставлена кратность шарниров

При наличии совмещённых шарниров описание структуры конструкции с вращательными парами графом Γ, как видно из примеров рисунка 2, теряет существенную часть информации, в отличии от описания её графом $G$.

## Основной вопрос о пространственных шарнирно-рычажных конструкциях

Для незакреплённых плоских шарнирно-рычажных конструкций известен критерий независимости уравнений системы (1):

**Теорема 2** (Поллячек-Гейрингер, Ламан)**.** *В типичном случае уравнения системы* (1) *независимы тогда и только тогда, когда для любой непустой совокупности $E$ рёбер графа $G$, с числом рёбер в ней $|E|$, число $|V|$ инцидентных им вершин удовлетворяет неравенству $|E| \leq 2|V| - 3$.*

В пространственном случае такой критерий пока не найден [7].

## Список литературы

[1] Dong K., Li D., Kong X. Representation of planar kinematic chains with multiple joints based on a modified graph and isomorphism identification // Mechanism and Machine Theory, 172, [104793]. https://doi.org/10.1016/j.mechmachtheory.2022.104793104793.

[2] Пейсах Э. Е., Нестеров В. А. Системы проектирования плоских рычажных механизмов. М.: Машиностроение. 1988.

[3] Диденко Е. В. Разработка и анализ плоских многоконтурных механизмов на основе теории графов : дис. ... канд. техн. наук : Москва, 2019. 125 с.

[4] Ковалёв М. Д. Геометрическая теория шарнирных устройств // Известия РАН. Серия математическая. 1994. Т. 58, № 1. С. 45–70.

[5] Харари Ф. Теория графов. М: Мир, 1973.

[6] Ковалёв М. Д. О структурных графах теории механизмов // Проблемы машиностроения и надёжности машин. 2023. № 1. С. 39–44.

[7] Ковалёв М. Д. Геометрические вопросы кинематики и статики. М.: Ленанд, URSS, 2019.

# О числе максимальных субпериодичностей в двоичных словах

**Колпаков Роман Максимович**

МГУ имени М. В. Ломоносова, Вычислительный центр им. А. А. Дородницына ФИЦ ИУ РАН, e-mail: roman.kolpakov@math.msu.ru

Пусть $w = w[1]w[2]\dots w[n]$ — произвольное формальное слово длины $|w| = n$. Натуральное число $p \le |w|$ называется *периодом* слова $w$, если $w[i] = w[i+p]$ для каждого $i = 1, \dots, n-p$. Мы обозначаем через $p(w)$ минимальный период слова $w$ и через $e(w)$ отношение $|w|/p(w)$, которое называется *порядком* слова $w$. Слово называется *периодическим*, если его порядок не меньше, чем 2. Вхождения периодических слов в некотором слове называются *периодичностями* в этом слове. Периодичность в некотором слове называется *максимальной*, если эта периодичность не может быть расширена в этом слове ни на один символ ни вправо, ни влево с сохранением ее минимального периода. Более строго, периодичность $r = w[i]w[i+1]...w[j]$ в слове $w$ называется *максимальной*, если она удовлетворяет следующим условиям:

1. Если $i > 1$, то $w[i-1] \ne w[i-1+p(r)]$.
2. Если $j < n$, то $w[j+1-p(r)] \ne w[j+1]$.

Известно [1–4], что в слове длины $n$ содержится $O(n)$ максимальных периодичностей. С другой стороны, нетрудно привести примеры слов длины $n$, содержащих $\Omega(n)$ максимальных периодичностей. Классическим примером слов, богатых максимальными периодичностями, являются *слова Фибоначчи*. $k$-ое слово Фибоначчи $f_k$ над двухбуквенным алфавитом $\{a, b\}$ определяется следующим рекурсивным образом: $f_0 = b$, $f_1 = a$ и $f_k = f_{k-1}f_{k-2}$ для $k \ge 2$. Длина $F_k$ слова $f_k$ является $(k+1)$-м числом Фибоначчи. В [1] показано, что слово $f_k$ содержит $2F_{k-2} - 3$ максимальных периодичностей.

Слово называется *субпериодическим* ($\delta$-*субпериодическим* для $0 < \delta < 1$), если его порядок меньше, чем 2, но больше, чем 1 (не меньше, чем $1 + \delta$). Вхождения субпериодических ($\delta$-субпериодических) слов в некотором слове называются *субпериодичностями* ($\delta$-*субпериодичностями*) в этом слове. Аналогично понятию максимальной периодичности, субпериодичность в слове называется *максимальной*, если она не может быть расширена в этом слове ни на один символ ни вправо, ни влево с сохранением ее минимального периода. Например, вхождение слова $r = ababcaba$ в слове $aababcabac$ является максимальной $\frac{3}{5}$-субпериодичностью с минимальным периодом $p(r) = 5$. В [5] было показано, что число максимальных $\delta$-субпериодичностей в слове длины $n$ не превосходит $n \ln n/\delta$. Данная оценка усилена в работах [6–8], где показано, что в слове длины $n$ содержится $O(n/\delta)$ максимальных $\delta$-субпериодичностей. С другой стороны, нетрудно показать, что в слове $w'_k = ab_1ab_2ab_3 \dots ab_ka$ содержится $\Omega(|w'_k|/\delta)$ максимальных $\delta$-субпериодичностей, тем самым максимальное возможное число максимальных $\delta$-субпериодичностей в слове длины $n$ равно $\Theta(n/\delta)$. Вместе с тем отметим, что рассмотренное слово $w'_k$ является примером слова над потенциально бесконечным алфавитом, поэтому представляет интерес построение примеров слов над конечным, в частности, двухбуквенным алфавитом, имеющих максимальное возможное число максимальных $\delta$-субпериодичностей. Отметим также, что вышеупомянутые слова Фибоначчи не являются примерами слов, богатых максимальными $\delta$-субпериодичностями.

**Утверждение 1.** *Слово $f_k$ не содержит максимальных субпериодичностей, кроме субпериодичностей $aba$ и самого слова $f_k$, как субпериодичности с минимальным периодом $F_{k-1}$.*

**Следствие 1.** *Для любого $\delta > 0$ слово $f_k$ содержит $O(|f_k|)$ максимальных $\delta$-субпериодичностей.*

Таким образом, оставался открытым вопрос о максимальном возможном числе максимальных $\delta$-субпериодичностей в словах над двухбуквенным алфавитом. В данной работе получен ответ на этот вопрос: найден пример слов над двоичным алфавитом, имеющих максимальное возможное по порядку число максимальных $\delta$-субпериодичностей. В качестве примера таких слов рассматриваются для четных $k$ слова $w''_k = 0^k(01)^{k/2}$ длины $2k$ над алфавитом $\{0, 1\}$, где через $v^k$ обозначается конкатенация $k$ копий некоторого слова $v$.

**Утверждение 2.** *Для $\delta = \frac{1}{2k}$ слово $w''_k$ содержит $\Theta(k^2) = \Theta(|w''_k|/\delta)$ максимальных $\delta$-субпериодичностей.*

Отметим, что посредством конкатенации как угодно большого числа слов $w''_k$ можно построить для $\delta = \frac{1}{2k}$ как угодно длинные слова $w$, содержащие $\Theta(|w|/\delta)$ максимальных $\delta$-субпериодичностей. Таким образом, из утверждения 2 вытекает следующий факт.

**Следствие 2.** *Для любого $\delta$ такого, что $0 < \delta \leq \frac{1}{2}$, максимальное возможное число максимальных $\delta$-субпериодичностей в словах длины $n$ над двоичным алфавитом равно $\Theta(n/\delta)$.*

## Список литературы

[1] Kolpakov R., Kucherov G. On maximal repetitions in words // Journal of Discrete Algorithms. 2000. V. 1, No 1. P. 159–186.

[2] Crochemore M., Ilie L. Maximal repetitions in strings // Journal of Computer and Systems Sciences. 2008. V. 74, No 5. P. 796–807.

[3] The "runs" theorem / H. Bannai, T. I, S. Inenaga, Y. Nakashima, M. Takeda, K. Tsuruta // SIAM Journal on Computing. 2017. V. 46, No 5. P. 1501–1514.

[4] Beyond the runs theorem / J. Fischer, S. Holub, T. I, M. Lewenstein // Lecture Notes in Computer Science. 2015. V. 9309. P. 277–286.

[5] Kolpakov R., Kucherov G. Ochem P. On maximal repetitions of arbitrary exponent // Information Processing Letters. 2010. V. 110, No 7. P. 252–256.

[6] Crochemore M., Kolpakov R., Kucherov G. Optimal Bounds for Computing $\alpha$-gapped Repeats // Lecture Notes in Computer Science. 2016. V. 9618. P. 245–255.

[7] Tighter Bounds and Optimal Algorithms for All Maximal $\alpha$-gapped Repeats and Palindromes / P. Gawrychowski, T. I, S. Inenaga, D. Köppl, F. Manea // Theory of Computing Systems. 2018. V. 62, No 1. P. 162–191.

[8] I T., Köppl D. Improved upper bounds on all maximal $\alpha$-gapped repeats and palindromes // Theoretical Computer Science. 2019. V. 753. P. 1–15.

# О сложности совместного вычисления элементов конечных абелевых групп

**Кочергин Вадим Васильевич**

МГУ имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

Пусть $G$ — конечная абелева группа (по умножению), а подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы — *базис* в группе $G$, т. е. $G$ раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества $B$:

$$G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q},$$

где $u_i$ — порядок элемента $a_i$, $i = 1, \ldots, q$.

Для элемента $g$ группы $G$ под *сложностью реализации над базисом* $B$, обозначаемой через $L(g; B)$, понимается минимальное число операций умножения,

достаточное для вычисления элемента $g$ с использованием элементов множества $B$, при этом все уже вычисленные элементы могут быть использованы многократно.

Определим функцию Шеннона $L(n)$ сложности реализации элементов абелевых групп равенством $L(n) = \max L(g, B)$, где максимум берется по всем элементам $g$ и по всем базисам $B$ всех абелевых групп порядка не более $n$.

Рост функции Шеннона $L(n)$ установлен с большой точностью — в [1] доказано, что при $n \to \infty$ справедливо равенство

$$L(n) = \log_2 n + \frac{\log_2 \log_2 n}{\log_2 n}(1 + o(1)).$$

В работах [1–4] изучались различные аспекты задачи о сложности вычисления элементов конечных абелевых групп. В данной работе формулируются результаты о сложности вычисления не одного элемента, а системы элементов конечной абелевой группы.

Для произвольного подмножества $M = \{g_1, g_2, \ldots, g_m\}$ элементов группы $G$ определим его *сложность реализации над базисом* $B$, обозначаемую через $L(M; B)$, как минимальное число операций умножения, достаточное для вычисления элементов множества $M$ с использованием элементов множества $B$.

Введем функцию Шеннона $L(n, m)$ сложности реализации систем элементов абелевых групп, положив

$$L(n, m) = \max L(M; B),$$

где максимум берется по всем абелевым группам порядка не более $n$, по всем их базисам $B$ и по всем $m$-элементным подмножествам $M$ этих групп.

**Теорема 1.** *Пусть при* $n \to \infty$ *выполняется условие* $m = m(n) = o(\log_2 \log_2 n)$. *Тогда*

$$L(n, m) \sim \log_2 n.$$

В работе [4] исследовался вопрос о возможной степени различия соответствующих величин в задаче Лупанова о сложности вычисления элементов конечной абелевой группы и задаче Беллмана о сложности вычисления нормированного одночлена от многих переменных (о задаче Беллмана подробнее см., например, [3]), который формализуется следующим образом.

Пусть $g$ — произвольный элемент конечной абелевой группы $G$, заданной своим базисом $B = \{a_1, \ldots, a_q\}$. Представление элемента $g$ в базисе $B$, имеющее вид

$$g = a_1^{n_1} a_2^{n_2} \ldots a_q^{n_q},$$

является *каноническим*, если для всех значений $j$, $1 \le j \le q$, выполняются неравенства $0 \le n_j \le u_j - 1$, где $u_j$ — порядок базисного элемента $a_j$.

Представлению элемента $g$ в базисе $B = \{a_1, \ldots, a_q\}$ конечной абелевой группы $G$ *соответствует* одночлен $x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q}$, у которого набор показателей степеней переменных в одночлене совпадает с набором показателей степеней базисных элементов в каноническом представлении элемента $g$ в базисе $B$. Одночлен, соответствующий представлению элемента $g$ в базисе $B$, обозначается через $P[g; B]$.

В [4] введена функция $\sigma(n)$, определяемая равенством $\sigma(n) = \max\{l(P[g; B]) - L(g; B)\}$, где максимум берется по всем элементам и всем базисам всех абелевых групп, имеющих порядок, не превосходящий $n$. Величина $\sigma(n)$ показывает на сколько вычисление элемента конечной абелевой группы порядка не более $n$ в каком-либо базисе этой группы может быть экономнее по сравнению с вычислением одночлена, соответствующего представлению этого элемента в выбранном базисе. В [4] установлено, что при $n \to \infty$ справедливо асимптотическое равенство

$$\sigma(n) \sim \frac{\log_2 n}{\log_2 \log_2 n}.$$

Важно отметить, что доказанная в теореме 2 работы [4] нижняя оценка величины $\sigma(n)$ ввиду использования мощностной нижней оценки для задачи Беллмана носит неконструктивный характер и не дает возможности предъявить элемент и базис конечной абелевой группы, для которых разность сложности для соответствующей задачи Беллмана и сложности этого элемента в выбранном базисе была достаточно велика. В то же время, как показано в примере из [4], при сравнении сложности реализации системы элементов конечных абелевых групп и сложности соответствующей системы одночленов ситуация может быть иной.

Формализуем эту задачу сравнения сложности реализации системы элементов конечной абелевой группы и сложности реализации соответствующей системы одночленов.

Пусть $M = \{g_1, g_2, \ldots, g_m\}$ — система элементов конечной абелевой группы, заданной своим базисом $B$. Положим

$$\hat{M} = \{P[g_1; B], P[g_2; B], \ldots, P[g_m; B]\}.$$

Обозначим через $l\left(\hat{M}\right)$ сложность реализации системы одночленов $\hat{M}$, т. е. минимально возможное число операций умножения, достаточное для получения системы $\hat{M}$ (подробнее об исследовании задачи о сложности вычисления систем одночленов, известной как задача Пиппенджера, см., например, [3]).

Наконец, положим

$$\sigma(n,m) = \max\left\{ l\left(\hat{M}\right) - L(M;B)\right\},$$

где максимум берется по всем $m$-элементным системам $M$ и всем базисам $B$ всех абелевых групп, имеющих порядок, не превосходящий $n$.

**Теорема 2.** *Пусть при* $n \to \infty$ *выполняются условия* $m \geq 2$ *и* $m(n) = o\left(\log_2 \log_2 n\right)$. *Тогда*

$$\sigma(n,m) \sim \frac{m-1}{m} \log_2 n.$$

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

Список литературы

[1] Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. 1992. Вып. 4. С. 178–217.

[2] Кочергин В. В. О некоторых мерах сложности конечных абелевых групп // Дискретная математика. 2015. Т. 27, № 3. С. 25–43.

[3] Кочергин В. В. Задачи Беллмана, Кнута, Лупанова, Пиппенджера и их вариации как обобщения задачи об аддитивных цепочках // Математические вопросы кибернетики. 2022. Вып. 20. С. 119–256.

[4] Кочергин В. В. Сравнение сложности вычисления одночленов и элементов конечных абелевых групп // Вестник Московского университета. Сер. 1. Математика. Механика. 2022. № 3. С. 6–11.

# Уточнение верхней и нижней оценок немонотонной сложности функций многозначной логики

**Кочергин Вадим Васильевич**[1], **Михайлович Анна Витальевна**[2]

[1] МГУ имени М. В. Ломоносова, e-mail: vvkoch@yandex.ru

[2] НИУ ВШЭ, e-mail: anna@mikhaylovich.com

Исследуется сложность реализации функций $k$-значной логики схемами из функциональных элементов над базисами $B$, имеющими вид:

$$B = M \cup \{\omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_k \setminus M,\ i = 1, \ldots, p, \qquad (*)$$

где $M$ — класс всех функций из $P_k$, монотонных относительно порядка

$$0 < 1 < \ldots < k-1,$$

причем функциям из множества $M$ приписан нулевой вес, а функциям $\omega_1, \ldots, \omega_p$ — единичный.

*Немонотонная сложность $I_B(S)$ схемы $S$ над базисом $B$* определяется как число немонотонных элементов схемы $S$.

Через $I_B(f)$ обозначается минимальная немонотонная сложность схем, вычисляющих над базисом $B$ функцию $k$-значной логики $f$, эту величину будем называть *немонотонной сложностью функции $f$ над базисом $B$*.

Последовательность

$$\tilde{\alpha}_1 = (\alpha_{11}, \ldots, \alpha_{1n}),\ \tilde{\alpha}_2 = (\alpha_{21}, \ldots, \alpha_{2n}),\ \ldots,\ \tilde{\alpha}_r = (\alpha_{r1}, \ldots, \alpha_{rn})$$

наборов из множества $E_k^n = \{0, 1, \ldots, k-1\}$ назовем *возрастающей цепью относительно порядка* $0 < 1 < \ldots < k-1$ или просто *цепью*, если все наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$ различны и выполняются неравенства

$$\alpha_{ij} \le \alpha_{i+1,j}, \quad i = 1, \ldots, r-1, \quad j = 1, \ldots, n.$$

Пусть $f(x_1, \ldots, x_n)$ — функция $k$-значной логики. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_k^n$, будем называть *обрывом для функции $f$*, если выполнены условия:

1) $\alpha_j \le \beta_j,\ j = 1, \ldots, n$;

2) $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Под *падением $d_C(f)$ функции $f$ на цепи $C$*, имеющей вид $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$, будем понимать число обрывов функции $f$ на парах вида $(\tilde{\alpha}_i, \tilde{\alpha}_{i+1})$.

*Спад $d(f)$* функции $f$ определим равенством $d(f) = \max d_C(f)$, где максимум берется по всем цепям $C$.

Для произвольной функции $k$-значной логики $f(x_1, x_2, \ldots, x_n)$ и произвольной цепи $C = (\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r)$ наборов из $E_k^n$ определим величину $u_C(f)$ как наибольшую длину $t$ подпоследовательности $\tilde{\beta}_1, \tilde{\beta}_2, \ldots, \tilde{\beta}_t$ последовательности $C$, удовлетворяющей условию $f(\tilde{\beta}_1) > f(\tilde{\beta}_2) > \ldots > f(\tilde{\beta}_t)$.

Определим *инверсионную силу $u(f)$ функции $f$* равенством

$$u(f) = \max u_C(f),$$

где максимум берется по всем цепям $C$ наборов из $E_k^n$.

Для базиса $B$ вида $(*)$ положим $u(B) = \max u(f)$, где максимум берется по всем функциям $f$ из базиса $B$.

Немонотонная сложность булевых функций в случае классического базиса $B_0 = \{x\&y, x \vee y, \overline{x}\}$, в котором конъюнкторы и дизъюнкторы «бесплатны» (а, значит, «бесплатны» и все монотонные функции, отличные от констант), а инверторы имеют единичную стоимость, изучалась А. А. Марковым [1], который установил точное значение немонотонной сложности, называемой

в этом случае инверсионной сложностью: для любой булевой функции $f$, отличной от константы, справедливо равенство

$$I_{B_0}(f) = \lceil \log_2(d(f)+1) \rceil .$$

В работе [2] для произвольной функции $k$-значной логики установлено точное значение немонотонной сложности над двумя естественными базисами $B_P = M \cup \{N_P(x)\}$ и $B_L = M \cup \{N_L(x)\}$, где $N_P(x)$ — отрицание Поста, т. е. функция $x+1 \pmod k$, а $N_L(x)$ — отрицание Лукасевича, т. е. функции $k-1-x$:

$$I_{B_P}(f) = \lceil \log_2(d(f)+1) \rceil , \qquad I_{B_L}(f) = \lceil \log_k(d(f)+1) \rceil .$$

В случае произвольного базиса $B$ вида $(*)$ из результатов работ [2, 3] следует, что найдется такая константа $c(B)$, что для любой функции $k$-значной логики $f$ выполняются неравенства

$$\left\lceil \log_{u(B)}(d(f)+1) \right\rceil - c(B) \le I_B(f) \le \left\lceil \log_{u(B)}(d(F)+1) \right\rceil .$$

Однако эти оценки далеки от окончательных, так как константа $c(B)$ может оказаться сколь угодно большой: для любого заданного значения $N$ найдется базис $B_N$ вида $M \cup \{h_N\}$ и функция $g_N$, для которых справедливо неравенство

$$\left\lceil \log_{u(B)}(d(g_N)+1) \right\rceil - I_{B_N}(g_N) > N.$$

В булевом случае удалось получить окончательный результат [4]: для любой булевой функции $f$ и любого базиса $B$, имеющего вид

$$B = M \cup \{\omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_2 \setminus M, \ i = 1, \ldots, p,$$

справедливо равенство

$$I_B(f) = \left\lceil \log_2 \left( \frac{d(f)}{D(B)} + 1 \right) \right\rceil ,$$

где $D(B) = \max\{d(\omega_1), \ldots, d(\omega_p)\}$.

Для случая реализации функций $k$-значной логики в работе [5] получены верхняя и нижняя оценка, отличающиеся на константу, не зависящую от базиса:

$$\left\lceil \log_{u(B)} \left( \frac{d(f)}{D(B)} + 1 \right) \right\rceil - (\log_2 k + 2) \le I_B(f) \le \left\lceil \log_{u(B)} \left( \frac{d(f)}{D(B)} + 1 \right) \right\rceil + k^2.$$

В настоящей работе усилены и верхняя, и нижняя оценки.

**Теорема.** *Для любой функции $k$-значной логики $f$ и для произвольного базиса $B$ вида*

$$B = M \cup \{\omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_k \setminus M,\ i = 1, \ldots, p,$$

*выполняются неравенства*

$$\left\lceil \log_{u(B)} \left( \frac{d(f)}{D(B)} + 1 \right) \right\rceil - 1 \le I_B(f) \le \left\lceil \log_{u(B)} \left( \frac{d(f)}{D(B)} + 1 \right) \right\rceil + 3 \log_2 k + 3,$$

*где* $D(B) = \max\{d(\omega_1), \ldots, d(\omega_p)\}$.

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

## Список литературы

[1] Марков А. А. Об инверсионной сложности систем функций // ДАН СССР. 1957. Т. 116, № 6. С. 917–919.

[2] Кочергин В. В., Михайлович А. В. О минимальном числе отрицаний при реализации систем функций $k$-значной логики // Дискретная математика. 2016. Т. 28, вып. 4. С. 80–90.

[3] Kochergin V. V., Mikhailovich A. V. Asymptotics of growth for non-monotone complexity of multi-valued logic function systems // Siberian Electronic Mathematical Reports (`http://semr.math.nsc.ru`). 2017. V. 14. P. 1100–1107.

[4] Кочергин В. В., Михайлович А. В. Точное значение немонотонной сложности булевых функций // Математические заметки. 2019. Т. 105, вып. 1. С. 32–41.

[5] Кочергин В. В., Михайлович А. В. Оценки немонотонной сложности функций многозначной логики // Ученые записки Казанского университета. Серия Физико-математические науки. 2020. Т. 162, № 3. С. 311–321.

# О деревьях с 5 или 6 листьями, имеющих наибольшее количество паросочетаний

**Кузьмин Никита Александрович**

НИУ ВШЭ, Нижний Новгород, e-mail: `nikita.kuz2000@gmail.com`

Химические соединения часто рассматриваются в форме молекулярных графов, где атомам соответствуют вершины графа, а связям между ними — ребра графа. При этом свойства соединений описываются в терминах так называемых топологических индексов, которые представляют собой некоторые инварианты графов и которые позволяют аналитически исследовать ряд аспектов химической структуры вещества.

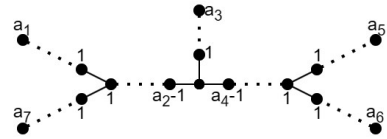


Рис. 1: Дерево $T_5(a_1, \ldots, a_7)$

В пионерской работе [1] японского химика Харуо Хосойи было показано, что некоторые физико-химические свойства алканов (в частности, их точки кипения) связаны со значением индекса их молекулярных графов, называемого теперь индексом Хосойи. *Индексом Хосойи графа* называется количество его паросочетаний, где *паросочетанием графа* называется любое множество (в том числе и пустое) попарно несмежных его ребер. Поскольку топологические индексы определяют ту или иную «энергию» химических соединений, то интересна задача по выявлению графов из заданных классов с экстремальным (минимальным или максимальным) значением того или иного топологического индекса.

В работе [2] было доказано, что среди деревьев с $n$ вершинами максимальный индекс Хосойи имеет только $n$-путь — единственное дерево на $n$ вершинах с 2 листьями. В той же работе [2] было показано, что для любого $n \geq 6$ в классе $n$-вершинных деревьев предмаксимальный граф единственен и получается соединением ребрами листа $(n-4)$-пути с концевыми вершинами двух 2-путей. Таким образом данный граф является максимальным элементом класса $n$-вершинных деревьев с тремя листьями. В работе [3] рассматривался случай $n$-вершинных деревьев с четырьмя листьями. Оказалось, что для любого $n \geq 11$ максимальное дерево не единственно. Одно из них получается соединением ребрами каждой висячей вершины $(n-8)$-пути с двумя 2-путями. А второе получается присоединением ребрами 2-пути к первой и $(n-8)$-пути к второй центральным вершинам 6-пути.

В данной работе рассматривается и решается задача максимизации индекса Хосойи в $n$-вершинных деревьях с 5 и 6 листьями. Оказалось, что для любого $n \geq 20$ имеется ровно три максимальных 5-листных $n$-вершинных дерева и что для любого $n \geq 26$ имеется ровно шесть максимальных 6-листных $n$-вершинных деревьев. Пусть $a_i, b_j, c_k$ — натуральные числа, причем выполнено

$$\sum_{i=1}^{7} a_i - 1 = \sum_{j=1}^{9} b_j - 2 = \sum_{k=1}^{9} c_k - 2 = n.$$

Через $T_5(a_1, \ldots, a_7), T_6^1(b_1, \ldots, b_9)$ и $T_6^2(c_1, \ldots, c_9)$ обозначим деревья, изображенные на рисунках 1 и 2.

Тогда справедлива следующая теорема:

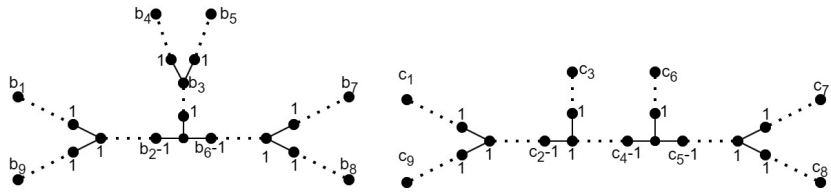


Рис. 2: Деревья $T_6^1(b_1, \ldots, b_9)$ и $T_6^2(c_1, \ldots, c_9)$

**Теорема 1.** *Для любого $n \geq 20$ множество максимальных 5-листных деревьев состоит из следующих трех деревьев:*

$$T_5(n-11, 2, \ldots, 2), T_5(2, n-11, 2, \ldots, 2), T_5(2, 2, n-11, 2, \ldots, 2).$$

*Для любого $n \geq 26$ множество максимальных 6-листных деревьев образовано двумя деревьями $T_6^1(n-14, 2, \ldots, 2)$ и $T_6^1(2, n-14, 2, \ldots, 2)$, а также следующими четырьмя деревьями:*

$$T_6^2(n-14, 2, \ldots, 2), T_6^2(2, n-14, 2, \ldots, 2),$$

$$T_6^2(2, 2, n-14, 2, \ldots, 2), T_6^2(2, 2, 2, n-14, 2, \ldots, 2).$$

Способ доказательства теоремы 1 использует метод, предложенный в [4]. *Псевдограф* (т. е. допускаются петли и кратные ребра) $G'$ называется *стяжкой* обыкновенного графа $G$, если $G$ получается подразбиениями ребер $G'$ и $G'$ содержит минимальное количество вершин. Сначала перечисляются все стяжки $n$-вершинных деревьев с 5 и 6 листьями. А далее предлагаются конкретные преобразования графов, увеличивающие индекс Хосойи и сохраняющие количества вершин, ребер и листьев, а также связность этих графов. Эти преобразования позволяют выявить стяжки именно максимальных деревьев и настроить параметры (т. е. количества подразбиений ребер) в них.

Автор выражает благодарность профессору Малышеву Д. С. за постановку задачи и внимание к работе.

## Список литературы

[1] Hosoya H. Topological index. A newly proposed quantity characterizing the topological nature of structural isomers of saturated hydrocarbons // Bulletin of the Chemical Society of Japan. 1971. Vol. 44, № 9. P. 2332–2339.

[2] Gutman I. Acyclic systems with extremal Hückel $\pi$-electron energy // Theoretica Chimica Acta. 1977. Vol. 45. P. 79–87.

[3] Wagner S. Extremal trees with respect to Hosoya Index and Merrifield-Simmons Index // MATCH Communications in Mathematical and in Computer Chemistry. 2007. Vol. 57. P. 221–233.

[4] Кузьмин Н. А., Малышев Д. С. Новое доказательство результата о полном описании $(n, n+2)$-графов с максимальным значением индекса Хосойи // Математические заметки. 2022. Т. 111, № 2. С. 258–276.

# Асимптотические оценки высокой степени точности для сложности реализации булевых операторов, связанных с классом симметрических функций, в модели клеточных схем.

**Ложкин Сергей Андреевич, Зизов Вадим Сергеевич**

Кафедра математической кибернетики факультета ВМК МГУ имени М. В. Ломоносова, e-mail: lozhkin@cs.msu.ru, vzs815@gmail.com

Впервые модель клеточных схем (КС) в «стандартном» базисе $Б_0$ из функциональных и коммутационных элементов, где под сложностью КС понималась ее площадь, была предложена в 1967 году С. С. Кравцовым в [1]. Она положила начало исследованиям, связанным с решением в рамках данной модели различных задач синтеза и, в частности, задачи индивидуального синтеза.

Эта задача связана с изучением сложности (площади) $A_Б(F)$, которая определяется для системы булевых функций (БФ) $F = (f_1, ..., f_m) \in P_2^m(n)$, где $P_2(n)$ — множество всех БФ от булевых переменных (БП) $X(n) = (x_1, \ldots, x_n)$, и равна минимальной площади реализующих ее КС в базисе Б. Считается, что базис Б является конечным полным базисом, состоящим из функциональных и коммутационных элементов, каждый из которых имеет форму единичного квадрата, причем входы и выходы элемента однократно располагаются на серединах его сторон.

Предполагается, что каждая КС над базисом Б представляет собой прямоугольник, состоящий из его элементов — квадратов, соединенных между собой "корректным" способом через середины общих сторон. При этом входные и выходные БП данной КС, связанные с её входами и выходами, однократно приписываются некоторым расположенным на границе схемы входам и выходам её элементов соответственно. Предполагается также, что структура "коммутационных" соединений входов, функциональных элементов и выходов КС задает схему из функциональных элементов над функциональной частью базиса Б.

Во многих случаях реализуемая система БФ $F$ имеет вид $F = \vec{H}$, где $H \subseteq P_2(n)$, то есть состоит из всех БФ множества $H$, упорядоченных в соответствии с лексикографической нумерацией их столбцов значений. При этом рассматривается, обычно, последовательность множеств

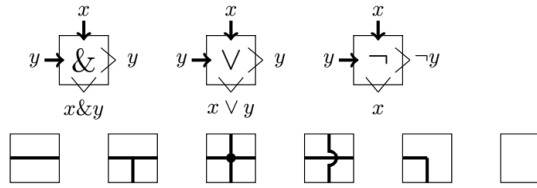


Рис. 1: Базис $Б_0'$: *функциональные элементы* — конъюнкция (&), дизъюнкция ($\vee$) и отрицание ($\neg$); *коммутационные элементы* (слева направо) — проводник, Т-образный разветвитель, разветвитель, пересечение без соединения, поворот, изолятор

$H(1), H(2), \ldots, H(n), \ldots$, где $H(n) \subseteq P_2(n)$ при всех $n, n = 1, 2, \ldots$, и устанавливается (асимптотическое) поведение последовательности $A_{Б}(\vec{H}(n))$ при $n = 1, 2, \ldots$ .

Так, в работе [1], а также в работе Н. А. Шкаликовой [2] был установлен порядок роста вида $n \cdot 2^n$ для площади $A_{Б_0}(\vec{K}(n))$, вида $n \cdot 2^{2^n}$ для площади $A_{Б_0}(\vec{P}_2(n))$ и вида $\log n \cdot 2^n$ для площади $A_{Б_0}(\vec{S}(n))$, где множество $K(n)$ состоит из всех элементарных конъюнкций ранга $n$ от БП $X(n)$, то есть $\vec{K}(n)$ является т. н. *дешифратором* порядка $n$, а множество $S(n)$ состоит из всех симметрических БФ из $P_2(n)$. Напомним, что система БФ $\vec{P}_2(n)$ называется, обычно, *универсальным многополюсником порядка* $n$. Напомним также, что симметрической называется функция, значение которой не зависит от перестановки её аргументов.

В работе [3] были установлены асимптотически точные верхние и нижние оценки для площади схем над базисом $Б_0'$ (см. рис. 1 и ср. с [1]), реализующих дешифратор порядка $n$, которые имеют вид $n2^{n-1}(1 \pm O(\frac{1}{n}))$ и аналогично работе [4] могут считаться асимптотическими оценками высокой степени точности (АОВСТ).

В работах [5, 6] были установлены верхние и нижние АОВСТ для сложности $A_{Б'_0}(\vec{P}_{2n}(n))$, то есть для площади универсального многополюсника порядка $n$ в модели клеточных схем над базисом $Б_0'$, имеющие вид

$$n \cdot 2^{2^n-1} - O(n^2) \leq A_{Б_0'}(\vec{P}_2(n)) \leq (n+6)2^{2^n-1} + \frac{3n}{2^n}2^{2^n-1}. \qquad (1)$$

В настоящей работе аналогичные АОВСТ получаются для системы всех симметрических функций.

**Утверждение 1.** *Для площади КСФКЭ $\Sigma_n$ над базисом $Б_0'$, реализующей систему всех симметрических функций $\vec{S}(n)$, верна верхняя оценка площади:*

$$A(\Sigma_n) \leqslant 2^n(\log n + 6) + O(n \log n).$$

**Утверждение 2.** *Для площади системы всех симметрических функций* $\vec{S}(n)$ *верна нижняя оценка:*

$$A_{B_0'}(\vec{S}(n)) \geqslant 2^n \log n - O(2^n).$$

Таким образом, основным результатом работы является следующая теорема

**Теорема.** *Для системы всех симметрических функций* $\vec{S}(n)$ *выполняется равенство*

$$A_{B_0'}(\vec{S}(n)) = 2^n(\log n \pm O(1)).$$

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075-15-2022-284.

## Список литературы

[1] Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. 1967. Вып. 19. С. 285–292.

[2] Шкаликова Н. А. О реализации булевых функций схемами из клеточных элементов // Математические вопросы кибернетики. Вып. 2. 1989. С. 177–197.

[3] Ложкин С. А., Зизов В. С. Уточненные оценки сложности дешифратора в модели клеточных схем из функциональных и коммутационных элементов // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2020. Т. 162, № 3. С. 322–334. doi: 10.26907/2541-7746.2020.3.322-334

[4] Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. М.: Наука, Физматлит. 1996. Вып. 6. С. 189–214.

[5] Ложкин С. А., Зизов В. С. Уточненные оценки сложности универсального многополюсника в модели клеточных схем // Материалы XIV Международного семинара «Дискретная математика и её приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2022 г.) Под редакцией В. В. Кочергина. М.: ИМП им. М. В. Келдыша, 2022. С. 80–81.

[6] Ложкин С. А., Зизов В. С. Уточнённые оценки сложности клеточного универсального многополюсника // Ломоносовские чтения. Научная конференция. 04—14 апреля 2023 г.: тезисы докладов. М.: Издательский отдел факультета ВМиК МГУ; МАКС Пресс, 2023. С. 146–147.

# Оптимальные вложения троичных деревьев подобных формул в прямоугольные решетки

**Ложкин Сергей Андреевич, Мо Ди**

Кафедра математической кибернетики ВМК МГУ имени М. В. Ломоносова, e-mail: lozhkin@cs.msu.ru, xdmodi1991@163.com

## Введение

Из задачи организации взаимодействия и моделирования вычислений возникает задача оптимального вложения деревьев в прямоугольные решетки (ПР), в узлах которых можно размещать вычислительные узлы, а по ребрам проводить соединяющие их проводники. Вложения могут быть описаны отображениями вершин дерева в узлы ПР, а ребер – в цепи решетки. При этом задача оптимизации вложения сводится к нахождению при определенных условиях минимальной высоты и площади допускающей его ПР.

Данная задача при дополнительном ограничении на расположение листьев на границе решетки была рассмотрена в [2, 3]. Там для оптимальной площади гомеоморфного вложения полного $k$-ярусного $d$-ичного, где $d = 2, 3$, дерева была получена асимптотически точная при $k = 1, 2, \ldots$ оценка порядка $kd^k$, в то время как высота построенного вложения не больше, чем на константу, отличалась от минимально возможного значения высоты ПР, допускающих указанное вложение, равного $\lceil (k+1)/(4-d) \rceil$.

В работе [4] исследовалась задача преобразования двоичных деревьев формул для построения оптимального по высоте их одностороннего вложения в прямоугольные решетки. В ней приводятся методы построения оптимального по высоте вложения среди всех вложений деревьев формул, подобных заданной, и имеющих глубину не более заданного числа. Эти вложения строят либо на основе полных двоичных деревьев, либо на основе специальных двоичных деревьев.

В работе [5] приведен аналогичный метод построения подобных формул для исходных формул над базисом $Б_0' = \{x_1 \& x_2 \& x_3, x_1 \vee x_2 \vee x_2, x_1 \vee x_2, x_1 \& x_2, \overline{x}\}$, а также троичных деревьев этих формул и их вложений. Исследовалась возможность использования специальных троичных деревьев для уменьшения высоты получаемых вложений и построения асимптотически оптимальных односторонних вложений при определенных ограничениях.

В данной работе продолжаются исследования [5] и рассматривается задача оптимального вложения троичных деревьев подобных формул арности 3 в прямоугольные решетки. Для некоторых классов указанных деревьев предложены методы их вложения, позволяющие получать близкую к минимальной высоту используемой решетки среди всех подобных исходной формуле формул не большей глубины. Все используемые здесь понятия можно найти в [1] и [5].

Формулу $F(x_1, \ldots, x_n)$ над базисом $Б_0'$ будем, как обычно, называть формулой с поднятыми отрицаниями, если все её элементы данного типа присоединены к входам $x_1, \ldots, x_n$. При этом сложность $L(F)$, глубину $D(F)$ и альтернирование $Alt(F)$ формулы $F$ определим как число её элементов, максимальную длину цепей в дереве формулы $F$ и максимальное число изменений типов её элементов $\&$, $\vee$ в этих цепях соответственно.

В работе [3] было построено семейство троичных деревьев $D(d, h)$, где $d = 1, 2, \ldots$ и $h = 1, 2, \ldots, d + 1$, которые имеют не более $d$ ярусов, $N(d, h)$ листьев, где $N(d, h) = \sum_{i=0}^{h-1} C_d^i 2^i$, и допускают «каноническое» гомеоморфное вложение в ПР высоты не более, чем $h$, с расположением листьев на нижней горизонтальной границе. Нетрудно убедиться в том, что при этом

$$N\left(d, \left\lceil \frac{2d+1}{3} \right\rceil\right) \geq 3^{d-1}. \tag{1}$$

Положим $\tilde{D}_d = D(d + 1, \lceil \frac{2}{3} d \rceil + 1)$ и заметим, что в силу (1) число листьев дерева $\tilde{D}_d$ не меньше, чем число листьев в полном троичном $d$-ярусном дереве $D_d$, его глубина на 1 больше, чем глубина $D_d$, но при этом высота ПР, допускающей вложение $D$, равна $\lceil \frac{2}{3} d \rceil + 1$, тогда как аналогичная высота дерева $D_d$ равна $d + 1$.

В работе [5] была предпринята попытка использования дерева $\tilde{D}_d$ вместо дерева $D_d$ при вложении деревьев подобных формул в ПР, в результате чего было доказано следующее утверждение.

**Теорема 1** ([5]). *Пусть $F(x_1, \ldots, x_n)$ — формула с поднятыми отрицаниями над базисом $Б_0'$, в которой минимальный ранг максимальных по включению букв БП $x_1, \ldots, x_n$ элементарных конъюнкций или дизъюнкции, являющихся её подформулами, не меньше, чем $3^s$. Тогда существует подобная $F$ формула $\hat{F}$ глубины не больше, чем $d$, где $d = \lceil \log_3(2L(F) + 1) \rceil + Alt(F) + 3$, а также каноническое вложение дерева этой формулы в прямоугольную решетку высоты не более, чем $d - \lfloor \frac{s}{3} \rfloor$.*

В настоящей работе предлагается подойти к указанному использованию с «другой» стороны, а основным результатом является следующее утверждение.

**Теорема 2.** *Пусть $F(x_1, \ldots, x_n)$ — формула с поднятыми отрицаниями над базисом $Б_0'$, в которой ранг любой её максимальной по включению букв БП $x_1, \ldots, x_n$ подформулы $F_i$, $i = 1, \ldots, t$, такой, что $Alt(F_i) < Alt(F)$, не превосходит $3^s$, где $s$ — натуральное число. Тогда существует подобная $F$ формула $\hat{F}$ глубины не больше чем $s + Alt(F) + \lceil \log_3 t \rceil$, допускающая каноническое вложение в решетку высоты не больше, чем $s + \lceil 2 \log_3 t \rceil + 3$.*

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075-15-2022-284.

## Список литературы

[1] Ложкин С. А. Лекции по основам кибернетики. М.: Изд-во МГУ, 2004.

[2] Ложкин С. А., Ли Да Мин. О некоторых оптимальных вложениях двоичных и троичных деревьев в плоские прямоугольные решетки // Вестн. Мок. ун-та. Сер. 15. Вычисл. матем. и киберн. 1995. № 4. С. 49–55.

[3] Ли Да Мин. Некоторые оптимальные вложения древовидных графов в плоские прямоугольные решетки. Дисс. канд. физ.-матем. наук МГУ, 1994.

[4] Ложкин С. В., Высоцкий Л. И. О некоторых асимптотически оптимальных односторонних вложениях деревьев подобных формул в прямоугольные решетки // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и кибер. 2017. № 2. С. 38–45.

[5] Ибрагимов Б. М. О некоторых асимптотически оптимальных односторонних вложениях троичных деревьев подобных формул в прямоугольные решетки. Дисс. маг. МГУ, 2020.

# Реализация подстановок чётной степени произведениями трёх инволюций без неподвижных точек

**Малышев Фёдор Михайлович**

Математический институт им. В. А. Стеклова РАН, Москва, e-mail: malyshevfm@mi-ras.ru

**1.** Если группа $G$ порождается таким своим подмножеством $Q$, что $Q = Q^{-1} = \{q^{-1} | \, q \in Q\}$, то длиной $l_Q(x)$ элемента $x \in G$ относительно $Q$ называют такое наименьшее целое неотрицательное число $r$, что $x$ есть произведение $r$ элементов из $Q$ [1]. Длины симплектических и ортогональных преобразований относительно инволюций в виде симметрий исследовали Э. Картан и Ж. Дьедонне (см. [2]). Для произвольных конечных простых групп $G$ в [3] доказано существование такой абсолютной константы $L$, что относительно всех инволюций $\mathcal{I} \subset G$ справедливо $l_{\mathcal{I}}(g) \leqslant L$ для всех $g \in G$. А. И. Кострикин высказал предположение, что любой элемент простой конечной группы представляется произведением не более 4 её инволюций. Если $G = A_m$ – знакопеременная группа, то, как установлено П. Картером, $l_{\mathcal{I}}(\pi) \leqslant 3$ для всех $\pi \in A_m$ при $m > 6$, $m \neq 10, 14$ [4].

**2.** В настоящей статье рассматривается система образующих $P_n \subset S_{2n}$, $n \geqslant 3$, состоящая из $n$ инволюций без неподвижных точек, называемых парноцикловыми подстановками. Как следствие упомянутого результата П.

Картера для подстановок $\pi$ из знакопеременной группы $A_{2n}$ при $n \neq 2, 3, 5, 7$ справедливо неравенство $l_{P_n}(\pi) \leqslant 6$, так как любая инволюция $\sigma \in A_{2n}$ может быть представлена произведением двух инволюций из $P_n$.

Обозначаем парноцикловые подстановки через $p$, $p_i \in S_{2n}$, $i \in \mathbb{N}$. Если для $\pi \in S_{2n}$ имеем $\pi = p_1 \cdot p_2 \cdot \ldots \cdot p_l$, то говорим, что подстановка $\pi$ является *$l$-представимой*. Для мощности множества $P_n \subset S_{2n}$ всех парноцикловых подстановок $p \in S_{2n}$ имеем $|P_n| = (2n-1) \cdot (2n-3) \cdot \ldots \cdot 5 \cdot 3 = (2n-1)!!$ Поскольку $(2n)!/2 = 2n \cdot (2n-2) \cdot \ldots \cdot 6 \cdot 4 \cdot (2n-1) \cdot (2n-3) \cdot \ldots \cdot 5 \cdot 3 > |P_n|^2$, то о 2-представимости значительной доли подстановок не может идти речи. При чётном $n$ все подстановки в $P_n$ чётные, а при нечётном $n$ — нечётные, поэтому 3-представимость для нечётных подстановок $\pi$ возможна при нечётных $n$, а для чётных $\pi$ – при чётном $n$.

Подстаноки будем представлять перечислением в скобках длин их циклов. Число циклов одинаковой длины допускается обозначать верхним индексом. Когда длины циклов не превосходят 6, не будем отделять их друг от друга запятыми. Число единичных циклов тоже будем указывать. Например, $p = (2^n)$, $p \in P_n$, $(2n)$ представляет все $(2n-1)!$ полноцикловых подстановок, а $(n, n) = (n^2)$ – подстановки, представимые двумя циклами длины $n$ каждый, $(1^{2n})$ – тождественная подстановка, у которой все циклы единичные. Достаточно рассматривать только одну какую-либо подстановку из полной их совокупности с заданной цикловой структурой.

Следующая теорема утверждает, что почти все подстановки одной чётности с чётностью половины её чётной степени являются 3-представимыми. В частности, если в подстановке есть цикл длиной не меньше 6 или два цикла длиной не меньше 4, то она 3-представима.

**Теорема.** *Пусть $\pi \in A_{2n}$ при чётном $n > 3$ или $\pi \in S_{2n} \setminus A_{2n}$ при нечётном $n \geqslant 3$. Тогда, если подстановка $\pi$ не является 3-представимой, то она содержится среди подстановок одной из следующих четырёх серий:*
*a)* $(532^i)$, *где* $i \geqslant 0$,
*b)* $(51^i)$, *где* $i \equiv 3 \pmod 4$,
*c)* $(431^i)$, *где* $i \equiv 3 \pmod 4$,
*d)* $(3^i 2^j 1^k)$, *где* $i \equiv 1 \pmod 4$, $j \geqslant 0$, $k \equiv 1 \pmod 4$, *причём либо* $j \leqslant 1$ *либо* $k = 1$.
*Обратно, если подстановка $\pi \in S_{2n}$ одной чётности с $n$ принадлежит одной из серий a), b), c) или серии d) с $i = 1$, то она не является 3-представимой.*

Для подстановок $\pi$ серии $d$) с $i \geqslant 5$ вопрос о их 3-представимости открыт. Автор не решается высказать напрашивающуюся здесь гипотезу ввиду большого числа комбинаторных возможностей на путях доказательства 3-представимости для каких-либо подстановок серии $d$) с $i \geqslant 5$.

**3.** Доказательство теоремы использует приводимую ниже серию выделеных курсивом утверждений, требующих индивидуальных конструкций.

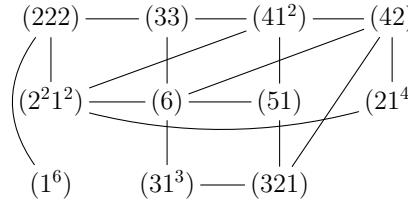


Рис. 1: Граф близости для $n = 3$

**3.1.** *Состоящее из трёх подстановок* $(22)$ *множество* $P_2$ *вместе с тождественной подстановкой* $(1^4)$ *образует группу из* 4 *элементов. В этой группе произведение двух различных элементов из* $P_2$ *равно третьему элементу из* $P_2$*. Произведение всех трёх элементов из* $P_2$ *равно единице группы.*

**3.2.** *Если множество циклов подстановки* $\pi \in S_{2n}$ *разбивается на два подмножества с чётными суммами их длин в подмножествах, то они образуют подстановки* $\pi_1 \in S_{2n_1}$, $\pi_2 \in S_{2n_2}$, $n_1 + n_2 = n$, $n_1 \geqslant 1$, $n_2 \geqslant 1$, *и из* 3*-приводимости подстановок* $\pi_1$, $\pi_2$ *следует* 3*-приводимость* $\pi$.

**3.3.** *Для любых парноцикловых подстановок* $p_1$, $p_2 \in P_n$ *их произведение* $p_1p_2$ *представляется несколькими парами циклов одинаковой длины в каждой паре. Обратно, если циклы подстановки* $\pi \in S_{2n}$ *можно разбить на пары одинаковой длины (в отдельных парах), то она* 2*-представима.*

**3.4.** *При нечётном* $n \in \mathbb{N}$ *имеем* 3*-представимость подстановки* $(2n)$.

Далее две подстановки $\pi_1, \pi_2 \in S_{2n}$ будем считать *близкими*, если $\pi_1 p = \pi_2$ для некоторой парноцикловой подстановки $p \in P_n$. Отношение близости симметрично. Это отношение удобно представлять неориентированным графом. Некоторые возможные при этом рёбра могут не указываться.

**3.5.** *В обозначениях утверждения* 3.2 *подстановки* $\pi, \pi' \in S_{2n}$ *близки, если близкими являются отвечающие им пары подстановок* $\pi_1, \pi_1' \in S_{2n_1}$ *и* $\pi_2, \pi_2' \in S_{2n_2}$.

Во всех доказательствах 3-представимости подстановки $\pi$ строится близкая $\pi$ подстановка, все циклы которой разбиваются на пары циклов одинаковой длины, т. е. близкая $\pi$ 2-представимая подстановка.

**3.6.** *При* $n = 3$ *имеет место граф близости, изображённый на рис. 1.*

**3.7.** *Для* $k \geqslant 2$ *имеем* $(42^{k-2}) \overset{a}{\text{——}} (2k) \overset{b}{\text{——}} (1^2 2^{k-1})$ .

**3.8.** $(1^3 52) \text{——} (55)$ .

**3.9.** *Для* $k_1 \geqslant 2$, $k_1 \geqslant 2$ *имеем* $(41^2 2^{k_1+k_2-2}) \overset{a}{\text{——}} (2k_1+1, 2k_2+1) \overset{b}{\text{——}} (4^2 2^{k_1+k_2-3})$ .

**3.10.** *Для* $k \geqslant 2$ *имеем* $(62^{k-1}) \overset{a}{\text{——}} (2k+1, 3) \overset{c}{\text{——}} (41^2 2^{k-1})$ ,

*а для* $k \geqslant 4$: $(2k+1, 3) \overset{b}{\text{——}} (4^2 1^4 2^{k-4})$ .

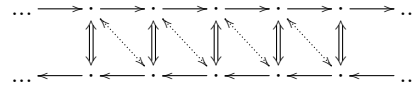

Рис. 2

**3.11.** *Для* $k \geqslant 2$ *имеем* $(312^{k-1}) \overset{a}{\text{——}} (2k+1,1) \overset{b}{\text{——}} (41^2 2^{k-2})$ ,
*а для* $k \geqslant 3$*:* $(2k+1,1) \overset{c}{\text{——}} (4^2 2^{k-3})$ .

**3.12.** *Для* $k_1 \geqslant 1$, $k \geqslant 2$, $k_2 \geqslant 1$ *имеем* $(2k_1+1, 2k, 2k_2+1)$——$(4^2 1^2 2^{k_1+k+k_2-4})$ .

**3.13.** *Для* $k \geqslant 3$ *имеем* $(1, 2k, 3)$ —— $(4^2 1^2 2^{k-3})$ .

**3.14.** *Для* $k \geqslant 2$ *имеем* $(1, 2k, 1)$ —— $(332^{k-2})$ .

**3.15.** $(422) \overset{a}{\text{——}} (143) \overset{b}{\text{——}} (61^2)$ .

Доказательства приведённых утверждений используют "погружения" подстановок $\pi$ в множество транспозиций парноцикловой подстановки $p$ (изображённых на рис. 2 двойными стрелками), при которых сближаются длинные участки циклов так, чтобы они были разнонаправлены, а соответствующие пары вершин из разных участков образовывали бы 2-циклы подстановки $p$.

Тогда в подстановке $\pi p$ будет подавляющее число циклов длины 2 в виде точек, причём можно добиться, чтобы длины остальных циклов не превосходили 6.

**4.** При доказательстве теоремы каждый раз проверка 3-представимости конкретной подстановки $\pi$ или семейства подстановок осуществляется по следующей схеме. Вначале всю совокупность циклов исследуемой подстановки разбиваем на отдельные подмножества, к каждому из которых применяем одно из утверждений 3.6–3.15. Применяя эти утверждения, подбираем такие варианты отдельных близких подстановок, чтобы вся совокупность их циклов (по всем подмножества циклов подстановки $\pi$) образовывала бы 2-представимую подстановку (у которой циклы разбиваются на пары одинаковой длины).

## Список литературы

[1] Бурбаки Н. Группы и алгебры Ли. Группы Кокстера и системы Титса. Группы, порождённые отражениями. Системы корней. М. : Мир, 1972.

[2] Артин Э. Геометрическая алгебра. М. : Наука, 1969.

[3] Петров Н. Т. О длине простых групп // Докл. АН СССР, **208**:3 (1973). С. 537–540.

[4] Семинар по алгебраическим группам. Сборник статей. М. : Мир, 1973.

# О минимальных рёберных 1-расширениях двух ориентаций цикла

**Моденова Ольга Владимировна, Абросимов Михаил Борисович**

Саратовский национальный исследовательский государственный университет, e-mail: oginiel@rambler.ru, mic@rambler.ru

В работе будут рассматриваться неориентированные и ориентированные графы. Неориентированным циклом (далее просто циклом) $C_n$ называется $n$-вершинный граф, состоящий из единственного цикла, содержащего все вершины. Будем рассматривать ориентации цикла $C_n$, которые получаются заменой каждого ребра цикла на дугу. Особым случаем ориентации цикла $C_n$ является контур $\overrightarrow{C_n}$, то есть ориентированный граф, состоящий из единственного контура, содержащего все вершины. В работе [1] было введено понятие оптимальной отказоустойчивой реализации графа в рамках исследования отказоустойчивости элементов дискретных систем. Позднее в работе [2] была введена модель для исследования отказов связей между элементами.

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным рёберным $k$-расширением* (MP-$k$P) $n$-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1. Граф $G^*$ является рёберным $k$-расширением графа $G$, то есть $G$ вкладывается в каждый граф, получающийся из $G^*$ удалением любых его $k$ рёбер (дуг).
2. Граф $G^*$ содержит $n$ вершин, то есть $|V^*| = |V|$.
3. $\alpha^*$ имеет минимальную мощность при выполнении условий 1 и 2.

В работе [2] предлагаются схемы построения MP-1P для циклов. Число дополнительных рёбер в этих расширениях равно $\lceil n/2 \rceil$. В работе [3] предлагаются другие схемы построения MP-1P циклов и доказывается, что при $n > 5$ они неизоморфны расширениям из работы [2].

**Теорема 1.** *Графы, изображённые на рисунке* 1*, являются MP-1P для цикла $C_n$ при чётном (слева) и нечётном (справа) числе вершин, причём при $n > 5$ они неизморфны расширениям, предложенным в работе* [2].

Рассмотрим ориентации цикла. Напомним, что расширение (вершинное или рёберное) $G^*$ графа $G$ называется неприводимым, если никакая его собственная часть не является расширением (вершинным или рёберным) графа $G$. Заметим, что неориентированный цикл можно рассматривать как ориентированный граф, в котором каждое ребро является парой встречных дуг. Нетрудно заметить, что цикл $C_n$ является неприводимым рёберным 1-расширением для произвольной ориентации $\overrightarrow{C_n}$ цикла $C_n$, что даёт оценку сверху для числа

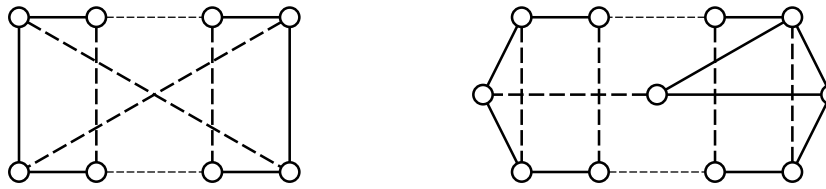

Рис. 1: MP-1P цикла $C_n$

дополнительных дуг в MP-1P ориентации цикла. Эта оценка является достижимой, например, для контура $\overrightarrow{C_n}$. Для получения нижней оценки заметим, что в цикле каждая вершина имеет степень 2, соответственно в ориентации цикла в каждой вершине будет 2 дуги (входящие или исходящие). Тогда в MP-1P в каждой вершине будет не менее 3 дуг. Это даёт нижнюю оценку числа дополнительных дуг $\lceil n/2 \rceil$. Получаем итоговую оценку:

**Теорема 2.** *Для числа дополнительных дуг MP-1P любой ориентации $\overrightarrow{C_n}$ цикла $C_n$ справедливо следующее неравенство:*

$$\lceil n/2 \rceil \leq ec(\overrightarrow{C_n}) \leq n.$$

Далее будут представлены схемы построения MP-1P для двух ориентаций циклов, которые показывают, что нижняя оценка является достижимой. С этой целью мы исследуем возможность ориентации MP-1P циклов из теоремы 1.

Рассмотрим цикл $C_n$ с чётным числом вершин, который ориентируем по схеме сток-источник. Обозначим такую ориентацию $\overrightarrow{CST_n}$. Очевидно, что в MP-1P орграфа $\overrightarrow{CST_n}$ все вершины, в которых есть 3 дуги, могут быть также только источниками или стоками.

**Теорема 3.** *Граф, изображённый на рисунке* 2*, является MP-1P для ориентации $\overrightarrow{CST_n}$ при $n = 4k + 2$.*

Пунктирными линиями на рисунке 2 показаны дополнительные дуги. Заметим, что ориентация направления каждой дуги выбирается естественным образом, чтобы сохранить источники и стоки. Очевидно, что такая ориентация невозможна при $n = 4k$, так как в этом случае вершины в противоположных углах прямоугольника будут иметь одинаковый тип (сток-сток или источник-источник). Любая ориентация диагонали не сможет сохранить источники и стоки.

Рассмотрим цикл $C_n$ с нечётным числом вершин. Его нельзя ориентировать по схеме сток-источник, поэтому рассмотрим другую ориентацию. В произвольной вершине ориентируем рёбра так, чтобы одно ребро было исходящим, а

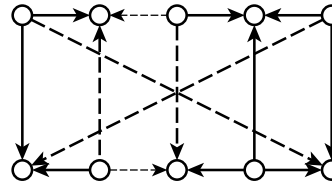

Рис. 2: MP-1P ориентации цикла $CST_n$

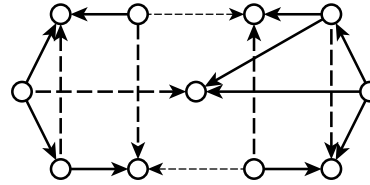

Рис. 3: MP-1P ориентации цикла $CSTN_n$

другое — входящим. Остальные вершины ориентируем по схеме сток-источник. Обозначим такую ориентацию $\overrightarrow{CSTN_n}$.

**Теорема 4.** *Граф, изображённый на рисунке 3, является MP-1P для ориентации* $\overrightarrow{CSTN_n}$.

## Список литературы

[1] Hayes J. P. A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C25. No. 9. P. 875–884.

[2] Harary F., Hayes J. P. Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135–142.

[3] Абросимов М. Б. О неизоморфных минимальных реберных 1-расширениях графов // Теоретические проблемы информатики и ее приложений. 2004. Вып. 6. С. 3–9.

# О реализации булевых функций самокорректирующимися схемами из ненадёжных функциональных элементов

**Попков Кирилл Андреевич**
ИПМ им. М. В. Келдыша РАН, e-mail: kirill-formulist@mail.ru

Рассматривается задача синтеза самокорректирующихся схем из функциональных элементов, реализующих заданные булевы функции (см. [1]). Схема из функциональных элементов (СФЭ) называется *самокорректирующейся* относительно некоторого перечня неисправностей, если при наличии в ней произвольных неисправностей из этого перечня она реализует ту же булеву функцию, что и при отсутствии в ней неисправностей.

В отличие от работ [2–10], в которых рассматривались самокорректирующиеся схемы, состоящие как из ненадёжных, так и из надёжных функциональных элементов (ФЭ), будем исследовать возможности реализации булевых функций схемами, состоящими только из ненадёжных ФЭ.

Описываемая далее модель неисправностей ФЭ, на наш взгляд, является наиболее общей в предположении, что неисправности различных ФЭ происходят независимо друг от друга и у каждого элемента возможна хотя бы одна неисправность. Пусть зафиксирован базис $B$ — некоторое множество булевых функций, каждая из которых существенно зависит от всех своих переменных. Будем предполагать, что для каждой функции $\varphi(\tilde{x}^m)$, где $\tilde{x}^m = (x_1, \ldots, x_m)$, из $B$ имеется сколь угодно много ФЭ, каждый из которых реализует в исправном состоянии эту функцию от своих входов; указанные элементы назовём *$\varphi$-элементами*. Для каждой функции $\varphi(\tilde{x}^m) \in B$ введём *допустимое* множество $M_\varphi = \{M_{\varphi,1}, \ldots, M_{\varphi,r}\}$, где $r \in \mathbb{N}$ и $M_{\varphi,i}$ для каждого $i \in \{1, \ldots, r\}$ — непустое множество (некоторых) отличных от $\varphi(\tilde{x}^m)$ булевых функций от $m$ переменных $x_1, \ldots, x_m$. Предполагается, что всевозможные $\varphi$-элементы разделены на $r$ типов и каждый такой элемент $i$-го типа, $i = 1, \ldots, r$, может перейти в одно из $|M_{\varphi,i}|$ неисправных состояний независимо от неисправностей других функциональных элементов и начать реализовывать вместо «правильной» функции $\varphi(\tilde{x}^m)$ некоторую функцию $\psi(\tilde{x}^m)$ (от своих входов) из множества $M_{\varphi,i}$. Условие $M_{\varphi,i} \neq \varnothing$, где $i = 1, \ldots, r$, означает, что для каждого $\varphi$-элемента $i$-го типа допустима хотя бы одна неисправность (нет «абсолютно надёжных» элементов). В случае $r = 1$ двойные фигурные скобки в записи множества $M_\varphi$ будем для простоты заменять на одинарные, т. е. вместо «$M_\varphi = \{M_{\varphi,1}\}$» писать «$M_\varphi = M_{\varphi,1}$».

**Теорема 1** ([11]). *Для любого целого $m \geqslant 3$ любую булеву функцию можно реализовать СФЭ в базисе $\{\varphi(\tilde{x}^m)\} = \{\overline{x_1 \& x_2 \& \ldots \& x_m}\}$, самокорректиру-*

*ющейся относительно неисправностей, задаваемых множеством* $M_\varphi = \{\overline{x_1 \& x_2}\}$, *произвольного числа элементов.*

**Теорема 2** ([11]). *Для любого натурального* $k$ *любую булеву функцию можно реализовать СФЭ в базисе* $\{\overline{x\&y}\}$, *самокорректирующейся относительно неисправностей, задаваемых множеством* $M_{\overline{x\&y}} = \{\overline{x}\}$, *не более* $k$ *элементов.*

**Теорема 3** ([11]). *Для любого натурального* $k$ *любую булеву функцию можно реализовать СФЭ в базисе* $\{x\&y, \overline{x}\}$, *самокорректирующейся относительно неисправностей, задаваемых множествами* $M_{x\&y} = \{x\}$, $M_{\overline{x}} = \{1\}$, *не более* $k$ *элементов.*

Теоремы 1–3 представляют собой, по-видимому, первые результаты, в которых установлена возможность реализации произвольной булевой функции самокорректирующимися схемами из ненадёжных ФЭ. Ранее при построении самокорректирующихся схем обычно предполагалось, что некоторые ФЭ являются надёжными, т. е. всегда исправными.

**Теорема 4** ([12]). *Никакую нелинейную булеву функцию нельзя реализовать СФЭ в каком бы то ни было базисе* $\{\varphi_1(\tilde{x}^{m_1}), \ldots, \varphi_l(\tilde{x}^{m_l})\}$, *где* $l \in \mathbb{N}$ *и* $m_1, \ldots, m_l \in \{0, 1, 2\}$, *самокорректирующейся относительно неисправностей, задаваемых хотя бы какими-нибудь допустимыми множествами* $M_{\varphi_1}, \ldots, M_{\varphi_l}$, *произвольного числа элементов.*

**Теорема 5.** *Никакую булеву функцию, существенно зависящую по крайней мере от двух переменных, нельзя реализовать СФЭ в каком бы то ни было базисе* $\{\varphi_1(\tilde{x}^{m_1}), \ldots, \varphi_l(\tilde{x}^{m_l})\}$, *где* $l \in \mathbb{N}$ *и* $m_1, \ldots, m_l \in \{0, 1, 2\}$, *самокорректирующейся относительно неисправностей, задаваемых хотя бы какими-нибудь допустимыми множествами* $M_{\varphi_1}, \ldots, M_{\varphi_l}$, *произвольного числа элементов.*

**Замечание 1.** *Для доказательства теоремы* 5 *достаточно доказать утверждение, получающееся из её формулировки добавлением перед словом «булеву» слова «линейную» — это следует из теоремы* 4.

**Замечание 2.** *Несложно показать, что утверждение теоремы* 5 *нельзя распространить ни на одну булеву функцию, существенно зависящую менее чем от двух переменных.*

Теорема 1 демонстрирует, что условие $m_1, \ldots, m_l \in \{0, 1, 2\}$ из формулировки теоремы 5 является существенным. Теоремы 2 и 3 показывают, что отсутствие ограничения на число неисправных элементов в схемах в формулировке теоремы 5 также является существенным.

Работа выполнена при финансовой поддержке Минобрнауки в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

## Список литературы

[1] Редькин Н. П. Надёжность и диагностика схем. М.: Изд-во Моск. ун-та, 1992. 192 с.

[2] Кириенко Г. И. О самокорректирующихся схемах из функциональных элементов // Проблемы кибернетики. 1964. Вып. 12. С. 29–37.

[3] Кириенко Г. И. Синтез самокорректирующихся схем из функциональных элементов для случая растущего числа ошибок в схеме // Дискретный анализ. 1970. Вып. 16. С. 38–43.

[4] Улиг Д. О синтезе самокорректирующихся схем из функциональных элементов с малым числом надёжных элементов // Математические заметки. 1974. Т. 15, № 6. С. 937–944.

[5] Турдалиев Н. И. О самокорректировании схем для некоторых последовательностей булевых функций // Дискретная математика. 1989. Т. 1, вып. 3. С. 77–86.

[6] Турдалиев Н. И. О самокорректирующихся схемах из функциональных элементов для линейной функции // Дискретная математика. 1990. Т. 2, вып. 2. С. 150–154.

[7] Редькин Н. П. Об асимптотически минимальных самокорректирующихся схемах для одной последовательности булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. 1996. № 3. С. 3–9.

[8] Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискретный анализ и исследование операций. 1996. Т. 3, № 2. С. 62–79.

[9] Чашкин А. В. Самокорректирующиеся схемы для функций полиномиального веса // Вестник Московского университета. Серия 1. Математика. Механика. 1997. № 5. С. 64–66.

[10] Краснов В. М. О сложности самокорректирующихся схем для одной последовательности булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. 2009. № 5. С. 55–57.

[11] Popkov K. A. On self-correcting logic circuits of unreliable gates // Lobachevskii Journal of Mathematics. 2021. Vol. 42, No. 11. P. 2637–2644.

[12] Попков К. А. О самокорректирующихся схемах из ненадёжных функциональных элементов, имеющих не более двух входов // Математические заметки. 2022. Т. 1, вып. 111. С. 145–148.

# Некоторые оценки длин проверяющих тестов относительно циклических сдвигов переменных

**Сагандыков Жандос Магауияевич**

МГУ имени М. В. Ломоносова, e-mail: jandosss1@gmail.com

## Введение

**Основные определения.** Пусть дана схема из функциональных элементов (СФЭ) $S$, реализующая функцию алгебры логики (ФАЛ) $f(x_1, x_2, \ldots, x_n)$ и некий источник неисправностей $U$, под действием которого схема может перейти в одно из конечного числа неисправных состояний, в которых реализуются функции:

$$g_1(x_1, \ldots, x_n) = f(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n).$$

Функции $g_1, g_2, \ldots, g_k$ называются *функциями неисправности*.

Множество $T$ входных наборов схемы $S$ называется *проверяющим тестом* относительно источника неисправностей $U$, если в этом множестве для произвольной функции неисправности $g(x_1, \ldots, x_n)$, неравной $f(x_1, \ldots, x_n)$, найдется набор $\widetilde{\alpha}$, на котором $f(\widetilde{\alpha}) \neq g(\widetilde{\alpha})$.

*Длиной теста* $T$ назовем количество $D(T)$ входных наборов в нем. Тест называется *минимальным*, если он имеет наименьшую возможную длину. $D_{det}(f, U) = \min D(T)$, где минимум берется по всем проверяющим тестам $T$ для функции $f$ относительно источника неисправностей $U$, — длина минимального проверяющего теста для функции $f$ относительно источника неисправностей $U$. $D_{det}(n, U) = \max\limits_{f \in P_2(n)} D_{det}(f, U)$ — *функция Шеннона* длины проверяющего теста относительно источника неисправностей $U$.

Рассмотрим источник неисправностей циклического сдвига переменных. Пусть $\varphi^k = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1^k & i_2^k & \ldots & i_n^k \end{pmatrix}$ некоторая перестановка, где $k \in [0, n-1]$. В этой перестановке для каждого натурального $j \in [1, n]$ верно следующее правило

$$i_j^k = \begin{cases} j + k, \text{ если } j + k \leq n \\ j + k - n, \text{ иначе.} \end{cases}$$

Для каждого входного набора $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ определим набор $\varphi^k(\widetilde{\alpha}) = (\alpha_{i_1^k}, \ldots, \alpha_{i_n^k})$. Пусть теперь наша функция $f(x_1, \ldots, x_n)$ под действиям источника неисправности циклического сдвига переходит в функцию $f_{\varphi_k}(x_1, \ldots, x_n) = f(\varphi^k(x_1, \ldots, x_n))$.

**Известные результаты.** Пусть $l(n)$ — функция Шеннона длины проверяющего теста относительно циклического сдвига переменных. В 2010 г. Снегирев И. О. [1] доказал следующую верхнюю оценку

$$l(n) \leq \log_2 n.$$

Также в работе [1] была доказана следующая оценка. Если $k$ — это количество различных простых множителей числа $n$, то верна следующая оценка:

$$l(n) \geq \begin{cases} 2k-2, \text{ если среди простых делителей } n \text{ есть "3" и "2"}, \\ 2k-1, \text{ если среди простых делителей } n \text{ есть "3" либо "2"}, \\ 2k, \text{ иначе.} \end{cases}$$

**Основная часть**

Пусть $\widetilde{\alpha}_i$ это двойчная $n$ — разрядная запись числа $i$. Разделим $2^n$ входных наборов на циклические множества по следующему алгоритму:

1. Выберем набор $\widetilde{\alpha}_1$.
2. Рассмотрим выбранный входной набор; если он не входит ни в одно уже существующее циклическое множество, то перейдем к шагу 3. В ином случае перейдем к шагу 4.
3. Добавим выбранный набор и все его циклические сдвиги в циклическое множество $A_{i+1}$, где $i$ — количество уже существующих циклических множеств.
4. Рассмотрим следующий набор. Если это набор $\widetilde{\alpha}_{2^n-1}$, то выходим из алгортма, в ином случае переходим к шагу 2.

   Пусть $s = |A_i|$ и $A_i = \{\widetilde{\alpha}_1^i, \widetilde{\alpha}_2^i, \ldots, \widetilde{\alpha}_s^i\}$.

**Лемма 1.** *Пусть $n$ — это простое число, тогда все циклические множества для $n$ имеют мощность $n$.*

*Доказательство.* Доказательство леммы 1 проводится от обратного. Доказывается, что если существует циклическое множество $A$, мощность которого меньше чем $n$, то в это множество входит либо единичный набор, либо нулевой набор. А это противоречит определению циклических множеств. □

**Определение.** *Функция $f(\widetilde{x}^n)$ активна относительно циклического множества $A_i$, если существуют $s \in \mathbb{N}$ и $p \in \mathbb{N}$, такие что $\widetilde{\alpha}_s \in A_i, \widetilde{\alpha}_p \in A_i$ и $s \neq p$, для которых верно, что $f(\widetilde{\alpha}_s) \neq f(\widetilde{\alpha}_p)$.*

| $n$ | $l(n)$ | $n$ | $l(n)$ |
|---|---|---|---|
| 4 | 2 | 16 | $[3,4]$ |
| 5 | 2 | 17 | 3 |
| 6 | 2 | 18 | $[3,4]$ |
| 7 | 2 | 19 | 3 |
| 8 | $[2,3]$ | 20 | 4 |
| 9 | $[2,3]$ | 21 | $[3,4]$ |
| 10 | 3 | 22 | 4 |
| 11 | 3 | 23 | 3 |
| 12 | 3 | 24 | 4 |
| 13 | 3 | 25 | $[3,4]$ |
| 14 | 3 | 26 | 4 |
| 15 | 3 | 27 | $[3,4]$ |

Таблица 1: Полученные результаты

Пусть $F_1$ — это множество функций, активных только относительно множества $A_1$ и неактивных относительно всех остальных множеств. $l'(n)$ — это функция Шеннона длины проверяющего минимального теста для функций из множества $F_1$.

**Теорема 1.** *Для простых $n$ верно, что $l(n) = l'(n)$.*

*Доказательство.* Мы рассматриваем циклические множества, на которых активна наша функция $f(\widetilde{x}^n)$, и сопоставляем каждому такому множеству функцию из $F_1$. После этого доказываем, что минимальный проверяющий тест каждой функции, соответствующей какому нибудь циклическому множеству, является тестом исходной функии $f(\widetilde{x}^n)$. □

Была написана программа, которая перебирает наборы длины $n$, строит таблицу неисправности и ищет минимальный тест. Программа работает до $n = 27$ включительно. По доказанной теореме 1 для простых $n$ этих наборов достаточно для получения точного значения функции Шеннона длины проверяющего теста. Для составных $n$ была получена некоторая нижняя оценка функции Шеннона длины проверяющего теста.

Для четных $n$ набор $\widetilde{\alpha}$ будем называть противоположным относительно середины, если $\alpha_i \neq \alpha_{\frac{n}{2}+i}$, где $i \in \{1, 2, \ldots, \frac{n}{2}\}$. Для четных $n$ была написана программа, которая перебирает наборы, противоположные относительно середины. До $n = 68$ включительно была получена нижняя оценка функции Шеннона, равная 4.

Список литературы

[1] Снегирев О. И. Исследование поведения функции шеннона длины проверяющего теста при некоторых перестановках входов схем : Дипломная работа. Москва: Московский государственный университет, 2010.

# Квантовая реализация предсказания задачи бинарной классификации методом случайный лес на Qiskit

**Сафина Лилия Ильхамовна, Хадиев Камиль Равилевич, Зиннатуллин Илнар Гумарович, Хадиева Алия Ихсановна**

Казанский федеральный университет, e-mail: liliasafina94@gmail.com, kamilhadi@gmail.com, galaxys4a@gmail.com, AlIHadieva@kpfu.ru

В данной работе мы предлагаем идею квантовой схемы [1, 2, 3], реализующей алгоритм предсказания для задачи бинарной классификации методом случайный лес [4]. Квантовая версия алгоритма предсказания с точки зрения запросной сложности квадратично более эффективна, чем класическая. Идея данного алгоритма предсказания представлена в работе [5].

**Постановка задачи.** Пусть $N$ — число деревьев в обученной модели, $h$ — заданная высота каждого дерева в лесу, $X$ — входной объект, для которого осуществляется предсказание. Для простоты мы использовали $X$ как набор, состоящий из нулей и единиц. Каждое значение из набора характеризует один параметр объекта $X$ и равняется нулю или единице. Через $|X|$ обозначим число параметров объекта $X$ (длина набора). Пусть $class_0$ — обозначение одного класса, а $class_1$ — обозначение другого класса. Необходимо для $X$ определить, к какому из заданных классов он принадлежит. Дан обученный лес, где число деревьев $N = 4$, высота каждого дерева $h = 3$, и входной объект $X$, число параметров которого $|X| = 3$. Листья деревьев содержат вероятность принадлежности объекта, дошедшего до листа, к классу $class_0$. Обозначим эти вероятности через $p^{i,j}_{class_0}$, где $i$ — номер дерева, а $j$ — номер листового узла в этом дереве. Результатом предсказания в лесу будет класс, среднее арифметическое вероятности которого будет наибольшим.

**Реализация.** В данной работе для описания квантовых регистров используются обозначения Дирака [3]. Рассмотрим квантовый регистр:

$$|X\rangle|i\rangle|h\rangle|j\rangle|class\rangle,$$

где $|X\rangle$ — входной объект, $|i\rangle$ — номер дерева в бинарном виде, $|h\rangle$ — однокубитный вспомогательный регистр, $|j\rangle$ — номер узла, $|class\rangle$ — однокубитный

регистр, характеризующий класс: $|0\rangle$ — $class_0$, $|1\rangle$ — $class_1$. Регистр $|X\rangle$ занимает $|X|$ кубитов, $|i\rangle$ — $\log_2 N$, $|j\rangle$ — $h$ кубитов (заданная высота дерева).

**Алгоритм предсказания в лесу:**

1. Подготовим регистр $|X\rangle$, применив отрицания в нужных позициях.
2. Применим к регистру $|i\rangle$ оператор Уолша-Адамара, который приведет регистр в равновероятностную суперпозицию всех индексов деревьев.
3. Применим предсказание на каждом дереве в зависимости от значения $|i\rangle$.
4. Измерим регистр $|class\rangle$.

**Алгоритм предсказания в дереве:**

1. Подготовим регистр $|j\rangle$, равным бинарной кодировке единицы: $|00\ldots01\rangle$.
2. Для нелистовых узлов в зависмости от значений $|j\rangle$, номера атрибута для этого листа в этом дереве и значения этого атрибута в $|X\rangle$ переводим значение $|j\rangle$ в $|2\cdot j\rangle$ или в $|2\cdot j+1\rangle$. Другими словами, уходим в левый или правый дочерний узел. Такие манипуляции совершаются с использванием регистра $|h\rangle$.
3. Для листовых узлов применяем оператор повората кубита в регистре $|class\rangle$ на угол, соотвествующий $p^{i,j}_{class_0}$ (угол поворота равняется $\arccos\left(\sqrt{p^{i,j}_{class_0}}\right)$).

Обученные деревья обладают характеристиками, соотвествующими рис. 1. Внутри нелистого узла отмечен номер атрибута входного объекта. Если этот атрибут равен 0, осуществляется переход в левый дочерний узел, если единице — в правый дочерний узел. Под листовыми узлами обозначены вероятности принадлежности к $class_0$ — $p^{i,j}_{class_0}$, $j=\overline{4,7}$. Числа в скобках соответствуют номерам узлов.

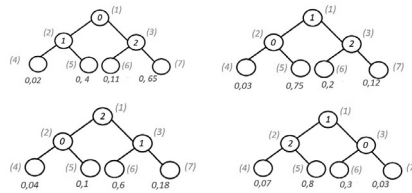


Рис. 1: Обученные деревья

Схема предсказания была реализована с использованием библиотеки квантового программирования qiskit [6].

**Результаты** Для тестирования были взяты 4 значения входных объектов $X$, они представлены в табл. 1.

| $X$ | $p_{class_0}$ |
|---|---|
| 000 | 4% |
| 011 | 25% |
| 101 | 70% |
| 110 | 11% |

Табл. 1: Тестовые входные объекты $X$

| $X$ | $\|0\rangle$-$class_0$ | $\|1\rangle$-$class_1$ |
|---|---|---|
| 000 | 6 | 94 |
| 011 | 31 | 69 |
| 101 | 68 | 32 |
| 110 | 17 | 83 |

Табл. 2: Число измерений 0 и 1 в регистре $|class\rangle$ при 100 запусках схемы

Построенная квантовая схема была запущена 100 раз. При измерении регистра $|class\rangle$ были получены результаты, представленные в табл. 2. В данной реализации схемы используются 159616 двухкубитных `CNot`-вентилей и 216198 однокубитных вентилей. В работе [7] рассмотрены и представлены идеи декомпозиции квантовых многокубитных вентилей. Схемная сложность этих алгоритмов около $O(4^n)$ `CNot`-вентилей и столько же однокубитных вентилей ($n$ — число кубитов). Наш алгоритм предсказания в лесу можно рассмотреть как 10-кубитный вентиль. Также отметим, что `CNot`-вентиль является более дорогой и сложной физически реализуемой операцией, чем однокубитный вентиль. По этим причинам мы можем сделать выводы, что полученная реализация и декомпозиция квантовой схемы лучше универсального разложения унитарной матрицы: число используемых вентилей более чем в 2 раза меньше, чем оценки разложений универсальных многокубитных вентилей. В будущем мы планируем проводить дальнейшую оптимизацию схемной сложности алгоритма предсказания в случайном лесу.

Работа выполнена за счёт средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 0671-2020-0065.

## Список литературы

[1] Гайнутдинова А. Ф. Квантовые вычисления. Казань: Казанский государственный университет. 2009.

[2] De Wolf R. Quantum computing: Lecture notes. 2019. arXiv:1907.09415.

[3] Nielsen M. A, Chuang I. L. Quantum computation and quantum information. Cambridge univ. press, 2010.

[4] Breiman L. Random forests // Machine Learning. 2001. V. 45, issue 1. P. 5–32.

[5] Khadiev K., Safina L. The Quantum Version of Prediction for Binary Classification Problem by Ensemble Methods // Proceedings of SPIE — The International Society for Optical Engineering. 2022. V. 12157, Art. № 1215726.

[6] Qiskit documentation, `https://qiskit.org/`

[7] Krol A. M., Sarkar A., Ashraf I., Al-Ars Z., Bertels K. Efficient decomposition of unitary matrices in quantum circuit compilers. 2021. arXiv:2101.02993.

# О проверке полиномиальности функций $k$-значной логики одной переменной по составному модулю $k$

**Селезнева Светлана Николаевна**

Кафедра математической кибернетики факультета ВМК МГУ имени М. В. Ломоносова, e-mail: `selezn@cs.msu.ru`

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, $P_k^{(n)} = \{f \mid f : E_k^n \to E_k\}$ — множество всех функций $k$-значной логики $n$ переменных, $n \geqslant 1$, и $P_k = \bigcup\limits_{n \geqslant 1} P_k^{(n)}$. Функция $f \in P_k$ называется полиномиальной, если ее можно представить полиномом над кольцом $Z_k = (E_k; +, \cdot)$ вычетов по модулю $k$. Множество всех полиномиальных функций $k$-значной логики $n$ переменных обозначим $Pol_k^{(n)}$, и пусть $Pol_k = \bigcup\limits_{n \geqslant 1} Pol_k^{(n)}$. Известно, что $Pol_k = P_k$ тогда и только тогда, когда $k$ — простое число. В [1] для каждого заданного составного числа $k$ предложен линейный алгоритм проверки полиномиальности функций $k$-значной логики, заданных векторами значений. В этом алгоритме полагается, что все полиномиальные функции $k$-значной логики одной переменной известны. В настоящей заметке предлагаются алгоритмы проверки полиномиальности функций $k$-значной логики одной переменной, заданных векторами значений.

Известен ряд критериев полиномиальности функций $k$-значной логики одной переменной при составных $k$ (см. [1, 2] и ссылки в них). Эти критерии основаны на различных подходах. В частности, рассматриваются подходы, опирающиеся на свойства конечных разностей, на свойства $d$-разностей, где $d$ — делитель числа $k$, на свойства координатных функций, на возможности решения в кольце $Z_k$ систем линейных уравнений относительности неизвестных коэффициентов полиномов. В настоящей заметке применяются конечные разности функций $k$-значной логики. Кроме того, конечные разности рассматриваются в соединении с каноническим видом полиномов полиномиальных

функций. Известны различные канонические виды полиномиальных функций $k$-значной логики (см. [1–3] и ссылки в них). Мы рассматриваем канонический вид из [3]. В итоге получены алгоритмические критерии полиномиальности, на основе которых построены алгоритмы проверки полиномиальности функций $k$-значной логики одной переменной, заданных векторами значений. При этом сложность полученных алгоритмов меньше, чем сложность других алгоритмов решения этой задачи.

Введем необходимые определения. Пусть $N = \{0, 1, 2, \ldots\}$ — множество натуральных чисел с нулем. Введем составную характеристику $c_{p,m}(s)$ числа $s \in N$ по отношению к простому числу $p$ и числу $m \geqslant 1$: положим $c_{p,m}(s) = t$, где $t \in N$ — такое наибольшее число из чисел $0, 1, \ldots, m-1, m$, что $s!$ делится нацело на $p^t$. Положим $s_p(m) = \max s$, где максимум берется по всем таким числам $s \in N$, что $c_{p,m}(s) < m$. Если $p$ — простое число, $m \geqslant 1$, то любую функцию $f(x)$ из $Pol_{p^m}^{(1)}$ можно записать единственным полиномом из $Z_{p^m}[x]$ следующего вида $f(x) = \sum\limits_{s=0}^{s_p(m)} a_s x^s$, где $a_s < p^{m-c_{p,m}(s)}$ для всех $s = 0, 1, \ldots, s_p(m)$ [3]. Определим конечные разности. Пусть $f(x) \in P_k^{(1)}$. Конечной разностью функции $f(x)$ назовем функцию $Df = f(x+1) - f(x) \in P_k^{(1)}$. При этом величина $(Df)(a)$, где $a \in E_k$, называется конечной разностью функции $f(x)$ в точке $a$. Если $s \in N$ и $s \geqslant 1$, то конечной разностью $D^{(s)}f$ порядка $s$ для функции $f(x)$ назовем функцию $Df \in P_k^{(1)}$ при $s = 1$ и функцию $D(D^{(s-1)}f) \in P_k^{(1)}$ при $s \geqslant 2$.

В работе доказаны следующие теоремы.

**Теорема 1**. *Пусть $p$ — простое число, $m \geqslant 1$, $f(x) \in Pol_{p^m}^{(1)}$ и верно условие $D^{(s_p(m)+1)}f = 0$. Пусть для всех $s = 0, 1, \ldots, s_p(m)$ функции $f_s \in P_{p^m}^{(1)}$ определяются следующим образом:*

1) *при $s = s_p(m)$ полагаем, что $f_s(x) = f(x)$;*

2) *при $s = 1, \ldots, s_p(m)$ полагаем, что $f_{s-1}(x) = f_s(x) - a_s x^s$, где $a_s$ — наименьшее решение в кольце $Z_{p^m}$ уравнения $(D^{(s)}f_s)(0) = s! \cdot z$ относительно неизвестной $z$, если уравнение имеет решения в кольце $Z_{p^m}$;*

3) *если при каком-то $s$, $1 \leqslant s \leqslant s_p(m)$, уравнение не имеет решений в кольце $Z_{p^m}$, то $f_t(x)$ — не определена для всех $t = 0, 1, \ldots, s-1$.*

*Тогда:*

1) *если при каком-то $s$, $1 \leqslant s \leqslant s_p(m)$, уравнение не имеет решений в кольце $Z_{p^m}$, то $f \notin Pol_{p^m}^{(1)}$;*

2) *если при каждом $s$, $s = 1, \ldots, s_p(m)$, уравнение имеет решения в кольце $Z_{p^m}$, то $f_0 = f(0)$, $f \in Pol_{p^m}^{(1)}$ и $f(x) = \sum\limits_{s=0}^{s_p(m)} a_s x^s$ — канонический полином для функции $f$, где $a_0 = f_0 \in E_{p^m}$.*

**Теорема 2**. *Пусть $p$ — простое число, $m \geqslant 1$, $f(x) \in Pol^{(1)}_{p^m}$. Пусть для всех $s = 0, 1, \ldots, s_p(m)$ функции $f_s \in P^{(1)}_{p^m}$ определяются следующим образом:*

*1) при $s = s_p(m)$ полагаем, что $f_s(x) = f(x)$;*

*2) при $s = 1, \ldots, s_p(m)$ полагаем, что $f_{s-1}(x) = f_s(x) - a_s x^s$, где $a_s$ — наименьшее решение в кольце $Z_{p^m}$ уравнения $(D^{(s)} f_s)(0) = s! \cdot z$ относительно неизвестной $z$, если уравнение имеет решения в кольце $Z_{p^m}$;*

*3) если при каком-то $s$, $1 \leqslant s \leqslant s_p(m)$, уравнение не имеет решений в кольце $Z_{p^m}$, то $f_t(x)$ — не определена для всех $t = 0, 1, \ldots, s-1$.*

*Тогда:*

*1) если при каком-то $s$, $1 \leqslant s \leqslant s_p(m)$, уравнение не имеет решений в кольце $Z_{p^m}$, то $f \notin Pol^{(1)}_{p^m}$;*

*2) если $f_0 \neq f(0)$, то $f \notin Pol^{(1)}_{p^m}$;*

*3) если при каждом $s$, $s = 1, \ldots, s_p(m)$, уравнение имеет решения в кольце $Z_{p^m}$ и $f_0 = f(0)$, то $f \in Pol^{(1)}_{p^m}$ и $f(x) = \sum\limits_{s=0}^{s_p(m)} a_s x^s$ — канонический полином для функции $f$, где $a_0 = f_0 \in E_{p^m}$.*

На основе теорем 1 и 2 построены алгоритмы проверки полиномиальности функций $p^m$-значной логики одной переменной, где $p$ — простое число, $m \geqslant 1$. При положительном ответе эти алгоритмы выдают канонический полином функции, которая подается на вход. Сложность этих алгоритмов будем оценивать в худшем случае через операции сложения и умножения в поле $Z_p$ с возможными константами из $E_p$. Считаем, элемент $a \in E_{p^m}$ задается как $(a_1, \ldots, a_m) \in E_p^m$, где $a_1 \ldots a_m$ — запись числа $a$ в $p$-ичной системе счисления. На вход алгоритма функция $f \in P^{(1)}_{p^m}$ подается в виде вектора значений $\alpha_f = (f(0), f(1), \ldots, f(p^m - 1)) \in E_{p^m}^{p^m}$. Пусть сложение, вычитание, умножение в кольце $Z_{p^m}$ двух элементов из $E_{p^m}$, а также проверку существования решения в кольце $Z_{p^m}$ уравнения $a \cdot z = b$, где $a, b \in E_{p^m}$, и поиска наименьшего его решения при положительном ответе можно вычислить при помощи не более $\varphi_p(m)$ операций поля $Z_p$ (с возможными константами). Отметим, что $\varphi_p(m) = O(m^2)$. Доказана следующая теорема.

**Теорема 3**. *Пусть $p$ — простое число. Существует детерминированный алгоритм, получающий на вход число $m \in N$, $m \geqslant 1$, и вектор значений $\alpha_f$ функции $f \in P^{(1)}_{p^m}$, выдающий «нет», если $f \notin Pol^{(1)}_{p^m}$, «да» и коэффициенты канонического полинома функции $f$, если $f \in Pol^{(1)}_{p^m}$, и имеющий сложность $L_p(m) = O(m \cdot p^m \cdot \varphi_p(m))$.*

Работа поддержана Минобрнауки в рамках выполнения программы Московского центра фундаментальной и прикладной математики по соглашению № 075-15-2022-284.

Список литературы

[1] Селезнева С. Н. Быстрый алгоритм построения для $k$-значных функций полиномов по модулю $k$ при составных $k$ // Дискретная математика. 2011. Т. 23, № 3. С. 3–22.

[2] Мещанинов Д. Г. Метод построения полиномов для функций $k$-значной логики // Дискретная математика. 1995. Т. 7, № 3. С. 48–60.

[3] Селезнева С. Н. О числе полиномиальных функций $k$-значной логики по составному модулю $k$ // Дискретная математика. 2016. Т. 28, № 2. С. 81–91.

# Об аддитивной сложности $B_k$-множеств

**Сергеев Игорь Сергеевич**

ФГУП «НИИ «Квант», e-mail: isserg@gmail.com

В работе изучается сложность реализации числовых множеств аддитивными цепочками. Напомним, что *аддитивная цепочка* — это начинающаяся с единицы последовательность, в которой каждый следующий член равен сумме каких-то двух предшествующих (возможно совпадающих):

$$1,\ y_1,\ y_2,\ \ldots,\ y_L.$$

Число $L$ называется *длиной* цепочки. Аддитивная цепочка *вычисляет* множество $A \subset \mathbb{N}$, если она содержит все числа из $A$. Длина кратчайшей цепочки, вычисляющей $A$, называется *аддитивной сложностью* множества $A$. Обозначим ее через $\mathsf{L}(A)$. Подробнее об аддитивных цепочках см. в [1].

Сложность множества $A$ мощности $n$ при $\max A = 2^{O(n)}$ удовлетворяет соотношениям $n - 1 \le \mathsf{L}(A) = O(n)$. Нижняя оценка тривиальна, а верхняя следует, например, из общего результата [2].

Естественно поставить задачу построения примеров множеств высокой сложности, $n+\Theta(n)$. Нижние оценки вида $n+\Omega(n)$ несложно доказываются для множеств с экспоненциальным размером элементов. Например, тривиально выполняется $\mathsf{L}(3,\ 3^2,\ \ldots,\ 3^n) = 2n$.

Наилучшие известные нижние оценки для множеств из элементов полиномиального размера получены в [3]. Они имеют вид

$$\mathsf{L}(2^p, 3^p, \ldots, n^p) \ge n + n^{2/3-o(1)}$$

при $p \ge 2$. Наиболее удобным объектом для приложения предложенной в [3] схемы рассуждения являются множества Сидона, свободные от сумм.

Множество $B$ элементов коммутативной группы называется *$B_k$-множеством*, $k \ge 2$, если все $k$-элементные суммы над $B$ попарно различны, т. е. равенство

$$a_1 + \ldots + a_k = b_1 + \ldots + b_k, \qquad a_i, b_j \in B,$$

выполняется только в том случае, когда совпадают мультимножества слагаемых: $\{a_1, \dots, a_k\} = \{b_1, \dots, b_k\}$.

$B_2$-множества, т. е. множества с различными попарными суммами, называются *множествами Сидона*.

Далее обозначение $A + B$ используется для суммы Минковского двух множеств, $A + B = \{a + b \mid a \in A,\, b \in B\}$.

Множество $B$ называется *свободным от сумм*, если $(B + B) \cap B = \emptyset$.

Основной результат работы заключается в следующем.

**Теорема 1.** *Пусть $B \subset \mathbb{N}$ — свободное от сумм $B_k$-множество. Тогда*

$$\mathsf{L}(B) \geq |B| + \frac{1}{5}|B|^{k/(k+1)}.$$

Доказательство опирается на следующую комбинаторную лемму.

**Лемма.** *Пусть $A \subset \mathbb{N}$ и $B \subset (A + A)$ — $B_k$-множество. Тогда*

$$|B| \leq |A|^{1+1/k} + 3|A|.$$

Лемма позволяет оценить снизу число элементов цепочки, вычисляющей $B_k$-множество $B$, не принадлежащих $B$.

Доказательство леммы, в свою очередь, опирается на оценку сверху числа ребер в $n$-вершинном графе, не содержащем циклов четной длины от 4 до $2k$.

Конкретные примеры $B_k$-множеств дает конструкция из [4]. Пусть $x$ — примитивный элемент поля $GF(q^k)$. Положим

$$D[q, k] = \{d_i \mid x^{d_i} - x \in GF(q),\ 1 \leq d_i < q^k\}.$$

Множество $D[q, k]$ является $B_k$-множеством мощности $q$ в $\mathbb{N}$ и даже в $\mathbb{Z}_{q^k-1}$.

Пример $B_k$-множества, свободного от сумм, можно получить при помощи сдвига. Таким множеством является, скажем, $D[q, k] + q^k$. Данный пример доказуемо является конструктивным (строится с полиномиальной относительно своего размера сложностью) только при постоянных либо очень медленно растущих $k$, поскольку его построение связано с решением задачи дискретного логарифмирования в группе, вообще говоря, негладкого порядка.

**Следствие 1.** *При любом $\varepsilon > 0$ можно явно указать множество $B \subset \mathbb{N}$ мощности $n$, для которого $\max B = O(n^{2+1/\varepsilon})$ и $\mathsf{L}(B) = n + \Omega(n^{1-\varepsilon})$.*

Явная при любом $k$ конструкция $B_k$-множества описана в [5]. Обозначим через $p_1, p_2, \dots$ записанные в порядке возрастания нечетные простые числа. Положим $r = 1 + \lceil k \log p_n \rceil$. Множество нечетных чисел-вычетов от 1 до $2^r - 1$ образует мультипликативную подгруппу $\mathbb{Z}^*_{2^r}$ кольца $\mathbb{Z}_{2^r}$, которая при

$r \geq 3$ имеет вид прямого произведения циклических групп порядков 2 и $2^{r-2}$, а именно, $\mathbb{Z}_{2^r}^* \cong \langle -1 \rangle_2 \langle 5 \rangle_{2^{r-2}}$, где $-1$ и 5 — порождающие элементы. Таким образом, любое нечетное число $x$ имеет однозначное представление $x \equiv (-1)^j \cdot 5^h \pmod{2^r}$, где $0 \leq j \leq 1$ и $0 \leq h < 2^{r-2}$.

Легко проверить, что множество

$$H[n,k] = \{h_i \mid p_i \equiv \pm 5^{h_i} \pmod{2^r},\ 0 \leq h_i < 2^{r-2},\ i = 1, \ldots, n\}$$

является $B_k$-множеством. При этом оно строится с полиномиальной сложностью, т.к. дискретное логарифмирование в группе порядка $2^r$ выполняется элементарно.

Рассматривая при $k \asymp \log n$ свободное от сумм множество $H[n,k] + 2^r$, получаем

**Следствие 2.** *Можно явно указать множество $B \subset \mathbb{N}$ мощности $n$ с размером элементов $n^{O(\log n)}$, для которого $\mathsf{L}(B) = n + \Omega(n)$.*

Вопрос о конструктивном задании $n$-элементного множества с полиномиальным размером элементов, имеющего сложность $n + \Omega(n)$, пока остается открытым. По всей видимости, одного лишь свойства быть $B_k$-множеством недостаточно. С одной стороны, при растущих $k$ элементы $B_k$-множества неизбежно имеют сверхполиномиальный размер. С другой стороны, оценка теоремы 1 не может быть существенно улучшена, по крайней мере, для множеств Сидона.

**Теорема 2.** *При любом $n$ можно указать свободное от сумм множество Сидона $B$ мощности $n$ и сложности $\mathsf{L}(B) = n + O(n^{2/3})$.*

## Список литературы


[1] Кнут Д. Э. Искусство программирования. Т. 2. Получисленные алгоритмы. М. : Вильямс, 2007. 832 с.

[2] Pippenger N. On the evaluation of powers and monomials // SIAM J. Comput. 1980. V. 9(2). P. 230–250.

[3] Dobkin D., Lipton R. J. Addition chain methods for the evaluation of specific polynomials // SIAM J. Comput. 1980. V. 9(1). P. 121–125.

[4] Bose R. C., Chowla S. Theorems in the additive theory of numbers // Commentarii Mathematici Helvetici. 1962. V. 37. P. 141–147.

[5] Sergeev I. S. An explicit finite $B_k$-sequence. 2023. arXiv e-prints. http://arxiv.org/abs/2304.03988.

# О новом семействе оптимальных графов с чётным значением рёберной связности

**Теребин Богдан Андреевич, Абросимов Михаил Борисович**

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, e-mail: bogdan.terebin@ya.ru, mic@rambler.ru

## Введение

В работе рассматриваются простые неориентированные графы и их основные меры связности. Основные понятия из теории графов используются в соответствии с работами [1, 2]. Напомним, что граф называется *связным*, если любая пара вершин в нём соединена путём, иначе граф называется *несвязным*. *Тривиальным* называется граф, состоящий из одной вершины. Граф называется *полным*, если любые две вершины в нём смежны.

**Определение.** Вершинной связностью $k$ *графа* $G$ *называется называется минимальное количество вершин, удаление которых приводит к тривиальному или несвязному графу.*

**Определение.** Рёберной связностью $\lambda$ *нетривиального графа* $G$ *называется минимальное количество рёбер, удаление которых приводит к несвязному графу.*

К примеру, деревья имеют вершинную и рёберную связности, равные 1. У полного $n$-вершинного графа значения вершинной и рёберной связностей равны $n-1$. Далее будут рассматриваться только связные графы.

Обозначим минимальную степень вершины в графе за $\delta$. Вершинная связность $k$, рёберная связность $\lambda$ и минимальная степень вершины $\delta$ каждого графа связаны неравенством, которое было найдено Уитни [3].

**Теорема 1.** *Для любого графа* $G$ *справедливо неравенство:* $k \leq \lambda \leq \delta$

Было доказано, что для любых подходящих значений $k$, $\lambda$ и $\delta$ существует соответствующий граф [4]:

**Теорема 2.** *Для любых натуральных чисел* $a, b, c$, *таких что* $0 < a \leq b \leq c$, *существует граф* $G$, *у которого* $k = a, \lambda = b, \delta = c$.

В работе [5] рассматривалась задача о поиске графов с наименьшим количеством вершин и рёбер для любых $a, b, c$ из теоремы 2. В работах [6, 7] рассматривается следующая задача: описания графов с заданным числом вершин $n$ и с минимальным количеством рёбер для пар возможных значений $k$ и $\lambda$. В них описываются графы для некоторых определенных областей

значений $k$ и $\lambda$, которые при заданном числе вершин имеют минимальное число рёбер. В данной работе описано множество графов для новой найденной области значений $k$ и $\lambda$.

Обозначим $N_{k,\lambda}$ — минимальное число вершин, из которого может состоять граф с заданной вершинной связностью $k$ и рёберной связностью $\lambda$.

**Теорема 3.**

$$N_{k,\lambda} = \begin{cases} 2(\lambda+1)-k, & \text{при } \lambda > k, \\ \lambda+1, & \text{при } \lambda = k. \end{cases}$$

Очевидно, что построить граф, состоящий из заданного числа вершин $n$ с минимальным числом рёбер для заданных значений $k$ и $\lambda$, можно только при $n \geq N_{k,\lambda}$. Если $k = \lambda = 1$, то $N_{1,1} = 2$. Легко видеть, что граф с минимальным числом рёбер для заданного числа вершин $n$ с $k = \lambda = 1$ — это будет дерево с числом рёбер $n - 1$.

**Определение.** Диагональю порядка $i$ *назовём множество пар* $(k, \lambda)$, *удовлетворяющих следующим условиям:*

1. $\lambda - k = i$.
2. *Для заданных* $k$ *и* $\lambda$ *можно построить граф с вершинной связностью* $k$ *и рёберной связностью* $\lambda$.
3. *Граф из условия 2 является либо* $\lambda$*-регулярным, либо одна из его вершин имеет степень* $\lambda + 1$, *а остальные вершины имеют степени* $\lambda$.
4. *Условие 3 должно выполняться для графов с любым числом вершин* $n \geq N_{k,\lambda}$.

Обозначим через $D$ множество диагоналей различных порядков.

### Основной результат

**Определение.** Чётным вертикальным множеством $V_i^{(2)}$ порядка $i$ *назовём множество пар* $(k, \lambda)$, *удовлетворяющих следующим условиям:*

*1)* $(k, \lambda) \notin D$;

*2)* $\lambda - k > 1$;

*3) для заданных* $k$ *и* $\lambda$ *можно построить граф с вершинной связностью* $k$ *и рёберной связностью* $\lambda$.

**Теорема 4.** *Пусть* $(k, \lambda) \in V_i^{(2)}$. *Тогда существует* $c$ — *константа, при которой для любого* $n$, $n \geq N_{k,\lambda} + c$, *существует* $\lambda$*-регулярный граф* $G$ *с заданными* $k$ *и* $\lambda$, *состоящий из* $n$ *вершин с минимальным количеством рёбер, равным* $\lceil \lambda n/2 \rceil$.

При $n = N_{k,\lambda}$ и $n = N_{k,\lambda} + 1$ графы с разными значениями $(k, \lambda)$ имеют разную структуру, которую нельзя описать одним шаблоном. Помимо этого, минимальное число рёбер в этих случаях также определяется индивидуально, поэтому нельзя вывести формулу для подсчёта.

**Следствие.** *Пусть $G$ – граф с заданными $k$ и $\lambda$, у которого $(k, \lambda) \in V_i^{(2)}$. Тогда при $n = N_{k,\lambda}$ граф будет иметь следующий вектор степеней:*

$$d = ((N_{k,\lambda} - k)^{\lambda}, k^{(N_{k,\lambda}-k)}),$$

*то есть $\lambda$ вершин имеют степень $(N_{k,\lambda} - k)$, а остальные $(N_{k,\lambda} - k)$ имеют степень $k$.*

## Список литературы

[1] Харари Ф. Теория графов. М.: Мир, 1973.

[2] Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М.: Наука, 1997.

[3] Whitney H. Congruent graphs and the connectivity of graphs // American Journal of Mathematics. 1932. Vol. 54, issue 1. P. 150–168.

[4] Chartrand G., Harary F. Graphs with prescribed connectivities // Theory of Graphs. NY : Academic Press, 1968. P. 61–63.

[5] Абросимов М. Б., Теребин Б. А. Оптимальные реализации графов с заданными мерами связности // Матем. заметки. 2023. Том 113, выпуск 3. С. 323–331.

[6] Теребин Б. А., Абросимов М. Б. Об одном семействе оптимальных графов с заданными мерами связности // Прикладная дискретная математика. Приложение. 2022. № 15. С. 116–119.

[7] Теребин Б. А., Абросимов М. Б. О графах с заданной рёберной связностью, точками сочленения и минимальным числом рёбер // Материалы XIV Международного семинара "Дискретная математика и ее приложения" имени академика О. Б. Лупанова. М.: ИПМ им. М. В. Келдыша, 2022. С. 200–203.

# Прототип цифрового двойника сети связи

**Терентьева Юлия Юрьевна**

Центр информационных технологий и систем органов исполнительной власти им. А. В. Старовойтова, e-mail: terjul@mail.ru

## 1. Введение

В современном мире объективные тренды развития технологического обеспечения процессов разработки сложных ресурсоемких объектов и систем,

включающих этапы проектирования, испытания, производства и эксплуатации, диктуют необходимость поиска цифровых технологий, позволяющих максимально приблизить эти процессы к действиям с виртуальным аналогом физического объекта. Одной из сложных ресурсоемких систем является, несомненно, сеть связи.

В 2011 г. Сектором стандартизации электросвязи Международного союза электросвязи (Швейцария, Женева) приняты рекомендации серии Y.3000 о концепции будущих сетей FN (FutureNetwork). В основу концепции FN положены методы и средства распределённого искусственного интеллекта, технология виртуализации, когнитивные модели сетей (в целях понимания и предсказания), принципы многоагентной самоорганизации с функциями самоконфигурации, самооптимизации и самовосстановления.

Цифровой двойник (DigitalTwin) сети связи, о прототипе которого далее пойдет речь, – это программный аналог сети связи, моделирующий внутренние процессы, технические характеристики и функционирование сети, в том числе в условиях воздействий помех и окружающей среды. Программное обеспечение «Прототип цифрового двойника сети связи» предназначено для автоматизированного решения широкого спектра инженерно-технических задач построения и анализа территориально распределенных телекоммуникационных сетей высокой размерности. Данное программное обеспечение может рассматриваться как инструментарий автоматизации проектирования, модернизации и эксплуатационного сопровождения сетей связи и неоднократно использовалось в процессе проектирования реальных сетей связи.

Отметим также, что тенденции государственной политики импортозамещения диктуют условия необходимости разработки отечественных программных аналогов. Наиболее близким по функциональной направленности можно считать ГИС «Панорама», которая, однако, требует немало дополнительных модулей для решения задач проектирования и/или модернизации сети связи.

## 2. Функциональные возможности разработанного программного обеспечения «Прототип цифрового двойника сети связи»

Назначение программного обеспечения реализуется посредством совокупности трех взаимосвязанных функциональных компонент. Это визуализация, управление данными и анализ.

### 2.1 Функции визуализации

1. Представление масштабируемой карты России (до 17 уровня включительно; уровень детализации – до номеров домов). При этом имеется возможность работы с различными поставщиками карт, такими как ГИС Панорама,

Яндекс-карты и др., а также с локальным, автономным, собственным сервером, содержащим картографическую информацию. (В настоящее время ведутся работы по переводу приложения полностью на WEB-технологии. Для работы приложения потребуется только браузер на клиенте и любой сервер карт, что значительно облегчит процедуру распространения данного ПО, обновления карт и, при необходимости, расширит круг используемых технических средств, включающих, например, планшеты и мобильные устройства.)

2. Представление топологии сети связи на карте РФ.
3. Разметка узлов связи различных типов.
4. Онлайн-раскрытие основной информации об узле связи.
5. Онлайн-раскрытие основной информации о линии связи.
6. Поиск и отображение узлов связи на картографической основе (на текущем масштабе и с приближением).
7. Поиск и отображение населенных пунктов России на текущем масштабе и с приближением (более 150000 объектов согласно ОКТМО).
8. Информирование о протяженности видимой области, км.
9. Представление маршрутов на картографической основе.
10. Отображение матрицы потоков на картографической основе.
11. Отображение моделей сети совместно в различных комбинациях.
12. Отображение магистрального сегмента сети связи.
13. Отображение оперативной информации в информационных окнах: интерактивная информация об объекте связи; оценка устойчивости; оценка пропускной способности при канальной и пакетной коммутации; матрицы потоков; маршруты; потоки при пакетной коммутации; перечень узлов связи, требующих дооснащения для пропуска заявленного потока; перечень оборудования на узле связи.
14. Отображение канальной коммутации в виде цветовой индикации загруженности каналов связи в зависимости от заявленного потока направления связи и пропускной способности оборудования.
15. Отображение новых линий связи, построенных вручную или автоматически, а также их суммарная протяженность.
16. Отображение событий выхода из строя объектов сети связи с эффектом мерцания на узлах связи и интерактивным представлением информации.
17. Отображение подсетей при функциональной фрагментации сети.
18. Отображение зон контроля центров управления.

### 2.2 Функции управления данными

1. Загрузка моделей сети (порядка десяти моделей).
2. Загрузка параметров оборудования, в том числе динамическая при изменении состава и характеристик арсенала оборудования.
3. Загрузка данных мониторинга сети (объекты связи, дифференцированно вышедшие из строя в результате воздействия внутренних дестабилизирующих факторов, либо внешних дестабилизирующих факторов).
4. Возможность загрузки внешних данных в унифицированном XML-формате, что упрощает взаимосвязь с другими системами.
5. Определение статуса объекта связи (узла связи и/или линии связи) как вышедшего из строя.
6. Генерация структуры и состава узлов связи заданного типа (магистральный, зоновый, транзитный, узлы связи других категорий) с равномерным распределением.
7. Генерация структуры и состава узлов связи заданного типа с параметрами, учитывающими численность населенных пунктов РФ.
8. Нанесение метки узла связи заданного типа на карту вручную на выбранную точку.
9. Удаление меток узлов и/или линий связи; очистка модельного пространства.
10. Построение образа новой линии связи вручную.
11. Задание/изменение комплектации оборудования на узле связи.
12. Назначение потоков на направлении связи.
13. Автоматизированное рандомное задание комплектации оборудования на узлах связи для пакетной коммутации.
14. Автоматизированное рандомное задание комплектации оборудования на узлах связи для канальной комплектации при выбранном направлении связи.
15. Выгрузка информации (с фильтром протяженности) о построенных линиях связи (в т. ч. в результате автоматического построения – см. аналитические функции) с указанием протяженности.
16. Выгрузка информации о близко расположенных (с параметром) узлах связи (с параметром отдаленности) с указанием протяженности.
17. Выгрузка топологии сети связи.
18. Выгрузка картографического изображения сети связи заданного масштаба (для распечатки карты, например, в формате A0).

### 2.3 Аналитические функции

1. Построение оптимального остовного дерева топологии сети для узлов сети связи.
2. Построение оптимальных привязок узлов связи потребителей к узлам доступа.
3. Расчет нагрузки на узлы доступа, дифференцированной по клиентским интерфейсам.
4. Оптимальное восстановление связности сети связи при фрагментации [4].
5. Определение оценки устойчивости направления связи и сети связи, в том числе в динамическом режиме с выводом узлов и линий связи из строя [5].
6. Нахождение независимых маршрутов направления связи (в том числе перестраивание маршрутов с учетом вышедших из строя объектов сети связи) [6].
7. Оптимизация количества и поиск максимального количества вершинно независимых маршрутов направления связи [6, 7].
8. Определение пропускной способности направления связи при канальной и пр при пакетной коммутации [8].
9. Построение структуры потоков при пакетной коммутации (в том числе перестраивание потоков с учетом вышедших из строя объектов сети связи).
10. Определение перечня узлов связи, требующих дооснащения для пропуска заявленного трафика установленного направления связи, для канальной коммутации.
11. Генерация местоположения узлов связи при равномерном распределении.
12. Генерация местоположения узлов связи с учетом численности населенных пунктов РФ, а также коэффициента рассеивания.
13. Построение оптимального резервного пути для заданного направления связи путем определения новых линий связи.
14. Расчет оптимальной подсети для обеспечения связанности заданных узлов при минимальном количестве транзитных узлов определенного типа (например, размещение ограниченного числа комплектов определенного оборудования на узлах связи при выполнении условия обеспечения связи для заданного подмножества узлов связи и т. п.).
15. Расчет надежности системы управления согласно модели, включающей информацию о топологии сети связи, о схеме резервирования, о надежностях центров управления (расчет производится согласно комплектации оборудования и их показателей наработки на отказ), с учетом (расчетом) надежности сети связи.

16. Реализация сценария деградации сети связи посредством вывода из строя узлов и линий связи с динамической оценкой показателей устойчивости, надежности системы управления, пропускной способности направления связи при канальной и пакетной коммутации, просмотром динамически меняющихся маршрутов, степени загрузки узлов и линий связи и т. п.

## 3. Заключение

Совокупность решаемых задач цифровым двойником сети связи отражает современную мировую тенденцию развития технологий электросвязи, а сам цифровой двойник является инструментарием обеспечения качества сети связи и может быть использован для осуществления контроля качества предоставляемых услуг связи сети связи, а также выработки оптимальных решений, направленных на достижение заданных показателей качества функционирования сети связи. В работе представлено описание программного обеспечения, так называемого прототипа цифрового двойника сети связи, с изложением его (прототипа) функциональных возможностей, являющихся в свою очередь важной ступенью к непосредственно самому цифровому двойнику сети связи.

Следующим этапом разработки прототипа цифрового двойника сети связи будет являться дальнейшее использование эвристических алгоритмов для решения NP-сложных задач. В частности, будут рассмотрены подходы к решению задачи коммивояжера, которая в свою очередь может возникать в процессе мониторинга установленных событий в сетях связи [10, 11].

Автор выражает благодарность профессору Мельникову Б. Ф. за содействие в систематизации исследований.

## Список литературы

[1] Saracco R. Digital twins: Bridging physical space and cyberspace // Computer. 2019, vol. 52, no. 12. P. 58–64.

[2] Madni A. M., Madni C. C., Lucero S. D. Leveraging digital twin technology in model-based systems engineering // Systems. 2019. Vol. 7, no. 1. P. 7.

[3] Darricelli B. R., Casiraghi D., Fogli D. A survey on digital twin: Definitions, characteristics, applications, and design implications // IEEE Access. 2019. Vol. 7. P. 167, 653–671.

[4] Терентьева Ю. Ю. Некоторые теоретические вопросы практических алгоритмов дефрагментации сети связи // International Journal of Open Information Technologies. 2021. Т. 9, № 3. С. 13–21.

[5] Терентьева Ю. Ю. Метод получения оценки надежности крупномасштабной сети связи с учетом зависимых путей // Информатизация и связь. 2017. № 1. С. 122–128.

[6] Мельников Б. Ф., Стариков П. П., Терентьева Ю. Ю. Об одной задаче анализа топологии коммуникационных сетей // International Journal of Open Information Technologies. ISSN: 2307-8162. 2022. Vol. 10, no. 6. P. 1–8.

[7] Терентьева Ю. Ю. Определение максимального множества независимых простых путей между вершинами графа // Международный научный журнал «Современные информационные технологии и ИТ-образование». 2021. Том 17, № 2. ISSN 2411-1473.

[8] Кормен Т. и др. Алгоритмы: построение и анализ. 2-е изд. М.: Вильямс, 2006. 1296 с.

[9] Melnikov B. F., Melnikova E. A., Pivneva S. V., Churikova N. P., Dudnikov V. A., Prus M. Y. Multi-heuristic and game approaches in search problems of the graph theory // Информационные технологии и нанотехнологии. Сборник трудов ИТНТ-2018. Самарский национальный исследовательский университет имени академика С.П. Королева. 2018. С. 2884–2882.

[10] Макаркин С. Б., Мельников Б. Ф. Геометрические методы решения псевдогеометрической задачи коммивояжера // Стохастическая оптимизация в информатике. 2013. Т. 9. № 2. С. 54–72.

# О деревьях с размером приведённой древесной колоды 2

**Томилов Дмитрий Александрович, Абросимов Михаил Борисович**

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, e-mail: tomilov.d.a@mail.ru, mic@rambler.ru

**Определение.** *Неориентированным графом* (далее просто графом) называется пара $G = (V, \alpha)$, где $\alpha$ — симметричное и антирефлексивное отношение на множестве вершин, называемое отношением смежности.

Основные определения по теории графов даются по работам [1, 2].

**Определение.** *Дерево* — это связный граф, в котором нет циклов. Вершина степени 1 в дереве называется висячей или листом.

**Определение.** *Подграф* — граф, получающийся удалением произвольного количества вершин и всех инцидентных с ними рёбер из исходного графа.

**Определение.** *Максимальный подграф* — подграф, получающийся удалением одной произвольной вершины и всех её рёбер.

**Определение.** *Колодой графа* называется список его максимальных подграфов.

**Определение.** *Поддерево* — дерево, получающееся удалением произвольного количества висячих вершин и всех инцидентных с ними рёбер из исходного дерева.

**Определение.** *Максимальное поддерево дерева* — поддерево, получающееся удалением одной произвольной висячей вершины.

**Определение.** *Древесной колодой дерева* будем называть список его максимальных поддеревьев.

**Определение.** *Приведённая древесная колода дерева* — список попарно неизоморфных максимальных поддеревьев дерева.

Один из традиционных вопросов, рассматриваемых в различных разделах математики, касается связи между структурой объекта и его подструктурами. Главный интерес представляет то, в какой мере структура объекта определяется структурой его частей. Особое значение имеет вопрос о том, можно ли реконструировать объект по его частям.

Гипотеза реконструируемости Келли — Улама является одной из самых знаменитых открытых проблем в теории графов.

**Гипотеза** (Келли — Улама о реконструируемости, 1945)**.** *Каждый неориентированный граф на более чем двух вершинах реконструируем.*

Для деревьев гипотеза Келли — Улама была доказана Келли [3]. Харари и Палмер [4] доказали, что деревья реконструируемы и по максимальным поддеревьям. Также было доказано, что деревья реконструируемы и по приведённой древесной колоде [5].

В данной работе рассматривается задача описания деревьев с заданным размером колоды. Ранее было получены некоторые результаты о деревьях с размером приведённой колоды 1 [6]. Обозначим через $SC$ центральные деревья с размером приведённой древесной колоды 1.

Рассмотрим деревья с размером приведённой древесной колоды 2, обозначим их $PSC$ (Path Star Central). Деревья с размером приведённой колоды 2 по своей структуре представляют собой цепь, на которую крепятся различные деревья $SC$.

В работе предлагается общий вид обозначения деревьев с размером приведённой колоды 2: $PSC_{n_0}(N_i, G_i, ...)$, где

$n_0$ — размер цепи,

$N_i$ — место крепления графа $G_i$ к цепи,

$G_i$ — прикрепляемое дерево $SC$.

Каждая компонента в обозначении состоит из пары $N_i$ и $G_i$. Количество компонент может быть от 1 до 4. Количество компонент обозначим $n_i$. Рассмотрим каждое количество компонент отдельно. При $n_i = 1$ компонента

крепится на край цепи, другой край цепи не содержит компоненты. При $n_i = 2$ граф может состоять из двух разных компонент, прикреплённых к концам цепи или двух одинаковых компонент, прикреплённых симметрично относительно центра цепи. Случай $n_i = 3$ возможен, когда основная цепь дерева имеет нечётное количество вершин, тогда к концам цепи крепятся две одинаковые компоненты и третья компонента к центру цепи. При $n_i = 4$ граф состоит из двух одинаковых компонент, прикреплённых к концам цепи и двух одинаковых компонент, прикреплённых симметрично относительно центра цепи.

Количество вершин $n$ дерева при этом находится по формуле:

$$n = n_0 - n_i + \sum_{i=1}^{n_i} n(G_i), \tag{1}$$

где $n(G_i)$ — количество вершин в графе $G_i$.

Для того чтобы построить деревья с заданным количеством вершин $n$, необходимо перебрать количества прикрепленных компонент $SC$ (от 1 до 4). Тогда по формуле (1) можем найти $\sum_{i=1}^{n_i} n(G_i)$. Перебирая $n(G_i)$, строим прикреплённые компоненты $SC$ по уже описанному правилу.

Примеры деревьев данного типа приведены на рисунках 1, 2, 3, 4.

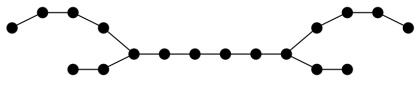

Рис. 1: $PSC_{14}(5, SC_{1,2}, 10, SC_{1,2})$

Рис. 2: $PSC_8(1, SC_{2,3}, 8, SC_{2,2})$

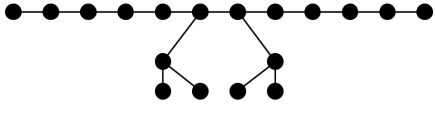

Рис. 3: $PSC_{12}(6, SC_{1,1,2,1}, 7, SC_{1,1,2,1})$

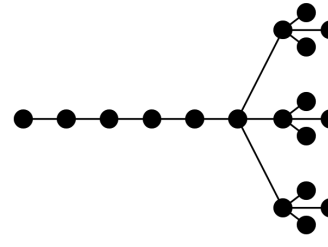

Рис. 4: $PSC_6(6, SC_{3,1,3,1})$

## Список литературы

[1] Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М. : Наука, Физматлит, 1997. 368 с.

[2] Харари Ф. Теория графов. М. : Мир, 1973. 300 с.

[3] Kelly P. J. A congruence theorem for trees // Pacific Journal of Mathematics. 1957. Volume 7. P. 961–968.

[4] Harary F., Palmer E. The reconstruction of a tree from its maximal subtrees // Canadian Journal of Mathematics. 1966. Volume 18. P. 803–810.

[5] Manvel B. Reconstruction of trees // Canadian Journal of Mathematics. 1970. Volume 22. P. 55–60.

[6] Абросимов М. Б., Володина П. А. О некоторых свойствах деревьев с размером приведенной колоды 1 // Материалы XIV Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2022 г.) / Под редакцией В. В. Кочергина. М. : ИПМ им. М. В. Келдыша, 2022. С. 172–174.

# О числе $p$-сократимых индуцированных вероятностных функций

**Трифонова Екатерина Евгеньевна**

ИПМ им. М. В. Келдыша РАН, e-mail: etrifonova@keldysh.ru

Преобразования бернуллиевских случайных величин с рациональными вероятностями посредством булевых функций были рассмотрены в работах Р. Л. Схиртладзе, Ф. И. Салимова и Р. М. Колпакова (см. [1, 2, 3], а также обзор в [4]).

Ранее автором были сформулированы [5] некоторые свойства, которыми должны обладать функции из конечно порождающего множества при условии, что функции индуцируют $p$-несократимые вероятностные функции. Если называть вероятностные функции, не являющиеся $p$-несократимыми, $p$-сократимыми, то возникает вопрос, какова доля $p$-сократимых вероятностных функций среди всех вероятностных функций, индуцированных булевыми функциями без фиктивных переменных. Особенно важной эта задача представляется в связи с тем, что универсальная функция, входящая в состав конечно порождающей системы, описанной Ф. И. Салимовым, индуцирует $p$-сократимую функцию.

Пусть $x$ — случайная величина, принимающая значение 1 и 0 с вероятностью $\widehat{x}$ и $1 - \widehat{x}$ соответственно. Тогда распределение этой случайной величины однозначно определяется значением $\widehat{x}$. Будем считать, что каждой случайной величине $x$, принимающей значения 0 и 1, сопоставлено число $\widehat{x} \in [0; 1]$.

Будем рассматривать преобразования, осуществляемые в результате подстановки независимых в совокупности случайных величин со значениями 0 и 1 вместо переменных булевых функций. При этом в качестве преобразователей будем брать только булевы функции без фиктивных переменных.

Пусть задана булева функция $f(x_1,\dots,x_n)\colon \{0,1\}^n \to \{0,1\}$, тогда *вероятностная функция* $\widehat{f}(\widehat{x}_1,\dots,\widehat{x}_n)\colon [0;1]^n \to [0;1]$, *индуцированная булевой функцией* $f(x_1,\dots,x_n)$, определяется соотношением:

$$\widehat{f}(\widehat{x}_1,\dots,\widehat{x}_n) = \sum_{\substack{(x_1,\dots,x_n):\\ f(x_1,\cdots,x_n)=1}} \prod_{i=1}^{n} (x_i\widehat{x}_i + (1-x_i)(1-\widehat{x}_i)).$$

Будем обозначать как $H(p^k)$ всевозможные правильные несократимые дроби со знаменателем $p^k$.

Пусть $f(x_1,\dots,x_n) \in P_2$ , $\widehat{f}(\widehat{x}_1,\dots,\widehat{x}_n)$ — индуцированная $f$ вероятностная функция, $p$ — простое, $p \geq 5$. Тогда если $\widehat{x}_i \in H(p^{k_i})$ для $i \in \{1,\dots,n\}$, то значение индуцированной функции $\widehat{f}$ можно представить как $\widehat{f}(\widehat{x}_1,\dots,\widehat{x}_n) = \frac{D}{p^m}$, $D \bmod p \neq 0$. При этом если $m = k_1 + \cdots + k_n$ для заданного $p$, любых $\widehat{x}_i \in H(p^{k_i})$, а также любых $k_i \in \mathbb{N}, i \in \{1,\dots,n\}$, то $\widehat{f}$ будем называть *$p$-несократимой функцией*.

Будем называть индуцированные функции, которые не обладают такими свойствами, *$p$-сократимыми функциями*. При этом заметим, что для каждой $p$-сократимой функции найдется хотя бы один такой набор значений переменных $\widehat{x}_i \in H(p^{k_i})$, что $m < k_1 + \cdots + k_n$, а равенство $m = k_1 + \cdots + k_n$ может как выполняться, так и не выполняться при других значения переменных $\widehat{x}_i \in H(p^{k_i})$.

Между булевой функцией и индуцированной ей функцией существует взаимнооднозначное соответствие. Говоря о числе $p$-сократимых функций, мы одновременно говорим и о числе булевых функций, индуцирующих $p$-сократимые функции.

Вероятностную функцию, индуцированную булевой функцией, можно записать в виде

$$\widehat{f}(\widehat{x}_1,\dots,\widehat{x}_n) = \sum_{\kappa_1,\dots,\kappa_n:\in\{0;1\}} \alpha_{\kappa_1\dots\kappa_n}\widehat{x}_1^{\kappa_1}\dots\widehat{x}_n^{\kappa_n},$$

где $\widehat{x}_i^0 = 1$, $\widehat{x}_i^1 = \widehat{x}_i$. Тогда будет ли являться функция $p$-сократимой или $p$-несократимой, определяется величиной коэффициента $\alpha_{1\dots1}$ при $\widehat{x}_1\dots\widehat{x}_n$. Очевидно, что $\widehat{f}$ будет $p$-сократимой в двух случаях:

1. $\alpha_{1\dots1} = 0$, в этом случае функцию $\widehat{f}$ будем называть $p$-сократимой первого типа;
2. $\alpha_{1\dots1} = p^tA$, где $t \geq 1$, $A \in \mathbb{Z}$, $A \bmod p \neq 0$, в этом случае функцию $\widehat{f}$ будем называть $p$-сократимой второго типа.

Заметим, что $p$-сократимые функции первого типа будут $p$-сократимыми для любого простого $p \geq 5$, а $p$-сократимые функции второго типа будут являться таковыми для одних $p$ и не будут для других.

Напомним, что для булевой функции $f(x_1, \ldots, x_n)$ единичными наборами называются совокупности значений переменных $x_1, \ldots, x_n$, на которых функция $f$ принимает единичное значение.

Обозначим число нулей в наборе $(x_1, \ldots, x_n)$ как

$$\theta(x_1, \ldots, x_n) = \sum_{i=1}^{n} (1 - x_i).$$

Число наборов с нечетным числом нулей среди единичных наборов булевой функции $f(x_1, \ldots, x_n)$ запишем как

$$\eta_o(f) = \sum_{\substack{(x_1,\ldots,x_n):\\ f(x_1,\ldots,x_n)=1}} \theta(x_1, \ldots, x_n) \bmod 2.$$

Выразим число наборов с четным числом нулей среди единичных наборов булевой функции $f(x_1, \ldots, x_n)$ следующим образом:

$$\eta_e(f) = \sum_{\substack{(x_1,\ldots,x_n):\\ f(x_1,\ldots,x_n)=1}} (1 - \theta(x_1, \ldots, x_n) \bmod 2).$$

**Лемма 1.** *Для булевой функции $f$ выполнено $\eta_e(f) = \eta_o(f)$ тогда и только тогда, когда либо $f$ содержит не менее одной фиктивной переменной, либо когда $f$ индуцирует $p$-сократимую функция первого типа.*

**Лемма 2.** *Если булева функция $f$ индуцирует $p$-сократимую функцию второго типа $\widehat{f}$, то разность $\eta_e(f) - \eta_o(f)$ будет кратна $p$.*

С использованием леммы 1 и леммы 2 доказаны следующие теоремы.

**Теорема 1.** *Доля $p$-сократимых функций первого типа среди всех индуцированных функций при $n \to \infty$ асимптотически равна $\sqrt{\frac{2}{\pi}} \frac{1}{2^{n/2}}$,*

**Теорема 2.** *Доля $p$-сократимых функций второго типа среди всех индуцированных функций при $n \to \infty$ асимптотически не превышает $\frac{1}{p}$.*

Таким образом, $p$-несократимые функции составляют асимптотически при $p \geq 5$ «большую часть» всех индуцированных вероятностных функций.

## Список литературы

[1] Схиртладзе Р. Л. О синтезе $p$-схемы из контактов со случайными дискретными состояниями // Сообщения АН ГрузССР. 1961. Т. 26, № 2. С. 181—186.

[2] Салимов Ф. И. Об одном семействе алгебр распределений // Изв. вузов. Математика. 1988. № 7. С. 64—72.

[3] Колпаков Р. М. Об оценках сложности порождения рациональных чисел вероятностными контактными $\pi$-сетями // Вестн. Моск. ун-та. Математика. Механика. 1992. № 6. С. 62—65.

[4] Яшунский А. Д. Алгебры вероятностных распределений на конечных множества // Тр. МИАН. 2018. Т. 301. С. 320–335.

[5] Трифонова Е. Е. О некоторых свойствах конечно порождающих систем преобразователей $p$-ичных дробей // Дискретный анализ и исследование операций. 2022. Т. 19. № 4. С. 124–135.

# О методе обработки большой совокупности аналоговых сигналов с целью выделения характеристических признаков источников сигналов

**Тяпаев Ливат Борисович[1], Анашин Владимир Сергеевич[2], Давыдов Виктор Вениаминович[3]**

[1] СГУ имени Н. Г. Чернышевского, e-mail: livat@yandex.ru
[2] МГУ имени М. В. Ломоносова, e-mail: vs-anashin@yandex.ru
[3] СГУ имени Н. Г. Чернышевского, e-mail: victorvd2208@yandex.ru

Вопрос классификации временных рядов по характеристикам, ассоциированным с физическими признаками, всегда является актуальным. В работе, в качестве временных рядов, используются сигналы ЭЭГ. Предлагается метод построения по временным рядам дендрограмм, соответствующих им префиксных кодов, и алгоритм классификации дендрограмм на основе геометрического представления длин кодовых последовательностей в евклидовом пространстве. Данная работа — это продолжение работы [1] по рассмотрению задачи классификации пациентов по типу психического заболевания на основе анализа дендрограмм, построенных по набору временных рядов ЭЭГ головного мозга. Мотивацией для данного исследования является метод анализа ЭЭГ для пациентов из нескольких групп — болезнь альцгеймера, шизофрения, депрессия, умеренное когнитивное расстройство и группа здоровые, предварительно разделенных по вынесенному врачебному вердикту, на основе величины p-адического квантового потенциала [2, 3]. В данном исследовании было решено пойти иным путём, а именно, провести анализ дендрограмм, как префиксных кодов. В [1], была выявлена следующая особенность: средние значения математического ожидания, энтропии и дисперсии для группы дендрограмм пациентов одного ментального класса, являются уникальными. В текущем исследовании было обнаружено следующее свойство: при сопоставлении пациенту точки на плоскости, где точка соответствует длинам двух выбранных ветвей его дендрограммы, для некоторых классов было обнаружено выстраивание их точек в параллельные линейные структуры, называемые

в дальнейшем эпсилон-цилиндрами. На основании найденного свойства был разработан алгоритм для их выявления и классификации по углам поворота относительно осей координат и линии сравнения.

В работе [1] уже было приведено описание исследуемых данных статьи [2], а также шаги преобразования записи ЭЭГ, или, точнее, преобразования набора временных рядов к набору префиксных кодов. Необходимо уточнить:

1. В исходном наборе данных всего 235 уникальных записей ЭЭГ. Есть 2 записи повторяющие уже существующие в группах mci и schiz.
2. Частоты дискретизации записей ЭЭГ не одинаковы. Встречаются как записи с частотой в 500 Герц, так и записи с частотой в 200 Герц.
3. На 2-м шаге процесса преобразования записи ЭЭГ выполнялась фильтрация данных посредством 2-х фильтров. Первым является режекторный фильтр с бесконечной импульсной характеристикой, используемый для исключения помех, вызванных колебаниями электрической сети. Вторым является фильтр высоких частот Баттерворта, используемый для исключения частот ниже 1 Герца.
4. На 5-м шаге выполнялась свертка временных рядов с шагом в 0.01 секунды. Свертка с таким шагом предполагает зависимость от частоты дискретизации сигнала. В данной работе свертка выполняется независимо — сворачивается окно в 5 единичных считываний сигнала.
5. На 6-м шаге выполняется построение дендрограммы посредством алгоритма аггломеративной кластеризации «ближайшая соседняя цепь», причем для вычисления расстояний между кластерами используется формула $\max(d(I, K), d(J, K))$, где $I$ и $J$ — это объединяемые кластеры, $K$ — любой другой, а $d$ — это отношение толерантности, определяющее расстояние между кластерами.

Для обнаружения описанного свойства нужно рассмотреть дендрограммы с геометрической точки зрения, где точка в пространстве представляется набором длин ветвей в соответствии с порядком электродов. Выстраивание точек в эпсилон-цилиндры происходит при внутриклассовой, поэлектродной нормализации. Данное свойство было обнаружено при визуальном рассмотрении комбинаций по 3 для разных зон коры головного мозга, в частности, комбинации 11(F7), 13(T3), 15(T5), соответствующей левой височной зоне.

Стоит уточнить, что эпсилон-цилиндр — это структура, состоящая из линии, определяемой двумя точками, окрестностью и точками, вошедшими в эту окрестность, а класс эпсилон-цилиндров — это набор эпсилон-цилиндров, у которых образующие линии имеют одинаковые углы наклона относительно осей координат и линии сравнения, которая необходима для ограничения общего числа классов эпсилон-цилиндров и задаётся параметрически.

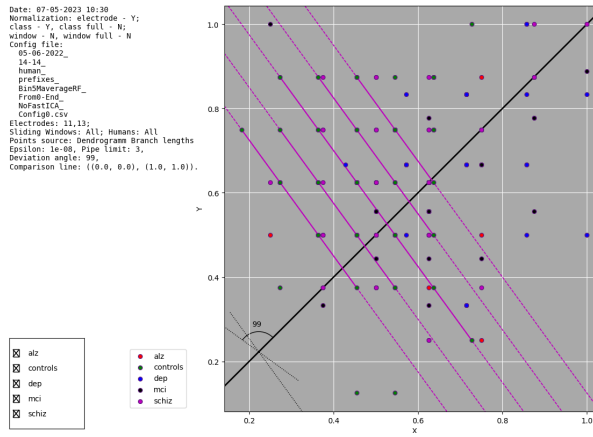


Рис. 1: Пример работы алгоритма «максимального потока точек». Рассматривается комбинация из 11 и 13 электродов. На рисунке изображен захват точек, принадлежащих только одной группе — controls ($83/96 \sim 86.5\%$)

Алгоритм «максимального потока точек» основан на расчете 2-х значений — расстояния от точки до прямой и угла между двумя прямыми. Первый шаг алгоритма — каждую пару точек связать с соответствующей им прямой, найти все точки входящие в её окрестность, так получаются эпсилон-цилиндры. Вторым шагом является вычисление для различных эпсилон-цилиндров углов относительно осей и линии сравнения. Последним шагом является построение распределения эпсилон-цилиндров согласно полученным углам.

Пример работы 2-мерной версии алгоритма изображен на рис. 1, где выделен класс эпсилон-цилиндров, захвативший точки лишь одной группы.

В отличие от алгоритма, описанного в работах [2, 3], предложенный алгоритм основан на простых геометрических вычислениях и не требует построения эмпирической функции распределения и вычисления вероятностных характеристик на основе квантового потенциала.

Стоит отметить, что предложенный метод анализа ЭЭГ может быть использован лишь как вспомогательное средство, указывающее возможный тип заболевания. Верный диагноз, посредством дополнительных исследований, может поставить только врач-специалист.

## Список литературы

[1] Анашин В. С., Тяпаев Л. Б., Давыдов В. В. Классификация психических заболеваний на основе дендрограмм ЭЭГ головного мозга и их характеристик // Труды XIV Международного научного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (20–25

июня 2022 г., Москва). М.: ИПМ им. М. В. Келдыша РАН, 2022. С. 207–210. https://doi.org/10.20948/dms-2022-64

[2] EEG $p$-adic quantum potential accurately identifies depression, schizophrenia and cognitive decline / O. Shor, A. Glik, A. Yaniv-Rosenfeld, A. Valevski, A. Weizman, A. Khrennikov, et al. // PLoS ONE 16(8): e0255529 (2021). https://doi.org/10.1371/journal.pone.0255529

[3] EEG-based spatio-temporal relation signatures for the diagnosis of depression and schizophrenia / O. Shor, A. Yaniv-Rosenfeld, A. Valevski et al. // Sci Rep 13, 776 (2023). https://doi.org/10.1038/s41598-023-28009-0

# О решении одной системы уравнений в поле Галуа

**Фаерштейн Игорь Семенович**

МГУ имени М. В. Ломоносова, e-mail: isfaer@rambler.ru

## Введение

**Определение.** *Пусть задан некоторый класс функций $K$. Будем говорить, что функция $f$, зависящая от того же множества переменных, что и функции из класса $K$, порождает функцию $g$ (при условии $g \in K$), если существует такое множество точек $X$, что $g(x)$ является единственной функцией, принадлежащей классу $K$ и удовлетворяющей соотношению $f(x) = g(x)$ для любого $x$ из множества $X$. Функция $f$ называется универсальной для класса $K$, если она порождает любую функцию из данного класса* [1].

При решении задачи о построении универсальной функции класса линейных функций, существенно зависящих от фиксированного числа переменных, была поставлена вспомогательная задача исследования систем полиномиальных уравнений определенного вида над полем $GF(2^m)$ на единственность имеющегося решения, состоящего из разных элементов, с точностью до перестановки переменных [2, 3]. Данные системы уравнений представляют собой равенства параметрам сумм нечетных степеней переменных.

**Постановка задачи**

Исследовать на единственность решения систему уравнений с точностью до перестановки переменных:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = a, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = b, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 = c, \\ x_1^7 + x_2^7 + x_3^7 + x_4^7 = d, \end{cases} \tag{1}$$

где $a, b, c, d \in GF(2^m)$ – константы, $x_1, x_2, x_3, x_4 \in GF(2^m), x_i \neq x_j$ при $i \neq j$ – попарно различные переменные.

**Доказываемое утверждение**

**Теорема.** *Если* $a^5+a^2b+a^{-1}b^2+c \neq 0$ *и существует набор попарно различных элементов поля Галуа, удовлетворяющий системе* (1)*, то система* (1) *имеет единственное решение.*

*Доказательство.* Выразим уравнения системы (1) через элементарные симметрические многочлены

$$\begin{cases} s_1 = x_1 + x_2 + x_3 + x_4, \\ s_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4, \\ s_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4, \\ s_4 = x_1x_2x_3x_4 \end{cases}$$

и подставим выражение $s_1 = a$ в остальные уравнения системы (1). Получим систему:

$$\begin{cases} a^3 + as_2 + s_3 = b, \\ a^5 + a^3s_2 + as_2^2 + a^2s_3 + s_2s_3 + as_4 = c, \\ a^7 + a^5s_2 + as_2^3 + a^4s_3 + a^2s_2s_3 + s_2^2s_3 + as_3^2 + a^3s_4 + s_3s_4 = d. \end{cases} \tag{2}$$

Пусть $a = 0, b \neq 0$. Тогда из системы (2) элементарные симметрические многочлены можно выразить следующим образом:

$$\begin{cases} s_1 = 0, \\ s_2 = b^{-1}c, \\ s_3 = b, \\ s_4 = b^{-2}c^2 + b^{-1}d. \end{cases}$$

Элементарные симметрические многочлены однозначно выражаются через правые части системы уравнений (1), что означает единственность решения системы для данного частного случая.

Пусть $a = 0, b = 0$. Тогда из системы (2) получаем следующее:

$$\begin{cases} a = b = c = d = 0, \\ s_1 = 0, \\ s_3 = 0, \\ x_1 + x_2 + x_3 + x_4 = 0, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 0. \end{cases}$$

Пусть $x_1 = \alpha, x_2 = \beta$. Тогда

$$\begin{cases} x_1 = \alpha, \\ x_2 = \beta, \\ x_3 = \alpha, \\ x_4 = \beta \end{cases}$$

или

$$\begin{cases} x_1 = \alpha, \\ x_2 = \beta, \\ x_3 = \beta, \\ x_4 = \alpha. \end{cases}$$

В данном частном случае система (1) не имеет решений, в которой все переменные принимают различные значения.

Пусть $a \neq 0$. Тогда из системы (2) элементарные симметрические многочлены можно выразить следующим образом:

$$\begin{cases} s_1 = a, \\ s_2 = (a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc), \\ s_3 = a^3 + a(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + b, \\ s_4 = ab + (a^2 + a^{-1}b)(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + a^{-1}c. \end{cases}$$

Элементарные симметрические многочлены однозначно выражаются через правые части системы уравнений (1), что означает единственность решения системы для данного частного случая.

Таким образом, для всех случаев, кроме $a^5 + a^2b + a^{-1}b^2 + c = 0$, если существует набор попарно различных элементов поля Галуа, удовлетворяющий системе (1), то система (1) имеет единственное решение. □

Возможность использования системы (1) для построения универсальных функций зависит от случая $a^5 + a^2b + a^{-1}b^2 + c = 0$.

Автор выражает благодарность профессору Вороненко А. А. за постановку задачи.

## Список литературы

[1] Вороненко А. А. Об универсальных частичных функциях для класса линейных функций // Дискретная математика. 2012. Т. 24, вып. 3. С. 62–65.

[2] Вороненко А. А., Окунева А. С. Универсальные функции для классов линейных функций двух переменных // Дискретная математика. 2020. Т. 32, вып. 1. С. 3–7.

[3] Вороненко А. А., Окунева А. С. Универсальные функции для классов линейных функций трех переменных // Прикладная математика и информатика. 2020. Т. 51. С. 114–121.

# Квантовая версия алгоритма поиска в глубину на графах

**Хадиев Камиль Равилевич**

Казанский федеральный университет, e-mail: kamilhadi@gmail.com

В данной работы была рассмотрена задача обхода графа $G = (V, E)$ в глубину, где $V$ — множество вершин, а $E$ — множество ребер. Существует целый набор алгоритмов на графах основой для которых является обход в глубину. К примеру, топологическая сортировка, поиск мостов, поиск точек сочленения, поиск циклов и т. д. [1]. Здесь мы акцентируем внимание на времени выполнения этого алгоритма. В рамках данного исследования предполагается, что граф задан списком смежности (списком соседей). Сложность классической (детерминированной) реализации алгоритма поиска в глубину равна $O(n+m)$, где $n = |V|, m = |E|$. Мы же будем исследовать задачу с точки зрения квантовых вычислений, в частности модели запросов [2, 3]. Известно, что существуют задачи, для которых разработаны квантовые алгоритмы, имеющие меньшую запросную сложность, чем классические аналоги [4]. Сложность лучшего квантового алгоритма реализующего поиск в глубину [5] равна $O(\sqrt{nm \log n})$. Обратим внимание, что при сильно разреженных графах, когда $m = o(n \log n)$, данный алгоритм оказывается хуже, чем классический. В данной работе предлагается алгоритм, сложность которого составляет $O(\sqrt{nm})$. Таким образом, наш алгоритм оказывается всегда не хуже, чем классический, а в случае когда $m = \omega(1)$ — асимптотически лучше классического. Заметим, что аналогичное ускорение можно получить и для алгоритмов, для которых поиск в глубину является основной процедурой [1].

Опишем алгоритм. Пусть $Visited \subseteq V$ будет множеством, в котором мы будем сохранять посещенные вершины. Для его реализации, к примеру, можно воспользоваться булевским массивом с диапазоном индексов от 0 до $n-1$, являющимся характеристическим вектором множества $Visited$. В этом случае, добавление нового или проверка наличия элемента в множестве выполняются за $O(1)$. Будем считать, что существуют процедуры ADD$(Visited, v)$, которая добавляет вершину $v$ в множество $Visited$; и CONTAINS$(Visited, v)$, которая возвращает $true$, если $v \in Visited$, и $false$ иначе.

Рассмотрим модифицированную реализацию алгоритма поиск в глубину. Далее мы реализуем рекурсивную процедуру $dfs(v)$, которая в качестве параметра принимает вершину $v \in V$. Также предположим, что у нас есть две дополнительные функции. Первая — функция GETNEIGHBOR$(v, i)$, которая возвращает $i$-го по счету соседа вершины $v$. Предполагаем, что сложность этой функции $O(1)$. Для этого хранение списка соседей можно сделать, к примеру, через массив. Вторая — функция NEXTNOTVISITEDNEIGHBOR$(v, i)$, которая возвращает индекс $j$ в списке соседей вершины $v$ такой, что $j > i$ и при этом соответствующая вершина $w$ не была еще посещена, т.е. $w \notin Visited$. В случае если такого индекса нет, функция вернет $NULL$. Чтобы получить минимальный индекс не посещенного соседа вершины $v$, необходима вызвать функцию с $-1$ в качестве второго аргумента. В результате мы получаем следующую реализацию функции $dfs(v)$:

ADD$(Visited, v)$
$i \leftarrow$ NEXTNOTVISITEDNEIGHBOR$(v, -1)$
**while** $(i \neq NULL)$
  $dfs($GETNEIGHBOR$(v, i))$
  $i \leftarrow$ NEXTNOTVISITEDNEIGHBOR$(v, i)$
**end while**

С точки зрения классического случая ничего не изменилось в сравнении со стандартной реализацией. В квантовом случае мы реализуем функцию NEXTNOTVISITEDNEIGHBOR$(v, i)$ воспользовавшись квантовым алгоритмом First-One-Search: поиска минимального аргумента удовлетворяющего условию [6, 7], базирующегося на квантовом алгоритме Гровера [8]. В качестве условия для индекса $x$ мы выберем предикат GETNEIGHBOR$(v, x) \notin Visited$. Сложность такого алгоритма составляет $O(\sqrt{j-i})$, где $j$ — результат работы алгоритма. В то же время алгоритм имеет вероятность ошибки 0.1. Мы имеем последовательный запуск нескольких алгоритмов First-One-Search при этом результат следующего запуска зависит от результата предыдущего. При таком построении алгоритма вероятность ошибки может накапливаться и стремиться к 1. Для того, чтобы этого не произошло, мы применяем технику

преобразования последовательности запусков First-One-Search из работы [7] базирующуюся на технике [9] с применением квантового алгоритма определения фазы [10]. В результате мы получаем алгоритм с характеристиками представленными в следующей теореме.

**Теорема 1.** *Сложность приведённого квантового алгоритма составляет* $O\left(\sqrt{nm}\right)$ *и вероятность ошибки константа не превышающая* 0.1.

**Доказательство.** Рассмотрим вершину $v$. Пусть $N_v$ — длина списка соседей $v$. Предположим, что в рамках работы $dfs(v)$ алгоритм посетил соседей вершины $v$ с индексами $j_1, \ldots, j_{L_v}$ в списке соседей, где $L_v$ — количество вершин, которое посетил алгоритм обрабатывая $v$. В этом случае сложность обработки вершины $v$ составит $O(\sqrt{j_1}+\sqrt{j_2-j_1}+\cdots+\sqrt{j_{L_v}-j_{L_v-1}})$ согласно сложности алгоритма First-One-Search [6, 7], и его последовательного запуска [7]. Эту величину в свою очередь можно ограничить следующим выражением согласно неравенству Коши-Буняковского-Шварца:

$$O(\sqrt{L_v \cdot (j_1 + j_2 - j_1 + \cdots + j_{L_v} - j_{L_v-1})}) = O(\sqrt{L_v \cdot j_{L_v}}) = O(\sqrt{L_v \cdot N_v}).$$

Итоговая сложность обработки всех вершин равна $O\left(\sum_{v\in V}\sqrt{L_v \cdot N_v}\right)$. Эту величину в свою очередь можно ограничить следующим выражением согласно неравенству Коши-Буняковского-Шварца

$$O\left(\sqrt{\sum_{v\in V} L_v} \cdot \sqrt{\sum_{v\in V} N_v}\right) = O\left(\sqrt{nm}\right).$$

Последние ограничение сверху верно в связи с тем, что выполняются условия $\sum_{v\in V} N_v \leq 2m$ (каждое ребро добавляет не более двух элементов в списки соседей) и $\sum_{v\in V} L_v \leq n$ (каждая вершина посещалась не более одного раза).

Вероятность ошибки не более 0.1, т. к. алгоритм представляет собой последовательный запуск алгоритма First-One-Search [7]. **Теорема 1 доказана.**

Работа выполнена за счёт средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект 0671-2020-0065.

## Список литературы

[1] Introduction to algorithms. / T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein. MIT press, 2022.

[2] Ambainis A. Understanding quantum algorithms via query complexity // Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018. 2018. P. 3265–3285.

[3] Ablayev F., Ablayev M., Huang J. Z., Khadiev K., Salikhova N., Wu D. On quantum methods for machine learning problems part I: Quantum tools // Big Data Mining and Analytics. 2019. V. 3, no. 1. P. 41–55.

[4] Jordan S. Quantum Algorithm Zoo: site. URL: http://quantumalgorithmzoo.org/ (дата обращения: 01.12.2023).

[5] Furrow B. A panoply of quantum algorithms // Quantum Information and Computation. 2008. V. 8, no. 8. P. 834–859.

[6] Fast classical and quantum algorithms for online $k$-server problem on trees / R. Kapralov, K. Khadiev, J. Mokut, Y. Shen, M. Yagafarov // CEUR Workshop Proceedings. 2022. V. 3072. P. 287–301.

[7] Kothari R. An optimal quantum algorithm for the oracle identification problem // 31st International Symposium on Theoretical Aspects of Computer Science. 2014. P. 482.

[8] Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of STOC'96. 1996. P. 212–219.

[9] Quantum query complexity of state conversion / T. Lee, R. Mittal, B. W. Reichardt, R. Spalek, M. Szegedy // 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. IEEE, 2011. P. 344–353.

[10] Search via quantum walk / F. Magniez, A. Nayak, J. Roland, M. Santha // Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing. 2007. P. 575–584.

# О вычислительной сложности некоторых инвариантов унографов

**Шкатов Владимир Михайлович, Абросимов Михаил Борисович**

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, e-mail: vmshkatov@gmail.com, mic@rambler.ru

В работе рассматриваются кликовое число, число независимости и хроматическое число унографов.

Здесь и далее используются основные определения по теории графов, данные в [1]. Все рассматриваемые графы неориентированные.

**Определение.** *Вектором степеней графа называется невозрастающая отсортированная последовательность степеней его вершин.*

**Определение.** *Будем называть граф унографом, если не существует никакого другого неизоморфного графа с таким же вектором степеней.*

Существуют эффективный алгоритм ответа на вопрос, является ли заданный граф унографом (см. статью [2]).

**Определение.** *Кликой графа называется любой полный подграф, содержащийся в данном графе.*

**Определение.** *Кликовым числом графа называется число вершин в наибольшей клике. Для краткости будем обозначать кликовое число графа $G$ как $clique(G)$.*

**Определение.** *Независимым множеством графа называется любое множество попарно несмежных вершин графа.*

**Определение.** *Числом независимости графа называется число вершин в наибольшем независимом множестве. Для краткости будем обозначать число независимости графа $G$ как $indep(G)$.*

**Определение.** *Хроматическим числом графа $G$ (обозначается как $\chi(G)$) называется минимальное число цветов, в которые можно окрасить вершины графа так, чтобы ни одна пара смежных вершин не была окрашена в одинаковый цвет.*

Задачи о клике, о независимом множестве и о покраске вершин графа являются классическими NP-полными задачами [3], поэтому эффективных универсальных алгоритмов для их решения неизвестно. Однако, для униграфов данные задачи могут быть решены за полиномиальное время.

### Распознавание униграфов

**Определение.** *Расщепляемым графом называется граф $G$, множество вершин которого можно разделить на два непересекающихся множества $A$ и $B$, где вершины из $A$ образуют клику, а вершины из $B$ образуют независимое множество.*

**Определение.** *Расщепляемой тройкой называется тройка $(G, A, B)$, где $G = (V, \alpha)$ — расщепляемый граф, $A$ — клика, $B$ — независимое множество, $A \cup B = V$ и $A \cap B = \emptyset$. Будем считать две тройки $(G_1, A_1, B_1)$ и $(G_2, A_2, B_2)$ изоморфными, если существует изоморфизм $\phi$ графов $G_1$ и $G_2$ и при этом $\phi(A_1) = A_2$, $\phi(B_1) = B_2$.*

**Определение.** *Пусть есть расщепляемая тройка $(G, A, B)$ и произвольный граф $H$ (при этом множества вершин $G$ и $H$ не пересекаются). Тогда композицией $F = (G, A, B) \circ H$ будем называть граф, полученный добавлением в объединение графов $G \cup H$ рёбер между каждой вершиной из $A$ и каждой вершиной из $H$. Произвольный граф $L$ называется разложимым, если его можно представить в виде подобной композиции, и неразложимым в противном случае.*

**Теорема.** *Любой граф $F$ можно представить в виде канонического разложения $F = (G_1, A_1, B_1) \circ \ldots \circ (G_k, A_k, B_k) \circ H$, где $H$ — неразложимый*

*нерасщепляемый граф, $G_i$ — неразложимые расщепляемые графы. При этом декомпозиция определяет граф с точностью до изоморфизма.*

**Теорема.** *Граф $F$ является униграфом тогда и только тогда, когда все графы в его каноническом разложении являются униграфами.*

К этой теореме в работе [4] также прилагается описание всех неразложимых униграфов в виде нескольких параметризованных классов. Структура этих графов известна, и по их вектору степеней можно легко определить класс и параметры графа, если он принадлежит к одному из них. Согласно работам [2] и [4], каноническое разложение графа ищется за линейное время, распознание принадлежности элемента разложения одному из классов неразложимых униграфов также выполнимо за линейное время.

## Быстрое вычисление кликового числа, хроматического числа и числа независимости униграфов

На основе свойств декомпозиции можно получить следующие утверждения о кликовом числе, хроматическом числе и числе независимости.

**Утверждение 1.** *Для композиции $F = (G, A, B) \circ H$, где $G$ неразложим, верно следующее соотношение: $clique(F) = clique(H) + |A|$.*

**Утверждение 2.** *Для композиции $F = (G, A, B) \circ H$, где $G$ неразложим, верно следующее соотношение: $\chi(F) = \chi(H) + |A|$.*

**Утверждение 3.** *Для композиции $F = (G, A, B) \circ H$, где $G$ неразложим, верно следующее соотношение: $indep(F) = indep(H) + |B|$.*

Утверждение 1 было впервые введено в [5], новые результаты позволили получить аналогичные утверждения 2 для хроматического числа и 3 для числа независимости.

На основе вышеизложенных в первом разделе теорем и утверждений 1, 2, 3, можно сформулировать следующую итоговую теорему.

**Теорема 1.** *Для униграфов возможно вычисление кликового числа, хроматического числа и числа независимости по вектору степеней за линейное время от числа элементов в нём.*

Для этого необходимо за линейное время получить декомпозицию графа (алгоритм описан в [2]), распознать каждый элемент полученной декомпозиции за линейное время и применить нужную формулу из одного из утверждений 1, 2, 3. При этом, поскольку структура нерасщепляемых униграфов известна, искомый инвариант определяется для них немедленно после определения их класса и параметров.

Список литературы

[1] Богомолов А. М. Алгебраические основы теории дискретных систем М. : Наука. Физматлит, 1997. 368 с.

[2] Тышкевич Р. И., Суздаль С. В. Декомпозиция графов // Избранные труды Белорусского Государственного Университета. 2001. Т. 6. С. 482–500.

[3] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи М. Мир, 1982. 416 с.

[4] Tyshkevich R. Decomposition of graphical sequences and unigraphs // Discrete Mathematics. 2000. Vol. 220. C. 201–238

[5] Шкатов В. М. Распознавание униграфов и быстрое вычисление их кликовых чисел // Проблемы теоретической кибернетики. Материалы XIX международной конференции. Под редакцией Ю. И. Журавлева. Казань: Казанский федеральный университет, 2021. С. 158–161.

# Применение тернарных квазигрупп к преобразованию слов

**Щучкин Николай Алексеевич**

Кафедра высшей математики и физики ВГСПУ, e-mail: nikolaj_shchuchkin@mail.ru

Известно широкое применение квазигруппы в криптографии (см., например, [1, 2, 3]). Здесь мы рассмотрим применения тернарных квазигрупп при шифровании. Наряду с цифровыми подписями и аутентификацией пользователя на основе пароля, шифрование является наиболее распространенным криптографическим средством, обеспечивающим безопасность связи (см. [4, стр. 26]).

Напомним, что множество $Q$ с одной тернарной операцией $f$, будем обозначать $\langle Q, f\rangle$, называют тернарной квазигруппой, если для любых элементов $a, b, c$ из $Q$ уравнения

$$f(x, b, c) = a, f(a, y, c) = b, f(a, b, z) = c \tag{1}$$

разрешимы однозначно ([5, стр. 6]).

В силу однозначной разрешимости уравнений (1), на множестве $Q$ имеются еще три тернарные операции $u, v, w$, заданные по правилам

$$u(a, b, c) = d \Leftrightarrow f(d, b, c) = a;$$

$$v(a, b, c) = d \Leftrightarrow f(a, d, c) = b;$$

$$w(a, b, c) = d \Leftrightarrow f(a, b, d) = c.$$

Операции $u, v, w$ и $f$ связаны тождествами

$$u(f(x,y,z),y,z) = x = f(u(x,y,z),y,z),$$

$$v(x,f(x,y,z),z) = y = f(x,v(x,y,z),z),$$
$$w(x,y,f(x,y,z)) = z = f(x,y,w(x,y,z)).$$

Пусть множество $Q$ конечно и $Q = \{1,2,\ldots,m\}$.

Тогда каждой тернарной квазигруппе $\langle Q, f\rangle$ соответствует 3-мерная матрица $m$-го порядка $B = (b_{ijk}|i,j,k = 1,2,\ldots,m)$ ([6], стр. 5), где $b_{ijk} = f(i,j,k)$, причем, в силу однозначной разрешимости уравнений (1), в строках направления $s$ для каждого индекса $s = 1,2,3$ стоят разные элементы из $Q$. Верно и обратное, любая 3-мерная матрица $m$-го порядка

$$B = (b_{ijk}|i,j,k = 1,2,\ldots,m),$$

у которой в строках направления $s$ для каждого индекса $s = 1,2,3$ стоят разные элементы из $Q$, определяет тернарную квазигруппу $\langle Q, f\rangle$, где $f(i,j,k) = b_{ijk}$. Между тернарными квазигруппами и 3-мерными матрицами указанного вида имеется взаимно однозначное соответствие.

Построение 3-мерной матрицы $B$ для тернарной квазигруппы $\langle Q, f\rangle$ является аналогом построения таблицы умножения для обычной квазигруппы $\langle Q, \circ\rangle$, эту таблицу называют латинским квадратом. Большое количество латинских квадратов, построенных на конечном множестве, позволяет активно использовать квазигруппы в криптографии. Аналогично имеется большое количество тернарных квазигрупп, построенных на конечном множестве. А значит, имеются перспективы использования тернарных квазигрупп в криптографии.

Преобразование слов в заданном алфавите с применением квазигрупп изучалось в работе [7], а в работах [8, 9, 10] были указаны различные преобразования слов с помощью $n$-квазигрупп. Мы же для преобразования слов будем использовать тернарные квазигруппы.

Рассмотрим конечную тернарную квазигруппу $\langle Q, f\rangle$, где $Q = \{1,\ldots,m\}$. Множество всех слов в алфавите $Q$ обозначим $Q^+ = \{x_1 \ldots x_s \mid x_i \in Q, s \geq 1\}$. Для фиксированной пары элементов $a, b$ из $Q$ на множестве $Q^+$ определим биективное отображение

$$F_{a,b}(x_1x_2\ldots x_s) = y_1y_2\ldots y_s = \begin{cases} y_1 = f(a,b,x_1), \\ y_2 = f(a,y_1,x_2), \\ y_i = f(y_{i-2},y_{i-1},x_i), i = 3,\ldots,s. \end{cases} \quad (2)$$

На множестве $Q^+$ строим еще одно отображение

$$G_{a,b}(y_1y_2\dots y_s)=x_1x_2\dots x_s=\begin{cases}x_1=w(a,b,y_1),\\ x_2=w(a,y_1,y_2),\\ x_i=w(y_{i-2},y_{i-1},y_i),\ i=3,\dots,s.\end{cases}\tag{3}$$

$G_{a,b}$ — обратное отображение для отображения $F_{a,b}$.

Для преобразования слов с помощью тернарных квазигрупп будем использовать композиции отображений вида (2). Выбираем тернарные квазигруппы $\langle Q,f_1\rangle$, $\langle Q,f_2\rangle$, ..., $\langle Q,f_t\rangle$ и упорядоченные пары $(a_1,b_1),(a_2,b_2),\dots,(a_t,b_t)$ элементов из $Q$ $(t>1)$. Строим по (2) отображения $F^1_{a_1,b_1},F^2_{a_2,b_2},\dots,F^t_{a_t,b_t}$, а затем рассматриваем композицию

$$F_{a_1,b_1,a_2,b_2,\dots,a_t,b_t}=F^1_{a_1,b_1}\circ F^2_{a_2,b_2}\circ\dots\circ F^t_{a_t,b_t}.\tag{4}$$

Для этих же тернарных квазигрупп и пар элементов строим по правилу (3) отображения $G^1_{a_1,b_1},G^2_{a_2,b_2},\dots,G^t_{a_t,b_t}$, и также рассматриваем композицию $G_{a_t,b_t,\dots,a_2,b_2,a_1,b_1}=G^t_{a_t,b_t}\circ\dots\circ G^2_{a_2,b_2}\circ G^1_{a_1,b_1}$. Очевидно, $G_{a_t,b_t,\dots,a_2,b_2,a_1,b_1}$ — обратное отображение для отображения $F_{a_1,b_1,a_2,b_2,\dots,a_t,b_t}$.

Отображение $F_{a,b}$ можно строить еще двумя способами:

$$F_{a,b}(x_1x_2\dots x_s)=y_1y_2\dots y_s=\begin{cases}y_1=f(a,x_1,b),\\ y_2=f(a,x_2,y_1),\\ y_i=f(y_{i-2},x_i,y_{i-1}),\ i=3,\dots,s,\end{cases}\tag{5}$$

или

$$F_{a,b}(x_1x_2\dots x_s)=y_1y_2\dots y_s=\begin{cases}y_1=f(x_1,a,b),\\ y_2=f(x_2,a,y_1),\\ y_i=f(x_i,y_{i-2},y_{i-1}),\ i=3,\dots,s.\end{cases}\tag{6}$$

Изучаются свойства указанных преобразований слов.

## Список литературы

[1] Глухов М. М. О применениях квазигрупп в криптографии // ПДМ. 2008. № 2. С. 28–32.

[2] Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K. On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems. 2013. Vol. 21, № 2. P. 117–130.

[3] Artamonov V. A., Chakrabarti S., Pal S. K. Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations // Discrete Applied Mathematics. 2016. P. 5–17.

[4] Венбо Мао. Современная криптография. Теория и практика. М., Киев: Издательский дом "Вильямс 2005. 768 с.

[5] Белоусов В. Д. $n$-Арные квазигруппы. Кишинев: Штиинца, 1972. 228 с.

[6] Соколов Н. П. Введение в теорию многомерных матриц. Киев: Наукова думка, 1972. 175 с.

[7] Markovski S., Gligoroski D., Bakeva V. Quasigroup string processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX. 1999. 1–2. P. 157–162.

[8] Щучкин Н. А. Преобразования строк с помощью $n$-квазигрупп // XVIII Междунар. конф. «Алгебра, теория чисел и дискретная геометрия», посвящ. 100-летию со дня рожд. проф. Б. М. Бредихина, В. И. Нечаева и С. Б. Стечкина. Тула, 23–26 сентября 2020 г. Тула: ТГПУ им. Л. Н. Толстого, 2020. С. 117–119.

[9] Щучкин Н. А. Преобразования слов в заданном алфавите // XIX Междунар. конф. «Алгебра, теория чисел, дискретная геометрия», посвящ. 200-летию со дня рожд. академика П.Л. Чебышёва. Тула: ТГПУ им. Л. Н. Толстого, 2021. С. 75–77.

[10] Щучкин Н. А. Преобразования слов с помощью $n$-квазигрупповых операций // XXI Междунар. конф. «Алгебра, теория чисел, дискретная геометрия», посвящ. 85-летию со дня рожд. А. А. Карацубы. Тула: ТГПУ им. Л. Н. Толстого, 2022. С. 119–122.

# Информация о прочитанных пленарных докладах

**Аблаев Фарид Мансурович** (Казань).
*Квантовое хеширование: эффективные конструкции, приложения.*

В докладе были представлены результаты исследований казанской квантовой группы в области квантового хеширования, вариант подхода к его возможной физической реализации. Проблема однонаправленности функции является ключевой в криптографии. Теорема Холево гарантирует свойство однонаправленности квантовой хеш-функции. Доказательство однонаправленности классических хеш-функций — открытый вопрос теории сложности. Представляются два варианта (некриптографического) использования квантовой хеш-функции: для эффективного квантового вычисления булевых функций; для эффективного поиска вхождения заданной строки в текст.

**Абросимов Михаил Борисович** (Саратов).
*Некоторые результаты, связанные с графовыми моделями отказоустойчивости.*

В докладе рассмотрены графовые модели отказоустойчивости. Основное внимание уделено моделям отказоустойчивости, предложенным Хейзом (1976) для исследования отказов элементов дискретных систем и Хейзом — Харари (1993) для исследования отказов связей. Дан обзор основных результатов и направлений исследования. Приведены некоторые последние результаты, полученные в этой области.

**Алексеев Валерий Борисович** (Москва).
*О результатах по дискретным функциям, графам, сложности алгоритмов.*

В докладе описаны основные задачи, рассматривавшиеся автором (описание замкнутых классов, оценки числа и распознавание свойств дискретных функций, разложение графов на планарные подграфы, сложность умножения матриц), и основные полученные результаты.

**Калачев Глеб Вячеславович** (Москва).
*О мерах сложности в различных моделях схем.*

Доклад был сфокусирован на различных моделях схем, включая клеточные плоские и объёмные схемы, а также их обобщения — укладки схем из функциональных элементов на графы с заданными локальными ограничениями. Помимо функциональных элементов, укладки схем включают коммутационные элементы, которые реализуют тождественные функции и играют роль проводов для передачи сигнала от одного функционального элемента к другому.

**Ковалёв Михаил Дмитриевич** (Москва).
*О математических моделях и структурных графах в теории механизмов.*

До сих пор теория плоских шарнирных конструкций (механизмов и ферм) не была в должной степени математически оформлена. Рассказано, что даёт для понимания геометрической стороны вопроса формализация в этой области. Введены две математических модели. Обсуждены особенности описания строения конструкций различными графами и условиях применимости так называемых структурных формул теории механизмов. Текст работы опубликован в данном сборнике.

**Ложкин Сергей Андреевич** (Москва).
*О некоторых результатах, полученных на кафедре математической кибернетики факультета ВМК МГУ в 2018–2022 годах.*

В докладе был представлен ряд результатов, полученных, в основном, в 2018–2022 годах и связанных, как правило, с защитой диссертаций сотрудниками или аспирантами кафедры математической кибернетики.

**Сергеев Игорь Сергеевич** (Москва).
*Сложность симметрических булевых функций.*

В докладе предпринят обзор результатов о сложности симметрических булевых функций в различных вычислительных моделях: булевы схемы, формулы, контактные схемы. Речь шла о вычислении симметрических функций общего вида, пороговых и периодических функций. Акцент сделан на результатах последних 20 лет.

# Авторский указатель

**Discrete Models in Control Systems Theory** : XI International Conference (Moscow, May 26–29, 2023) : Proceedings : M.E.: S.A. Lozhkin, D.S. Romanov, V.V. Podymov. – M. : MAKS Press, 2023. – 130 p.

ISBN 978-5-317-07114-1

The collection represents proceedings of the XI International Conference "Discrete Models in Control Systems Theory" (Moscow, May 26–29, 2023). The conference subject area includes: discrete functional systems; discrete functions properties; control systems synthesis, complexity, reliability, and diagnostics; automata; graph theory; combinatorics; coding theory; mathematical methods of information security; theory of pattern recognition; mathematical theory of intelligence systems; applied mathematical logic.

Keywords: discrete functional systems, discrete functions properties, control systems synthesis and complexity, control systems reliability and diagnostics, automata, graph theory, combinatorics, coding theory, mathematical methods of information theory, pattern recognition, intelligence systems, applied mathematical logic.

*Научное издание*

ДИСКРЕТНЫЕ МОДЕЛИ
В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ

XI Международная конференция
Москва и Подмосковье

26–29 мая 2023 г.

Издательство «МАКС Пресс»
Главный редактор: *Е.М. Бугачева*
Обложка: *А.В. Кононова*

Подписано в печать 21.12.2023 г.
Формат 60x90 1/16. Усл. печ. л. 8,125. Тираж 56 экз. Заказ 207.

Издательство ООО «МАКС Пресс»
Лицензия ИД N 00510 от 01.12.99 г.

119992, ГСП-2, Москва, Ленинские горы, МГУ им. М.В. Ломоносова,
2-й учебный корпус, 527 к.
Тел. 8495939-3890/91. Тел./Факс 8495 939-3891.

Отпечатано в полном соответствии с качеством
предоставленных материалов в ООО «Фотоэксперт»
109316, г. Москва, Волгоградский проспект, д. 42,
корп. 5, эт. 1, пом. I, ком. 6.3-23Н