МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

*Научный журнал*

**2023** **№ 60**

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

**УЧРЕДИТЕЛЬ**
**Томский государственный университет**



**Адрес редакции и издателя:** 634050, г. Томск, пр. Ленина, 36
**E-mail:** pank@mail.tsu.ru

*В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.*

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Редактор-переводчик *Т. В. Бутузова*
Верстка *И. А. Панкратовой*

---

Подписано к печати 05.06.2023. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 15. Тираж 300 экз.
Заказ № 5480. Цена свободная. Дата выхода в свет 08.06.2023.

---

Отпечатано на оборудовании
Издательства Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

# СОДЕРЖАНИЕ

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ



## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ



## ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ



## ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ ДИСКРЕТНЫХ АВТОМАТОВ



## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ



## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

# CONTENTS

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/20710410/60/1

## ХАРАКТЕРИЗАЦИЯ БИЕКТИВНЫХ APN-ОТОБРАЖЕНИЙ В ТЕРМИНАХ РАССТОЯНИЯ МЕЖДУ ПОДГРУППАМИ СИММЕТРИЧЕСКОЙ ГРУППЫ

А. Р. Белов

*Ярославский государственный университет им. П. Г. Демидова, г. Ярославль, Россия*

**E-mail:** ashmedey@gmail.com

Изучаются биективные APN-отображения, заданные на конечном поле чётной характеристики. Свойство биективного отображения быть APN-отображением выражается в терминах расстояния Хэмминга между подгруппами симметрической группы. Предложен новый подход к построению биективных APN-отображений: задача построения APN-перестановки сведена к поиску подгруппы симметрической группы, которая далека (в смысле расстояния Хэмминга) от группы сдвигов конечного поля $\mathbb{F}_{2^n}$, и решению системы уравнений сопряжения.

**Ключевые слова:** *APN-отображение, перестановка, симметрическая группа, расстояние Хэмминга.*

## CHARACTERIZATION OF APN-PERMUTATIONS IN TERMS OF HAMMING DISTANCE BETWEEN SUBGROUPS OF SYMMETRIC GROUP

A. R. Belov

*P. G. Demidov Yaroslavl State University, Yaroslavl, Russia*

In the paper, we give a characterization of APN-permutations in terms of the Hamming distance between subgroups of the symmetric group. Let

$$T = \{\tau_\alpha \in S(\mathbb{F}_{2^n}) : \alpha \in \mathbb{F}_{2^n} \ \& \ \forall x \in \mathbb{F}_{2^n} \ (\tau_\alpha(x) = x + \alpha)\}.$$

Then permutation $\pi \in S(\mathbb{F}_{2^n})$ is APN if and only if $\mathrm{d}(T, T') = 2^n - 2$, where $T' = \pi^{-1} \cdot T \cdot \pi$ and $\mathrm{d}(T, T')$ is the Hamming distance between subgroups $T, T' \leqslant S(\mathbb{F}_{2^n})$. Using this characterization, a new approach to the construction of APN-permutations is proposed: the problem of constructing an APN-permutation is reduced to finding a suitable group $T'$ and solving the simultaneous conjugation problem $T = x^{-1} \cdot T' \cdot x$. To find suitable groups $T'$, a combinatorial approach is used, which consists in constructing some graph $G(T)$ associated with the group $T$ and searching in that graph for a maximum independent sets. Let $T' = \langle \tau_1, \tau_2, \ldots, \tau_n \rangle$. Then $\mathrm{d}(\langle \tau_i \rangle, T) = 2^n - 2$ if and only if a set of transpositions in decomposition of $\tau_i$ is a maximum independent set in $G(T)$. We have listed all maximum independent sets in the graph $G(T)$ associated with the translation group $T$ of the field $\mathbb{F}_{2^4}$. In this case the group $T'$ cannot be

constructed. Thus we have obtained the well-known result about the non-existence of APN permutations in $\mathbb{F}_{2^4}$. APN-permutations in the field $\mathbb{F}_{2^3}$ are classified by listing all possible candidates for the group $T'$: there are 8 possible groups.

**Keywords:** *APN mapping, permutation, symmetric group, Hamming distance, simultaneous conjugacy.*

## Введение

Одной из характеристик нелинейных элементов блочных шифров, которая обеспечивает устойчивость к некоторым методам анализа, является *дифференциальная равномерность* [1]. Отображения, обладающие оптимальной дифференциальной равномерностью, называются *почти совершенно нелинейными отображениями* или *APN-отображениями*.

**Определение 1.** Отображение

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

называется *APN-отображением*, если для всех $a \in \mathbb{F}_{2^n}^*$ и $b \in \mathbb{F}_{2^n}$ уравнение

$$f(x + a) - f(x) = b$$

имеет не более двух решений.

Проблема существования биективных APN-отображений на сегодняшний день не решена. Известно, что для полей $\mathbb{F}_{2^n}$, где $n = 2, 4$, таких отображений не существует [2]. Первым примером APN-перестановки для полей чётной размерности была перестановка, построенная в работе [3] для $n = 6$. Для других чётных значений $n > 6$ вопрос остаётся открытым.

Для характеризации APN-свойства будем использовать понятие *расстояния Хэмминга между перестановками*. Пусть $\Omega$ — конечное множество из $n$ элементов, $S(\Omega)$ — симметрическая группа на $\Omega$.

**Определение 2.** *Расстоянием Хэмминга между перестановками* $f, g \in S(\Omega)$ называется

$$\mathrm{d}(f, g) = |\{x \in \Omega : f(x) \neq g(x)\}|.$$

**Определение 3.** *Расстоянием Хэмминга между подгруппами* $G, G' < S(\Omega)$ называется

$$\mathrm{d}(G, G') = \min_{\substack{g \in G \setminus \{e\} \\ g' \in G' \setminus \{e\}}} \mathrm{d}(g, g').$$

**Утверждение 1.** Пусть разложение перестановок $f, g \in S(\Omega)$ в произведение независимых циклов имеет вид

$$f = \omega_1 \dots \omega_s \tau_1 \dots \tau_k, \quad g = \omega_1 \dots \omega_s \sigma_1 \dots \sigma_l,$$

где $\tau_i, \omega_i, \sigma_i$ — транспозиции и $\tau_i \neq \sigma_j$ для всех $i, j$. Тогда

$$\mathrm{d}(f, g) = n - 2s - |\mathrm{fix}(f) \cap \mathrm{fix}(g)|,$$

где $\mathrm{fix}(\pi) = \{x \in \Omega : \pi(x) = x\}$.

## 1. Характеризация биективных APN-отображений

Любой элемент поля $\alpha \in \mathbb{F}_{2^n}$ определяет биективное отображение

$$\tau_\alpha : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}, \quad x \longmapsto x + \alpha.$$

Множество всех таких отображений $T = \{\tau_\alpha : \alpha \in \mathbb{F}_{2^n}\}$ образует подгруппу симметрической группы $S(\mathbb{F}_{2^n})$. Отметим простейшие свойства группы $T$:

1) $T$ состоит из перестановок порядка 2;
2) каждая перестановка $\tau \in T \setminus \{e\}$ не имеет неподвижных точек;
3) каждая перестановка $\tau \in T \setminus \{e\}$ раскладывается в произведение независимых циклов следующим образом:

$$\tau = (\alpha_1\alpha_2)(\alpha_3\alpha_4)\dots(\alpha_{2^n-1}\alpha_{2^n}),$$

где $\alpha_i$, $i = 1, \dots, 2^n$ — различные элементы поля $\mathbb{F}_{2^n}$;
4) группа $T$ изоморфна прямому произведению $n$ циклических групп порядка 2.

Если $\{e_1, e_2, \dots, e_n\}$ — некоторый базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$, то в качестве образующих группы $T$ можно взять перестановки $\tau_{e_1}, \tau_{e_2}, \dots, \tau_{e_n}$.

Свойство биективного отображения $f$ быть APN-отображением можно выразить через метрические отношения между элементами сопряжённых групп.

**Утверждение 2.** Перестановка $f \in S(\mathbb{F}_{2^n})$ является APN-отображением тогда и только тогда, когда

$$\mathrm{d}(T, T') = 2^n - 2,$$

где $T' = f^{-1} \cdot T \cdot f$.

***Доказательство.*** Пусть $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — биективное APN-отображение. Тогда по определению уравнение

$$f(x + a) - f(x) = b$$

имеет не более двух решений для всех $a \in \mathbb{F}_{2^n}^*$ и $b \in \mathbb{F}_{2^n}$. Это уравнение можно переписать в виде

$$f(x + a) = f(x) + b.$$

Если посмотреть на $f$ как на элемент группы $S(\mathbb{F}_{2^n})$, то в этом уравнении слева стоит произведение перестановок $\tau_a$ и $f$, а справа — произведение $f$ и $\tau_b$. С учётом этого уравнение можно записать в виде

$$[\tau_a \cdot f](x) = [f \cdot \tau_b](x), \tag{1}$$

где через $f \cdot g$ обозначается произведение перестановок $f$ и $g$ [4], определённое по правилу $[f \cdot g](x) = g(f(x))$. Домножив обе части уравнения (1) слева на $f^{-1}$, получим

$$[f^{-1} \cdot \tau_a \cdot f](x) = \tau_b(x).$$

При таком преобразовании число решений не изменилось.

Введём обозначение $\tau'_a = f^{-1} \cdot \tau_a \cdot f$. Тогда уравнение примет окончательный вид

$$\tau'_a(x) = \tau_b(x), \tag{2}$$

где в левой части на $x$ действует перестановка из $T'$, а в правой — один из сдвигов группы $T$. Пусть $m_{a,b}$ — число решений уравнения (2). Тогда

$$m_{a,b} = 2^n - \mathrm{d}(\tau'_a, \tau_b).$$

Так как по условию $m_{a,b} \leqslant 2$, то $\mathrm{d}(\tau'_a, \tau_b) \geqslant 2^n - 2$. Неравенство верно для всех $\tau'_a \in \in T' \setminus \{e\}$ и $\tau_b \in T \setminus \{e\}$, а значит, $\mathrm{d}(T, T') \geqslant 2^n - 2$.

Так как перестановки $\tau'_a$ и $\tau_b$ сопряжены, они имеют одинаковую цикловую структуру. Выпишем разложение в произведение независимых циклов перестановки $\tau'_a$ и всех перестановок группы $T$:

$$\begin{aligned}
\tau'_a &= \sigma_1 \dots \sigma_{2^n}, \\
\tau_1 &= e, \\
\tau_2 &= \pi_{1,2} \dots \pi_{2^{n-1},2}, \\
&\dots \\
\tau_{2^n} &= \pi_{1,2^n} \dots \pi_{2^{n-1},2^n}.
\end{aligned}$$

Все транспозиции $\pi_{i,j}$ различны. Их количество равно $(2^n-1)2^{n-1}$, что совпадает с числом всевозможных транспозиций, составленных из $2^n$ элементов поля $\mathbb{F}_{2^n}$. Значит, для любой транспозиции $\sigma_i$ из разложения $\tau'_a$ найдётся элемент $\tau_j$, для которого $\sigma_i = \pi_{s,j}$. Кроме того, $\sigma_i$ — единственная транспозиция из разложения $\tau'_a$, которая встречается в разложении $\tau_j$. Поэтому, используя утверждение 1, получаем

$$d(\tau'_a, \tau_j) = 2^n - 2 \cdot 1 - 0 = 2^n - 2.$$

Значит, $\mathrm{d}(T, T') = 2^n - 2$.

Обратно, пусть $\mathrm{d}(T, T') = 2^n - 2$. Если предположить, что $f$ не является APN-перестановкой, то получим для некоторых $\tau'_a \in T' \setminus \{e\}$ и $\tau_b \in T \setminus \{e\}$ расстояние

$$\mathrm{d}(\tau'_a, \tau_b) = 2^n - m_{a,b} < 2^n - 2,$$

что противоречит условию $\mathrm{d}(T, T') = 2^n - 2$. ■

## 2. Комбинаторный подход к построению APN-перестановок

Используя полученную характеризацию, можно предложить следующий подход к построению APN-перестановок:

1) Найти подгруппу $T' \leqslant S(\mathbb{F}_{2^n})$, изоморфную группе сдвигов $T$, для которой $\mathrm{d}(T, T') = 2^n - 2$. Эта подгруппа должна удовлетворять свойствам 1–4 группы $T$.
2) Найти такую сопрягающую перестановку $f \in S(\mathbb{F}_{2^n})$, что $T' = f^{-1} \cdot T \cdot f$.
   Для этого нужно решить систему уравнений сопряжения. Достаточно искать сопрягающую перестановку, которая переводит образующие одной группы в образующие другой группы. Таким образом, система состоит из $n$ уравнений сопряжения.

Основная сложность здесь заключается в поиске подходящей группы $T'$. Для решения второй задачи можно воспользоваться одним из алгоритмов решения подобных систем [5–7].

**Пример 1.** Пусть $n = 3$ и поле $\mathbb{F}_{2^3}$ задано корнем $\alpha$ полинома $x^3 + x + 1$. Тогда если каждому элементу поля $a_0 + a_1\alpha + a_2\alpha^2$ поставить в соответствие целое число $a_0 + a_1 2 + a_2 2^2$, то группа $T$ состоит из следующих элементов:

$$\begin{gathered}
\tau_0 = e; \\
\tau_1 = (01)(23)(45)(67);\ \tau_2 = (02)(13)(46)(57); \\
\tau_3 = (03)(12)(47)(56);\ \tau_4 = (04)(15)(26)(37); \\
\tau_5 = (05)(14)(27)(36);\ \tau_6 = (06)(17)(24)(35); \\
\tau_7 = (07)(16)(25)(34).
\end{gathered}$$

В качестве $T'$ возьмём группу из следующих элементов:

$$\tau'_0 = e;$$
$$\tau'_1 = (01)(27)(34)(56);\ \tau'_2 = (07)(12)(35)(46);$$
$$\tau'_3 = (02)(17)(36)(45);\ \tau'_4 = (03)(14)(26)(57);$$
$$\tau'_5 = (04)(13)(25)(67);\ \tau'_6 = (05)(16)(24)(37);$$
$$\tau'_7 = (06)(15)(23)(47).$$

Для неё $\mathrm{d}(T, T') = 2^3 - 2 = 6$. Если мы найдём отображение, которое сопряжением переводит $T$ в $T'$, то оно будет искомым биективным APN-отображением. Для этого достаточно найти отображение, которое переводит множество порождающих перестановок группы $T$ в множество порождающих группы $T'$, т. е. решить уравнение

$$x^{-1} \cdot \{\tau_1, \tau_2, \tau_4\} \cdot x = \{\tau'_1, \tau'_2, \tau'_6\}.$$

Допустим, что искомая перестановка $f$ переводит $\tau_1$ в $\tau'_1$, $\tau_2$ в $\tau'_2$, $\tau_4$ в $\tau'_6$ и $f(0) = 0$. Тогда транспозиция $(01)$ должна переходить в $(01)$, $(02)$ — в $(07)$, а транспозиция $(04)$ — в $(05)$. Отсюда $f(1) = 1$, $f(2) = 7$, $f(4) = 5$. Используя эти данные, получаем, что $(23)$ должна переходить в $(27)$, $(45)$ — в $(56)$, $(46)$ — в $(35)$. Значит, $f(3) = 2$, $f(5) = 6$, $f(6) = 3$. Наконец, транспозиция $(67)$ должна переходить в $(34)$, откуда $f(7) = 4$. Искомая перестановка равна

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 7 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}.$$

В примере 1 для построения группы $T'$ использована известная APN-перестановка:

$$T' = \mathrm{inv}^{-1} \cdot T \cdot \mathrm{inv},$$

где $\mathrm{inv} = (2,5)(3,6)(4,7)$ — перестановка обращения в поле $\mathbb{F}_{2^3}$. Но как построить $T'$ без использования известных APN-перестановок?

Можно попытаться построить группу $T'$, используя следующую стратегию:

1) найти инволюцию $\tau' \in S(\mathbb{F}_{2^n})$ без неподвижных точек с условием $\mathrm{d}(T, \langle \tau' \rangle) = 2^n - 2$;
2) достроить $\langle \tau' \rangle$ до группы $\langle \tau', \tau'_2, \tau'_3, \ldots, \tau'_n \rangle$, изоморфной $T$ и находящейся на расстоянии $2^n - 2$ от неё.

Переведём первую подзадачу на язык теории графов. Определим граф $G = (V, E)$ следующим образом: $V$ — множество всевозможных транспозиций из $S(\mathbb{F}_{2^n})$; $(v_1, v_2) \in E \iff v_1$ и $v_2$ зависимы или $v_1$ и $v_2$ входят в разложение некоторого сдвига $\tau \in T$.

**Пример 2.** Для группы сдвигов из примера 1 часть графа $G$, соответствующая сдвигам $\tau_1, \tau_3, \tau_5$, приведена на рис. 1. Рёбра чёрного цвета обусловлены вхождением транспозиций в разложение сдвигов $\tau_1, \tau_3, \tau_5$, а цветные рёбра — зависимостью транспозиций.

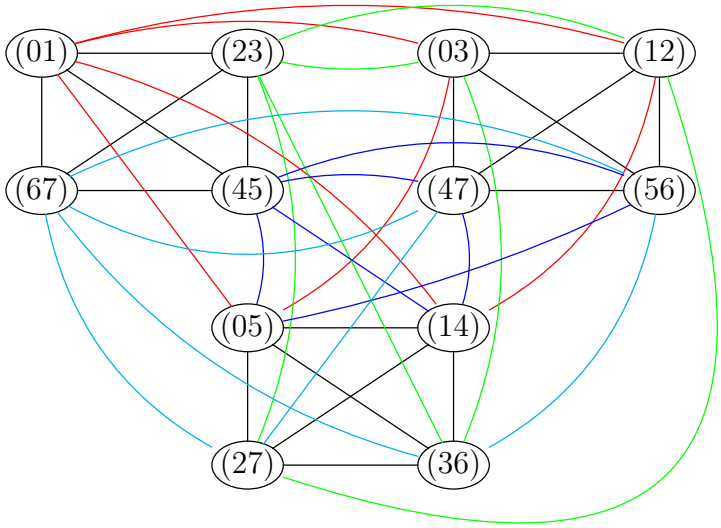


Рис. 1

**Утверждение 3.** Пусть $\tau' = \omega_1 \dots \omega_{2^{n-1}} \in S(\mathbb{F}_2^n)$ — инволюция без неподвижных точек; $\omega_i$ — независимые транспозиции ($i = 1, \dots, 2^{n-1}$). Тогда условие $\mathrm{d}(\langle \tau' \rangle, T) = 2^n - 2$ выполнено тогда и только тогда, когда множество вершин $\{\omega_1, \dots, \omega_{2^{n-1}}\}$ является наибольшим независимым множеством в графе $G$.

***Доказательство.*** Следует из определения графа $G$ и утверждения 1. ■

Для построения всех подходящих инволюций можно воспользоваться алгоритмом перечисления максимальных независимых подмножеств, среди которых нужно выбрать наибольшие. В работе [8] предложен алгоритм решения этой задачи, имеющий сложность $O(ve\mu)$, где $v, e, \mu$ — число вершин, рёбер и максимальных независимых множеств в графе соответственно. В данном случае граф $G$ имеет $v = (2^n - 1)2^{n-1}$ вершин и является $d$-регулярным, где $d = (2^{n-1} - 1) + 2(2^n - 2)$. Поэтому число вершин равно $e = vd/2 = 5 \cdot 2^{n-3}(2^n - 2)(2^n - 1)$. Параметр $\mu$ можно грубо оценить сверху количеством независимых множеств $i(G)$ в графе $G$. В работе [9] дана оценка на $i(G)$ для $d$-регулярных графов:

$$i(G) \leqslant (2^{d+1} - 1)^{v/2d}.$$

Перечисление всех возможных инволюций возможно лишь при значениях $n < 5$. Так, для $n = 4$ число максимальных независимых множеств в графе равно $\mu = 1390080$, среди которых имеется 167040 наибольших.

Пусть инволюция $\tau'$ уже построена. Достроим её до группы $\langle \tau', \tau'_2, \dots, \tau'_n \rangle \cong T$. Образующие этой группы следует искать среди инволюций без неподвижных точек $g$, для которых выполнены следующие два условия:

1) $g$ коммутирует с $\tau'$, т. е. $g\,\tau' g^{-1} = \tau'$;
2) разложение $g$ в произведение независимых циклов образует наибольшее независимое множество в графе $G$.

Подсчитаем количество всевозможных инволюций $g$, для которых выполнено первое условие. Обозначим множество таких $g$ через $C(\tau')$. Пусть разложение $\tau'$ имеет вид

$$\tau' = (a_1, b_1) \dots (a_{2^{n-1}}, b_{2^{n-1}}).$$

Тогда из условия 1 следует

$$g\,\tau' g^{-1} = (g(a_1), g(b_1)) \dots (g(a_{2^{n-1}}), g(b_{2^{n-1}})) = \tau',$$

т. е. $g$ перемешивает циклы $\tau'$: для любой транспозиции $(a_i, b_i)$ найдётся другая транспозиция $(a_j, b_j)$, такая, что $g(a_i) = a_j$, $g(b_i) = b_j$ или $g(a_i) = b_j$, $g(b_i) = a_j$. Таким образом, для построения всевозможных инволюций $g$ достаточно $\mathrm{C}^2_{2^{n-1}}\mathrm{C}^2_{2^{n-1}-2}\dots\mathrm{C}^2_2$ способами разбить на пары транспозиции из разложения $\tau'$, а затем для каждого варианта $2^{n-2}$ способами выбрать значения $g(a_i), g(b_i), 1 \leqslant i \leqslant 2^{n-1}$. Получаем

$$|C(\tau')| = 2^{n-2}\mathrm{C}^2_{2^{n-1}}\mathrm{C}^2_{2^{n-1}-2}\dots\mathrm{C}^2_2.$$

Среди всех $g \in C(\tau')$ нужно оставить только те, которые удовлетворяют условию 2. Обозначим множество таких инволюций через $MC(\tau')$. Для построения группы $T'$ осталось выбрать $n-1$ образующих $\tau'_2, \dots, \tau'_n \in MC(\tau')$. Такой способ построения группы $T'$ возможен для небольших значений $n \leqslant 5$.

Приведём результаты вычислительных экспериментов для $n = 3, 4$. В случае $n = 3$ граф $G$ имеет 56 наибольших независимых множеств. Каждому независимому множеству соответствует инволюция $\tau'$, для которой $|C(\tau')| = 12$, $|MC(\tau')| = 6$. По каждому множеству $MC(\tau')$ восстанавливается группа $T'$. Таким образом получены все восемь групп, удовлетворяющих условиям утверждения 2:

$$\begin{aligned}
T_1 &= \langle (01)(25)(37)(46),\ (02)(15)(36)(47),\ (06)(14)(23)(57)\rangle;\\
T_2 &= \langle (01)(27)(35)(46),\ (06)(14)(25)(37),\ (07)(12)(36)(45)\rangle;\\
T_3 &= \langle (01)(26)(34)(57),\ (02)(16)(35)(47),\ (07)(15)(24)(36)\rangle;\\
T_4 &= \langle (01)(24)(36)(57),\ (06)(13)(25)(47),\ (07)(15)(23)(46)\rangle;\\
T_5 &= \langle (01)(26)(35)(47),\ (02)(16)(37)(45),\ (07)(14)(23)(56)\rangle;\\
T_6 &= \langle (01)(25)(36)(47),\ (03)(16)(24)(57),\ (07)(14)(26)(35)\rangle;\\
T_7 &= \langle (01)(24)(37)(56),\ (03)(17)(25)(46),\ (06)(15)(27)(34)\rangle;\\
T_8 &= \langle (01)(27)(34)(56),\ (06)(15)(23)(47),\ (07)(12)(35)(46)\rangle.
\end{aligned}$$

Среди $8! = 40320$ перестановок имеется 10752 APN-перестановок, которые разбиваются на восемь классов эквивалентности: каждая APN-перестановка является решением одной из восьми систем уравнений сопряжения $T_i = x^{-1} \cdot T \cdot x$. Для $n = 4$ граф $G$ имеет 167040 наибольших независимых множеств. При этом для каждого независимого множества и соответствующей инволюции $\tau'$ выполняется $|C(\tau')| = 1680$, $|MC(\tau')| = 0$, что соответствует известному результату [2] о несуществовании APN-перестановок для $n = 4$.

## Заключение

В работе представлен способ характеризации биективных APN-отображений с помощью метрических отношений между элементами сопряжённых групп. Предложен подход к построению биективных APN-отображений: задача сведена к поиску группы $T'$ специального вида и решению уравнения сопряжения $T' = x^{-1} \cdot T \cdot x$, где $T$ — группа сдвигов поля $\mathbb{F}_{2^n}$. Целью дальнейших исследований в этом направлении является изучение задачи эффективного построения группы $T'$.

## ЛИТЕРАТУРА


1. *Городилова А. А.* От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3 (33). С. 16–44.
2. *Hou X.-D.* Affinity of permutations of $F_2^n$ // Discr. Appl. Math. Special Issue: Coding and Cryptography Archive. 2006. V. 154. P. 313–325.
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
4. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: Учебник. 2-е изд., испр. и доп. СПб.: Лань, 2015. 608 с.
5. *Fontet M.* Calcul de Centralisateur d'un Grupe de Permutatations // Bull. Soc. Math. France Mem. 1977. No. 49–50. P. 53–63.
6. *Sridhar M. A.* A fast algorithm for testing isomorphism of permutation networks // IEEE Trans. Computers. 1989. No. 38 (6). P. 903–909.
7. *Brodnik A., Malnič A., and Požar R.* The Simultaneous Conjugacy Problem in the Symmetric Group. `https://arxiv.org/abs/1907.07889`. 2020.
8. *Tsukiyama S., Ide M., Ariyoshi H., and Shirakawa I.* A new algorithm for generating all the maximal independent sets // SIAM J. Comput. 1977. No. 6. P. 505–517.
9. *Zhao Y.* The number of independent sets in a regular graph // Combinatorics, Probability and Computing. 2010. V. 19. P. 315–320.


## REFERENCES


1. *Gorodilova A. A.* Ot kriptoanaliza shifra k kriptograficheskomu svoystvu bulevoy funktsii [From cryptanalysis to cryptographic property of a Boolean function]. Prikladnaya Diskretnaya Matematika, 2016, no. 3 (33), pp. 16–44. (in Russian)
2. *Hou X.-D.* Affinity of permutations of $F_2^n$. Discr. Appl. Math. Special Issue: Coding and Cryptography Archive, 2006, vol. 154, pp. 313–325.
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six. Amer. Math. Soc., 2010, no. 518, pp. 33–42.
4. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Uchebnik [Algebra: Textbook]. Saint Petersburg, Lan Publ., 2015. 608 p. (in Russian)
5. *Fontet M.* Calcul de Centralisateur d'un Grupe de Permutatations. Bull. Soc. Math. France Mem., 1977, no. 49–50, pp. 53–63.
6. *Sridhar M. A.* A fast algorithm for testing isomorphism of permutation networks. IEEE Trans. Computers, 1989, no. 38 (6), pp. 903–909.
7. *Brodnik A., Malnič A., and Požar R.* The Simultaneous Conjugacy Problem in the Symmetric Group. `https://arxiv.org/abs/1907.07889`, 2020.
8. *Tsukiyama S., Ide M., Ariyoshi H., and Shirakawa I.* A new algorithm for generating all the maximal independent sets. SIAM J. Comput., 1977, no. 6, pp. 505–517.
9. *Zhao Y.* The number of independent sets in a regular graph. Combinatorics, Probability and Computing, 2010, vol. 19, pp. 315–320.

УДК 511.321 + 519.111.1 DOI 10.17223/20710410/60/2

# СВОЙСТВА ЭКСПОНЕНЦИАЛЬНЫХ ПРЕОБРАЗОВАНИЙ КОНЕЧНЫХ ПОЛЕЙ

А. А. Груба

*ООО «Центр сертификационных исследований», г. Москва, Россия*

**E-mail:** andreyka7kc@gmail.com

Изучаются экспоненциальные преобразования, действующие на множестве всех векторов заданной длины над простым полем. Для них исследуются степень нелинейности, разностная и линейная характеристики.

**Ключевые слова:** *конечные поля, линейные рекуррентные последовательности, разностная характеристика, линейная характеристика.*

# PROPERTIES OF EXPONENTIAL TRANSFORMATIONS OF FINITE FIELD

A. A. Gruba

*Certification Research Center, Moscow, Russia*

We consider exponential transformations acting on the set $V_n(p)$ of all vectors of length $n$ over a prime field $P_0 = \mathrm{GF}(p)$ ($p$ is a prime number). For every element $\gamma \in P = \mathrm{GF}(p^n)$ with a minimal polynomial $F(x)$ of degree $n$ over the field $P_0$, consider the mapping $\hat{s} : P \to P$, where $\hat{s}(0) = 0$ and if $x \neq 0$, then $\hat{s}(x) = \gamma^{\sigma(x)}$, $\sigma : P \to \{0, 1, \ldots, p^n - 1\}$ is a mapping that matches each element $x \in P$ with the number $\sigma(x) = x_0 + px_1 + \ldots + p^n x_{n-1}$, $\mathbf{x} = (x_0, \ldots, x_{n-1})$ is given by its coordinates in the basis $\alpha$ of the vector space $P_{P_0}$. Transformation $s = \tau^{-1} \cdot \hat{s} \cdot \varkappa$, where $\tau : P \to V_n(p)$ matches $x \in P$ to its set of coordinates in the basis $\alpha$ of $P_{P_0}$ and the mapping $\varkappa : P \to V_n(p)$ matches $x$ to its set of coordinates in the dual basis $\beta$ of the basis $\alpha$, is called an exponential transformation. We prove estimates for the degree of nonlinearity for an exponential transformation $s$: $(p-1)\left(n - \lceil \log_p(n+1) \rceil\right) \leqslant \deg s \leqslant n(p-1)-1$, where $\lceil z \rceil$ is the minimum integer greater or equal to $z$. It is proved that $\deg s = n(p-1)-1$ if and only if the system $\gamma/(\gamma-1)$, $(\gamma/(\gamma-1))^p, \ldots, (\gamma/(\gamma-1))^{p^{n-1}}$ is a basis of the vector space $P_{P_0}$. We also study some properties of the linear and differential characteristics of the transformation $s$.

**Keywords:** *finite fields, linear recurrence, difference characteristic, linear characteristic.*

## Введение

В работе [1] предложен и изучен класс экспоненциальных подстановок, действующих на множестве всех двоичных векторов заданной длины. Данные подстановки были использованы при построении S-боксов в алгоритме блочного шифрования BelT [2]. Координатные функции подстановок задаются с использованием отрезков линейных рекуррентных последовательностей (ЛРП) над полем GF(2) из двух элементов.

В данной работе исследуются более общий класс экспоненциальных преобразований, действующих на множестве всех векторов заданной длины над полем $\mathrm{GF}(p)$, где $p$ — простое число. Часть результатов работы [1] удаётся обобщить на предложенный класс преобразований.

Получены верхняя и нижняя оценки степени нелинейности экспоненциальных преобразований, приведены условия достижимости полученной верхней оценки, доказаны достижимые верхние и нижние оценки разностной характеристики. Для оценки линейной характеристики, которая сформулирована в асимптотическом виде в работе [3], удалось вычислить точные значения констант.

## 1. Определение экспоненциальных преобразований

Пусть $p \in \mathbb{N}$ — простое число, $P_0 = \mathrm{GF}(p) = \{0, 1, \ldots, p-1\}$ — поле из $p$ элементов, $P = \mathrm{GF}(p^n)$ — его расширение степени $n \geqslant 2$, $V_n(p) = P_0^n$ — множество всех $n$-мерных $p$-ичных векторов. Для каждого базиса $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ векторного пространства $P_{P_0}$ рассмотрим отображение $\tau : P \to V_n(p)$, действующее на каждый элемент $x \in P$ по правилу

$$\tau(x) = (x_0, x_1, \ldots, x_{n-1}),$$

где $x = x_0\alpha_0 + \ldots + x_{n-1}\alpha_{n-1}$, $x_i \in P_0$, $i = 0, 1, \ldots, p-1$, т. е. $\tau$ сопоставляет каждому элементу $x \in P$ его набор координат в базисе $\alpha$. Рассмотрим отображение $\sigma : P \to \{0, 1, \ldots, p^n - 1\}$, сопоставляющее каждому элементу $x \in P$ с координатами $\mathbf{x} = (x_0, \ldots, x_{n-1})$ число

$$\sigma(x) = x_0 + px_1 + \ldots + p^{n-1}x_{n-1}.$$

Введём обозначение $v = \tau^{-1} \cdot \sigma$, т. е. отображение $v : V_n(p) \to \{0, 1, \ldots, p^n - 1\}$ сопоставляет каждому вектору величину

$$v(\mathbf{x}) = v(x_0, \ldots, x_{n-1}) = x_0 + px_1 + \ldots + p^{n-1}x_{n-1},\ \mathbf{x} \in V_n(p).$$

Для каждого элемента $\gamma$ поля $P$, имеющего минимальный многочлен $F(x)$ степени $n$ над полем $P_0$, рассмотрим преобразование $\hat{s} : P \to P$, заданное равенствами

$$\hat{s}(x) = \begin{cases} 0, & \text{если } x = 0, \\ \gamma^{\sigma(x)}, & \text{если } x \in P \setminus \{0\}. \end{cases} \tag{1}$$

Преобразование $\hat{s}$ однозначно задаётся элементом $\gamma$ и базисом $\alpha$.

Сопоставим преобразованию $\hat{s}$, определённому равенством (1), преобразование $s$ на множестве $V_n(p)$. Пусть $\mathrm{tr} = \mathrm{tr}_{P_0}^{P}$ — функция «след» из поля $P$ в подполе $P_0$, определённая при всех $x \in P$ по правилу $\mathrm{tr}(x) = x + x^p + \ldots + x^{p^{n-1}}$. Обозначим через $\beta = (\beta_0, \ldots, \beta_{n-1})$ базис, двойственный к базису $\alpha$, т. е. удовлетворяющий условию

$$\mathrm{tr}(\alpha_i\beta_j) = \begin{cases} 0, & \text{если } i \neq j, \\ 1, & \text{если } i = j. \end{cases}$$

Такой базис существует и находится однозначно [4]. Определим отображение $\varkappa : P \to V_n(p)$, которое сопоставляет каждому элементу $x \in P$ его набор координат $(y_0, \ldots, y_{n-1})$ в базисе $\beta$:

$$\varkappa(x) = (y_0, \ldots, y_{n-1}),\ x = y_0\beta_0 + \ldots + y_{n-1}\beta_{n-1}.$$

Пусть $\varkappa_i$ — $i$-я координатная функция отображения $\varkappa$, $i = 0, 1, \ldots, n-1$. В силу линейности функции «след» имеем

$$\operatorname{tr}(\alpha_i x) = \operatorname{tr}\left(\alpha_i \sum_{j=0}^{n-1} y_j \beta_j\right) = \sum_{j=0}^{n-1} y_j \operatorname{tr}(\alpha_i \beta_j) = y_i = \varkappa_i(x). \tag{2}$$

Преобразование $s$ на множестве $V_n(p)$, определённое по правилу

$$s = \tau^{-1} \cdot \hat{s} \cdot \varkappa, \tag{3}$$

будем называть *экспоненциальным преобразованием.*

**Утверждение 1.** Для всех $\mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}$

$$s(\mathbf{x}) = \varkappa\left(\gamma^{v(\mathbf{x})}\right) = (\operatorname{tr}(\alpha_0 \gamma^{v(\mathbf{x})}), \ldots, \operatorname{tr}(\alpha_{n-1} \gamma^{v(\mathbf{x})})).$$

***Доказательство.*** Пусть $s_i$ — $i$-я координатная функция преобразования $s$, где $i = 0, 1, \ldots, n-1$. Тогда в силу равенств (2) и (3) для всех $\mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}$ имеем

$$s_i(\mathbf{x}) = \varkappa_i(\hat{s}(\tau^{-1}(\mathbf{x}))) = \varkappa_i(\gamma^{\sigma(\tau^{-1}(\mathbf{x}))}) = \varkappa_i(\gamma^{v(\mathbf{x})}) = \operatorname{tr}(\alpha_i \gamma^{v(\mathbf{x})}).$$

Утверждение 1 доказано. ■

Установим связь экспоненциальных преобразований с ЛРП над полем $P_0$. Выберем базис $u_0, u_1, \ldots, u_{n-1}$ пространства $L_{P_0}(F)$ всех ЛРП над полем $P_0$ с характеристическим многочленом $F(x)$ [4–6]. Представим ЛРП $u_j$, $j = 0, 1, \ldots, n-1$, с использованием функции «след» [4–6]:

$$u_j(i) = \operatorname{tr}(\theta_j \gamma^i), \ i \geqslant 0. \tag{4}$$

Здесь $\theta_j$ — однозначно определённый элемент поля $P$. Пусть $(0)$ — нулевая последовательность. Заметим, что для всех $c_0, \ldots, c_{n-1} \in P_0$ соотношение $c_0 u_0 + \ldots + c_{n-1} u_{n-1} = (0)$ равносильно условию $\operatorname{tr}((c_0\theta_0 + \ldots + c_{n-1}\theta_{n-1})\gamma^i) = 0$ для всех $i \geqslant 0$, а это, в свою очередь, означает, что $c_0\theta_0 + \ldots + c_{n-1}\theta_{n-1} = 0$. Таким образом, $u_0, \ldots, u_{n-1}$ — базис векторного пространства $L_{P_0}(F)$ тогда и только тогда, когда $\theta_0, \ldots, \theta_{n-1}$ — базис векторного пространства $P_{P_0}$. Зададим отображение $\pi : P_0^n \to P_0^n$, действующее по правилу, указанному в табл. 1.

Таблица 1

| $x_0$ | $x_1$ | ... | $x_{n-2}$ | $x_{n-1}$ | $\pi(x_0, \ldots, x_{n-1})$ |
|---|---|---|---|---|---|
| 0 | 0 | ... | 0 | 0 | $\mathbf{0}$ |
| 1 | 0 | ... | 0 | 0 | $(u_0(0), \ldots, u_{n-1}(0))$ |
| 2 | 0 | ... | 0 | 0 | $(u_0(1), \ldots, u_{n-1}(1))$ |
| | | ... | | | ... |
| $p-1$ | 0 | ... | 0 | 0 | $(u_0(p-2), \ldots, u_{n-1}(p-2))$ |
| 0 | 1 | ... | 0 | 0 | $(u_0(p-1), \ldots, u_{n-1}(p-1))$ |
| | | ... | | | ... |
| $p-1$ | $p-1$ | ... | $p-1$ | $p-1$ | $(u_0(p^n-2), \ldots, u_{n-1}(p^n-2))$ |

Аргументы $\mathbf{x}$ в таблице перечисляются в лексикографическом порядке (в порядке возрастания величин $v(\mathbf{x})$). Если многочлен $F(x)$ является примитивным над полем $P_0$, то среди векторов $(u_0(i), \ldots, u_{n-1}(i))$, $i = 0, 1, \ldots, p^n - 2$, появляются все ненулевые

векторы из $V_n(p)$, причём ровно по одному разу [7, 8], и отображение $\pi$ является подстановкой на множестве $V_n(p)$.

Выберем $\theta_0 = \alpha_0\gamma, \ldots, \theta_{n-1} = \alpha_{n-1}\gamma$, где $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$ — базис векторного пространства $P_{P_0}$. Ясно, что $\theta = (\theta_0, \ldots, \theta_{n-1})$ также является базисом пространства $P_{P_0}$. Согласно равенству (4) и утверждению 1, для $j$-й координатной функции $\pi_j$, $j = 0, 1, \ldots, n-1$, преобразования $\pi$ имеем

$$\pi_j(\mathbf{x}) = u_j(v(\mathbf{x}) - 1) = \mathrm{tr}(\theta_j\gamma^{v(\mathbf{x})-1}) = \mathrm{tr}(\alpha_j\gamma^{v(\mathbf{x})}) = s_j(\mathbf{x}),\ \mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}.$$

Таким образом, $s = \pi$. При фиксированном $\gamma$ и произвольном выборе базисов $\alpha$ множество всех экспоненциальных преобразований совпадает с множеством всех преобразований $\pi$, соответствующих всем базисам $\theta$ векторного пространства $P_{P_0}$ (или, что то же самое, всем базисам $u_0, u_1, \ldots, u_{n-1}$ пространства $L_{P_0}(F)$).

**Утверждение 2.** Число всех экспоненциальных преобразований на множестве $V_n(p)$ находится по формуле

$$\frac{1}{n}(p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})\sum_{d|n}\mu(d)p^{n/d},$$

где $\mu$ — функция Мебиуса.

***Доказательство.*** При фиксированном корне $\gamma$ неприводимого многочлена $F(x)$ число экспоненциальных преобразований равно числу базисов векторного пространства $L_{P_0}(F)$:

$$(p^n - 1)(p^n - p)\ldots(p^n - p^{n-1}).$$

Если выбрать другой корень $\gamma'$ многочлена $F(x)$, то получим такой же класс преобразований, что и при выборе элемента $\gamma$. При различных неприводимых многочленах $F_1(x)$ и $F_2(x)$ выполнено $L_{P_0}(F_1) \cap L_{P_0}(F_2) = \{(0)\}$ [4, 6]. Остаётся заметить [4, 6], что число неприводимых многочленов степени $n$ над полем $P_0$ равно

$$\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}.$$

Утверждение 2 доказано. ■

## 2. Степень нелинейности экспоненциальных преобразований

Рассмотрим степень нелинейности $\deg s$ экспоненциального преобразования (3). Она вычисляется [9] по формуле

$$\deg s = \min_{(a_0,\ldots,a_{n-1})\in V_n(p)\setminus\{\mathbf{0}\}} \deg(a_0 s_0(x_0, \ldots, x_{n-1}) + \ldots + a_{n-1}s_{n-1}(x_0, \ldots, x_{n-1}))$$

и равна минимальной из степеней многочленов (алгебраически нормальных форм) всех нетривиальных линейных комбинаций координатных функций $s_0, \ldots, s_{n-1}$ преобразования $s$.

Пусть $F(x)$ — неприводимый многочлен степени $n$ над полем $P_0$ с периодом $T(F)$ [4, 6], равным $(p^n-1)/d$, где $d$ — некоторый делитель числа $p^n-1$; $\gamma$ — корень многочлена $F(x)$ в расширении $P$. Рассмотрим ненулевую ЛРП $u$ с характеристическим многочленом $F(x)$ над полем $P_0$. Построим функцию $f(x_0, \ldots, x_{n-1}) = f_u(x_0, \ldots, x_{n-1})$ по правилу, указанному в табл. 2.

Таблица 2

| $x_0$ | $x_1$ | ... | $x_{n-2}$ | $x_{n-1}$ | $f(x_0,\ldots,x_{n-1})$ |
|---|---|---|---|---|---|
| 0 | 0 | ... | 0 | 0 | 0 |
| 1 | 0 | ... | 0 | 0 | $u(0)$ |
| 2 | 0 | ... | 0 | 0 | $u(1)$ |
| | | ... | | | |
| $p-1$ | 0 | ... | 0 | 0 | $u(p-2)$ |
| 0 | 1 | ... | 0 | 0 | $u(p-1)$ |
| | | ... | | | |
| $p-1$ | $p-1$ | ... | $p-1$ | $p-1$ | $u(p^n-2)$ |

Обозначим через $B_n(F)$ множество всех функций $f_u(x_0,\ldots,x_{n-1})$, где $u$ пробегает всё множество ненулевых ЛРП над полем $P_0$ с характеристическим многочленом $F(x)$. Ясно, что $|B_n(F)| = |L_{P_0}(F)\backslash(0)| = p^n - 1$. Учитывая совпадение экспоненциальных преобразований с преобразованиями, построенными на основе ЛРП, получим

$$\deg s = \min_{f\in B_n(F)} \deg f.$$

Таким образом, необходимо изучить величину $\deg f$. Рассмотрим многочлен, задающий функцию $f(x_0,\ldots,x_{n-1}) \in B_n(F)$:

$$f(x_0,\ldots,x_{n-1}) = \sum_{\mathbf{a}=(a_0,\ldots,a_{n-1})\in V_n(p)} C(\mathbf{a}) x_0^{a_0}\ldots x_{n-1}^{a_{n-1}}.$$

Обозначим через $\mathbf{b} = (p-1,\ldots,p-1)$ вектор, у которого все координаты равны $p-1$. Тогда $C(\mathbf{b})$ — коэффициент в многочлене функции $f \in B_n(F)$ при мономе $x_0^{p-1}\ldots x_{n-1}^{p-1}$.

**Утверждение 3.** Для любой функции $f_u \in B_n(F)$ выполнено $C(\mathbf{b}) = 0$. В частности, для экспоненциального преобразования $s$, определённого равенством (3), справедливо неравенство $\deg s \leqslant n(p-1)-1$.

***Доказательство.*** Пусть $f = f_u$. Согласно [10],

$$C(\mathbf{b}) = -\sum_{a_0,\ldots,a_{n-1}\in P_0} f(a_0,\ldots,a_{n-1}) = -(u(0)+u(1)+\ldots+u(p^n-2)).$$

Так как $T(F) = (p^n-1)/d$, то

$$C(\mathbf{b}) = -d\left(u(0)+u(1)+\ldots+u(T(F)-1)\right).$$

Пусть $u(i) = \mathrm{tr}(a\gamma^i)$, где $a \in P$, $\gamma$ – корень многочлена $F(x)$ в поле $P$, $i \geqslant 0$. Получим

$$C(\mathbf{b}) = -d\left(\mathrm{tr}(a)+\mathrm{tr}(a\gamma)+\ldots+\mathrm{tr}\left(a\gamma^{T(F)-1}\right)\right) = -d\,\mathrm{tr}\left(a\frac{\gamma^{T(F)}-1}{\gamma-1}\right).$$

Мультипликативный порядок $\mathrm{ord}\,\gamma$ элемента $\gamma$ равен $T(F)$, следовательно, $\gamma^{T(F)} = 1$, а значит, $C(\mathbf{b}) = 0$. ■

Пусть $k \in \{0,1,\ldots,n-1\}$. Обозначим через

$$\mathbf{b}_k = (p-1,\ldots,p-1,p-2,p-1,\ldots,p-1) = (b_0,\ldots,b_{n-1})$$

вектор, у которого $b_k = p-2$, а остальные координаты равны $p-1$. Тогда $C(\mathbf{b}_k)$ — коэффициент в многочлене, задающем функцию $f \in B_n(F)$, при мономе

$$x_0^{p-1}\ldots x_{k-1}^{p-1}x_k^{p-2}x_{k+1}^{p-1}\ldots x_{n-1}^{p-1}.$$

**Теорема 1.** Пусть $u \in L_{P_0}(F)$, $u(i) = \operatorname{tr}(a\gamma^i)$, где $i \geqslant 0$, $a \in P$, $\gamma$ — корень многочлена $F(x)$ в поле $P$. Тогда для любой функции $f = f_u \in B_n(F)$ верно равенство

$$C(\mathbf{b}_k) = \operatorname{tr}\left(a\gamma^{-1}\left(\frac{\gamma}{\gamma-1}\right)^{p^{n-k-1}}\right),\ k = 0, 1, \ldots, n-1.$$

***Доказательство.*** Обозначим через $P_0^*$ мультипликативную группу поля $P_0$. Согласно [10], имеем

$$C(\mathbf{b}_k) = -\sum_{\mathbf{a}=(a_0,\ldots,a_{n-1})\in P_0^n} a_k f(\mathbf{a}) = -\sum_{a_k\in P_0^*} a_k \sum_{a_0,\ldots,a_{k-1},a_{k+1},\ldots,a_{n-1}\in P_0} f(\mathbf{a}) =$$
$$= -\sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \sum_{i=0}^{p^{n-1-k}-1} u(sp^{n-k} + jp^{n-1-k} + i - 1).$$

Так как $u(i) = \operatorname{tr}(a\gamma^i)$, $i \geqslant 0$, то

$$C(\mathbf{b}_k) = -\sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \sum_{i=0}^{p^{n-1-k}-1} \operatorname{tr}\left(\alpha\gamma^{sp^{n-k}+jp^{n-1-k}+i-1}\right).$$

В силу линейности функции «след» получим

$$C(\mathbf{b}_k) = -\sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \operatorname{tr}\left(a\gamma^{-1}\gamma^{sp^{n-k}+jp^{n-1-k}}\,\frac{\gamma^{p^{n-1-k}}-1}{\gamma-1}\right) =$$
$$= -\sum_{j=1}^{p-1} j \operatorname{tr}\left(a\gamma^{-1}\gamma^{jp^{n-1-k}}\,\frac{\gamma^{p^{n-1-k}}-1}{\gamma-1}\,\frac{\left(\gamma^{p^{n-k}}\right)^{p^k}-1}{\gamma^{p^{n-k}}-1}\right).$$

Так как $\operatorname{ord}\gamma$ делит $p^n - 1$, то $\gamma^{p^n} = \gamma$. Значит,

$$C(\mathbf{b}_k) = -\sum_{j=1}^{p-1} \operatorname{tr}\left(ja\gamma^{-1}\,\frac{\gamma^{p^{n-1-k}}-1}{\gamma^{p^{n-k}}-1}\,\gamma^{jp^{n-1-k}}\right).$$

Пусть $\widetilde{\gamma} = \gamma^{p^{n-1-k}}$. Обозначим $S_{\widetilde{\gamma}}^{(n)} = \widetilde{\gamma} + \widetilde{\gamma}^2 + \ldots + \widetilde{\gamma}^n = \widetilde{\gamma}\,\dfrac{\widetilde{\gamma}^n - 1}{\widetilde{\gamma} - 1}$. Рассмотрим сумму

$$S = \sum_{j=1}^{p-1} j\widetilde{\gamma}^j = \widetilde{\gamma} + 2\widetilde{\gamma}^2 + \ldots + (p-1)\widetilde{\gamma}^{p-1}.$$

Ясно, что $S = S_{\widetilde{\gamma}}^{(p-1)} + \widetilde{\gamma}S_{\widetilde{\gamma}}^{(p-2)} + \ldots + \widetilde{\gamma}^{p-2}S_{\widetilde{\gamma}}^{(1)}$. Тогда

$$S = \widetilde{\gamma}\,\frac{\widetilde{\gamma}^{p-1}-1}{\widetilde{\gamma}-1} + \widetilde{\gamma}\left(\widetilde{\gamma}\,\frac{\widetilde{\gamma}^{p-2}-1}{\widetilde{\gamma}-1}\right) + \ldots + \widetilde{\gamma}^{p-3}\left(\widetilde{\gamma}\,\frac{\widetilde{\gamma}^2-1}{\widetilde{\gamma}-1}\right) + \widetilde{\gamma}^{p-2}\widetilde{\gamma} =$$
$$= \frac{\widetilde{\gamma}}{\widetilde{\gamma}-1}\left(\left(\widetilde{\gamma}^{p-1}-1\right) + \left(\widetilde{\gamma}^{p-1}-\widetilde{\gamma}\right) + \ldots + \left(\widetilde{\gamma}^{p-1}-\widetilde{\gamma}^{p-3}\right) + \left(\widetilde{\gamma}^{p-1}-\widetilde{\gamma}^{p-2}\right)\right) =$$
$$= \frac{\widetilde{\gamma}}{\widetilde{\gamma}-1}\left((p-1)\widetilde{\gamma}^{p-1} - \frac{\widetilde{\gamma}^{p-1}-1}{\widetilde{\gamma}-1}\right) = \frac{\widetilde{\gamma}}{(\widetilde{\gamma}-1)^2}\left(1-\widetilde{\gamma}^p\right).$$

Следовательно,

$$C(\mathbf{b}_k) = -\operatorname{tr}\left(a\gamma^{-1}\,\frac{\gamma^{p^{n-k-1}}-1}{\gamma^{p^{n-k}}-1}\,\frac{\gamma^{p^{n-k-1}}}{\left(\gamma^{p^{n-k-1}}-1\right)^2}\,\left(1-\left(\gamma^{p^{n-k-1}}\right)^p\right)\right) =$$
$$= \operatorname{tr}\left(a\gamma^{-1}\,\frac{\gamma^{p^{n-1-k}}}{\gamma^{p^{n-k-1}}-1}\right).$$

Таким образом,

$$C(\mathbf{b}_k) = \operatorname{tr}\left(a\gamma^{-1}\left(\frac{\gamma}{\gamma-1}\right)^{p^{n-k-1}}\right).$$

Теорема 1 доказана. ■

**Утверждение 4.** Для каждой функции $f \in B_n(F)$ равенство $\deg f = n(p-1)-1$ имеет место тогда и только тогда, когда система

$$\frac{\gamma}{\gamma-1},\ \left(\frac{\gamma}{\gamma-1}\right)^p,\ \ldots,\ \left(\frac{\gamma}{\gamma-1}\right)^{p^{n-1}} \tag{5}$$

является базисом векторного пространства $P_{P_0}$.

***Доказательство.*** Обозначим через $P^*$ мультипликативную группу поля $P$. Положим для $k = 0, 1, \ldots, n-1$

$$\widehat{\gamma}_k = \left(\frac{\gamma}{\gamma-1}\right)^{p^k}.$$

Согласно теореме 1, доказываемый факт равносилен тому, что для всех $x \in P^*$

$$(\operatorname{tr}(x\widehat{\gamma}_0), \operatorname{tr}(x\widehat{\gamma}_1), \ldots, \operatorname{tr}(x\widehat{\gamma}_{n-1})) \neq \mathbf{0}. \tag{6}$$

Пусть $\mathbf{x} = (x_0, \ldots, x_{n-1})$ — координаты элемента $x$ в базисе $\alpha$, $\mathbf{A}_k = (a_0^{(k)}, \ldots, a_{n-1}^{(k)})$ — координаты элемента $\widehat{\gamma}_k$, $k = 0, 1, \ldots, n-1$, в базисе $\beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$, который является двойственным к базису $\alpha$. Тогда

$$\operatorname{tr}(x\widehat{\gamma}_k) = \operatorname{tr}\left(\sum_{i=0}^{n-1} x_i\alpha_i \sum_{j=0}^{n-1} a_j^{(k)}\beta_j\right) = \sum_{i=0}^{n-1} a_i^{(k)}x_i = \mathbf{A}_k x^{\downarrow}.$$

Пусть

$$A = \begin{pmatrix} \mathbf{A}_0 \\ . \\ . \\ . \\ \mathbf{A}_{n-1} \end{pmatrix}_{n\times n},$$

тогда соотношение (6) равносильно неравенству $Ax^{\downarrow} \neq 0^{\downarrow}$. Таким образом, равенство (6) имеет место для всех $x \in P^*$ тогда и только тогда, когда матрица $A$ обратима над полем $P_0$, то есть система векторов (5) линейно независима. В свою очередь, это равносильно тому, что система

$$\left(\frac{\gamma}{\gamma-1}\right)^{p^k},\ k = 0, 1, \ldots, n-1,$$

является базисом векторного пространства $P_{P_0}$. ■

**Следствие 1.** Для экспоненциального преобразования $s$, определённого равенством (3), $\deg s = n(p-1)-1$ тогда и только тогда, когда система (5) является базисом векторного пространства $P_{P_0}$.

**Утверждение 5.** Пусть $\delta = \gamma/(\gamma-1)$, где $\gamma$ — корень неприводимого многочлена степени $n$ над полем $P_0$. Тогда $\delta$ — корень неприводимого многочлена степени $n$.

***Доказательство.*** Рассмотрим $m_{\delta,P_0}(x)$ — минимальный многочлен элемента $\delta$ над полем $P_0$. Пусть $k = \deg m_{\delta,\,P_0}(x)$. Согласно [6], $k$ — наименьшее натуральное число, такое, что

$$\frac{\gamma}{\gamma-1} = \left(\frac{\gamma}{\gamma-1}\right)^{p^k},$$

т. е. $\gamma(\gamma^{p^k}-1) = \gamma^{p^k}(\gamma-1)$, а значит, $\gamma = \gamma^{p^k}$. Так как $\gamma$ — корень неприводимого многочлена степени $n$, наименьшее число $k$ с таким условием равно $n$. ■

Приведём нижнюю оценку степени нелинейности экспоненциального преобразования.

**Теорема 2.** Пусть $F(x)$ — неприводимый многочлен степени $n$ над полем $P_0$. Тогда для всех $f_u \in B_n(F)$ имеет место неравенство

$$\deg f_u \geqslant (p-1)\left(n - \lceil \log_p(n+1)\rceil\right),$$

где $\lceil z\rceil$ — минимальное целое число, которое больше либо равно $z$. В частности, для экспоненциального преобразования $s$, определённого равенством (3), справедлива оценка

$$\deg s \geqslant (p-1)\left(n - \lceil \log_p(n+1)\rceil\right).$$

***Доказательство.*** Пусть $f = f_u$, где $u$ — ЛРП с характеристическим многочленом $F(x)$. Тогда $u(i) = \operatorname{tr}(\beta\gamma^i)$, $i \geqslant 0$, $\beta \in P^*$, и выполнены соотношения

$$f(\mathbf{0}) = 0, \quad f(\mathbf{x}) = u(v(\mathbf{x})-1) = \operatorname{tr}\left(\beta\gamma^{v(\mathbf{x})-1}\right), \mathbf{x} \neq \mathbf{0}.$$

Положим

$$\varepsilon = \begin{cases} 1, & \text{если } n \text{ нечётное,} \\ -1, & \text{если } n \text{ чётное.} \end{cases}$$

Тогда в силу того, что $\prod\limits_{s=1}^{p-1} s = p-1 \pmod p$ [6], для всех $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in V_n(p)$ справедливо равенство

$$f(\mathbf{x}) = \operatorname{tr}\left(\beta\gamma^{-1}\gamma^{\sum\limits_{i=0}^{n-1} x_i p^i}\right) + \varepsilon \operatorname{tr}\left(\beta\gamma^{-1}\right) \prod_{i=0}^{n-1}\prod_{s=1}^{p-1}(x_i - s).$$

Пусть $\gamma_i = \gamma^{p^i}$, $i = 0, 1, \ldots, n-1$, значит,

$$f(\mathbf{x}) = \operatorname{tr}\left(\beta\gamma^{-1}\gamma_0^{x_0}\gamma_1^{x_1}\ldots\gamma_{n-1}^{x_{n-1}}\right) + \varepsilon \operatorname{tr}\left(\beta\gamma^{-1}\right) \prod_{i=0}^{n-1}\prod_{s=1}^{p-1}(x_i - s).$$

Пусть $j \in \{0, 1, \ldots, n-1\}$. Для всех $s \in P_0$ обозначим через $f^s_{x_j}$ функцию, полученную из $f$ фиксацией переменной $x_j$ значением $s$:

$$f(x_0, \ldots, x_{j-1}, s, x_{j+1}, \ldots, x_{n-1}) = f^s_{x_j}.$$

Рассмотрим оператор $\Delta_j$ взятия суммы всех элементов поля $P_0$ по переменной $x_j$ в функции $f$, т. е.

$$\Delta_j f = \sum_{a_j \in P_0} f_{x_j}^{a_j}.$$

Тогда

$$\Delta_j f = \sum_{a_j \in P_0} \operatorname{tr}\left(\beta\gamma^{-1}\gamma_0^{x_0}\dots\gamma_{j-1}^{x_{j-1}}\gamma_j^{a_j}\gamma_{x_{j+1}}^{x_{j+1}}\dots\gamma_{n-1}^{x^{n-1}}\right) + (-1)^p\varepsilon\operatorname{tr}(\beta\gamma^{-1})\prod_{i=0,i\neq j}^{n-1}\prod_{s=1}^{p-1}(x_i-s).$$

Следовательно,

$$\begin{gathered}\Delta_j f = \operatorname{tr}\left(\beta\gamma^{-1}\frac{\gamma_j^p-1}{\gamma_j-1}\gamma_0^{x_0}\dots\gamma_{j-1}^{x_{j-1}}\gamma_{j+1}^{x_{j+1}}\dots\gamma_{n-1}^{x_{n-1}}\right)+\\ +(-1)^p\varepsilon\operatorname{tr}\left(\beta\gamma^{-1}\right)\prod_{i=0,i\neq j}^{n-1}\prod_{s=1}^{p-1}(x_i-s).\end{gathered} \tag{7}$$

С другой стороны,

$$\begin{aligned}\Delta_j f &= \sum_{c\in P_0}\sum_{\mathbf{a}=(a_0,\dots,a_{n-1})\in V_n(p)} C(\mathbf{a})x_0^{a_0}\dots x_{j-1}^{a_{j-1}}c^{a_j}x_{j+1}^{a_{j+1}}\dots x_{n-1}^{a_{n-1}} =\\ &= \sum_{a_j,\,c\in P_0} c^{a_j}\sum_{a_0,\dots,a_{j-1},a_{j+1},\dots,a_{n-1}\in P_0} C(\mathbf{a})x_0^{a_0}\dots x_{j-1}^{a_{j-1}}x_{j+1}^{a_{j+1}}\dots x_{n-1}^{a_{n-1}}.\end{aligned}$$

Справедливо равенство [10]

$$\sum_{c\in P_0} c^{a_j} = \begin{cases} p-1, & \text{если } a_j = p-1,\\ 0, & \text{если } a_j < p-1.\end{cases}$$

Значит, если $\Delta_j f$ является ненулевой функцией, то переменная $x_j$ входит в многочлен функции $f$ в степени $p-1$ и $\sum\limits_{a_j\in P_0} f(x_0,\dots,x_{j-1},a_j,x_{j+1},\dots,x_{n-1})$ содержит все те слагаемые (ненулевые), которые имеют вид

$$-C(a_0,\dots,a_{j-1},p-1,a_{j+1},\dots,a_{n-1})x_0^{a_0}\dots x_{j-1}^{a_{j-1}}x_j^{p-1}x_{j+1}^{a_{j+1}}\dots x_{n-1}^{a_{n-1}}.$$

Следовательно, если $\Delta_j f$ — ненулевая функция, то

$$\deg f \geqslant p-1+\deg(\Delta_j f). \tag{8}$$

Пусть $\Delta_k\dots\Delta_{n-2}\Delta_{n-1}f = g(x_0,\dots,x_{k-1})$, где $k = 0,1,\dots,n-1$. Согласно (7), будем иметь

$$\begin{gathered}g(x_0,\dots,x_{k-1}) =\\ = \operatorname{tr}\left(\beta\gamma^{-1}\frac{\gamma_k^p-1}{\gamma_k-1}\dots\frac{\gamma_{n-1}^p-1}{\gamma_{n-1}-1}\gamma_0^{x_0}\dots\gamma_{k-1}^{x_{k-1}}\right)+(-1)^{(n-k)p}\varepsilon\operatorname{tr}\left(\beta\gamma^{-1}\right)\prod_{i=0}^{k-1}\prod_{s=1}^{p-1}(x_i-s).\end{gathered}$$

Рассмотрим вектор

$$\begin{gathered}(g(1,0,\dots,0),\dots,g(p-1,0,\dots,0,),g(0,1,0\dots,0),\dots,g(p-1,\dots,p-1)) =\\ = \left(\omega(0),\omega(1),\dots,\omega(p^k-2)\right),\end{gathered}$$

где

$$\omega(i) = \operatorname{tr}\left(\beta\gamma^{-1}\frac{\gamma_k^p - 1}{\gamma_k - 1}\dots\frac{\gamma_{n-1}^p - 1}{\gamma_{n-1} - 1}\gamma^i\right),\ i \geqslant 0.$$

Так как $\gamma_0, \gamma_1, \dots, \gamma_{n-1}$ — корни многочлена $F(x)$ в поле $P$, то $\operatorname{ord}\gamma_i = T(F)$, $i = 0, 1, \dots, n-1$ [4, 6],

$$\frac{\gamma_k^p - 1}{\gamma_k - 1}\dots\frac{\gamma_{n-1}^p - 1}{\gamma_{n-1} - 1} \neq 0$$

и последовательность $w$ является ЛРП с характеристическим многочленом $F(x)$. Если $p^k - 1 \geqslant n$, то любой отрезок длины $p^k - 1$ ЛРП $w$ не является нулевым. Тогда если $k \geqslant \lceil \log_p(n+1) \rceil$, то $g(x_0, \dots, x_{k-1})$ — ненулевая функция. В итоге с использованием неравенства (8) получим

$$\deg f \geqslant (p-1)(n-k) + \deg g \geqslant (p-1)(n-k) \geqslant (p-1)(n - \lceil \log_p(n+1) \rceil).$$

Теорема 2 доказана. ■

Доказанная теорема обобщает на случай произвольного простого числа $p$ и неприводимого многочлена $F(x)$ соответствующую теорему из работы [1].

### 3. Разностная характеристика экспоненциальных подстановок

Пусть на множестве $V_n(p)$ заданы две операции $*$ и $\circ$, причём $(V_n(p), *)$ и $(V_n(p), \circ)$ — абелевы группы с нейтральным элементом $\mathbf{0}$. Для преобразования $s : V_n(p) \to V_n(p)$, определённого равенством (3), и векторов $\mathbf{a}, \mathbf{b}$, где $\mathbf{a} \neq \mathbf{0}$, определим число

$$\rho_{\mathbf{a},\mathbf{b}}(s) = \left|\{\mathbf{x} \in V_n(p) : s(\mathbf{x} * \mathbf{a}) = s(\mathbf{x}) \circ \mathbf{b}\}\right|.$$

Тогда величину

$$\rho_{*,\circ}(s) = \max_{\mathbf{a},\mathbf{b} \in V_n(p),\, \mathbf{a} \neq \mathbf{0}} \rho_{\mathbf{a},\mathbf{b}}(s)$$

назовём *разностной характеристикой* преобразования $s$ относительно операций $*$ и $\circ$.

Рассмотрим четыре операции на $V_n(p)$, определённые для всех $\mathbf{x}, \mathbf{y} \in V_n(p)$ по правилам

$$\mathbf{x} \oplus \mathbf{y} = \tau\left(\tau^{-1}(\mathbf{x}) + \tau^{-1}(\mathbf{y})\right), \quad \mathbf{x} \ominus \mathbf{y} = \tau\left(\tau^{-1}(\mathbf{x}) - \tau^{-1}(\mathbf{y})\right),$$
$$\mathbf{x} \boxplus \mathbf{y} = v^{-1}\left(v(\mathbf{x}) + v(\mathbf{y}) \bmod p^n\right), \quad \mathbf{x} \boxminus \mathbf{y} = v^{-1}\left(v(\mathbf{x}) - v(\mathbf{y}) \bmod p^n\right),$$

при этом справа в первых двух равенствах операции сложения и вычитания рассматриваются в поле $P$, а в последних двух — в кольце целых чисел. Операция $\ominus$ является симметричной относительно операции $\oplus$, а $\boxminus$ — относительно операции $\boxplus$. Для любого вектора $\mathbf{a} \in V_n(p)$ через $\boxminus\mathbf{a}$ будем обозначать симметричный вектор относительно операции $\boxplus$ для вектора $\mathbf{a}$. Для доказательства следующего результата воспользуемся методом, описанным в работе [1].

**Теорема 3.** Пусть $s$ — экспоненциальная подстановка, определённая равенством (3). Тогда

1) если $p \geqslant 3$, то $2 \leqslant \rho_{\boxplus,\oplus}(s) \leqslant 3$;
2) если $p = 2$, то $2 \leqslant \rho_{\boxplus,\oplus}(s) \leqslant 4$, причём $\rho_{\boxplus,\oplus}(s) = 4$ тогда и только тогда, когда $F(x)$ делит хотя бы один из многочленов вида

$$x^{2^{n-1}} + x^t + 1,\ t = 1, 2, \dots, 2^{n-1} - 1. \tag{9}$$

***Доказательство.*** Заметим, что $\rho_{\boxplus,\oplus}(s) \geqslant 2$. Действительно, если $\rho_{\boxplus,\oplus}(s) = 1$, то для всех ненулевых $\mathbf{a} \in V_n(p)$ отображение $g_{\mathbf{a}} : V_n(p) \to V_n(p)$, действующее по правилу

$$g_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}),$$

является биекцией. Следовательно, принимает значение $\mathbf{0}$, что противоречит биективности подстановки $s$. Зафиксируем вектор $\mathbf{a} \in V_n(p) \setminus \{\mathbf{0}\}$. Пусть $v(\mathbf{a}) = t_0$. Найдём наибольшее значение величины $\rho_{\mathbf{a},\mathbf{b}}(s)$ при всех $\mathbf{b} \in V_n(p)$. Эта величина равна наибольшему числу появлений вектора $\mathbf{b} \in V_n(p)$ в мультимножестве (множестве с повторениями)

$$M(\mathbf{a}) = \{s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}) : \mathbf{x} \in V_n(p)\}.$$

Заметим, что мультимножество $M(\mathbf{a})$ при замене $\mathbf{t} = \mathbf{x} \boxplus \mathbf{a}$ превращается в мультимножество

$$\{s(\mathbf{t}) \ominus s(\mathbf{t} \boxminus \mathbf{a}) : \mathbf{t} \in V_n(p)\}.$$

Следовательно, $\rho_{\mathbf{a},\mathbf{b}}(s) = \rho_{\boxminus\mathbf{a},\ominus\mathbf{b}}(s)$. Справедливы равенства

$$\begin{gathered}
M(\mathbf{a}) = \{s(\mathbf{a})\} \cup \{s(\boxminus\mathbf{a})\} \cup \{s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}) : \mathbf{x} \in V_n(p),\, \mathbf{x} \neq \mathbf{0},\, \mathbf{x} \neq \boxminus\mathbf{a}\} = \\
= \left\{\varkappa(\gamma^{v(\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{v(\boxminus\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{v(\mathbf{x}\boxplus\mathbf{a})}) \ominus \varkappa(\gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p),\, \mathbf{x} \neq \mathbf{0},\, \mathbf{x} \neq \boxminus\mathbf{a}\right\} = \\
= \left\{\varkappa(\gamma^{v(\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{v(\boxminus\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n}) \ominus \varkappa(\gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus\mathbf{a}\right\} = \\
= \left\{\varkappa(\gamma^{v(\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{v(\boxminus\mathbf{a})})\right\} \cup \left\{\varkappa(\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n} - \gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p),\, \mathbf{x} \neq \mathbf{0},\, \mathbf{x} \neq \boxminus\mathbf{a}\right\}.
\end{gathered}$$

Рассмотрим мультимножество

$$N(\mathbf{a}) = \{\gamma^{v(\mathbf{a})}\} \cup \left\{\gamma^{v(\boxminus\mathbf{a})}\right\} \cup \{\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n} - \gamma^{v(\mathbf{x})} : \mathbf{x} \in V_n(p),\, \mathbf{x} \neq \mathbf{0},\, \mathbf{x} \neq \boxminus\mathbf{a}\}.$$

Ясно, что $\rho_{\mathbf{a},\mathbf{b}}(s)$ равно числу появлений элемента $b = \varkappa^{-1}(\mathbf{b})$ среди элементов мультимножества $N(\mathbf{a})$. Так как $v(\mathbf{a}) = t_0$, то $v(\boxminus\mathbf{a}) = p^n - t_0$. Если $t = v(\mathbf{x})$ и $\mathbf{x}$ пробегает множество $V_n(p) \setminus \{\mathbf{0}, \boxminus\mathbf{a}\}$, то параметр $t$ пробегает все значения из множества $\{0, 1, \ldots, p^n - 1\} \setminus \{0, p^n - t_0\}$. Если $p \geqslant 3$, имеем

$$\begin{gathered}
N(\mathbf{a}) = \left\{\gamma^{t_0},\, \gamma^{p^n - t_0}\right\} \cup \left\{\gamma^{t+t_0} - \gamma^t : t = 1, 2, \ldots, p^n - t_0 - 1\right\} \cup \\
\cup \left\{\gamma^{t+t_0} - \gamma^t : t = p^n - t_0 + 1, p^n - t_0 + 2, \ldots, p^n - 1\right\},
\end{gathered}$$

причём все три мультимножества в этом объединении являются множествами. Отсюда получим, что $\rho_{\boxplus,\oplus}(s) \leqslant 3$, и п. 1 доказан.

Докажем п. 2. Если $p = 2$ и $t_0 = 2^{n-1}$, то множество $\left\{\gamma^{t_0}, \gamma^{2^n - t_0}\right\}$ является мультимножеством. Следовательно, $\rho_{\boxplus,\oplus}(s) \leqslant 4$, причём $\rho_{\boxplus,\oplus}(s) = 4$ тогда и только тогда, когда найдётся такое число $t \in \{1, 2, \ldots, 2^{n-1} - 1\}$, что выполнено равенство

$$\gamma^{2^{n-1}} = \gamma^{t+2^{n-1}} + \gamma^t.$$

Умножив левую и правую части на ненулевой элемент $\gamma^{-t}$, получим

$$\gamma^{2^{n-1}} + \gamma^{2^{n-1}-t} + 1 = 0.$$

Это означает, что минимальный многочлен $F(x)$ элемента $\gamma$ делит некоторый многочлен вида (9). ■

### 4. Линейная характеристика экспоненциальных преобразований

Для любого $b \in P_0^*$ через $\chi_b$ будем обозначать аддитивный характер поля $P_0$ [4]:

$$\chi_b(x) = e^{2\pi i b x/p},\ x \in P_0.$$

В дальнейшем будем использовать обозначение $\chi_e = \chi$. Пусть $f, g : P_0^n \to P_0$ — некоторые функции. Определим коэффициент кросс-корреляции между функциями $f$ и $g$ [11] равенством

$$C_b(f,g) = \sum_{\mathbf{x}\in P_0^n} \chi_b(f(\mathbf{x}) - g(\mathbf{x})).$$

Введём обозначение

$$C(f,g) = \max_{b\in P_0^*} |C_b(f,g)|.$$

Обозначим через $\langle \mathbf{a}, \mathbf{x}\rangle$ скалярное произведение векторов $\mathbf{a}, \mathbf{x} \in P_0^n$. Пусть $g$ пробегает всё множество аффинных функций от $n$ переменных над полем $P_0$, т. е.

$$g(\mathbf{x}) = g(x_0, \ldots, x_{n-1}) = \langle \mathbf{a}, \mathbf{x}\rangle + c = a_0x_0 + a_1x_1 + \ldots + a_{n-1}x_{n-1} + c,$$

где $a_0, \ldots, a_{n-1}, c \in P_0$. Линейная характеристика функции $f$ определяется по правилу [12, 13]

$$C(f) = \max_g C(f,g) = \max_g \max_{b\in P_0^*} |C_b(f,g)|,$$

где максимум берётся по всем аффинным функциям $g$ от $n$ переменных.

Пусть $s$ — экспоненциальное преобразование, определённое равенством (3), $s_0, \ldots, s_{n-1}$ — его координатные функции. Тогда линейная характеристика преобразования $s$ определяется равенством

$$C(s) = \max_{(a_0,\ldots,a_{n-1})\in V_n(p)\setminus\{\mathbf{0}\}} C(a_0s_0 + \ldots + a_{n-1}s_{n-1}).$$

Таким образом,

$$C(s) = \max_{f\in B_n(F)} C(f) = \max_{f\in B_n(F)} \max_g \max_{b\in P_0^*} |C_b(f,g)|.$$

Приведём результат из работы [3], который был получен в асимптотическом виде. В доказательстве будем использовать более удобные обозначения и вычислим значения соответствующих констант.

**Теорема 4.** Пусть $T(F) \geqslant p^{n/2}n$. Тогда для любого $n$ в случае $p \geqslant 3$ и для $n \geqslant 5$, если $p = 2$, для каждой функции $f \in B_n(F)$ справедлива оценка

$$|C(f)| \leqslant \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4}n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}}\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right)\right)^{1/2}.$$

***Доказательство.*** Выберем число $r \in \{0, 1, \ldots, n-1\}$, удовлетворяющее неравенствам

$$p^r \leqslant T(F)^{1/2}p^{n/4}n^{1/2} < p^{r+1}. \tag{10}$$

Такое число найдётся при выполнении неравенства

$$p^{3n/4}n^{1/2} < p^n,$$

которое имеет место всегда в случае $p \geqslant 3$ и при $n \geqslant 5$, если $p = 2$. Пусть $g(\mathbf{x}) = a_0x_0 + \\ + \ldots + a_{n-1}x_{n-1} + c$, где $a_0, \ldots, a_{n-1}, c \in P_0$. Рассмотрим для функции $f = f_u \in B_n(F)$, соответствующей ЛРП $u$, и функции $g$ коэффициент кросс-корреляции

$$C_b(f, g) = \sum_{\mathbf{x} \in P_0^n} \chi_b(f(\mathbf{x}) - g(\mathbf{x})) = 1 + C,$$

где

$$C = \sum_{\mathbf{x} \in P_0^n \setminus \{\mathbf{0}\}} \chi_b(f(\mathbf{x}) - g(\mathbf{x})) = \sum_{\mathbf{x} \in P_0^n \setminus \{\mathbf{0}\}} \chi_b(u(v(\mathbf{x}) - 1) - a_0x_0 - \ldots - a_{n-1}x_{n-1} - c),$$

$v(\mathbf{x}) = x_0 + px_1 + \ldots + p^{n-1}x_{n-1}$. Тогда

$$C = \sum_{(x_0, \ldots, x_{r-1}) \in V_r(p)} \chi_b(-a_0x_0 + \ldots + a_{r-1}x_{r-1} - c) \times$$
$$\times \sum_{(x_r, \ldots, x_{n-1}) \in V_{n-r}(p),\, \mathbf{x} \neq \mathbf{0}} \chi_b(u(v(\mathbf{x}) - 1) - a_rx_r - \ldots - a_{n-1}x_{n-1})$$

и справедливы равенства

$$C = C_1 + C_2, \tag{11}$$

где

$$C_1 = \sum_{(x_r, \ldots, x_{n-1}) \in V_{n-r}(p) \setminus \{\mathbf{0}\}} \chi_b(u(v(0, \ldots, 0, x_r, \ldots, x_{n-1}) - 1) - a_rx_r - \ldots - a_{n-1}x_{n-1} - c),$$
$$C_2 = \sum_{(x_0, \ldots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \chi_b(-a_0x_0 - \ldots - a_{r-1}x_{r-1} - c) \times$$
$$\times \sum_{(x_r, \ldots, x_{n-1}) \in V_{n-r}(p)} \chi_b(u(v(\mathbf{x}) - 1) - a_rx_r - \ldots - a_{n-1}x_{n-1}),$$
$$|C| \leqslant |C_1| + |C_2|,\ |C_1| \leqslant p^{n-r} - 1.$$

Оценим величину $C_2$. Имеем

$$|C_2| \leqslant \sum_{(x_0, \ldots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \left| \sum_{(x_r, \ldots, x_{n-1}) \in V_{n-r}(p)} \chi_b((u(v(\mathbf{x}) - 1) - a_rx_r - \ldots - a_{n-1}x_{n-1}) \right|.$$

Используя неравенство Коши — Буняковского — Шварца, получим

$$|C_2|^2 \leqslant$$
$$\leqslant (p^r - 1) \sum_{(x_0, \ldots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \left| \sum_{(x_r, \ldots, x_{n-1}) \in V_{n-r}(p)} \chi_b((u(v(\mathbf{x}) - 1) - a_rx_r - \ldots - a_{n-1}x_{n-1}) \right|^2.$$

В силу линейности функции «след» можем записать

$$|C_2|^2 \leqslant p^r \sum_{\substack{(x_0, \ldots, x_{r-1}) \in \\ \in V_r(p) \setminus \{\mathbf{0}\}}} \sum_{\substack{(x_r, \ldots, x_{n-1}), \\ (x'_r, \ldots, x'_{n-1}) \in V_{n-r}(p)}} \chi_b \left( u(v(\mathbf{x}) - 1) - \sum_{i=r}^{n-1} a_ix_i - u(v(\mathbf{x}') - 1) + \sum_{i=r}^{n-1} a_ix'_i \right),$$

где $\mathbf{x}' = (x_0, \ldots, x_{r-1}, x'_r, \ldots, x'_{n-1})$. Отсюда

$$|C_2|^2 \leqslant p^r \sum_{\substack{(x_r, \ldots, x_{n-1}), \\ (x'_r, \ldots, x'_{n-1}) \in V_{n-r}(p)}} \left| \sum_{(x_0, \ldots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \chi_b \left( u(v(\mathbf{x}) - 1) - u(v(\mathbf{x}') - 1) \right) \right|.$$

Если $(x_r, \ldots, x_{n-1}) = (x'_r, \ldots, x'_{n-1})$, то

$$\left| \sum_{(x_0,\ldots,x_{r-1})\in V_r(p)\setminus\{\mathbf{0}\}} \chi_b\left(u(v(\mathbf{x})-1) - u(v(\mathbf{x}')-1)\right)\right| = p^r - 1.$$

Если $(x_r, \ldots, x_{n-1}) \neq (x'_r, \ldots, x'_{n-1})$, то знаки

$$u(v(\mathbf{x})-1) - u(v(\mathbf{x}')-1),\ (x_0, \ldots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}$$

представляют собой знаки последовательности $w = x^t u - x^s u$, где $t, s \in \mathbb{N} \cup \{0\}$ и $t \neq s$. Без ограничения общности считаем, что $t > s$ и $t \leqslant T(F) - 1$. Последовательность $w$ является ЛРП с характеристическим многочленом $F(x)$. В силу реверсивности $F(x)$ имеет место: $w = (0)$ тогда и только тогда, когда $(x^t - x^s)u = (0)$, что равносильно $F(x)|(x^t - x^s)$ и эквивалентно $F(x)|(x^{t-s} - 1)$. Это соотношение не выполняется. Значит, при $(x_r, \ldots, x_{n-1}) \neq (x'_r, \ldots, x'_{n-1})$ с использованием неравенства из [14–18] имеем

$$\left| \sum_{(x_0,\ldots,x_{r-1})\in V_r(p)\setminus\{\mathbf{0}\}} \chi_b\left(u(v(\mathbf{x})-1) - u(v(\mathbf{x}')-1)\right)\right| \leqslant \left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right) p^{n/2}.$$

Следовательно,

$$|C_2|^2 \leqslant p^r \left( \sum_{(x_r,\ldots,x_{n-1})=(x'_r,\ldots,x'_{n-1})} (p^r - 1) + \sum_{(x_r,\ldots,x_{n-1})\neq(x'_r,\ldots,x'_{n-1})} \left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right) p^{n/2} \right) =$$

$$= p^r(p^r - 1)p^{n-r} + p^r\left(p^{2(n-r)} - p^{n-r}\right)\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right) p^{n/2} <$$

$$< p^{n+r} + p^{2n-r}\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right) p^{n/2}.$$

Согласно (10), $r \leqslant 3n/4 + (\log_p n)/2$ и $r + 1 > 3n/4 + (\log_p n)/2$. Тогда

$$p^{2n-r} < p^{2n-3n/4-\log_p n^{1/2}+1} = \frac{p^{5n/4+1}}{n^{1/2}}, \quad p^{n+r} < p^{n+3n/4+(\log_p n)/2} = p^{7n/4} n^{1/2}$$

и справедливо неравенство

$$|C_2| < \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}}\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right)\right)^{1/2}. \tag{12}$$

В итоге в силу (11) и (12) имеем

$$|C| < \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}}\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right)\right)^{1/2}.$$

Теорема 4 доказана. ■

**Следствие 2.** В условиях теоремы 4 для экспоненциального преобразования, определённого равенством (3), справедлива оценка

$$|C(s)| \leqslant \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}}\left(\frac{4}{\pi^2}\ln T(F) + \frac{9}{5}\right)\right)^{1/2}.$$

Правая часть неравенства из следствия 2 при фиксированном $p$ имеет вид $O\left(p^{7n/8} n^{1/4}\right)$, где $n \to \infty$.

## Заключение

В работе рассмотрен класс экспоненциальных преобразований, обобщающий класс, изученный в [1]. Удалось найти верхнюю и нижнюю оценки степени нелинейности экспоненциальных преобразований, условия достижимости верхней оценки, а также оценки разностной и линейной характеристик экспоненциальных преобразований.

## ЛИТЕРАТУРА


1. *Агиевич С. В., Афоненко А. А.* О свойствах экспоненциальных подстановок // Вести НАН Беларуси. 2005. № 1. С. 106–112.
2. *Агиевич С. В., Галинский В. А., Микулич Н. Д., Харин Ю. С.* Об одном алгоритме блочного шифрования // Управление защитой информации. 2002. Т. 6. № 4. С. 404–412.
3. *Shparlinski I. E. and Winterhof A.* On nonlinearity of linear recurrence sequences // Appl. Math. Let. 2005. V. 19. No. 4. P. 340–344.
4. *Лидл Р., Ниддерайтер Г.* Конечные поля. М.: Мир, 1988. 808 с.
5. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.
6. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. СПб.; М.; Краснодар: Лань, 2015. 608 с.
7. *Лаксов Д.* Линейные рекуррентные последовательности над конечными полями // Математика. Сборник переводов. 1967. Т. 11. № 6. С. 145–158.
8. *Камловский О. В.* Оценки числа появлений векторов на циклах линейных рекуррентных последовательностей над конечным полем // Дискретная математика. 2008. Т. 20. № 6. С. 102–112.
9. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
10. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 97–122.
11. *Golomb S. W. and Gong G.* Signal for Good Correlation. For Wireless Communication, Cryptography, and Radar. Cambridge: Cambridge Univ. Press, 2005. 438 p.
12. *Бугров Д. А.* Кусочно-аффинные подстановки конечных полей // Прикладная дискретная математика. 2015. № 4(30). С. 5–23.
13. *Камловский О. В., Панков К. Н.* Классы сбалансированных функций над конечными полями, обладающих малым значением линейной характеристики // Проблемы передачи информации. 2022. Т. 58. Вып. 4. С. 103–117.
14. *Камловский О. В.* Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа // Математический сборник. 2009. Т. 200. № 4. С. 31–52.
15. *Камловский О. В.* Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
16. *Коробов Н. М.* Распределение невычетов и первообразных корней в рекуррентных рядах // Доклады АН СССР. 1953. Т. 88. № 4. С. 603–606.
17. *Niederreiter H.* Distribution properties of feedback shift register sequences // Problems Control Inform. Theory. 1986. V. 15. No. 1. P. 19–34.
18. *Нечаев В. И.* Распределение знаков в последовательности прямоугольных матриц над конечным полем // Труды матем. ин-та им. В. А. Стеклова. 1997. Т. 218. С. 335–442.

REFERENCES


1. *Agievich S. V. and Afonenko A. A.* O svoystvakh eksponentsial'nykh podstanovok [On properties of exponential substituons]. Vesti NAN Belarusi, 2005, no. 1, pp. 106–112. (in Russian)
2. *Agievich S. V., Galinskiy V. A., Mikulich N. D., and Kharin Yu. S.* Ob odnom algoritme blochnogo shifrovaniya [About one block cipher algorithm]. Upravlenie Zashchitoy Informatsii, 2002, vol. 6, no. 4, pp. 404–412. (in Russian)
3. *Shparlinski I. E. and Winterhof A.* On nonlinearity of linear recurrence sequences. Appl. Math. Let., 2005, vol. 19, no. 4, pp. 340–344.
4. *Lidl R. and Niederreiter H.* Finite Fields. Addison-Wesley Publ., 1983.
5. *Kurakin V. L., Kuz'min A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules. J. Math. Sci., 1995, vol. 76, no. 6, pp. 2793–2915.
6. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Uchebnik [Algebra: Textbook]. Saint Petersburg; Moscow; Krasnodar, Lan Publ., 2015. 608 p. (in Russian)
7. *Laksov D.* Lineynye rekurrentnye posledovatel'nosti nad konechnymi polyami [Linear recurrences over finite fields]. Matematika. Sbornik Perevodov, 1967, vol. 11, no. 6, pp. 145–158. (in Russian)
8. *Kamlovskiy O. V.* Otsenki chisla poyavleniy vektorov na tsiklakh lineynykh rekurrentnykh posledovatel'nostey nad konechnym polem [Estimates of the number of occurrences of vectors on cycles of linear recurring sequences over a finite field]. Diskretnaya Matematika, 2008, vol. 20, no. 6, pp. 102–112. (in Russian)
9. *Cheremushkin A. V.* Additivnyy podkhod k opredeleniyu stepeni nelineynosti diskretnoy funktsii [An additive approach to nonlinear degree of discrete function]. Prikladnaya Diskretnaya Matematika, 2010, no. 2(8), pp. 22–33. (in Russian)
10. *Kuz'min A. S., Nechaev A. A., and Shishkin V. A.* Bent- i giperbent-funktsii nad konechnym polem [Bent and hyper-bent functions over the finite field]. Trudy po Diskretnoy Matematike, 2007, vol. 10, pp. 97–122. (in Russian)
11. *Golomb S. W. and Gong G.* Signal for Good Correlation. For Wireless Communication, Cryptography, and Radar. Cambridge, Cambridge Univ. Press, 2005. 438 p.
12. *Bugrov D. A.* Kusochno-affinnye podstanovki konechnykh poley [Piecewise-affine permutations of finite fields]. Prikladnaya Diskretnaya Matematika, 2015, no. 4(30), pp. 5–23. (in Russian)
13. *Kamlovskiy O. V. and Pankov K. N.* Klassy sbalansirovannykh funktsiy nad konechnymi polyami, obladayushchikh malym znacheniem lineynoy kharakteristiki [Some classes of balanced functions over finite fields with a small value of the linear characteristic]. Problemy Peredachi Informatsii, 2022, vol. 58, iss. 4, pp. 103–117. (in Russian)
14. *Kamlovskiy O. V.* Chastotnye kharakteristiki lineynykh rekurrentnykh posledovatel'nostey nad kol'tsami Galua [Frequency characteristics of linear recurrence sequences over Galois rings]. Matematicheskiy Sbornik, 2009, vol. 200, no. 4, pp. 31–52. (in Russian)
15. *Kamlovskiy O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
16. *Korobov N. M.* Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh ryadakh [Distribution of non-residues and primitive roots in recurrent series]. Doklady USSR Academy of Sciences, 1953, vol. 88, no. 4, pp. 603–606. (in Russian)

17. *Niederreiter H.* Distribution properties of feedback shift register sequences. Problems Control Inform. Theory, 1986, vol. 15, no. 1, pp. 19–34.
18. *Nechaev V. I.* Raspredelenie znakov v posledovatel'nosti pryamougol'nykh matrits nad konechnym polem [Distribution of signs in a sequence of rectangular matrices over a finite field]. Proc. Steklov Mathematical Institut, 1997, vol. 218, pp. 335–342. (in Russian)

УДК 519.4 DOI 10.17223/20710410/60/3

# ЧИСЛО ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ ИЗ ЗАДАННОГО ПОДМНОЖЕСТВА НА ОТРЕЗКАХ УСЛОЖНЕНИЙ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. С. Тиссин

*ООО «Центр сертификационных исследований», г. Москва, Россия*

**E-mail:** at_science@mail.ru

Пусть $v$ — последовательность, построенная по правилу $v(i) = f(u_1(i), \ldots, u_k(i))$, $i \geqslant 0$, где $u_1, \ldots, u_k$ — линейные рекуррентные последовательности над полем $P$ с характеристическим многочленом $F(x)$. Изучается величина $N_l(H, v)$, равная количеству появлений элементов из подмножества $H \subset P$ среди элементов $v(0)$, $v(1)$, …, $v(l-1)$; получены её нетривиальные оценки снизу и сверху, вычислены границы для некоторых подмножеств $H$. Результаты обобщаются на случай $r$-грамм.

**Ключевые слова:** *конечные поля, фильтрующие генераторы, кривизна дискретной функции, линейные рекуррентные последовательности, характеры абелевых групп.*

# THE NUMBER OF OCCURRENCES OF ELEMENTS FROM A GIVEN SUBSET ON THE COMPLICATION SEGMENTS OF LINEAR RECURRENCE SEQUENCES

A. S. Tissin

*Certification Research Center, LLC, Moscow, Russia*

Let $v$ be a sequence constructed by the rule $v(i) = f(u_1(i), \ldots, u_k(i))$, $i \geqslant 0$, where $u_1, \ldots, u_k$ are linear recurrence sequences over the field $P$ with characteristic polynomial $F(x)$. We study the value $N_l(H, v)$, which is equal to the number of occurrences of elements from the subset $H \subset P$ among the elements $v(0), v(1), \ldots, v(l-1)$. We have obtained non-trivial estimates for the value $N_l(H, v)$ and considered special cases when the set $H$ is a subgroup of the group $P^*$, $H$ is the set of all primitive elements of the field $P$. Results are generalized to the case of $r$-tuples for the value $N_l(H, \mathbf{s}, v) = |\{i \in \{0, \ldots, l-1\} : v(i+s_1) \in H, \ldots, v(i+s_r) \in H\}|$, where $\mathbf{s} = (s_1, \ldots, s_r)$ is a set of non-negative integers.

**Keywords:** *finite fields, filter generators, discrete function curvature, linear recurrence sequences, characters of abelian group.*

## Введение

Пусть $P = \mathrm{GF}(q)$ — конечное поле из $q$ элементов, где $q = p^t$, $p$ — простое число; $F(x)$ — унитарный реверсивный (старший коэффициент равен $e$ — единице поля $P$ — и $F(0) \neq 0$) многочлен степени $m$ над полем $P$, $f : P^k \to P$.

Будем изучать частотные характеристики последовательности $v$, построенной по правилу

$$v(i) = f(u_1(i), u_2(i), \ldots, u_k(i)), \quad i \geqslant 0, \tag{1}$$

где $u_j = (u_j(i))_{i=0}^{\infty}$ — линейная рекуррентная последовательность (ЛРП) над полем $P$ для всех $j = 1, 2, \ldots, k$ с характеристическим многочленом $F(x)$. В случае, когда $u_1$, $u_2$, $\ldots$, $u_k$ являются сдвигами одной ЛРП $u$, $v$ является выходной последовательностью фильтрующего генератора, усложняющего ЛРП $u$ с использованием фильтрующей функции $f$.

В работе изучается величина $N_l(H, v)$, равная количеству появлений элементов из подмножества $H \subset P$ среди элементов $v(0), v(1), \ldots, v(l-1)$. В случае $|H| = 1$ для последовательности $v$, вырабатываемой фильтрующим генератором, оценки величины $N_l(H, v)$ получены в [1]. В случае $H \subset P$, где $H$ — подгруппа мультипликативной группы $P$ или множество всех примитивных элементов поля $P$, величины $N_l(H, u)$ для ЛРП $u$ рассмотрены в работах [2–5]. Таким образом, рассматриваемая постановка задачи является обобщением ранее изученных случаев.

Получены нетривиальные оценки частот $N_l(v, H)$ для случаев, когда $H$ — подгруппа группы $P^*$ и $H$ — множество всех примитивных элементов поля $P$. Приведены обобщения этих результатов для частот появлений $r$-грамм.

## 1. Оценки частот появлений элементов на отрезках усложнений ЛРП

Опишем частотные характеристики последовательности $v$.

Назовём систему ЛРП $u_1, u_2, \ldots, u_k$ устойчивой, если для всех $a_1, a_2, \ldots, a_k \in P$, которые не все равны нулю, последовательности $a_1u_1 + a_2u_2 + \ldots + a_ku_k$ имеют один и тот же минимальный многочлен [1].

Для каждого $c \in P$ рассмотрим аддитивный характер поля $P$

$$\chi_c(x) = e^{2\pi i \operatorname{Tr}_{P_0}^{P}(cx)/p}, \quad x \in P,$$

где $P_0 = \mathrm{GF}(p)$; $\operatorname{Tr}_{P_0}^{P}(x) = x + x^p + \ldots + x^{p^{t-1}}$.

Известно [6], что группа аддитивных характеров поля $P$ имеет вид $\{\chi_c : c \in P\}$.

Для каждого $\mathbf{c} = (c_1, \ldots, c_k) \in P^k$ рассмотрим отображение $\chi_{\mathbf{c}} : P^k \to \mathbb{C}^*$, действующее по правилу

$$\chi_{\mathbf{c}}(\mathbf{x}) = \chi_{c_1}(x_1)\,\chi_{c_2}(x_2)\ldots\chi_{c_k}(x_k), \quad \text{где } \mathbf{x} = (x_1, \ldots, x_k) \in P^k.$$

Тогда группа характеров группы $P^k = \underbrace{P \oplus \ldots \oplus P}_{k}$ имеет вид $\{\chi_{\mathbf{c}} : \mathbf{c} \in P^k\}$ [6].

Определим отображение $\mu_c : P^k \to \mathbb{C}^*$, где $c \in P$, равенством

$$\mu_c(\mathbf{x}) = \chi_c(f(\mathbf{x})), \quad \mathbf{x} \in P^k. \tag{2}$$

Разложим отображение $\mu_c$ по базису характеров группы $P^k$:

$$\mu_c(\mathbf{x}) = \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c})\chi_{\mathbf{c}}(\mathbf{x}). \tag{3}$$

Известно [7], что

$$\nu_{\mu_c}(\mathbf{c}) = \frac{1}{q^k} \sum_{\mathbf{x} \in P^k} \mu_c(\mathbf{x})\overline{\chi}_{\mathbf{c}}(\mathbf{x}), \tag{4}$$

где $\overline{\chi}_{\mathbf{c}}$ — характер, сопряжённый характеру $\chi_{\mathbf{c}}$.

Для каждого реверсивного многочлена $F(x)$ степени $m$ и периода $T(F)$ над полем $P$ определим параметр $C_l(F)$ следующими равенствами:

$$C_l(F) = \begin{cases} \left(\dfrac{4}{\pi^2}\ln T(F) + \dfrac{9}{5}\right) q^{m/2}, & \text{если } l < T(F), \\ \left(q^m - T(F)\right)^{1/2}, & \text{если } l = T(F). \end{cases}$$

**Лемма 1** [1]. Пусть $F(x)$ — реверсивный многочлен над полем $P$ степени $m$ с периодом $T(F)$. Тогда для каждой ЛРП $w$ с минимальным многочленом $F(x)$ и каждого $l \leqslant T(F)$ выполнено неравенство

$$\left|\sum_{i=0}^{l-1} \chi_c(w(i))\right| \leqslant C_l(F),$$

где $\chi_c$ — произвольный нетривиальный ($c \neq 0$) аддитивный характер поля $P$.

Кривизной функции $f : P^k \to P$ назовём следующую величину [8]:

$$\sigma(f) = \max_{c \in P} \sum_{\mathbf{c} \in P^k} \left|\nu_{\mu_c}(\mathbf{c})\right|.$$

Для непустого подмножества $H$ поля $P$ введём обозначение

$$\varkappa(H) = \max_{c \in P^*} \Big| \sum_{h \in H} \chi_c(h)\Big|.$$

Следующая теорема устанавливает для каждого натурального $l$ оценку величины

$$N_l(H, v) = \left|\{i \in \{0, \ldots, l-1\} : v(i) \in H\}\right|.$$

Обозначим через $f^{-1}(H)$ полный прообраз множества $H$ при действии отображения $f$.

**Теорема 1.** Пусть $F(x)$ — реверсивный многочлен степени $m$ над полем $P = \mathrm{GF}(q)$, $u_1, u_2, \ldots, u_k$ — устойчивая система ЛРП с характеристическим многочленом $F(x)$, $v$ — последовательность, определённая по правилу (1). Тогда для любого непустого подмножества $H \subset P$ при $l \leqslant T(F)$ справедлива оценка

$$\left|N_l(H, v) - \left|f^{-1}(H)\right| \frac{l}{q^k}\right| \leqslant \frac{q-1}{q} \varkappa(H) \sigma(f) C_l(F).$$

***Доказательство.*** Из соотношения ортогональности для характеров [6] получим

$$\frac{1}{q} \sum_{c \in P} \chi_c(x) = \begin{cases} 1, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

Тогда справедливы равенства

$$N_l(H, v) = \sum_{h \in H} \sum_{i=0}^{l-1} \frac{1}{q} \sum_{c \in P} \chi_c(v(i) - h) = \frac{1}{q} \sum_{c \in P} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(v(i)).$$

Выделим отдельно слагаемое, соответствующее случаю $c = 0$:

$$N_l(H, v) = \frac{l}{q} |H| + \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(v(i)).$$

Так как $v(i) = f(u_1(i), u_2(i), \ldots, u_k(i))$, то

$$N_l(H, v) - \frac{l}{q} |H| = \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(f(u_1(i), u_2(i), \ldots, u_k(i))) =$$

$$= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \mu_c(u_1(i), u_2(i), \ldots, u_k(i)) =$$

$$= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c}) \chi_{\mathbf{c}}(u_1(i), u_2(i), \ldots, u_k(i)) =$$

$$= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \overline{\chi}_c(h) \sum_{i=0}^{l-1} \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c}) \chi(u_{\mathbf{c}}(i)),$$

где $u_{\mathbf{c}}(i) = c_1u_1(i) + c_2u_2(i) + \ldots + c_ku_k(i)$, $i \geqslant 0$; $\chi = \chi_e$ — канонический аддитивный характер поля $P$.

Выделим отдельно слагаемое, соответствующее случаю $\mathbf{c} = \mathbf{0}$:

$$N_l(H,v) - \frac{l\,|H|}{q} = \frac{1}{q}\sum_{c\neq 0}\sum_{h\in H}\overline{\chi}_c(h)\sum_{i=0}^{l-1}\nu_{\mu_c}(\mathbf{0}) + \frac{1}{q}\sum_{c\neq 0}\sum_{h\in H}\overline{\chi}_c(h)\sum_{i=0}^{l-1}\sum_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})\chi(u_{\mathbf{c}}(i)).$$

Введём обозначение

$$\delta_l(H) = \frac{l\,|H|}{q} + \frac{1}{q}\sum_{c\neq 0}\sum_{h\in H}\overline{\chi}_c(h)\sum_{i=0}^{l-1}\nu_{\mu_c}(\mathbf{0}).$$

Изучим отдельно $\delta_l(H)$. В силу того, что $\nu_{\mu_0}(\mathbf{0}) = 1$, получим

$$\delta_l(H) = \frac{1}{q}\sum_{c\in P}\sum_{h\in H}\overline{\chi}_c(h)\sum_{i=0}^{l-1}\nu_{\mu_c}(\mathbf{0}).$$

Далее, используя формулу (4), запишем

$$\delta_l(H) = \frac{1}{q}\sum_{c\in P}\sum_{h\in H}\overline{\chi}_c(h)\sum_{i=0}^{l-1}\frac{1}{q^k}\sum_{\mathbf{b}\in P^k}\mu_c(\mathbf{b}).$$

Тогда, согласно (2) и соотношению ортогональности характеров, будем иметь

$$\delta_l(H)=\frac{l}{q^{k+1}}\sum_{c\in P}\sum_{h\in H}\overline{\chi}_c(h)\sum_{\mathbf{b}\in P^k}\chi(cf(\mathbf{b}))=\frac{l}{q^{k+1}}\sum_{c\in P}\sum_{h\in H}\sum_{\mathbf{b}\in P^k}\chi(c(f(\mathbf{b})-h))=\frac{l}{q^k}\,|f^{-1}(H)|\,.$$

Следовательно,

$$\begin{aligned}\left|N_l(H,v) - \frac{l}{q^k}\,\left|f^{-1}(H)\right|\right| &= \frac{1}{q}\left|\sum_{c\neq 0}\sum_{h\in H}\overline{\chi}_c(h)\sum_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right| \leqslant \\ &\leqslant \frac{q-1}{q}\max_{c\neq 0}\left|\sum_{h\in H}\overline{\chi}_c(h)\sum_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})\textstyle\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right|.\end{aligned} \tag{5}$$

Введём обозначение

$$R_c = c \neq 0_{h\in H}\overline{\chi}_c(h)c \neq 0_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})c \neq 0_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i)).$$

Заметим, что для любого $c \in P^*$ верно

$$\begin{aligned}|R_c| &= \left|\sum_{h\in H}\overline{\chi}_c(h)\sum_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right| = \left|\sum_{h\in H}\overline{\chi}_c(h)\right|\left|\sum_{\mathbf{c}\neq\mathbf{0}}\nu_{\mu_c}(\mathbf{c})\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right| \leqslant \\ &\leqslant \varkappa(H)\Big(\sum_{\mathbf{c}\neq\mathbf{0}}|\nu_{\mu_c}(\mathbf{c})|\Big)\max_{\mathbf{c}\neq\mathbf{0}}\left|\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right| \leqslant \varkappa(H)\,\sigma(f)\max_{\mathbf{c}\neq\mathbf{0}}\left|\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right|.\end{aligned}$$

Тогда из устойчивости системы ЛРП $u_1, u_2, \ldots, u_k$ и леммы 1 получим, что

$$|R_c| \leqslant \varkappa(H)\,\sigma(f)\max_{\mathbf{c}\neq\mathbf{0}}\left|\sum_{i=0}^{l-1}\chi(u_{\mathbf{c}}(i))\right| \leqslant \varkappa(H)\,\sigma(f)\cdot C_l(F).$$

Таким образом, согласно (5), будем иметь

$$\left|N_l(H,v) - \frac{l}{q^k}\,\left|f^{-1}(H)\right|\right| \leqslant \frac{q-1}{q}\varkappa(H)\,\sigma(f)\,C_l(F).$$

Теорема 1 доказана. ■

**Замечание 1.** Из теоремы 1 при $|H| = 1$ получим оценку из работы [1].

## 2. Приложения результатов для некоторых подмножеств $H$

Приведём известные оценки величин $\varkappa(H)$, справедливые при определённом выборе $H$ и уточняющие тривиальную оценку $\varkappa(H) \leqslant |H|$.

**Лемма 2** [4]. Пусть $d$ — делитель $q-1$, $H$ — множество всех элементов вида $a^d$, где $a \in P$. Тогда для величины $\varkappa(H)$ справедлива оценка

$$\varkappa(H) \leqslant \frac{d-1}{d}(\sqrt{q}+1).$$

Непосредственно из леммы 2 и теоремы 1 получим следующий результат.

**Следствие 1.** Пусть $d$ делит $q-1$ и $H$ — множество всех элементов вида $a^d$, где $a \in P$, тогда в условиях теоремы 1 выполнено

$$\left| N_l(H,v) - \left|f^{-1}(H)\right| \frac{l}{q^k} \right| \leqslant \frac{(d-1)(\sqrt{q}+1)}{d} \frac{q-1}{q} C_l(F)\sigma(f).$$

**Лемма 3** [4]. Пусть $d$ делит $q-1$ и $H$ — подгруппа группы $P^*$, имеющая порядок $(q-1)/d$, тогда

$$\varkappa(H) \leqslant \frac{(d-1)\sqrt{q}+1}{d}.$$

Из леммы 3 и теоремы 1 вытекает

**Следствие 2.** Пусть $d$ делит $q-1$ и $H$ — подгруппа группы $P^*$, имеющая порядок $(q-1)/d$, тогда в условиях теоремы 1 выполнено

$$\left| N_l(H,v) - \left|f^{-1}(H)\right| \frac{l}{q^k} \right| \leqslant \frac{(d-1)\sqrt{q}+1}{d} \frac{q-1}{q} C_l(F)\,\sigma(f).$$

Далее рассмотрим задачу о количестве примитивных элементов на отрезках последовательности $v$. Для этого понадобятся некоторые вспомогательные свойства функции Мёбиуса $\mu$ [3].

**Лемма 4** [3]. Для всех $n \in \mathbb{N}$ верно равество

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n},$$

где $\varphi$ — функция Эйлера.

**Лемма 5** [3]. Для всех $n \in \mathbb{N}$ справедливо равенство

$$\sum_{d|n} |\mu(d)| = 2^s,$$

где $s$ — количество различных простых чисел в каноническом разложении числа $n$.

**Теорема 2.** Пусть в условиях теоремы 1 $H$ — множество всех примитивных элементов поля $P$ и $f$ — сбалансированное отображение, тогда

$$\left| N_l(H,v) - \frac{l\varphi(q-1)}{q} \right| \leqslant \frac{q-1}{\sqrt{q}}\, 2^s\, C_l(F)\,\sigma(f),$$

где $s$ — количество различных простых делителей числа $q-1$.

***Доказательство.*** Для каждого делителя $n$ числа $q-1$ обозначим через $M_l(n)$ количество элементов $c \in P^*$ среди знаков $v(0), v(1), \ldots, v(l-1)$, имеющих мультипликативный порядок $\operatorname{ord} c = n$. Рассмотрим число

$$\sum_{d|n} M_l(d).$$

Оно равно количеству элементов $c \in P^*$, таких, что $c^n = e$ в группе $P^*$, т. е. элементов из группы $\langle \gamma^{(q-1)/n} \rangle$, где $\gamma$ — примитивный элемент поля $P$. Отсюда получим

$$\sum_{d|n} M_l(d) = V_l\big((q-1)/n\big),$$

где $V_l\big((q-1)/n\big)$ — количество элементов $c \in P^*$ среди $v(0), v(1), \ldots, v(l-1)$, имеющих вид $a^{(q-1)/n}$, $a \in P^*$. Применив формулу обращения Мёбиуса, получим

$$M_l(n) = \sum_{d|n} \mu(d) V_l\big((q-1)d/n\big).$$

В частности,

$$N_l(H, v) = M_l(q-1) = \sum_{d|(q-1)} \mu(d) V_l(d).$$

Пусть $H_d$ — множество всех элементов вида $a^d$, $a \in P^*$. Тогда, согласно следствию 2,

$$V_l(d) = |f^{-1}(H_d)| \frac{l}{q^k} + \theta_d \frac{q-1}{q} C_l(F) \sigma(f),$$

где $\theta_d$ — некоторое действительное число $|\theta_d| \leqslant \sqrt{q}$. Тогда получим

$$N_l(H, v) = \frac{l}{q^k} \sum_{d|(q-1)} |f^{-1}(H_d)|\, \mu(d) + \frac{q-1}{q}\, C_l(F)\, \sigma(f) \sum_{d|(q-1)} \mu(d)\, \theta_d.$$

Так как $f$ — сбалансированное отображение, для любого $d$ получим

$$\big|f^{-1}(H_d)\big| = q^{k-1} |H_d| = q^{k-1} \frac{q-1}{d}.$$

Отсюда, используя сбалансированность $f$ и результаты лемм 4 и 5, имеем

$$\left| N_l(H, v) - \frac{l\varphi(q-1)}{q} \right| \leqslant \frac{q-1}{q} C_l(F) \sigma(f) \sum_{d|(q-1)} |\mu(d)||\theta_d| \leqslant$$
$$\leqslant C_l(F) \sigma(f) \frac{(q-1)\sqrt{q}}{q} \sum_{d|(q-1)} |\mu(d)| = \frac{q-1}{\sqrt{q}} 2^s\, C_l(F)\, \sigma(f).$$

Теорема 2 доказана. ■

Полученные в п. 2 оценки частот $N_l(H, v)$ обобщают соответствующие результаты работ [1, 2, 7, 9, 10].

### 3. Обобщение на случай $r$-грамм

Для набора $\mathbf{s} = (s_1, \ldots, s_r)$ целых неотрицательных чисел и непустого подмножества $H \subset P$ для каждого натурального $l$ рассмотрим величину

$$N_l(H, \mathbf{s}, v) = \left|\{i \in \{0, \ldots, l-1\} : v(i+s_1) \in H, \ldots, v(i+s_r) \in H\}\right|.$$

Пусть $w$ — последовательность над полем $P$ и $k \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Обозначим через $x^k w$ сдвиг последовательности $w$ на $k$ шагов влево, т. е.

$$x^k w = (w(k), w(k+1), \ldots).$$

В дальнейшем будем рассматривать ситуацию, когда набор $\mathbf{s} = (s_1, s_2, \ldots, s_r)$ удовлетворяет условию, что система ЛРП

$$x^{s_1}u_1, \ldots, x^{s_r}u_1, x^{s_1}u_2, \ldots, x^{s_r}u_2, \ldots, x^{s_1}u_k, \ldots, x^{s_r}u_k \tag{6}$$

устойчива.

**Лемма 6** [1]. Пусть $\chi$ — канонический аддитивный характер поля $P = \mathrm{GF}(q)$, $z_1, \ldots, z_r \in P$, $\mu_c$ — отображение, определённое соотношением (2), где $c \in P$. Тогда

$$\frac{1}{q^{(k-1)r}} \left|f^{-1}(z_1)\right| \cdots \left|f^{-1}(z_r)\right| = \sum_{\mathbf{c}=(c_1,\ldots,c_r)\in P^r} \chi(-c_1z_1 - \ldots - c_rz_r)\nu_{\mu_{c_1}}(\mathbf{0}) \ldots \nu_{\mu_{c_r}}(\mathbf{0}).$$

Непосредственно из леммы 6 следует

**Лемма 7.** В условиях леммы 6 для любого непустого подмножества $H \subset P$ справедливо равенство

$$\frac{1}{q^{(k-1)r}} \left|f^{-1}(H)\right|^r = \sum_{h_1,\ldots,h_r\in P} \sum_{c_1,\ldots,c_r\in P} \chi(-c_1h_1 - \ldots - c_rh_r)\nu_{\mu_{c_1}}(\mathbf{0}) \ldots \nu_{\mu_{c_r}}(\mathbf{0}).$$

**Теорема 3.** Пусть $F(x)$ — унитарный реверсивный многочлен степени $m$ над полем $P = \mathrm{GF}(q)$, $v$ — последовательность, удовлетворяющая равенству (1). Тогда если набор $\mathbf{s}$ выбран так, что система (6) устойчива, то для всех $l \leqslant T(F)$ справедлива оценка

$$\left|N_l(H, \mathbf{s}, v) - |f^{-1}(H)|^r \frac{l}{q^{kr}}\right| \leqslant C_l(F) \frac{(\varkappa(H)\sigma(f)(q-1)+1)^r - 1}{q^r}.$$

***Доказательство.*** Справедливо равенство

$$N_l(H, \mathbf{s}, v) = \sum_{i=0}^{l-1} \left(\frac{1}{q} \sum_{c_1\in P} \sum_{h_1\in H} \chi(c_1(v(i+s_1) - h_1))\right) \ldots \left(\frac{1}{q} \sum_{c_r\in P} \sum_{h_r\in H} \chi(c_r(v(i+s_r) - h_r))\right).$$

Отсюда будем иметь

$$N_l(H, \mathbf{s}, v) = \frac{1}{q^r} \sum_{\mathbf{c}=(c_1,\ldots,c_r)\in P^r} \sum_{\mathbf{h}=(h_1,\ldots,h_r)\in H^r} \chi(-\mathbf{ch}) \sum_{i=0}^{l-1} \chi(c_1v(i+s_1)) \ldots \chi(c_rv(i+s_r)),$$

где $\mathbf{c}\cdot\mathbf{h} = (c_1, \ldots, c_r)(h_1, \ldots, h_r) = c_1h_1 + \ldots + c_rh_r$. Выделяя слагаемое, соответствующее случаю $(c_1, \ldots, c_r) = (0, \ldots, 0) = \mathbf{0}$, получим

$$N_l(H, \mathbf{s}, v) - |H|^r \frac{l}{q^r} = \frac{1}{q^r} \sum_{\mathbf{c}\in P^r\setminus\{\mathbf{0}\}} \sum_{\mathbf{h}\in H^r} \chi(-\mathbf{ch}) D_l(\mathbf{c}),$$

где

$$D_l(\mathbf{c}) = \sum_{i=0}^{l-1} \chi(c_1 v(i+s_1)) \dots \chi(c_r v(i+s_r)).$$

Обозначим через $||\mathbf{c}||$ вес (количество ненулевых координат) вектора $\mathbf{c} \in P^r$. Тогда

$$N_l(H, \mathbf{s}, v) - |H|^r \frac{l}{q^r} = \frac{1}{q^r} \sum_{d=1}^{r} \sum_{\mathbf{h} \in H^r} \sum_{\mathbf{c} \in P^r \setminus \{\mathbf{0}\}, ||\mathbf{c}||=d} \chi(-\mathbf{ch}) D_l(\mathbf{c}). \tag{7}$$

Пусть вектор $\mathbf{c} = (c_1, \dots, c_r) \in P^r$ имеет вес $d$, ненулевые элементы в нём стоят на местах $j_1, \dots, j_d$ и выполнено равенство $c_{j_1} = \gamma_1, \dots, c_{j_d} = \gamma_d$. Тогда для $D_l(\mathbf{c})$, используя равенство (2), получим

$$D_l(\mathbf{c}) = \sum_{i=0}^{l-1} \mu_{\gamma_1}(u_1(i+s_1), \dots, u_k(i+s_1)) \dots \mu_{\gamma_d}(u_1(i+s_d), \dots, u_k(i+s_d)).$$

С учётом (3) запишем

$$D_l(\mathbf{c}) = \sum_{i=0}^{l-1} \Big( \sum_{\mathbf{a_1} \in P^k} \nu_{\mu_{\gamma_1}}(\mathbf{a_1}) \chi_{\mathbf{a_1}}(u_1(i+s_1), \dots, u_k(i+s_1)) \Big) \dots$$
$$\dots \Big( \sum_{\mathbf{a_d} \in P^k} \nu_{\mu_{\gamma_d}}(\mathbf{a_d}) \chi_{\mathbf{a_d}}(u_1(i+s_d), \dots, u_k(i+s_d)) \Big).$$

Тогда

$$D_l(\mathbf{c}) = \sum_{\mathbf{a_1}, \dots, \mathbf{a_d} \in P^k} \nu_{\mu_{\gamma_1}}(\mathbf{a_1}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{a_d}) \sum_{i=0}^{l-1} \chi(\omega_{\mathbf{a_1}, \dots, \mathbf{a_d}}(i)),$$

где $\omega_{\mathbf{a_1}, \dots, \mathbf{a_d}}$ — последовательность над полем $P$, элементы которой определены для всех векторов $\mathbf{a_1} = \left(a_1^{(1)}, \dots, a_k^{(1)}\right), \dots, \mathbf{a_d} = \left(a_1^{(d)}, \dots, a_k^{(d)}\right)$ равенством

$$\omega_{\mathbf{a_1}, \dots, \mathbf{a_d}}(i) = a_1^{(1)} u_1(i+s_1) + \dots + a_k^{(1)} u_k(i+s_1) + \dots$$
$$\dots + a_1^{(d)} u_1(i+s_d) + \dots + a_k^{(d)} u_k(i+s_d), \quad i \geqslant 0.$$

Так как система (6) устойчива над полем $P$, то минимальный многочлен последовательности $\omega_{\mathbf{a_1}, \dots, \mathbf{a_d}}$ равен $F(x)$, кроме случая, когда $\mathbf{a_1} = \dots = \mathbf{a_d} = \mathbf{0}$. Выделив отдельно этот случай, получим

$$D_l(\mathbf{c}) = l \cdot \nu_{\mu_{\gamma_1}}(\mathbf{0}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{0}) + D_l^*(\mathbf{c}),$$

где

$$D_l^*(\mathbf{c}) = \sum_{(\mathbf{a_1}, \dots, \mathbf{a}_d) \neq \mathbf{0}} \nu_{\mu_{\gamma_1}}(\mathbf{a_1}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{a_d}) \sum_{i=0}^{l-1} \chi(\omega_{\mathbf{a_1}, \dots, \mathbf{a}_d}(i)),$$

где суммирование производится по всем наборам $(\mathbf{a_1}, \dots, \mathbf{a}_d)$, в которых хотя бы один из векторов $\mathbf{a_1}, \dots, \mathbf{a_d}$ ненулевой.

Подставив $D_l(\mathbf{c})$ в соотношение (7), можем записать

$$N_l(H, \mathbf{s}, v) - \delta_l(H) = \frac{1}{q^r} \sum_{d=1}^{r} \sum_{\substack{\mathbf{c} \in P^r, \\ ||\mathbf{c}||=d}} \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{ch}) D_l^*(\mathbf{c}), \tag{8}$$

где

$$\delta_l(H) = |H|^r \frac{l}{q^r} + \frac{l}{q^r} \sum_{d=1}^{r} \sum_{\substack{\mathbf{c}\in P^r,\\ ||\mathbf{c}||=d}} \sum_{\mathbf{h}\in H^r} \chi(-\mathbf{ch}) \nu_{\mu_{\gamma_1}}(\mathbf{0}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{0}).$$

Для вычисления $\delta_l(H)$ воспользуемся леммой 7 и равенством $\nu_{\mu_0}(\mathbf{0}) = 1$:

$$\begin{aligned} \delta_l(H) &= |H|^r \frac{l}{q^r} \underbrace{\nu_{\mu_0}(\mathbf{0}) \dots \nu_{\mu_0}(\mathbf{0})}_{r} + \frac{l}{q^r} \sum_{\mathbf{h}\in H^r} \sum_{\mathbf{c}\in P^r\setminus\{\mathbf{0}\}} \chi(-\mathbf{ch}) \nu_{\mu_{c_1}}(\mathbf{0}) \dots \nu_{\mu_{c_r}}(\mathbf{0}) = \\ &= \frac{l}{q^r} \sum_{\mathbf{h}\in H^r} \sum_{\mathbf{c}\in P^r} \chi(-\mathbf{ch}) \nu_{\mu_{c_1}}(\mathbf{0}) \dots \nu_{\mu_{c_r}}(\mathbf{0}) = \frac{l}{q^{kr}} |f^{-1}(H)|^r. \end{aligned} \tag{9}$$

Из леммы 1 для $D_l^*(\mathbf{c})$ получим

$$\begin{aligned} |D_l^*(\mathbf{c})| &\leqslant C_l(F) \sum_{(\mathbf{a_1},\dots,\mathbf{a}_d)\neq\mathbf{0}} |\nu_{\mu_{\gamma_1}}(\mathbf{a_d})| \dots |\nu_{\mu_{\gamma_d}}(\mathbf{a_d})| \leqslant \\ &\leqslant C_l(F) \Big( \sum_{\mathbf{a_1}\in P^k} |\nu_{\mu_{\gamma_1}}(\mathbf{a_1})| \Big) \dots \Big( \sum_{\mathbf{a_d}\in P^k} |\nu_{\mu_{\gamma_d}}(\mathbf{a_d})| \Big) \leqslant C_l(F) \sigma(f)^d. \end{aligned} \tag{10}$$

Тогда, используя соотношения (8), (9) и оценку (10), будем иметь

$$\left| N_l(H, \mathbf{s}, v) - \frac{l}{q^{kr}} |f^{-1}(H)|^r \right| \leqslant \frac{1}{q^r} \sum_{d=1}^{r} \sum_{\substack{\mathbf{c}\in P^r,\\ ||\mathbf{c}||=d}} \left| \sum_{\mathbf{h}\in H^r} \chi(-\mathbf{ch}) \right| C_l(F) \sigma(f)^d. \tag{11}$$

Пусть $\mathbf{c} = (c_1, \dots, c_r) \in P^r$, $|\mathbf{c}| = d$ и $c_{\gamma_1} \neq 0, \dots, c_{\gamma_d} \neq 0$, тогда

$$\begin{aligned} \left| \sum_{\mathbf{h}\in H^r} \chi(-\mathbf{ch}) \right| &= \left| \sum_{h_{\gamma_1}\in H} \chi(-c_{\gamma_1} h_{\gamma_1}) \dots \sum_{h_{\gamma_d}\in H} \chi(-c_{\gamma_d} h_{\gamma_d}) \right| \leqslant \\ &\leqslant \left| \sum_{h_{\gamma_1}\in H} \chi(-c_{\gamma_1} h_{\gamma_1}) \right| \dots \left| \sum_{h_{\gamma_d}\in H} \chi(-c_{\gamma_d} h_{\gamma_d}) \right| \leqslant \varkappa(H)^d. \end{aligned}$$

Учитывая, что количество векторов $\mathbf{c} \in P^r$, таких, что $||\mathbf{c}|| = d$, равно $\binom{r}{d}(q-1)^d$, из неравенства (11) получим

$$\begin{aligned} \left| N_l(H, \mathbf{s}, v) - \frac{l}{q^{kr}} |f^{-1}(H)|^r \right| &\leqslant \frac{1}{q^r} \sum_{d=1}^{r} \binom{r}{d} (q-1)^d \varkappa(H)^d C_l(F) \sigma(f)^d = \\ &= C_l(F) \frac{(\varkappa(H)\sigma(f)(q-1)+1)^r - 1}{q^r}. \end{aligned}$$

Теорема 3 доказана. ■

Отметим, что при $r = 1$ оценка теоремы 3 совпадает с оценкой из теоремы 1. Таким образом, получено обобщение теоремы 1 на случай $r$-грамм.

## ЛИТЕРАТУРА

1. *Камловский О. В.* Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. №3(21). С. 11–25.
2. *Коробов Н. М.* Распределение невычетов и первообразных корней в рекуррентных рядах // Доклады АН СССР. 1953. Т. 88. №4. С. 603–606.

3. *Виноградов И. М.* Основы теории чисел. М.: Наука, 1972. 168 с.
4. *Камловский О. В.* Неабсолютные оценки для неполных тригонометрических сумм от линейных рекуррент и их приложения // Матем. вопр. криптогр. 2014. Т. 65. № 3. С. 17–34.
5. *Нечаев В. И., Степанова Л. Л.* Распределение невычетов и первообразных корней в рекуррентых последовательностях над полем алгебраических чисел // Успехи матем. наук. 1965. Т. 20. № 3. С. 197–203.
6. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. 822 с.
7. *Сидельников В. М.* Оценки для числа появлений знаков на отрезках рекуррентной последовательности над конечным полем // Дискретная математика. 1991. Т. 3. № 2. С. 87–95.
8. *Логачев О. А., Федоров С. Н., Ященко В. В.* Булевы функции как точки на гиперсфере в евклидовом пространстве // Дискретная математика. 2018. Т. 30. № 1. С. 39–55.
9. *Шпарлинский И. Е.* Распределение невычетов и первообразных корней в рекуррентных последовательностях // Матем. заметки. 1978. Т. 24. № 5. С. 603–613.
10. *Шпарлинский И. Е.* О распределении значений рекуррентных последовательностей // Проблемы передачи информации. 1989. Т. 25. № 2. С. 46–53.

## REFERENCES

1. *Kamlovskiy O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
2. *Korobov N. M.* Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh ryadakh [Distribution of non-decomposable and first-order roots in recurrence series]. Dokl. AS USSR, 1953, vol. 88, no. 4, pp. 603–606. (in Russian)
3. *Vinogradov I. M.* Osnovy teorii chisel [Fundamentals of Number Theory]. Moscow, Nauka Publ., 1972. 168 p. (in Russian)
4. *Kamlovskiy O. V.* Neabsolyutnye otsenki dlya nepolnykh trigonometricheskikh summ ot lineynykh rekurrent i ikh prilozheniya [Non-absolute estimates for incomplete trigonometric sums from linear recurrences and their applications]. Matem. Vopr. Kriptogr., 2014, vol. 65, no. 3, pp. 17–34. (in Russian)
5. *Nechaev V. I. and Stepanova L. L.* Raspredelenie nevychetov i pervoobraznykh korney v rekurrentykh posledovatel'nostyakh nad polem algebraicheskikh chisel [Distribution of non-decomposables and first-order roots in recurrence sequences over a field of algebraic numbers]. Uspekhi Matem. Nauk, 1965, vol. 20, no. 3, pp. 197–203. (in Russian)
6. *Lidl R. and Niderrayter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988. 822 p. (in Russian)
7. *Sidel'nikov V. M.* Otsenki dlya chisla poyavleniy znakov na otrezkakh rekurrentnoy posledovatel'nosti nad konechnym polem [Estimates for the number of occurrences of signs in recurrence sequence segments over a finite field]. Diskretnaya Matematika, 1991, vol. 3, no. 2, pp. 87–95. (in Russian)
8. *Logachev O. A., Fedorov S. N., and Yashchenko V. V.* Bulevy funktsii kak tochki na gipersfere v evklidovom prostranstve [Boolean functions as points on a hypersphere in Euclidean space]. Diskretnaya Matematika, 2018, vol. 30, no. 1, pp. 39–55. (in Russian)
9. *Shparlinskiy I. E.* Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh posledovatel'nostyakh [Distribution of non-decomposable and first-order roots in recurrence sequences]. Matem. Zametki, 1978, vol. 24, no. 5, pp. 603–613. (in Russian)
10. *Shparlinskiy I. E.* O raspredelenii znacheniy rekurrentnykh posledovatel'nostey [On the distribution of values of recurrent sequences]. Problemy Peredachi Informatsii, 1989, vol. 25, no. 2, pp. 46–53. (in Russian)

# МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 004.056 + 004.051 + 004.414.22 + 004.67 DOI 10.17223/20710410/60/4

## СПОСОБЫ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ КРАТКИХ НЕИНТЕРАКТИВНЫХ АРГУМЕНТОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ И АНАЛИЗ ДОСТИГНУТЫХ РЕЗУЛЬТАТОВ

И. В. Мартыненков

*АО «КВАНТ-ТЕЛЕКОМ», г. Москва, Россия*

**E-mail:** mivpost@yandex.ru

Рассматриваются способы повышения производительности кратких неинтерактивных аргументов с нулевым разглашением на основе полиномиальных наборов с использованием различных вычислительных методов. Проводится сравнительный анализ протоколов по размерам главных ссылочных строк и доказательств достоверности вычислений, затратам формирования доказательств и их верификации.

**Ключевые слова:** *краткие неинтерактивные аргументы, повышение производительности, анализ производительности, размер публичных параметров.*

## WAYS TO IMPROVE THE PERFORMANCE OF ZERO-KNOWLEDGE SUCCINCT NON-INTERACTIVEARGUMENTS OF KNOWLEDGE AND THE ANALYSIS OF THE RUSULTS ACHIEVED

I. V. Martynenkov

*JSC «KVANT-TELECOM», Moscow, Russia*

We consider ways to improve the performance of zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) based on polynomial sets, such as quadratic arithmetic programs (QAP), square arithmetic programs (SAP), quadratic span programs (QSP), square span programs (SSP), quadratic polynomial programs (QPP), etc. To improve the performance of zk-SNARK, batch data processing methods, various modifications of exponentiation problems, bilinear pairings based on elliptic curves, etc. are used. A comparative analysis of the complexity of the common reference strings formation, the construction and verification of the calculations reliability proofs, as well as the sizes of common reference strings and proofs has been carried out.

**Keywords:** *succinct non-interactive arguments, performance improvement, performance analysis, size of public parameters.*

### Введение

Рассматриваются способы повышения производительности кратких неинтерактивных аргументов с нулевым разглашением. Далее используется наименование «прото-

кол zk-SNARK» согласно [1]. Представлено применение ключевых/бесключевых хеш-функций, позволяющих выполнять верификацию доказательств с затратами, независимыми от размера ввода/вывода, но с издержками на дайджесты. Быстродействие может повышаться за счёт более адаптированных к протоколам zk-SNARK хеш-функций над простым полем [2, 3] или на решётках [4–6], как представлено в [7]. Появляется компромисс между сложностью вычислений доказывающего и верификатора, владеющего секретными значениями, определяемый хешированием части открытого входа.

Для деления полиномов может использоваться многоточечная оценка и интерполяция [8, 9], а для умножения — множественное возведение в степень [10, 11] на основе таблиц промежуточных степеней и др. [11–14]. Структурные свойства набора полиномов в виде квадратичных арифметических программ (Quadratic Arithmetic Program, QAP) [15] предполагают наличие нулевых многочленов, позволяющих сократить размер ключей [14]. Отдельного внимания заслуживают сокращение размера доказательства и асимметричное билинейное спаривание [16] с компонентами доказательств из разных групп [17].

Приводятся примеры разделения публичных параметров главной ссылочной строки (Common Reference String, CRS) на более компактные части, формируемые отдельно для доказывающих и верификаторов протоколов zk-SNARK [15, 17, 18]. На примере протоколов zk-SNARK из [19] представлена пакетная верификация доказательств, являющаяся более эффективной компоновкой частей доказательств для уменьшения сложности вычислений. Отмечены работы, использующие объединение набора доказательств протоколов zk-SNARK в одно заключительное доказательство.

Представлен сравнительный анализ протоколов zk-SNARK [7–9, 12–15, 17, 18, 20–36] по размерам CRS и доказательств достоверности вычислений, а также по сложностям вычислений доказывающих и верификаторов.

## 1. Способы применения хеш-функций

Верифицируемые вычисления (Verifiable Computation, VC) [20] предназначены для двустороннего вычисления функций по частным входным данным. Согласно [37], в схемах VC независимо от длины ввода $f(x)$ вывод доказывающего может дополнительно сокращаться. Для этого вместо $f(x)$ используются ключевые функции $\mathsf{MAC}_k(f(x))$. В результате верификация становится независимой от длины ввода/вывода, однако возникают издержки верификатора на вычисление хеш-функции. На стороне верификатора для подготовки входных данных асимметричные криптографические преобразования остаются прежними.

Вычисления верификатора протоколов zk-SNARK [15, 38] линейны по размеру открытого входа $\mathbf{u}$ с основными затратами на вычисление $g^{v_{\text{in}}(s)}$, где $g$ — порождающий элемент группы; $v_{\text{in}}(s) = \sum\limits_{k \in I_{\text{in}}} a_k v_k(x)$ — сумма многочленов из состава полиномиального набора QAP или программ квадратичного диапазона (Quadratic Span Programs, QSP) [15]; $s$ — секретная точка. Вычисление сокращается за счёт применения хеш-функции $\mathsf{H}$ для получения постоянного по размеру $\mathbf{u}' = \mathsf{H}(\mathbf{u})$. Значение $\mathbf{u}'$ становится новым открытым входом, а $\mathbf{u}$ — частью секрета $\mathbf{w}$, знание которого доказывается. Однако хеширование увеличивает объём вычислений доказывающего, так как впоследствии дополнительно необходимо верифицировать $\mathbf{u}' = \mathsf{H}(\mathbf{u})$. Компромисс между вычислениями доказывающего и верификатора определяется хешированием части входных данных $\mathbf{u}$.

В случае протокола zk-SNARK с фиксированным верификатором (Designated Verifier, DV) [15, 38] верификатор владеет секретами $\alpha, \beta_v, \beta_w \in \mathbb{Z}_p^*$, по которым с использованием $g^{v_{\text{mid}}(s)}, g^{w(s)}, g^{h(s)}$ он способен сформировать часть доказательства. Значения $v_{\text{mid}}(s), w(s), h(s)$ также основаны на полиномиальных наборах QAP/QSP [15]. Поэтому доказывающий может применить более лаконичные доказательства за счёт хеша $\mathbf{D} = \mathsf{H}(g^{\alpha v_{\text{mid}}(s)}, g^{\alpha w(s)}, g^{\alpha h(s)}, g^{\beta_v v_{\text{mid}}(s) + \beta_w w(s)})$ и отправить $\boldsymbol{\pi} = (\boldsymbol{g^{v_{\text{mid}}(s)}, g^{w(s)}, g^{h(s)}, \mathbf{D}})$. Затем верификатор выводит аналогичные недостающие значения, проверяет совпадение с $\mathbf{D}$ и проводит верификацию доказательства обычным способом. Для протокола DV zk-SNARK [39, 40] хеш-функции назначаются верификаторами на этапе формирования публичных параметров в виде CRS.

Кроме того, хеш-функции над большим простым полем, например «POSEIDON» [2] или хеш Педерсена [3], используемые для доказательства знания прообраза, лучше адаптированы к протоколам zk-SNARK по сравнению с классическими схемами, за счёт чего повышают их быстродействие. Вариант [3] отображает последовательность бит в сжатую точку на эллиптической кривой. В [13] вычисляется хэш Меркла с использованием SHA-1, в то время как в [7] хеш-функция основана на решётке

$$\mathsf{h}(\mathbf{x}, \mathbf{y}) = \mathbf{L}\mathbf{x} + \mathbf{R}\mathbf{y} \bmod q, \tag{1}$$

где $\mathbf{L}, \mathbf{R} \in \mathbb{Z}_q^{k \times m}$; $\mathbf{x}, \mathbf{y} \in \{1, \ldots, N\}^m$ [41]. В связи со свойством аддитивного гомоморфизма данной хеш-функции дайджест $\mathsf{d}(\mathbf{S})$ полученного хеш-дерева Меркла может выражаться в виде

$$\mathsf{d}(\mathbf{S}) = \sum_i \mathbf{S}[i] f(i) \bmod q, \tag{2}$$

где $f(i) \in \{0,1\}^m$ — функция индекса $i$ как «частичная метка» [42]; $\mathbf{S}[i]$ — вектор в позиции $i$ как скаляр в $\mathbb{Z}_q$. Дайджесты векторов кратчайших путей [7] вычисляются с использованием (1) и (2), которые вместе с предварительно вычисленными расстояниями и путями обрабатываются HMAC, а затем передаются на вычисление серверу в недоверенной среде. Для всех векторов разной длины, хранящих предварительно вычисленные расстояния, строится доказательство протокола zk-SNARK [13]. Возможным недостатком подходов [7] по сравнению с [13] является увеличение размера доказательства. Размер доказательства схемы [13] составляет 288 байт. Доказательство [7] содержит 256-битный (32 байта) HMAC для каждого ребра графа с кратчайшим путём, поэтому размер доказательства пропорционален количеству таких рёбер $|R|$. В общем случае доказательство [7] составляет $|R| \times 32 + 288$ байт. Примеры криптографических алгоритмов на решётках представлены в [4–6].

Например, протокол zk-SNARK [43] строится на основе симметричных хеш-функций и схем обязательств, обеспечивая «постквантовую» защиту. В [44] представлена новая схема обязательств для полиномов над конечными полями, использующая целочисленные представления многочленов и групп неизвестного порядка (Diophantine Argument of Knowledge, «DARK»). В общем виде уравнение $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ с параметрами $a_1, \ldots, a_n$ и неизвестными $x_1, \ldots, x_m$ считается разрешимым при данных $a_1, \ldots, a_n$, если существуют наборы чисел $x_1, \ldots, x_m$, при которых равенство верно. В [44] представлено преобразование интерактивных доказательств в неинтерактивные на основе «DARK» для протокола zk-SNARK «Supersonic» с формированием CRS без секретных значений. Протокол zk-SNARK «Ligero» [45] также формирует CRS без секретных значений, использует произвольные хеш-функции, симметричные примитивы и преобразуется в неинтерактивный режим эвристикой Фиата — Шамира [46].

## 2. Способы выполнения алгебраических операций

В общем случае алгоритмы формирования ключей и доказательств протоколов zk-SNARK имеют высокие криптографические накладные расходы, так как выполняется значительное количество возведений в степень в группах $\mathbb{G}_1$ и $\mathbb{G}_2$.

Например, доказательство протокола zk-SNARK [15, 38] состоит из семи элементов группы. Выбираются случайные $\delta_{v_{\text{mid}}}, \delta_w \in \mathbb{F}$, за счёт которых «маскируются» $v'_{\text{mid}}(x) = v_{\text{mid}}(x) + \delta_{v_{\text{mid}}} t(x)$, $w'(x) = w(x) + \delta_w t(x)$, $h'(x) = v'_{\text{mid}}(x) w'(x)/t(x)$. Используются случайные $\alpha, \beta_v, \beta_w \in \mathbb{F}$. Доказательство принимает вид

$$\begin{gathered}\boldsymbol{\pi} = (\pi'_{v_{\text{mid}}}, \pi'_w, \pi'_h, \pi'_{v'_{\text{mid}}}, \pi'_{w'}, \pi'_{h'}, \pi'_y) = \\ = (g^{v'_{\text{mid}}(s)}, g^{w'(s)}, g^{h'(s)}, g^{\alpha v'_{\text{mid}}(s)}, g^{\alpha w'(s)}, g^{\alpha h'(s)}, g^{\beta_v v'_{\text{mid}}(s) + \beta_w w'(s)}).\end{gathered} \tag{3}$$

Согласно [15], в доказательстве (3) из-за структуры многочленов QAP/QSP значения $v_0(x) + \sum\limits_k a_k v_k(x)$ и $w_0(x) + \sum\limits_k b_k w_k(x)$ могут вычисляться в поле $\mathbb{F}$ за линейное число операций, исключая $h(x)$. С помощью многоточечной оценки и интерполяции [8, 9] частное $h(x) = \big(v_0(x) + \sum\limits_k a_k v_k(x)\big)\big(w_0(x) + \sum\limits_k b_k w_k(x)\big)/t(x)$ может вычисляться со сложностью $O(s \cdot \text{poly}(\log(s)))$ и квадратичным вычислением доказательства $\boldsymbol{\pi}$.

В [13] демонстрируются подходы повышения производительности, которые являются общими для протоколов zk-SNARK. Порождающий элемент группы $g$ возводится в экспоненты, что ускоряется методом множественного возведения в степень [10, 11], основанным на построении таблиц промежуточных степеней. Таким образом, вычисление доказывающего вида $g^{v(s)} = \prod\limits_i g_i^{e_i}$ требует использования $g_1, \ldots, g_m \in \mathbb{G}$ и степеней $e_1, \ldots, e_m \in \mathbb{Z}$ для некоторого большого $m$. В данном случае применима техника построения небольшой таблицы степеней для каждой пары оснований. Например, для первых двух оснований с окном размера 1, используя одно умножение, вычисляются $\{g_1^0, g_2^0, g_1^0, g_2^1, g_1^1, g_2^0, g_1^1, g_2^1\}$. Затем рассматриваются старшие биты $e_1$ и $e_2$, указывающие на значение в таблице, которое умножается на «накопитель». Все пары оснований проходят аналогичную процедуру, после чего «накопитель» возводится в квадрат для перехода на следующий уровень. Такие таблицы могут увеличить производительность в 3–4 раза [13]. Для $g \in \mathbb{G}$ вычисление кортежей $(g^{a^i}, \ldots, g^{a^m})$ выполняется стандартной техникой предварительного вычисления таблиц степеней.

Для последующего использования верификаторам протоколов zk-SNARK целесообразно строить долговременные таблицы степеней порождающих элементов $g^i$ и секретных точек $s^j$ в фоновом режиме. Доказывающий вычисляет полином $h(x)$, который может храниться в виде оценки от корней QAP/QSP и др. Для этого выводится полином $p(x)$, а затем в открытом виде (без криптографических преобразований) для получения $h(x)$ выполняется деление полиномов, что ускоряется умножением на основе быстрого преобразования Фурье (БПФ) со сложностью $O(n \log n)$ и алгоритмом полиномиальной интерполяции [47] для построения двоичного дерева полиномов со сложностью $O(n \log^2 n)$. Для ускорения вычислений $h(x)$ доказывающий также может хранить не содержащие секретов таблицы возведения в степень и полиномиальное дерево, которые потенциально могут передаваться между разными доказывающими.

В протоколе zk-SNARK [14] используются структурные свойства QAP из арифметических схем, сокращающие размер ключа доказывающего, который формируется на основе порождающего элемента $P$ группы $\mathbb{G}_1$ или $\mathbb{G}_2$ и скаляров $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ для вычисления $\alpha_1 P, \ldots, \alpha_n P$. Арифметическая схема $C$ с $m$ проводами (Wires) и $d$ вентилями (Gates) преобразуется в QAP размера $m$ степени $d$. Далее строятся три

матрицы $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{F}^{(m+1)\times d}$, кодирующие топологию схемы $C$: $j$-е столбцы $\mathbf{A}/\mathbf{B}$ кодируются левыми/правыми входами $j$-го логического элемента, а $j$-е столбцы $\mathbf{C}$ — выходами логических элементов, $j \in \{1, \ldots, d\}$. Рассматривается $S \subset \mathbb{F}$ как множество размера $d$, $Z(z) = \prod_{\omega \in S}(z - \omega)$ и для $i \in \{1, \ldots, m\}$ полином $A_i$ — расширение низкой степени $i$-й строки $\mathbf{A}$. Аналогично определяются $B_i, C_i$. Примечательно, что в [14] отмечается наличие нулевых строк матриц $\mathbf{A}, \mathbf{B}, \mathbf{C}$, соответствующих нулевым многочленам. Например, если $i$-й провод никогда не имеет ненулевого значения в качестве левого входа вентиля, то $i$-я строка $\mathbf{A}$ является нулевой, поэтому $A_i$ — нулевой многочлен. Этот факт используется для сокращения размера ключа доказательства за счёт уменьшения количества ненулевых многочленов в матрицах [14], что снижает стоимость вычислений.

В протоколах zk-SNARK [12, 13] для вычисления доказательств $\boldsymbol{\pi}$ используются универсальные мультискалярные умножения. В протоколе zk-SNARK [14] доказывающий использует вектор $\boldsymbol{\alpha} \in \mathbb{F}^{d+1}$ в виде коэффициентов многочлена-частного $h(x)$ степени $d$ или $\boldsymbol{\alpha} = (1, \mathbf{s}, \delta_1, \delta_2, \delta_3) \in \mathbb{F}^{4+m}$ для случайных $\delta_1, \delta_2, \delta_3 \in \mathbb{F}$. В первом случае $\boldsymbol{\alpha}$ представляется случайным, поэтому может использоваться алгоритм Бос-Костера [11] из-за меньших требований к памяти. Во втором случае $\mathbf{s}$ зависит от ввода схемы $C(\mathbf{x}, \mathbf{a})$ и формирователя арифметических схем $C$, где $\mathbf{x}$ — открытый вход; $\mathbf{a}$ — секретный вход, знание которого доказывается. Теперь $\boldsymbol{\alpha}$ может содержать $\mathbf{s}$ с дополнительными элементами. Секрет $\mathbf{s}$ рассматривается как список значений проводов схемы $C$ при вычислении на $(\mathbf{x}, \mathbf{a})$. Разрядность проводов зависит от выбора переменной типа байт, слово и т. д., а производительность повышается предварительной группировкой элементов из $\boldsymbol{\alpha}$ по типам данных и применением метода [11].

Дополнительный вклад в быстродействие может внести асимметричное билинейное спаривание $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, где $\mathbb{G}_1$ — «базовая» группа точек эллиптической кривой [16], а $\mathbb{G}_2$ — группа точек эллиптической кривой «кручения» [16] и $\mathbb{G}_1 \neq \mathbb{G}_2$. Операции над «базовой» кривой выполняются быстрее. Если один из входов функции билинейного спаривания фиксирован, применяются методы предварительного вычисления [48–50], идейно схожие с пакетной верификацией [19]. Вычислительные методы, обеспечивающие производительное билинейное спаривание, также представлены в [51–60]. Например, доказывающий может вычислять $g_w^{w(s)}$ над кривой «кручения», а остальные значения — над «базовой» кривой. Такая асимметрия предполагает, что элемент поля может отображаться в виде значения первой, второй или обеих групп. Возможно использование сокращённого преобразования Тейта [61, 62] для эллиптической кривой $E$ над $\mathbb{F}_q$ для простого числа $q$ с группами $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$, эквивалентными подгруппам в $(E(\mathbb{F}_q), E(\mathbb{F}_q^k), \mathbb{F}_{q^k}^*)$ соответственно. Эллиптические кривые, удобные для билинейного спаривания, имеют размер элементов группы $\mathbb{G}_1$ меньший, чем размер элементов группы $\mathbb{G}_2$ [63]. Поэтому в протоколе zk-SNARK [17] для повышения производительности $\mathbf{A}, \mathbf{C} \in \mathbb{G}_1$ и $\mathbf{B} \in \mathbb{G}_2$. Выбор групп позволяет гибко настраивать уровень защищённости и производительности операций.

Отдельно стоит обратить внимание на потенциальную возможность сокращения размера доказательств. Например, по сравнению с протоколом zk-SNARK [17] на основе QAP из арифметических схем с выходом в виде набора бит и доказательством из трёх элементов поля протокол zk-SNARK [18] на основе SSP из логических схем с выходом один бит имеет доказательство из двух элементов поля. Доказательство протокола zk-SNARK [17] также сокращается до двух элементов поля за счёт переписывания схемы с использованием только вентилей возведения в квадрат. Детальнее,

каждый элемент умножения $a \cdot b = c$ переписывается как $(a+b)^2 - (a-b)^2 = 4c$. Если используются только элементы возведения в квадрат, то полиномы QAP, соответствующие левым и правым входам логических элементов, равны $(u_i(x) = v_i(x)$ для всех $i)$. Зафиксировав значения секретных рандомизаторов $r = s \in \mathbb{Z}_p$, отвечающих за введение свойства нулевого разглашения, и используя компоненты ключа верификации $\beta, \alpha \in \mathbb{Z}_p^*$, формируем $\mathbf{B} = \mathbf{A} + \beta - \alpha$ [17]. Поэтому необходимо построить только два элемента доказательства $\mathbf{A}$ и $\mathbf{C}$ [17]. Однако описанный метод может удвоить количество вентилей и требует дополнительных проводов для вычитания квадратов. Поэтому уменьшение размера доказательства связано с дополнительными вычислительными затратами.

### 3. Разделение публичных параметров главной ссылочной строки

В протоколах zk-SNARK [15, 18] экономия ресурсов достигается за счёт предварительного вычисления наборов $\{g_1^{v_i(s)}\}_{i>l_u}$, $g_1^{t(s)}$ и $\{g_1^{v_i(s)}\}_{i=0}^{m}$, $g_2^{t(s)}$, где $v_i(x), t(x)$ — многочлены QAP/QSP; $s$ — секретная точка; $l_u$ — разрядность открытого входа; $l_w$ — разрядность секретного входа. Для оценки многочлена-частного $h(x)$ в $m$-корнях $r_1, \ldots, r_m$ целевого полинома $t(x) = \prod\limits_{i=1}^{m}(x - r_i)$ доказывающий может применять дискретное преобразование Фурье, как представлено в [18]. В результате повышение производительности протокола zk-SNARK [18] достигается модификацией CRS доказывающего:

$$\boldsymbol{\sigma}_P = \Big(r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2, \{g_1^{v_i(s)}\}_{i>l_u}, \{g_2^{v_i(s)}\}_{i>l_u}, \{g_1^{\beta v_i(s)}\}_{i>l_u},$$
$$g_1^{\beta t(s)}, g'_2, g'^{\beta}_2, \gamma, \{t(r'_j)^{-1}\}_{j=1}^{d}, \{g_1^{l'_j(s)}\}_{j=1}^{d}, g_1^{t(s)}, Q\Big).$$

Верификатор протокола zk-SNARK [18] вычисляет $V = g_1^{v_0(s)+\sum\limits_{i=1}^{l_u} a_i v_i(s)} V_w$ и проводит верификацию, при этом полная CRS заменяется компактным вариантом с $l_u + 6$ элементами группы:

$$\boldsymbol{\sigma}_V = (r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, \{g_1^{v_i(s)}\}_{i=0}^{l_u}, g_2, g_2^{t(s)}, g'_2, g'^{\beta}_2).$$

Если CRS формируется верификатором, то за счёт знания применяемых секретов, например $\beta$ и $\tau$ в [18], сложность верификации дополнительно сокращается с помощью соответствующих предварительных вычислений.

Другим примером является протокол zk-SNARK [17], в котором если каждый вентиль соединён с постоянным числом проводов, то набор QAP является разреженным, а сложность вычисления линейной — $O(n)$, где $n = \deg(t(x))$, или зависит от параметра безопасности. При этом для $q = 1, \ldots, n$ выполняются следующие оценки полиномов:

$$\sum_{i=0}^{m} a_i u_i(r_q) = \sum_{i=0}^{m} a_i u_{i,q}, \quad \sum_{i=0}^{m} a_i v_i(r_q) = \sum_{i=0}^{m} a_i v_{i,q}, \quad \sum_{i=0}^{m} a_i w_i(r_q) = \sum_{i=0}^{m} a_i w_{i,q}. \tag{4}$$

Если $r_1, \ldots, r_m$ — корни $t(x)$ при подходящем простом $p$, то $h(x)$ вычисляется с использованием БПФ в $\mathbb{Z}_p$ за $O(n \log n)$ операций. Вычисление коэффициентов в (4) возможно за счёт БПФ, на основе которых доказывающий выполняет $m + 3n - l_u + 3$ возведений в степень в $\mathbb{G}_1$, $n+1$ — в $\mathbb{G}_2$. С увеличением параметра (уровня) безопасности порядок групп растёт и возведение в степень становится трудозатратнее. В таком случае CRS [17]

$$\boldsymbol{\sigma}_1 = \begin{pmatrix} \alpha, \beta, \delta, \{x^i\}_{i=0}^{n-1}, \{(\beta u_i(x) + \alpha v_i(x) + w_i(x))/\gamma\}_{i=0}^{l_u}, \\ \{(\beta u_i(x) + \alpha v_i(x) + w_i(x))/\delta\}_{i=l_u+1}^{m}, \{x^i t(x)/\delta\}_{i=0}^{n-2} \end{pmatrix}, \boldsymbol{\sigma}_2 = \big(\beta, \gamma, \delta, \{x^i\}_{i=0}^{n-1}\big) \tag{5}$$

расширяется такими элементами $[u_i(x)]_1, [v_i(x)]_1, [w_i(x)]_2$ для $i \in \{1, \ldots, m\}$ при $[z_i(x)]_j = g_j^{z_i(x)}$, что $\mathbf{A}$ и $\mathbf{B}$ доказательства $\boldsymbol{\pi}$ [17], а именно

$$\begin{gathered}\mathbf{A} = \alpha + \sum_{i=0}^{m} a_i u_i(x) + r\delta, \quad \mathbf{B} = \beta + \sum_{i=0}^{m} a_i v_i(x) + s\delta, \\ \mathbf{C} = \left( \sum_{i=l_u+1}^{m} a_i(\beta u_i(x) + \alpha v_i(x) + w_i(x)) + h(x)t(x) \right) / \delta + \mathbf{A}s + \mathbf{B}r - rs\delta,\end{gathered} \tag{6}$$

становится возможным строить без вычисления коэффициентов $\sum\limits_{i=0}^{m} a_i u_i(x)$ и $\sum\limits_{i=0}^{m} a_i v_i(x)$ и последующего возведения в степень. В результате в случае QSP/SSP коэффициенты $a_i \in \{0, 1\}$ расширяют CRS и доказывающий может выполнить $m$ умножений для каждой компоненты $\mathbf{A}$ и $\mathbf{B}$. Модифицированная CRS, предполагающая более быстрое вычисление доказательств, формируется из исходной CRS, поэтому свойства защищённости протокола не нарушаются [17].

Кроме того, верификатору протокола zk-SNARK [17] не требуется полная CRS (5). Достаточно знать $l_u + 2$ элементов $\mathbb{G}_1$, три элемента $\mathbb{G}_2$ и один элемент $\mathbb{G}_T$. В данном случае формирование ключей преобразуется к виду $(\sigma_P, \sigma_V, \tau) \leftarrow \mathsf{Setup}(R)$ с компонентом

$$\sigma_V = \left( p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, [1]_1, \left\{ \left[ \frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma} \right]_1 \right\}_{i=0}^{l_u}, [1]_2, [\gamma]_2, [\delta]_2, [\alpha\beta]_T \right). \tag{7}$$

Верификация подтверждает, что доказательство (6) состоит из трёх корректных элементов $\mathbf{A}, \mathbf{B}, \mathbf{C}$:

$$[\mathbf{A}]_1 \cdot [\mathbf{B}]_2 = [\alpha]_1 \cdot [\beta]_2 + \sum_{i=0}^{l_u} a_i \left[ \tfrac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\gamma} \right]_1 \cdot [\gamma]_2 + [\mathbf{C}]_1 \cdot [\delta]_2.$$

Верификатор вычисляет $l_u$ возведений в степень в $\mathbb{G}_1$, ряд умножений и три билинейных спаривания, где предполагается, что $[\alpha\beta]_T = [\alpha]_1 \cdot [\beta]_2$ предварительно вычисляются в $\sigma_V$ (7).

## 4. Пакетная верификация доказательств

Пакетная верификация ускоряет работу протоколов zk-SNARK. Например, для всех протоколов zk-SNARK [19] вместо проверки $P$ равенств вида $X_i = Y_i$ для $i \in [1, \ldots, P]$ верификатор может сгенерировать случайные $\tau_i \in \mathbb{Z}_p$ для $i \in [1, \ldots, P-1]$, а затем проверить равенство $\prod\limits_{i=1}^{P-1} X_i^{\tau_i} \cdot X_P = \prod\limits_{i=1}^{P-1} Y_i^{\tau_i} \cdot Y_P$. Если $X_i$ и $Y_i$ имеют подходящую структуру, то пакетная верификация экономит ресурсы. Например, если $X_i = e(U_i, V)$, где $V$ не зависит от $i$, то при вычислении $\prod\limits_{i=1}^{P-1} X_i^{\tau_i} \cdot X_P = e\left( \prod\limits_{i=1}^{P-1} U_i^{\tau_i} \cdot U_P, V \right)$ выполняется одно билинейное спаривание и $(P-1)$ возведений в степень.

В [19] представлено пять видов пакетной верификации, соответствующих разным протоколам zk-SNARK. Используются случайные секретные значения $\chi, \gamma, \delta \in \mathbb{Z}_p$. Значения вида $\pi_{ij}$ являются ранее сформированными доказательствами [19].

**Пакетная верификация достоверности обязательств.** Проверка выполнения равенств вида $e(A_{i1}, g_2^{\gamma}) = e(g_1, A_{i2}^{\gamma})$ для $i \in [1, \ldots, P]$ требует $2P$ билинейных спарива-

ний. Пакетная версия $\prod\limits_{i=1}^{P} e(A_{i1}, g_2^{\gamma})^{\tau_i} = \prod\limits_{i=1}^{P} e(g_1, A_{i2}^{\gamma})^{\tau_i}$ или ещё производительнее:

$$e\left(\prod_{i=1}^{P} A_{i1}^{\tau_i}, g_2^{\gamma}\right) = e\left(g_1, \prod_{i=1}^{P} A_{i2}^{\gamma\tau_i}\right),$$

при $\tau_i \in \mathbb{Z}_p$ и $\tau_P = 1$ требует двух билинейных спариваний, по $1 \times (P-1)$ возведений в степень в $\mathbb{G}_2$ и $\mathbb{G}_1$ для левой и правой частей.

**Пакетная верификация доказательств знания результата произведения.** Если верификатор получает $P$ доказательств $\pi_i = ((A_{i1}, A_{i2}^{\gamma}), (B_{i1}, B_{i2}^{\gamma}), (C_{i1}, C_{i2}^{\gamma})$, то наивная верификация уравнений $e(A_{i1}, B_{i2}^{\gamma}) = e(g_1, C_{i2}^{\gamma}) e(\pi_i, g_2^{\gamma Z(\chi)})$ требует $3P$ билинейных спариваний. Тогда рассматривается $Z(X) = \prod\limits_{i=1}^{n}(X - w^{i-1}) = X^n - 1$ — единственный многочлен $n$-й степени, для которого $Z(w^{i-1}) = 0$ при $i \in [1, \ldots, n]$, и пакетная версия

$$\prod_{i=1}^{P} e(A_{i1}, B_{i2}^{\gamma})^{\tau_i} = e\left(g_1, \prod_{i=1}^{P} C_{i2}^{\gamma\tau_i}\right) e\left(\prod_{i=1}^{P} \pi_i^{\tau_i}, g^{\gamma Z(\chi)}\right)$$

требует только $(P+2)$ билинейных спариваний, $1 \times P$ возведений в степень в $\mathbb{G}_1$, по $1 \times (P-1)$ возведений в степень в $\mathbb{G}_2$ и $\mathbb{G}_T$. Если $A_{i1} = A_1$ фиксировано, то за счёт изменения первого преобразования на $e\left(A_1, \prod\limits_{i=1}^{P} B_{i2}^{\gamma}\right)^{\tau_i}$ вычисления сокращаются до трёх билинейных спариваний, $1 \times (P-1)$ возведений в степень в $\mathbb{G}_1$ и $2 \times (P-1)$ возведений в степень в $\mathbb{G}_2$. Случай фиксированного $B_{i2}^{\gamma} = B_2$ аналогичен.

**Пакетная верификация доказательств знания циклического сдвига вектора.** Если верификатор получает $P$ доказательств $\pi_i{=}(\pi_{i1}, \pi_{i2}^{\delta}){=}((A_{i1}, A_{i2}^{\gamma}), (B_{i1}, B_{i2}^{\gamma}))$, то наивная верификация требует $4P$ билинейных спариваний. Пакетная версия

$$e\left(\prod_{i=1}^{P} \pi_{i1}^{\tau_i} \prod_{i=P+1}^{2P} (B_{i1}\pi_{i1})^{\tau_i}, g_2^{\delta Z(\chi)}\right) = e\left(g_1^{Z(\chi)}, \prod_{i=1}^{P} \pi_{i2}^{\delta\tau_i}\right) e\left(\prod_{i=P+1}^{2P} A_{i1}^{\tau_i}, g_2^{\delta Z(\chi) Z^*(\chi)}\right)$$

требует три билинейных спаривания, $1 \times (P-1)$ и $1 \times (2P-1)$ возведений в степень в $\mathbb{G}_1$, $1 \times P$ возведений в степень в $\mathbb{G}_2$.

**Пакетная верификация доказательств знания суммы элементов множеств.** Протокол zk-SNARK доказательства знания суммы элементов, входящих в конечное множество, рассматривает такой набор $\mathbf{S} = ((S_1, \ldots, S_n), s)$ при $S_i, s \in \mathbb{Z}_p$, для которого существует вектор $\mathbf{b} \in \{0,1\}^n$ и выполняется равенство $\sum\limits_{i=1}^{n} S_i b_i = s$. Доказывается знание открытия обязательства $(B_1, B_2^{\gamma})$ к вектору $\mathbf{b}$, при котором выполняется указанное равенство.

Таким образом, верификатор генерирует случайные $\tau_i$, $i \in \{1, \ldots, 8\}$, $\tau_6 = \tau_8 = 1$, и строит $l_i(X) = \prod\limits_{j \neq i}((X - w^{j-1})/(w^{i-1} - w^{j-1}))$ — $i$-й базисный многочлен Лагранжа, являющийся единственным многочленом степени $n-1$, для которого $l_i(w^{i-1}) = 1$ и $l_i(w^{j-1}) = 0$ при $j \neq i$. Выполняется две проверки:

$$e(B_1^{\tau_1} C_1^{\tau_2} D_1^{\tau_3}, g_2^{\gamma}) e((B_1/g_1)^{\tau_4} (S_1')^{\tau_5}, B_2^{\gamma}) e((g_1^{l_1(\chi)})^{\tau_6}, D_2^{\gamma}/(g_2^{\gamma l_1(\chi)})^{s}) =$$
$$= e(g_1, B_2^{\gamma\tau_1} C_2^{\gamma(\tau_2+\tau_5)} D_2^{\gamma\tau_3}) e(\pi_1^{\tau_4} \pi_2^{\tau_5} \pi_4^{\tau_6}, g_2^{\gamma Z(\chi)}),$$
$$e(\pi_{31}^{\tau_7}(D_1/C_1\pi_{31})^{\tau_8}, g_2^{\delta Z(\chi)}) = e((g_1^{Z(\chi)})^{\tau_7}, \pi_{32}^{\delta}) e(D_1^{\tau_8}, g_2^{\delta Z(\chi) Z^*(\chi)}).$$

В результате требуется только восемь билинейных спариваний, $2\times 3$ и $2\times 2$ возведений в степень в $\mathbb{G}_1$, три дополнительных возведения в степень в $\mathbb{G}_1$, $1\times 3$ возведений в степень в $\mathbb{G}_2$ и одно дополнительное возведение в степень в $\mathbb{G}_2$.

**Пакетная верификация доказательств принадлежности диапазону.** В протоколе zk-SNARK подтверждения принадлежности элемента общедоступному диапазону $[L,\ldots,H]$ доказывается знание открытия обязательства $(A_1, A_2^{\gamma})$ к значению $a\in[L,\ldots,H]$. Это будет означать, что публичный вход $(A_1, A_2^{\gamma})$ корректно привязан к вектору $\mathbf{a}$ с $a_1 = a$ и $a_i = 0$ для $i > 1$. Диапазон $[L,\ldots,H]$ можно заменить на $[0,\ldots,H-L]$, а затем использовать гомоморфные свойства схемы формирования обязательств, чтобы добавить $L$ к зафиксированному значению. Поэтому предполагается, что диапазон равен $[0,\ldots,H]$ при $H\geqslant 1$. Данный вариант похож на протокол zk-SNARK доказательства знания суммы элементов, входящих в конечное множество, где дополнительно фиксируется значение $a\in[0,\ldots,H]$ и используется разреженный вектор $\mathbf{S}$ с $S_i = \lfloor (H+2^{i-1})/2^i \rfloor$. Доказываетя, что для обязательств $(A_1, A_2^{\gamma})$ зафиксированного значения $a$ выполняется равенство $\sum\limits_{i=1}^{n} S_i b_i = a$.

Таким образом, верификатор генерирует случайные $\tau_i$, $i\in\{0,\ldots,8\}$, $\tau_6=\tau_8=1$, и выполняет две проверки:

$$e(A_1^{\tau_0}B_1^{\tau_1}C_1^{\tau_2}D_1^{\tau_3}, g_2^{\gamma})\, e(g_1^{-\tau_1}(B_1/g_1)^{\tau_4}(S_1')^{\tau_5}, B_2^{\gamma})\, e((g_1^{l_1(\chi)})^{\tau_6}, D_2^{\gamma}/A_2^{\gamma}) =$$
$$= e(g_1, A_2^{\gamma\tau_0}C_2^{\gamma(\tau_2+\tau_5)}D_2^{\gamma\tau_3})\, e(\pi_1^{\tau_4}\pi_2^{\tau_5}\pi_4^{\tau_6}, g_2^{\gamma Z(\chi)}),$$
$$e(\pi_{31}^{\tau_7}(D_1/C_1\pi_{31})^{\tau_8}, g_2^{\delta Z(\chi)}) = e((g_1^{Z(\chi)})^{\tau_7}, \pi_{32}^{\delta})\, e(D_1^{\tau_8}, g_2^{\delta Z(\chi)Z^*(\chi)}).$$

В результате требуется только восемь билинейных спариваний, $1\times 4$, $2\times 3$ и $1\times 2$ возведений в степень в $\mathbb{G}_1$, три дополнительных возведения в степень в $\mathbb{G}_1$, $1\times 3$ возведений в степень в $\mathbb{G}_2$.

В [21] представлен протокол zk-SNARK «Dory» с публичным формированием CRS без использования секретных значений, который строит доказательства знания результата сопряжения векторов двух групп и использует схему доказательств на основе преобразования Фиата — Шамира [46]. Протокол также объединяет доказательства в пакет, повышая производительность верификации. Кроме того, производительность [21] достигается за счёт симметрии сообщений и ключей, применяемых для формирования доказательств: если сообщение принадлежит $\mathbb{G}_1$, то ключ для формирования доказательства принадлежит $\mathbb{G}_2$, и наоборот.

## 5. Рекурсивная композиция доказательств

Объединение цепочки доказательств протоколов zk-SNARK в одно заключительное доказательство, которое имеет размер и сложность верификации, аналогичные отдельным доказательствам, является важной характеристикой систем достоверных вычислений. Например, протокол zk-SNARK [64] представляет развитие идей поэтапных вычислений с верификацией результатов на каждом промежуточном шаге (инкрементные доказываемые вычисления) [65–67] с произвольным компонентным протоколом zk-SNARK, например [8, 9] и др. Применяется рекурсивная композиция протокола zk-SNARK с фиксированным количеством шагов, что сокращает трудозатраты на формирование CRS за счёт её повторного использования. В результате понятие zk-SNARK расширяется до распределённой среды. После каждого этапа выводится текущее состояние и доказательство его корректности, а вычисления представляются в виде ориентированных ациклических графов, разворачивающихся во времени. В кон-

це цепочки верификатор протокола zk-SNARK получает единственное доказательство достоверности всех шагов.

Протокол zk-SNARK «FRACTAL» [68] представляет новую методологию рекурсивной композиции доказательств с публичным формированием CRS без использования секретных значений. Ядром схемы является постквантовый протокол zk-SNARK с системой ограничений ранга 1 (Rank-1 Constraint System, R1CS). Подобно [69, 70], схема [68] также использует коды Рида — Соломона при работе с R1CS и построении вероятностно-проверяемых доказательств.

Протоколы zk-SNARK семейства «Spartan» [71] также формируют CRS без использования секретных значений. В частности, реализация протокола zk-SNARK «Halo» [72] представляет рекурсивную композицию доказательств, в которой для группы $\mathbb{G}$ простого порядка $p$, случайного вектора $\mathbf{G} \in \mathbb{G}^d$, $d \in \mathbb{Z}$, значений $r, H \in \mathbb{G}$, коэффициентов $a_i \in \mathbb{F}_p$, являющихся членами $i$-й степени QAP-полинома $p(X)$, формируется CRS в виде $\boldsymbol{\sigma} = (\mathbb{G}, \mathbb{F}_p, \mathbf{G}, H)$, а схема формирования обязательств имеет следующий вид:

$$\mathsf{Com}(\boldsymbol{\sigma}, p(X); r) = \langle \mathbf{a}, \mathbf{G} \rangle + [r]H.$$

Здесь $\langle \mathbf{a}, \mathbf{G} \rangle = a_0 G_0 + a_1 G_1 + a_2 G_2 + \ldots$ — скалярное произведение векторов; $[r]H$ — $r$-кратное сложение точки эллиптической кривой. В качестве секретов выступают $\mathbf{a}, r$.

Источник [73] обобщает конструкцию «Halo» [72], продолжая развитие рекурсивных доказательств с использованием компактных схем обязательств для доказательства достоверности оценки полиномов в секретных точках. «Halo Infinite» [73] демонстрирует новую методологию построения систем доказательств знания «Bulletproofs» без протокола zk-SNARK, используя свойство агрегации внутренних доказательств. Версия «Halo Infinite» [73] объединяет линейные комбинации обязательств в краткое обязательство, открываемое при необходимости.

## 6. Сравнительный анализ производительности протоколов zk-SNARK

В таблице приведено сравнение протоколов zk-SNARK [7–9, 12–15, 17, 18, 20–36] по размерам CRS и доказательств, а также по сложности вычислений доказывающих и верификаторов. Используются следующие обозначения: $n$ — количество логических элементов дискретных функций (вентилей арифметической/логической схемы); $\lambda$ — параметр безопасности; $\mathbb{G}$ — размер элемента группы; $A, M, E, P$ — затраты на сложение, умножение, возведение в степень и билинейное спаривание; $l_u, l_w, l_o$ — разрядность открытого и секретного входов и выхода; $m$ — количество переменных дискретной функции (проводов арифметической/логической схемы); $n_M$ — количество элементов умножения дискретной функции (арифметической/логической схемы); $l$ — размер открытого входа в элементах группы. Для протокола zk-SNARK [30] на основе полиномиальных наборов QPP введены дополнительные обозначения: $d$ — количество корней полиномов набора QPP; $v = \max\limits_{i=1,\ldots,m} \{n_i\}$ — максимальная степень полиномов набора QPP; $n_i$ — степень выходного полинома $c_i(z)$ набора QPP для $i = 1, \ldots, m$; $m$ — количество выходных полиномов; $T$ — сложность вычисления всех полиномов $c_i(z)$.

Анализ таблицы показывает, что с точки зрения практической реализации наиболее приемлемыми являются протоколы zk-SNARK [12–14, 17, 18, 32–35], которые для произвольных дискретных функций всегда имеют фиксированный размер доказательств и постоянное количество уравнений верификации.

Выделяются работы [15, 30, 31], которые также имеют фиксированные размеры доказательств. Тем не менее сложность верификации протокола zk-SNARK [15] зави-

**Сравнительный анализ производительности протоколов zk-SNARK**

| Протокол | CRS | Доказ-во | Доказывающий | Верификатор |
|---|---|---|---|---|
| Й. Грот и др. [22] | $O(1)\ \mathbb{G}$ | $O(n)\ \mathbb{G}$ | $O(n)\ E$ | $O(n)\ P$ |
| Й. Грот и др. [23] | $O(1)\ \mathbb{G}$ | $O(n)\ \mathbb{G}$ | $O(n)\ E$ | $O(n)\ E$ |
| М. Эйб и др. [24] | $O(1)\ \mathbb{G}$ | $O(n)\ \mathbb{G}$ | $O(n)\ E$ | $O(n)\ E$ |
| Дж. Джентри [25] | $O(1)\ \mathbb{G}$ | $l_w\lambda^{O(1)}\ \mathbb{G}$ | $n\lambda^{O(1)}\ M$ | $n\lambda^{O(1)}\ M$ |
| Й. Грот [26] | $O(n^{1/2})\ \mathbb{G}$ | $O(n^{1/2})\ \mathbb{G}$ | $O(n)\ M$ | $O(n)\ M$ |
| Р. Дженнаро и др. [20] | $O(n\ poly(\lambda))\ \mathbb{G}$ | $O(l_o)\ \mathbb{G}$ | $O(n\ poly(\lambda))\ M$ | $O(l_o\ poly(\lambda))\ M$ |
| Й. Грот [27] | $O(n)\ \mathbb{G}$ | $O(n)\ \mathbb{G}$ | $O(n)\ E$ | $O(n)\ M$ |
| Й. Грот [27] | $O(n)\ \mathbb{F}_2$ | $O(n)\ \mathbb{F}_2$ | $O(n)\ M$ | $O(n)\ M$ |
| Й. Грот [8] | $O(n^{2/3})\ \mathbb{G}$ | $O(n^{2/3})\ \mathbb{G}$ | $O(n^{4/3})\ E$ | $O(n)\ M$, $O(n^{2/3})\ P$ |
| Х. Липмаа [9] | $n^{1/3+O(1)}\ \mathbb{G}$ | $O(n^{2/3})\ \mathbb{G}$ | $O(n^{4/3})\ A, n^{1+O(1)}\ E$ | $O(n)\ M, O(n^{2/3})\ P$ |
| Х. Липмаа [28] | $O(n)\ \mathbb{G}$ | $O(1)\ \mathbb{G}$ | $O(n\log n)\ E$ | $O(1)\ P$ |
| Э. Бен-Сассон и др. [12] | $O(11n+3l+2)\ \mathbb{G}_1$, $6\ \mathbb{G}_2$ | $11\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(n)\ \mathbb{G}_1, \mathbb{G}_2$ | $O(l)\ E, 21\ P$ |
| Р. Дженнаро и др. [15] | $O(n)\ \mathbb{G}$ | $9\ \mathbb{G}$ | $O(n+n\log^2 n)\ E$ | $O(l_u+l_w)\ E/P$ |
| Б. Парно и др. [13] | $O(7m+n_M-2l)\ \mathbb{G}$ | $8\ \mathbb{G}$ | $O(7m+n_M-2l)\ E$ | $O(l)\ E, 11\ P$ |
| П. Фаузи и др. [29] | $n^{(1+O(1))/2}\ \mathbb{G}$ | $O(n^{1/2})\ \mathbb{G}$ | $n^{(1+O(1))/2} \times$ $\times\ O(n^{1/2}(1+\log n))\ M$ | $O(n)\ M$, $O(n^{1/2})\ P$ |
| Г. Данезис и др. [18] | $O(2m+n-2l)\ \mathbb{G}_1$, $O(m+n-l)\ \mathbb{G}_2$ | $3\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(m+n-l)\ E_1$ | $O(l)\ M_1, 6\ P$ |
| Ю. Чжан и др. [7] | $O(m)\ \mathbb{G}$ | $O(l_w)\ \mathbb{G}$ | $O(m\log m)\ E$ | $O(l_w)\ E, P$ |
| А. Косба и др. [30] | $O(dl)\ \mathbb{G}$ | $8\ \mathbb{G}$ | $O(T+dv \times$ $\times\ (\log(dv)+m))\ E$ | $O(\sum_{i\in[l]} n_i)\ M$ |
| Х. Липмаа [31] | $O(n\log n)\ \mathbb{G}$ | $O(1)\ \mathbb{G}$ | $O(n\log^2 n)\ E$, $O(n\log n)\ M$ | $O(\log n)\ P$ |
| Э. Бен-Сассон и др. [32] | $O(6m+n_M+l)\ \mathbb{G}_1$, $O(m)\ \mathbb{G}_2$ | $7\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(6m+n_M-l)\ E_1$, $O(m)\ E_2$ | $O(l)\ E_1, 12\ P$ |
| К. Костелло и др. [33] | $O(7m+n_M-2l)\ \mathbb{G}$ | $8\ \mathbb{G}$ | $O(7m+n_M-2l)\ E$ | $O(l)\ E, 11\ P$ |
| М. Бакес и др. [34] | $O(1+7m+n-2l)\ \mathbb{G}$ | $3+8\ \mathbb{G}$ | $O(3l+7m+n-2l)\ E$ | $6+11\ P, O(l)\ M$, $O(1+l)\ E$ |
| Й. Грот [17] | $O(m+2n_M)\ \mathbb{G}_1$, $O(n_M)\ \mathbb{G}_2$ | $2\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(m+3n_M-l)\ E_1$, $O(n_M)\ E_2$ | $O(l)\ E_1, 3\ P$ |
| Й. Грот и др. [35] | $O(m+4n_M+5)\ \mathbb{G}_1$, $O(2n_M+3)\ \mathbb{G}_2$ | $2\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(m+4n_M-l)\ E_1$, $O(2n_M)\ E_2$ | $O(l)\ E_1, 6\ P$ |
| Э. Бен-Сассон и др. [14] | $O(6m+n_M-l)\ \mathbb{G}_1$, $O(m)\ \mathbb{G}_2$ | $7\ \mathbb{G}_1, 1\ \mathbb{G}_2$ | $O(6m+n_M-l)\ E_1$, $O(m)\ E_2$ | $O(l)\ E_1, 12\ P$ |
| А. Кьеза и др. [36] | $O(4n+2)\ \mathbb{G}_1$, $2\ \mathbb{G}_2$ | $13\ \mathbb{G}_1, 8\ \mathbb{F}_q$ | $O(22n)\ \mathbb{G}_1$, $O(n\log m)\ \mathbb{F}_q$ | $2\ P\ \mathbb{G}_1$, $O(l_u+\log n)\ \mathbb{F}_q$ |
| Дж. Ли [21] | – | $1\ \mathbb{G}_T$, $O(6\log d)\ \mathbb{G}_T$ | $O(d^{1/2})\ P$ | $O(\log d)\ M$, $1\ P$ |

сит от разрядностей открытого и секретного входов дискретной функции, в протоколе zk-SNARK [31] сложность верификации зависит от количества логических элементов дискретной функции, а сложность верификации протокола zk-SNARK [30] — от степеней полиномов, соответствующих выходам дискретной функции.

Характерно, что многие рассмотренные протоколы имеют структуру, унаследованную или соответствующую развитию исторически основополагающих криптографических протоколов zk-SNARK [15, 13].

Отдельного внимания заслуживают протоколы zk-SNARK [22, 23], которые характеризуются простотой описания и могут быть реализованы с меньшими трудозатратами. Однако у данных протоколов размер доказательств и количество билинейных спариваний при верификации зависят линейно от количества логических элементов дискретной функции. Вопрос об их модификации для фиксирования размера доказательств и количества билинейных спариваний остаётся открытым. Тем не менее в ряде

случаев применение протоколов zk-SNARK [22, 23] может оказаться целесообразным, например для дискретных функций с небольшим количеством логических элементов.

В таблице рассматриваются протоколы zk-SNARK для фиксированных дискретных функций с формированием CRS доверенной стороной с использованием секретных значений. В качестве сравнения с ними приведены характеристики производительности протокола zk-SNARK «Marlin» [36], который однократно строит универсальную и обновляемую CRS, впоследствии используемую для различных дискретных функций. По аналогичным соображениям приведены характеристики производительности протокола zk-SNARK «Dory» [21] доказательства корректности произведения полиномов степени $d$, который не требует предварительного формирования CRS доверенной стороной с использованием секретных значений.

## Заключение

Рассмотрены основные способы повышения производительности, которые в зависимости от конструкции могут являться общими для разных протоколов zk-SNARK. Они основаны на применении хеш-функций, в том числе более адаптированных к рассматриваемым протоколам [2–6, ] методах производительного деления [8, 9], умножения и возведения в степень [10–14] элементов множеств, разделении CRS на лаконичные компоненты [15, 17, 18] для доказывающих и верификаторов, а также на более эффективных билинейных спариваниях [16, 17]. Аналогично [18], доказательство протокола zk-SNARK [17] может сжиматься до двух элементов группы. Относительно применения хеш-функций существуют компромиссы между уменьшением размера доказательств и увеличением затрат на формирование доказательств/верификацию, уменьшением затрат на формирование доказательств и увеличением затрат на верификацию, фиксацией размера открытого входа и увеличением затрат на верификацию и др.

Зафиксирована возможность объединения цепочки промежуточных доказательств протоколов zk-SNARK в одно заключительное доказательство [64, 68, 71–73]. На примере протокола zk-SNARK [14] показаны структурные свойства полиномиального набора QAP, характеризующиеся наличием нулевых многочленов, что также сокращает трудозатраты. Представлен мощный инструмент пакетной верификации доказательств протоколов zk-SNARK [19], значительно сокращающий сложность вычислений за счёт более эффективной группировки элементов доказательств.

Сравнительный анализ протоколов zk-SNARK [7–9, 12–15, 17, 18, 20–36] показал, что конструкции [12–14, 17, 18, 32–35] формируют доказательства фиксированного размера и используют постоянное количество уравнений верификации, поэтому в большей степени подходят для практической реализации. Отдельно выделены работы [15, 30, 31] с фиксированными размерами доказательств, но со сложностью верификации, зависящей от входов, количества логических элементов и степеней полиномов выходов дискретных функций. Протоколы zk-SNARK [22, 23] выделяются простотой описания, однако в зависимости от количества логических элементов дискретных функций размеры доказательств и количество билинейных спариваний изменяются. Фиксирование размера доказательств и количества билинейных спариваний позволит [22, 23] приобрести более широкое распространение. Характерно, что многие рассмотренные протоколы имеют структуру, унаследованную или развитую от исторически основополагающих криптографических протоколов zk-SNARK [13, 15].

## ЛИТЕРАТУРА


1. *Мартыненков И. В.* Краткие неинтерактивные аргументы с нулевым разглашением на основе наборов полиномов // Прикладная дискретная математика. 2023. № 59. С. 20–57.
2. *Grassi L., Khovratovich D., Rechberger C., et al.* Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. Cryptology ePrint Archive. Paper 2019/458. 2019. `https://eprint.iacr.org/2019/458`.
3. *Baylina J. and Bellés M.* 4-bit Window Pedersen Hash On The Baby Jubjub Elliptic Curve. 2019. `https://docs.iden3.io/publications/pdfs/Pedersen-Hash.pdf`. 8 p.
4. *Regev O.* New lattice based cryptographic constructions // Proc. 35th Ann. ACM Symp. on Theory of Computing. N.Y.: ACM, 2003. P. 407–416.
5. *Regev O.* New lattice-based cryptographic constructions // J. ACM. 2004. V. 51. Iss. 6. P. 899–942.
6. *Regev O.* On lattices, learning with errors, random linear codes, and cryptography // Proc. 37th Ann. ACM Symp. on Theory of Computing. N.Y.: ACM, 2005. P. 84–93.
7. *Zhang Y., Papamanthou C., and Katz J.* ALITHEIA: Towards practical verifiable graph processing // Proc. CCS'14. N.Y.: ACM, 2014. P. 856–867.
8. *Groth J.* Short pairing-based non-interactive zero-knowledge arguments // LNCS. 2010. V. 6477. P. 321–340.
9. *Lipmaa H.* Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments // LNCS. 2012. V. 7194. P. 169–189.
10. *Pippenger N.* On the evaluation of powers and related problems // 17th Ann. Symp. SFCS'1976. Houston, TX, USA, 1976. P. 258–263.
11. *Bos J. and Coster M.* Addition chain heuristics // LNCS. 1990. V. 435. P. 400–407.
12. *Ben-Sasson E., Chiesa A., Genkin D., et al.* SNARKs for C: Verifying program executions succinctly and in zero knowledge // LNCS. 2013. V. 8043. P. 90–108.
13. *Parno B., Howell J., Gentry C., and Raykova M.* Pinocchio: Nearly practical verifiable computation // Proc. 34th IEEE Symp. on Security and Privacy. Berkeley, CA, USA, 2013. P. 238–252.
14. *Ben-Sasson E., Chiesa A., Tromer E., and Virza M.* Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Updated version, 2019. `https://eprint.iacr.org/2013/879.pdf`. 37 p.
15. *Gennaro R., Gentry C., Parno B., and Raykova M.* Quadratic span programs and succinct NIZKs without PCPs // LNCS. 2013. V. 7881. P. 626–645.
16. *Costello C.* Pairings for Beginners. `https://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf`. 2012. 146 p.
17. *Groth J.* On the size of pairing-based non-interactive arguments // LNCS. 2016. V. 9666. P. 305–326.
18. *Danezis G., Fournet C., Groth J., and Kohlweiss M.* Square span programs with applications to succinct NIZK arguments // LNCS. 2014. V. 8873. P. 532–550.
19. *Lipmaa H.* Almost Optimal Short Adaptive Non-Interactive Zero Knowledge. Tech. Rep. 2014/396. International Association for Cryptologic Research, 2014. `http://eprint.iacr.org/2014/396`. 20 p.
20. *Gennaro R., Gentry C., and Parno B.* Non-interactive verifiable computing: Outsourcing computation to untrusted workers // LNCS. 2010. V. 6223. P. 465–482.
21. *Lee J.* Dory: Efficient, transparent arguments for generalised inner products and polynomial commitments // LNCS. 2021. V. 13043. P. 1–34.
22. *Groth J., Ostrovsky R., and Sahai A.* Perfect non-interactive zero knowledge for NP // LNCS. 2006. V. 4004. P. 339–358.

23. *Groth J., Ostrovsky R., and Sahai A.* Non-interactive zaps and new techniques for NIZK // LNCS. 2006. V. 4117. P. 97–111.
24. *Abe M. and Fehr S.* Perfect NIZK with adaptive soundness // LNCS. 2007. V. 4392. P. 118–136.
25. *Gentry G.* Fully homomorphic encryption using ideal lattices // Proc. 41 Ann. ACM Symp. Theory of Computing. V. 9. N.Y.: ACM, 2009. P. 169–178.
26. *Groth J.* Linear algebra with sub-linear zero-knowledge arguments // LNCS. 2009. V. 5677. P. 192–208.
27. *Groth J.* Short non-interactive zero-knowledge proofs // LNCS. 2010. V. 6477. P. 341–358.
28. *Lipmaa H.* Succinct non-interactive zero knowledge arguments from span programs and linear error-correcting codes // LNCS. 2013. V. 8269. P. 41–60.
29. *Fauzi P., Lipmaa H., and Zhang B.* Efficient modular NIZK arguments from shift and product // LNCS. 2013. V. 8257. P. 92–121.
30. *Kosba A.E., Papadopoulos D., Papamanthou C., et al.* TRUESET: Nearly Practical Verifiable Set Computations. Cryptology ePrint Archive. Report 2014/160. 2014. `http://eprint.iacr.org/2014/160`. 30 p.
31. *Lipmaa H.* Efficient NIZK arguments via parallel verification of benes networks // LNCS. 2014. V. 8642. P. 416–434.
32. *Ben-Sasson E., Chiesa A., Tromer E., and Virza M.* Scalable zero knowledge via cycles of elliptic curves // LNCS. 2014. V. 8617. P. 276–294.
33. *Costello C., Fournet C., Howell J., et al.* Geppetto: Versatile verifiable computation // Proc. IEEE Symp. SP'15. IEEE Computer Society, USA, 2015. P. 253–270.
34. *Backes M., Barbosa M., Fiore D., and Reischuk R. M.* ADSNARK: Nearly practical and privacy-preserving proofs on authenticated data // IEEE Symp. on Security and Privacy, San Jose, CA, USA, 2015. P. 271–286.
35. *Groth J. and Maller M.* Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs. IACR Cryptology ePrint Archive. 2017. 36 p.
36. *Chiesa A., Hu Y., Maller M., et al.* Marlin: Preprocessing zk-SNARKs with universal and updatable SRS // LNCS. 2020. V. 12105. P. 738–768.
37. *Applebaum B., Ishai Y., and Kushilevitz E.* From secrecy to soundness: Efficient verification via secure computation // LNCS. 2020. V. 6198. P. 152–163.
38. *Reitwiebner C.* zkSNARKs in a Nutshell. 2017. `https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/`. 15 p.
39. *Bitansky N., Canetti R., Chiesa A., and Tromer E.* From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again // Proc. ITCS'12. N.Y.: ACM, 2012. P. 326–349.
40. *Goldwasser S., Lin H., and Rubinstein A.* Delegation of Computation without Rejection Problem from Designated Verifier CS-proofs. Cryptology ePrint Archive. Report 2011/456. 2011. 30 p.
41. *Ajtai M.* Generating hard instances of lattice problems (extended abstract) // Proc. STOC'96. N.Y.: ACM, 1996. P. 99–108.
42. *Papamanthou C., Shi E., Tamassia R., and Yi K.* Streaming authenticated data structures // LNCS. 2013. V. 7881. P. 353–370.
43. *Katz J., Kolesnikov V., and Wang X.* Improved non-interactive zero knowledge with applications to post-quantum signatures // Proc. ACM SIGSAC Conf. CCS'18. N.Y.: ACM, 2018. P. 525–537.

44. *Bünz B., Fisch B., and Szepieniec A.* Transparent SNARKs from DARK Compilers. Cryptology ePrint Archive. Paper 2019/1229. 2019. https://eprint.iacr.org/2019/1229. 59 p.
45. *Ames S., Hazay C., Ishai Y., and Venkitasubramaniam M.* Ligero: Lightweight sublinear arguments without a trusted setup // Proc. ACM SIGSAC Conf. CCS'17. N.Y.: ACM, 2017. P. 2087–2104.
46. *Fiat A. and Shamir S.* How to prove yourself: Practical solutions to identification and signature problems // LNCS. 1986. V. 263. P. 186–194.
47. *Aho A., Hopcroft J., and Ulman J.* The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974. 470 p.
48. *Scott M.* Implementing cryptographic pairings // Proc. 1st First Intern. Conf. on Pairing-Based Cryptography. Berlin; Heidelberg: Springer Verlag, 2007. P. 177–196.
49. *Galbraith S. D., Harrison K., and Soldera D.* Implementing the Tate pairing // LNCS. 2002. V. 2369. P. 324–337.
50. *Barreto P. S. L. M., Lynn B., and Scott M.* Constructing elliptic curves with prescribed embedding degrees // LNCS. 2003. V. 2576. P. 257–267.
51. *Vercauteren F.* Optimal pairings // IEEE Trans. Inform. Theory. 2020. V. 56. No. 1. P. 455–461.
52. *Beuchat J. L., González-Díaz J. E., Mitsunari S., et al.* High-speed software implementation of the optimal ate pairing over Barreto — Naehrig curves // LNCS. 2010. V. 6487. P. 21–39.
53. *Scott M., Benger N., Charlemagne M., et al.* On the final exponentiation for calculating pairings on ordinary elliptic curves // LNCS. 2009. V. 5671. P. 78–88.
54. *Granger R. and Scott M.* Faster squaring in the cyclotomic subgroup of sixth degree extensions // LNCS. 2010. V. 6056. P. 209–223.
55. *Fuentes-Castañeda L., Knapp E., and Rodríguez-Henríquez F.* Faster hashing to $\mathbb{G}_2$ // LNCS. 2012. V. 7118. P. 412–430.
56. *Kim T., Kim S., and Cheon J. H.* On the final exponentiation in Tate pairing computations // IEEE Trans. Inform. Theory. 2013. V. 59. No. 6. P. 4033–4041.
57. *Solinas J. A.* ID-based Digital Signature Algorithms. 2003. http://cacr.uwaterloo.ca/conferences/2003/ecc2003/solinas.pdf. 32 p.
58. *Scott M.* Computing the Tate pairing // LNCS. 2005. V. 3376. P. 293–304.
59. *Granger R. and Smart N.* On Computing Products of Pairings. Cryptology ePrint Archive. Report 2006/172. 2006. 11 p.
60. *Arène C, Lange T., Naehrig M., and Ritzenthaler C.* Faster computation of the Tate pairing // J. Number Theory. 2022. V. 131. No. 5. P. 842–857.
61. *Frey G. and Rück H.-G.* A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves // Mathematics of Computation. 1994. V. 62. No. 206. P. 865–874.
62. *Frey G., Muller M., and Rück H.-G.* The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems // IEEE Trans. Inform. Theory. 2006. V. 45. No. 5. P. 1717–1719.
63. *Galbraith S. D., Paterson K. G., and Smart N. P.* Pairings for cryptographers // Discrete Appl. Math. 2008. V. 156. No. 16. P. 3113–3121.
64. *Bitansky N., Canetti R., Chiesa A., and Tromer E.* Recursive Composition and Bootstrapping for Snarks and Proof-Carrying Data. IACR Cryptology ePrint Archive. 2012. http://eprint.iacr.org/2012/095. 61 p.
65. *Valiant P.* Incrementally verifiable computation or proofs of knowledge imply time/space efficiency // LNCS. 2008. V. 4948. P. 1–18.
66. *Crescenzo G. D. and Lipmaa H.* Succinct NP proofs from an extractability assumption // LNCS. 2008. V. 5028. P. 175–185.

67. *Mei T.* Polylogarithmic two-round argument systems // J. Math. Cryptol. 2008. V. 2. No. 4. P. 343–363.
68. *Chiesa A., Ojha D., and Spooner N.* FRACTAL: Post-quantum and transparent recursive proofs from holography // LNCS. 2020. V. 12105. P. 769–793.
69. *Kattis A., Panarin K., and Vlasov A.* RedShift: Transparent SNARKs from List Polynomial Commitment IOPs. Cryptology ePrint Archive. Paper 2019/1400. 2019. `https://eprint.iacr.org/2019/1400`. 20 p.
70. *Ben-Sasson E., Bentov I., Horesh Y., and Riabzev M.* Fast Reed — Solomon interactive oracle proofs of proximity // 45th Intern. Colloquium ICALP'2018. V. 107. Prague, Czech Republic, 2018. P. 1–17. `https://doi.org/10.4230/LIPIcs.ICALP.2018.14`.
71. *Setty S.* Spartan: Efficient and general-purpose zkSNARKs without trusted setup // LNCS. 2020. V. 12172. P. 704–737.
72. *Bowe S., Grigg J., and Hopwood D.* Recursive Proof Composition without a Trusted Setup. Cryptology ePrint Archive. Paper 2019/1021. 2019. `https://eprint.iacr.org/2019/1021`. 31 p.
73. *Boneh D., Drake J., Fisch B., and Gabizon A.* Halo Infinite: Recursive zk-SNARKs from any Additive Polynomial Commitment Scheme. Cryptology ePrint Archive. Paper 2020/1536. 2020. `https://eprint.iacr.org/2020/1536`. 66 p.

## REFERENCES

1. *Martynenkov I. V.* Kratkie neinteraktivnye argumenty s nulevym razglasheniem na osnove naborov polinomov [Zero-knowledge succinct non-interactive arguments of knowledge based on sets of polynomials]. Prikladnaya Diskretnaya Matematika, 2023, no. 59, pp. 20–57. (in Russian)
2. *Grassi L., Khovratovich D., Rechberger C., et al.* Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. Cryptology ePrint Archive, Paper 2019/458, 2019. `https://eprint.iacr.org/2019/458`.
3. *Baylina J. and Bellés M.* 4-bit Window Pedersen Hash On The Baby Jubjub Elliptic Curve. 2019. `https://docs.iden3.io/publications/pdfs/Pedersen-Hash.pdf`. 8 p.
4. *Regev O.* New lattice based cryptographic constructions. Proc. 35th Ann. ACM Symp. on Theory of Computing, N.Y., ACM, 2003, pp. 407–416.
5. *Regev O.* New lattice-based cryptographic constructions. J. ACM, 2004, vol. 51, iss. 6, pp. 899–942.
6. *Regev O.* On lattices, learning with errors, random linear codes, and cryptography. Proc. 37th Ann. ACM Symp. on Theory of Computing. N.Y., ACM, 2005, pp. 84–93.
7. *Zhang Y., Papamanthou C., and Katz J.* ALITHEIA: Towards practical verifiable graph processing. Proc. CCS'14. N.Y., ACM, 2014, pp. 856–867.
8. *Groth J.* Short pairing-based non-interactive zero-knowledge arguments. LNCS, 2010, vol. 6477, pp. 321–340.
9. *Lipmaa H.* Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. LNCS, 2012, vol. 7194, pp. 169–189.
10. *Pippenger N.* On the evaluation of powers and related problems. 17th Ann. Symp. SFCS'1976, Houston, TX, USA, 1976, pp. 258–263.
11. *Bos J. and Coster M.* Addition chain heuristicse LNCS, 1990, vol. 435, pp. 400–407.
12. *Ben-Sasson E., Chiesa A., Genkin D., et al.* SNARKs for C: Verifying program executions succinctly and in zero knowledge. LNCS, 2013, vol. 8043, pp. 90–108.

13. *Parno B., Howell J., Gentry C., and Raykova M.* Pinocchio: Nearly practical verifiable computation. Proc. 34th IEEE Symp. on Security and Privacy, Berkeley, CA, USA, 2013, pp. 238–252.
14. *Ben-Sasson E., Chiesa A., Tromer E., and Virza M.* Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture, Updated version, 2019. `https://eprint.iacr.org/2013/879.pdf`. 37 p.
15. *Gennaro R., Gentry C., Parno B., and Raykova M.* Quadratic span programs and succinct NIZKs without PCPs. LNCS, 2013, vol. 7881, pp. 626–645.
16. *Costello C.* Pairings for Beginners. `https://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf`, 2012. 146 p.
17. *Groth J.* On the size of pairing-based non-interactive arguments. LNCS, 2016, vol. 9666, pp. 305–326.
18. *Danezis G., Fournet C., Groth J., and Kohlweiss M.* Square span programs with applications to succinct NIZK arguments. LNCS, 2014, vol. 8873, pp. 532–550.
19. *Lipmaa H.* Almost Optimal Short Adaptive Non-Interactive Zero Knowledge. Tech. Rep. 2014/396. International Association for Cryptologic Research, 2014. `http://eprint.iacr.org/2014/396`. 20 p.
20. *Gennaro R., Gentry C., and Parno B.* Non-interactive verifiable computing: Outsourcing computation to untrusted workers. LNCS, 2010, vol. 6223, pp. 465–482.
21. *Lee J.* Dory: Efficient, transparent arguments for generalised inner products and polynomial commitments. LNCS, 2021, vol. 13043, pp. 1–34.
22. *Groth J., Ostrovsky R., and Sahai A.* Perfect non-interactive zero knowledge for NP. LNCS, 2006, vol. 4004, pp. 339–358.
23. *Groth J., Ostrovsky R., and Sahai A.* Non-interactive zaps and new techniques for NIZK. LNCS, 2006, vol. 4117, pp. 97–111.
24. *Abe M. and Fehr S.* Perfect NIZK with adaptive soundness. LNCS, 2007, vol. 4392, pp. 118–136.
25. *Gentry G.* Fully homomorphic encryption using ideal lattices. Proc. 41 Ann. ACM Symp. Theory of Computing, vol. 9, N.Y., ACM, 2009, pp. 169–178.
26. *Groth J.* Linear algebra with sub-linear zero-knowledge arguments. LNCS, 2009, vol. 5677, pp. 192–208.
27. *Groth J.* Short non-interactive zero-knowledge proofs. LNCS, 2010, vol. 6477, pp. 341–358.
28. *Lipmaa H.* Succinct non-interactive zero knowledge arguments from span programs and linear error-correcting codes. LNCS, 2013, vol. 8269, pp. 41–60.
29. *Fauzi P., Lipmaa H., and Zhang B.* Efficient modular NIZK arguments from shift and product. LNCS, 2013, vol. 8257, pp. 92–121.
30. *Kosba A.E., Papadopoulos D., Papamanthou C., et al.* TRUESET: Nearly Practical Verifiable Set Computations. Cryptology ePrint Archive, Report 2014/160, 2014. `http://eprint.iacr.org/2014/160`. 30 p.
31. *Lipmaa H.* Efficient NIZK arguments via parallel verification of benes networks. LNCS, 2014, vol. 8642, pp. 416–434.
32. *Ben-Sasson E., Chiesa A., Tromer E., and Virza M.* Scalable zero knowledge via cycles of elliptic curves. LNCS, 2014, vol. 8617, pp. 276–294.
33. *Costello C., Fournet C., Howell J., et al.* Geppetto: Versatile verifiable computation. Proc. IEEE Symp. SP'15, IEEE Computer Society, USA, 2015, pp. 253–270.
34. *Backes M., Barbosa M., Fiore D., and Reischuk R. M.* ADSNARK: Nearly practical and privacy-preserving proofs on authenticated data. IEEE Symp. on Security and Privacy, San Jose, CA, USA, 2015, pp. 271–286.

35. *Groth J. and Maller M.* Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs. IACR Cryptology ePrint Archive, 2017. 36 p.
36. *Chiesa A., Hu Y., Maller M., et al.* Marlin: Preprocessing zk-SNARKs with universal and updatable SRS. LNCS, 2020, vol. 12105, pp. 738–768.
37. *Applebaum B., Ishai Y., and Kushilevitz E.* From secrecy to soundness: Efficient verification via secure computation. LNCS, 2020, vol. 6198, pp. 152–163.
38. *Reitwiebner C.* zkSNARKs in a Nutshell. 2017. `https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/`. 15 p.
39. *Bitansky N., Canetti R., Chiesa A., and Tromer E.* From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. Proc. ITCS'12, N.Y., ACM, 2012, pp. 326–349.
40. *Goldwasser S., Lin H., and Rubinstein A.* Delegation of Computation without Rejection Problem from Designated Verifier CS-proofs. Cryptology ePrint Archive, Report 2011/456, 2011. 30 p.
41. *Ajtai M.* Generating hard instances of lattice problems (extended abstract). Proc. STOC'96, N.Y., ACM, 1996, pp. 99–108.
42. *Papamanthou C., Shi E., Tamassia R., and Yi K.* Streaming authenticated data structures. LNCS, 2013, vol. 7881, pp. 353–370.
43. *Katz J., Kolesnikov V., and Wang X.* Improved non-interactive zero knowledge with applications to post-quantum signatures. Proc. ACM SIGSAC Conf. CCS'18, N.Y., ACM, 2018, pp. 525–537.
44. *Bünz B., Fisch B., and Szepieniec A.* Transparent SNARKs from DARK Compilers. Cryptology ePrint Archive, Paper 2019/1229, 2019. `https://eprint.iacr.org/2019/1229`. 59 p.
45. *Ames S., Hazay C., Ishai Y., and Venkitasubramaniam M.* Ligero: Lightweight sublinear arguments without a trusted setup. Proc. ACM SIGSAC Conf. CCS'17, N.Y., ACM, 2017, pp. 2087–2104.
46. *Fiat A. and Shamir S.* How to prove yourself: Practical solutions to identification and signature problems. LNCS, 1986, vol. 263, pp. 186–194.
47. *Aho A., Hopcroft J., and Ulman J.* The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974. 470 p.
48. *Scott M.* Implementing cryptographic pairings. Proc. 1st First Intern. Conf. on Pairing-Based Cryptography, Berlin; Heidelberg, Springer Verlag, 2007, pp. 177–196.
49. *Galbraith S. D., Harrison K., and Soldera D.* Implementing the Tate pairing. LNCS, 2002, vol. 2369, pp. 324–337.
50. *Barreto P. S. L. M., Lynn B., and Scott M.* Constructing elliptic curves with prescribed embedding degrees. LNCS, 2003, vol. 2576, pp. 257–267.
51. *Vercauteren F.* Optimal pairings. IEEE Trans. Inform. Theory, 2020, vol. 56, no. 1, pp. 455–461.
52. *Beuchat J. L., González-Díaz J. E., Mitsunari S., et al.* High-speed software implementation of the optimal ate pairing over Barreto — Naehrig curves. LNCS, 2010, vol. 6487, pp. 21–39.
53. *Scott M., Benger N., Charlemagne M., et al.* On the final exponentiation for calculating pairings on ordinary elliptic curves. LNCS, 2009, vol. 5671, pp. 78–88.
54. *Granger R. and Scott M.* Faster squaring in the cyclotomic subgroup of sixth degree extensions. LNCS, 2010, vol. 6056, pp. 209–223.
55. *Fuentes-Castañeda L., Knapp E., and Rodríguez-Henríquez F.* Faster hashing to $\mathbb{G}_2$. LNCS, 2012, vol. 7118, pp. 412–430.

56. *Kim T., Kim S., and Cheon J. H.* On the final exponentiation in Tate pairing computations. IEEE Trans. Inform. Theory, 2013, vol. 59, no. 6, pp. 4033–4041.
57. *Solinas J. A.* ID-based Digital Signature Algorithms. 2003. `http://cacr.uwaterloo.ca/conferences/2003/ecc2003/solinas.pdf`. 32 p.
58. *Scott M.* Computing the Tate pairing LNCS, 2005. vol. 3376, pp. 293–304.
59. *Granger R. and Smart N.* On Computing Products of Pairings. Cryptology ePrint Archive, Report 2006/172, 2006. 11 p.
60. *Arène C, Lange T., Naehrig M., and Ritzenthaler C.* Faster computation of the Tate pairing. J. Number Theory, 2022, vol. 131, no. 5, pp. 842–857.
61. *Frey G. and Rück H.-G.* A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation, 1994, vol. 62, no. 206, pp. 865–874.
62. *Frey G., Muller M., and Rück H.-G.* The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans. Inform. Theory, 2006, vol. 45, no. 5, pp. 1717–1719.
63. *Galbraith S. D., Paterson K. G., and Smart N. P.* Pairings for cryptographers. Discrete Appl. Math., 2008, vol. 156, no. 16, pp. 3113–3121.
64. *Bitansky N., Canetti R., Chiesa A., and Tromer E.* Recursive Composition and Bootstrapping for Snarks and Proof-Carrying Data. IACR Cryptology ePrint Archive, 2012. `http://eprint.iacr.org/2012/095`. 61 p.
65. *Valiant P.* Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. LNCS, 2008, vol. 4948, pp. 1–18.
66. *Crescenzo G. D. and Lipmaa H.* Succinct NP proofs from an extractability assumption. LNCS, 2008, vol. 5028, pp. 175–185.
67. *Mei T.* Polylogarithmic two-round argument systems. J. Math. Cryptol., 2008, vol. 2, no. 4, pp. 343–363.
68. *Chiesa A., Ojha D., and Spooner N.* FRACTAL: Post-quantum and transparent recursive proofs from holography. LNCS, 2020. vol. 12105, pp. 769–793.
69. *Kattis A., Panarin K., and Vlasov A.* RedShift: Transparent SNARKs from List Polynomial Commitment IOPs. Cryptology ePrint Archive, Paper 2019/1400, 2019. `https://eprint.iacr.org/2019/1400`. 20 p.
70. *Ben-Sasson E., Bentov I., Horesh Y., and Riabzev M.* Fast Reed — Solomon interactive oracle proofs of proximity. 45th Intern. Colloquium ICALP'2018, vol. 107, Prague, Czech Republic, 2018, pp. 1–17. `https://doi.org/10.4230/LIPIcs.ICALP.2018.14`.
71. *Setty S.* Spartan: Efficient and general-purpose zkSNARKs without trusted setup. LNCS, 2020, vol. 12172, pp. 704–737.
72. *Bowe S., Grigg J., and Hopwood D.* Recursive Proof Composition without a Trusted Setup. Cryptology ePrint Archive, Paper 2019/1021, 2019. `https://eprint.iacr.org/2019/1021`. 31 p.
73. *Boneh D., Drake J., Fisch B., and Gabizon A.* Halo Infinite: Recursive zk-SNARKs from any Additive Polynomial Commitment Scheme. Cryptology ePrint Archive, Paper 2020/1536, 2020. `https://eprint.iacr.org/2020/1536`. 66 p.

УДК 519.7 DOI 10.17223/20710410/60/5

# ON ADDITIVE DIFFERENTIAL PROBABILITIES OF A COMPOSITION OF BITWISE XORS[1]

I. A. Sutormin*, N. A. Kolomeec**

*Novosibirsk State University, Novosibirsk, Russia
**Sobolev Institute of Mathematics, Novosibirsk, Russia

**E-mail:** ivan.sutormin@gmail.com, kolomeec@math.nsc.ru

We study the additive differential probabilities $\mathrm{adp}_k^{\oplus}$ of compositions of $k-1$ bitwise XORs. For vectors $\alpha^1,\dots,\alpha^{k+1} \in \mathbb{Z}_2^n$, it is defined as the probability of transformation input differences $\alpha^1,\dots,\alpha^k$ to the output difference $\alpha^{k+1}$ by the function $x^1 \oplus \dots \oplus x^k$, where $x^1,\dots,x^k \in \mathbb{Z}_2^n$ and $k \geqslant 2$. It is used for differential cryptanalysis of symmetric-key primitives, such as Addition-Rotation-XOR constructions. Several results which are known for $\mathrm{adp}_2^{\oplus}$ are generalized for $\mathrm{adp}_k^{\oplus}$. Some argument symmetries are proven for $\mathrm{adp}_k^{\oplus}$. Recurrence formulas which allow us to reduce the dimension of the arguments are obtained. All impossible differentials as well as all differentials of $\mathrm{adp}_k^{\oplus}$ with the probability 1 are found. For even $k$, it is proven that $\max\limits_{\alpha^1,\dots,\alpha^k} \mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(0,\dots,0,\alpha^{k+1} \to \alpha^{k+1})$. Matrices that can be used for efficient calculating $\mathrm{adp}_k^{\oplus}$ are constructed. It is also shown that the cases of even and odd $k$ differ significantly.

**Keywords:** *ARX, XOR, additive differential probabilities, differential cryptanalysis.*

# РАЗНОСТНЫЕ ХАРАКТЕРИСТИКИ ПО МОДУЛЮ $2^n$ КОМПОЗИЦИИ НЕСКОЛЬКИХ ПОБИТОВЫХ ИСКЛЮЧАЮЩИХ ИЛИ

И. А. Сутормин*, Н. А. Коломеец**

*Новосибирский государственный университет, г. Новосибирск, Россия
**Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

Исследуются разностные характеристики $\mathrm{adp}_k^{\oplus}$ по модулю $2^n$ композиции $k-1$ побитовых XOR. Для векторов $\alpha^1,\dots,\alpha^{k+1} \in \mathbb{Z}_2^n$ они определяются как вероятность преобразования функцией $x^1 \oplus \dots \oplus x^k$ входных разностей $\alpha^1,\dots,\alpha^k$ в выходную разность $\alpha^{k+1}$, где $x^1,\dots,x^k \in \mathbb{Z}_2^n$ и $k \geqslant 2$. Данные характеристики используются при разностном криптоанализе симметричных алгоритмов, в том числе ARX-конструкций, использующих только три операции: сложение по модулю $2^n$, побитовый XOR и циклический сдвиг битов. Показано, что многие свойства, известные для $\mathrm{adp}_2^{\oplus}$, обобщаются на $\mathrm{adp}_k^{\oplus}$. Доказаны симметрии аргументов $\mathrm{adp}_k^{\oplus}$. Получены рекуррентные формулы, позволяющие уменьшить на 1 размерность аргументов $n$. Найдены все несовместные разности и все разности, при которых $\mathrm{adp}_k^{\oplus}$ равна 1. Для чётного $k$ доказано, что $\max\limits_{\alpha^1,\dots,\alpha^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(0,\dots,0,\alpha^{k+1} \to \alpha^{k+1})$. Построены матрицы, которые можно

[1]The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. FWNF–2022–0018).

использовать для вычисления $\mathrm{adp}_k^{\oplus}$ за линейное по $n$ время. Показано, что случаи чётного и нечётного $k$ существенно различаются.

**Ключевые слова:** *ARX, XOR, разностные характеристики, сложение по модулю, разностный криптоанализ.*

## 1. Introduction

Symmetric cryptography is used in many areas in the modern world: for fast data encryption (block and stream ciphers), for checking data integrity, for creating an electronic signature (cryptographic hash functions), etc. ARX is one of the constructions being used to develop these algorithms. All cryptographic primitives of this architecture use only three operations: addition modulo $2^n$ (Addition, $\boxplus$), circular shift (Rotation, $\lll$) and bitwise addition modulo 2 (XOR, $\oplus$). Examples of ARX-based ciphers include the block ciphers FEAL [1], Threefish [2], one of the eSTREAM winners, the stream cipher Salsa20 [3] and its modification ChaCha20 [4] (it is a part of TLS 1.3), as well as SHA-3 finalists hash functions BLAKE [5] and Skein [2]. One of the well known problems of ARX ciphers is the complexity of their differential cryptanalysis.

Differential cryptanalysis is a statistical method for the analysis of symmetric-key primitives. It was proposed by E. Biham and A. Shamir in [6]. This attack uses pairs of the input differences $\Delta P$ and output differences $\Delta C$ with a high probability of ccurrence. The ordered pair $(\Delta P, \Delta C)$ is called a differential. A common way to find such differential with a high probability is to construct a differential trail, i.e., a sequence $(\Delta P = \Delta X_0, \Delta X_1, \ldots, \Delta X_p, \Delta C = \Delta X_{p+1})$, where $\Delta X_1, \ldots, \Delta X_p$ are some intermediate values that would occur after some operations. A common technique to construct a differential trail is to use a "greedy" strategy to pick the intermediate differences $\Delta X_{i+1}$ which have the highest probability of occurring for fixed $\Delta X_i$. Under some assumptions, we can multiply all the probabilities of a differential trail and obtain an estimation for the probability of the differential $(\Delta P, \Delta C)$.

As for ARX ciphers, the difference $\Delta$ is typically one of their basic operations (addition or XOR). There are also approaches that use other $\Delta$ or even several different $\Delta$, see, for instance, [7–10]. If we express the differences using addition modulo $2^n$, the additive differential probabilities are what we need. For an arbitrary function $f : (\mathbb{Z}_2^n)^k \to \mathbb{Z}_2^n$ the probability $\mathrm{adp}^f(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, is defined as

$$\frac{1}{2^{nk}} \left| \{x^1, \ldots, x^k \in \mathbb{Z}_2^n : f(x^1 \boxplus \alpha^1, \ldots, x^k \boxplus \alpha^k) = f(x^1, \ldots, x^k) \boxplus \alpha^{k+1}\} \right|.$$

However, the probability obtained by "greedy" strategy may be significantly different from the real one. For instance, even simple composition $x \oplus y \oplus z$ can produce a high error. Let us choose the input differences $\alpha$, 0, 0 for the first, second and third arguments respectively. Then the "greedy" strategy gives us

$$\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha, 0 \to \Delta X_1) \cdot \mathrm{adp}^{\oplus}(\Delta X_1, 0 \to \Delta X_2).$$

It is known [11] that $\max\limits_{\gamma} \mathrm{adp}^{\oplus}(\alpha, 0 \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha)$. Thus, we should choose $\Delta X_1 = \alpha$ and then $\Delta X_2 = \alpha$ and obtain the result $P = (\mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha))^2$. At the same time, the function is symmetric, i.e., we can swap the first and the last arguments without changing the value/probabilities:

$$\mathrm{P} = \mathrm{adp}^{\oplus}(0, 0 \to \Delta X_1) \cdot \mathrm{adp}^{\oplus}(\Delta X_1, \alpha \to \Delta X_2).$$

But $\mathrm{adp}^{\oplus}(0,0 \to 0) = 1$ is obviously the maximum value and $\max\limits_{\beta,\gamma} \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma) = \mathrm{adp}^{\oplus}(0, \alpha \to \alpha) = \mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha)$. In this case, the "greedy" strategy gives us a different result: $\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha)$.

Thus, if we apply this for the function $x^1 \oplus x^2 \oplus \ldots \oplus x^k$, we obtain two different results: $\mathrm{P} = (\mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha))^k$ and $\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha)$. We can make the difference between them as big as we want by choosing $\alpha$ and $k$. Similar examples for other compositions can be found in [12].

One of the possible ways to reduce the error is to use the differential probabilities for the whole composition $x^1 \oplus \ldots \oplus x^k$:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \frac{1}{2^{nk}} \left| \{x^1, \ldots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} (\alpha^i \boxplus x^i) = \alpha^{k+1} \boxplus \bigoplus_{i=1}^{k} x^i\} \right|,$$

where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$. Though it is difficult to meet this operation for large $k$ in real ciphers, at least $x^1 \oplus x^2 \oplus x^3$ is used, for instance, in EDON-R [13].

In this paper, we study the properties of $\mathrm{adp}_k^{\oplus}$. As a rule, $n = 32$ is used in ARX constructions that makes an exhaustive search inefficient. We generalize results obtained in [11, 14] for $\mathrm{adp}^{\oplus} = \mathrm{adp}_2^{\oplus}$. Symmetries, impossible differentials, maximums, where one of the arguments is fixed, are considered. All these things are interesting for constructing differential trails. In [14] a way to compute $\mathrm{adp}^{\oplus}$ in linear time multiplying special matrices was proposed. It was also generalized in [15]. We describe special matrices that can be used for calculating $\mathrm{adp}_k^{\oplus}$.

**The outline.** Section 2 gives us necessary definitions. In Section 3, symmetries of $\mathrm{adp}_k^{\oplus}$ are proven (Theorem 1). Section 4 contains recurrence formulas that can be used to reduce the dimension of the arguments (Theorem 2). All impossible differentials (Theorem 3) and all differentials with the probability 1 (Theorem 4) are found in Section 5 (see also Remark 3). Section 6 provides maximums of the $\mathrm{adp}_k^{\oplus}$, where one of its argument is fixed and $k$ is even (Theorem 5). In Section 7, matrices that allow us to calculate $\mathrm{adp}_k^{\oplus}$ are constructed (Theorem 6 and eq. (6)). We note that the cases of even and odd $k$ significantly differ. Some operations are not symmetries for odd $k$. The structure of the matrices is a little bit more complex for odd $k$. The maximums for odd $k$ do not generalize the maximums for $k = 2$.

## 2. Definitions

Let $\mathbb{Z}_2^n$ be a vector space of dimension $n$ over a field consisting of two elements. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be elements of $\mathbb{Z}_2^n$. Then $x1$ and $x0$ are the vectors $(x_1, \ldots, x_n, 1)$ and $(x_1, \ldots, x_n, 0)$ from $\mathbb{Z}_2^{n+1}$ respectively. The bitwise XOR is denoted by $x \oplus y$. Also, $\overline{x} = (x_1 \oplus 1, \ldots, x_n \oplus 1) \in \mathbb{Z}_2^n$. We say that $y \preceq x$ if $y_i \leqslant x_i$ for all $i$, $1 \leqslant i \leqslant n$. We denote *the Hamming weight* of the vector $x$ by $\mathrm{wt}(x)$. We associate the vector $x$ with the integer $x_1 2^{n-1} + x_2 2^{n-2} + \ldots + x_n$. Thus, $x \boxplus y = (x + y) \bmod 2^n$, where $x$ and $y$ are considered as the corresponding integers. Also, $-x$ is the vector from $\mathbb{Z}_2^n$ whose corresponding integer is $-x \bmod 2^n$.

*Additive differential probability of the function* $f(x^1, \ldots, x^k) = x^1 \oplus \ldots \oplus x^k$, $x^1, \ldots, x^k \in \in \mathbb{Z}_2^n$, for *a differential* $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ is defined as

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \frac{1}{2^{nk}} \left| \{x^1, \ldots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} (\alpha^i \boxplus x^i) = \alpha^{k+1} \boxplus \bigoplus_{i=1}^{k} x^i\} \right|. \quad (1)$$

Also, we denote $\mathrm{adp}_2^{\oplus}$ by $\mathrm{adp}^{\oplus}$. Hereinafter we assume that $k \geqslant 2$.

## 3. Argument symmetries of $\mathrm{adp}_k^{\oplus}$

Argument symmetries were proven for $\mathrm{adp}^{\oplus}$ in [11]. In this Section, we generalize that result for $\mathrm{adp}_k^{\oplus}$, $k \geqslant 3$. It is straightforward that we can rearrange $\alpha^1, \ldots, \alpha^k$ calculating $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, see the definition of $\mathrm{adp}_k^{\oplus}$. Let us show that we can rearrange all $\alpha^1, \ldots, \alpha^{k+1}$.

**Proposition 1.** For any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $j \in \{1, \ldots, k\}$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^j, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^{k+1}, \ldots, \alpha^k \to \alpha^j).$$

In other words, $\mathrm{adp}_k^{\oplus}$ is symmetric.

***Proof.*** Since we can rearrange the arguments $\alpha^1, \ldots, \alpha^k$, we can only show that

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^{k+1}, \alpha^2, \ldots, \alpha^k \to \alpha^1).$$

Substituting in (1) $\bigoplus_{i=1}^{k} x^i = y^1$, $x^i = y^i$ for all $i = 2, \ldots, k$, we get that

$$\frac{1}{2^{nk}} \left| \left\{ y^1, \ldots, y^k \in \mathbb{Z}_2^n : \left( \left( \bigoplus_{i=1}^{k} y^i \right) \boxplus \alpha^1 \right) \oplus \bigoplus_{i=2}^{k} (\alpha^i \boxplus y^i) = y^1 \boxplus \alpha^{k+1} \right\} \right|,$$

which is equivalent to

$$\frac{1}{2^{nk}} \left| \left\{ y^1, \ldots, y^k \in \mathbb{Z}_2^n : (y^1 \boxplus \alpha^{k+1}) \oplus \bigoplus_{i=1}^{k} (\alpha^i \boxplus y^i) = \left( \bigoplus_{i=1}^{k} y^i \right) \boxplus \alpha^1 \right\} \right|.$$

We have the definition of $\mathrm{adp}_k^{\oplus}(\alpha^{k+1}, \alpha^2, \ldots, \alpha^k \to \alpha^1)$. ■

**Proposition 2.** For any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 2^{n-1}, \alpha^2 \boxplus 2^{n-1}, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1}).$$

***Proof.*** It is not difficult to see that $a \boxplus 2^{n-1} = a \oplus 2^{n-1}$ since the vector $2^{n-1} \in \mathbb{Z}_2^n$ has 1 only in the most significant position. We can transform the condition from the definition of $\mathrm{adp}_k^{\oplus}$:

$$\begin{aligned}(\alpha^1 \boxplus x^1) \oplus (\alpha^2 \boxplus x^2) &= (\alpha^1 \boxplus x^1) \oplus 2^{n-1} \oplus (\alpha^2 \boxplus x^2) \oplus 2^{n-1} = \\ &= (\alpha^1 \boxplus x^1 \boxplus 2^{n-1}) \oplus (\alpha^2 \boxplus x^2 \boxplus 2^{n-1}) = \\ &= \big((\alpha^1 \boxplus 2^{n-1}) \boxplus x^1\big) \oplus \big((\alpha^2 \boxplus 2^{n-1}) \boxplus x^2\big).\end{aligned}$$

There is no need to change the terms containing $\alpha^3, \ldots, \alpha^{k+1}$. ■

**Proposition 3.** For any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1, \ldots, -\alpha^k \to -\alpha^{k+1}).$$

***Proof.*** By definition,

$$\begin{aligned}\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) &= \frac{1}{2^{nk}} \left| \left\{ x^1, \ldots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} (\alpha^i \boxplus x^i) = \left( \bigoplus_{i=1}^{k} x^i \right) \boxplus \alpha^{k+1} \right\} \right| = \\ &= \frac{1}{2^{nk}} \left| \left\{ x^1, \ldots, x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} x^i = \bigoplus_{i=1}^{k} (\alpha^i \boxplus x^i) \boxplus -\alpha^{k+1} \right\} \right|.\end{aligned}$$

Substituting $y^i = x^i \boxplus \alpha^i$ for all $i = 1, \ldots, k$ and using $x^i = y^i \boxplus -\alpha^i$, we can rewrite the definition:

$$\frac{1}{2^{nk}} \left| \left\{ y^1, \ldots, y^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} (-\alpha^i \boxplus y^i) = \left( \bigoplus_{i=1}^{k} y^i \right) \boxplus -\alpha^{k+1} \right\} \right|.$$

We have got exactly $\mathrm{adp}_k^{\oplus}(-\alpha^1, \ldots, -\alpha^k \to -\alpha^{k+1})$. ■

**Proposition 4.** For any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1, -\alpha^2, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1}).$$

***Proof.*** First of all, we show that $-x = \overline{x} \boxplus 1$ for any $x \in \mathbb{Z}_2^n$:

$$-x = (2^n - 1 - x) \boxplus 1 = \overline{x} \boxplus 1.$$

Therefore, $\overline{x} = -x \boxplus -1$ and for any $y \in \mathbb{Z}_2^n$

$$\overline{x \boxplus y} = -(x \boxplus y) \boxplus -1 = -x \boxplus -1 \boxplus -y = \overline{x} \boxplus -y.$$

It is easy to see that for any bits $x_i, y_i \in \mathbb{Z}_2$ the equality $\overline{x_i} \oplus \overline{y_i} = x_i \oplus y_i$ holds. Therefore, for any $x, y \in \mathbb{Z}_2^n$ it holds that $\overline{x} \oplus \overline{y} = x \oplus y$. Now, we transform the condition from the definition of $\mathrm{adp}_k^{\oplus}$:

$$(\alpha^1 \boxplus x^1) \oplus (\alpha^2 \boxplus x^2) = (\overline{\alpha^1 \boxplus x^1}) \oplus (\overline{\alpha^2 \boxplus x^2}) = (-\alpha^1 \boxplus \overline{x^1}) \oplus (-\alpha^2 \boxplus \overline{x^2}).$$

Using $y^i = \overline{x^i}$ for $i = 1, 2$, we obtain the following:

$$(-\alpha^1 \boxplus y^1) \oplus (-\alpha^2 \boxplus y^2).$$

We have got the condition from the definition of $\mathrm{adp}_k^{\oplus}(-\alpha^1, -\alpha^2, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1})$. ■

Finally, Propositions 1–4 give us the following theorem.

**Theorem 1.** Let $k \geqslant 2$, $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $\beta^1, \ldots, \beta^{k+1} \in \mathbb{Z}_2^n$. Then

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\beta^1, \ldots, \beta^k \to \beta^{k+1})$$

if $\beta^1, \ldots, \beta^{k+1}$ are any of the following:

1) $\beta^i = \alpha^{\pi(i)}$ for all $i$, $1 \leqslant i \leqslant k+1$, where $\pi$ is a permutation on the set $\{1, \ldots, k+1\}$;
2) for arbitrary $S \subseteq \{1, \ldots, k+1\}$, where $|S|$ is even,

$$\beta^i = \alpha^i \boxplus 2^{n-1} \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S;$$

3) for arbitrary $S \subseteq \{1, \ldots, k+1\}$, where $|S|$ is even,

$$\beta^i = -\alpha^i \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S;$$

4) if $k$ is even, for arbitrary $S \subseteq \{1, \ldots, k+1\}$

$$\beta^i = -\alpha^i \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S.$$

***Proof.*** The first point directly follows from Proposition 1. To prove the second point, we just need to apply $|S|/2$ times Proposition 2 together with the first point. The same applies to the third point: it is sufficient to use Proposition 4 instead of Proposition 2. Let us prove the last point. Since $k$ is even, the third point guaranties that

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1, \ldots, -\alpha^k \to \alpha^{k+1}).$$

By Proposition 3,

$$\mathrm{adp}_k^{\oplus}(-\alpha^1, \ldots, -\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to -\alpha^{k+1}),$$

which implies that

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to -\alpha^{k+1}).$$

Applying this equality $|S|$ times together with the first point gives us the last point. ■

## 4. Recurrence formulas for the $\mathrm{adp}_k^{\oplus}$

The recurrence formulas for the $\mathrm{adp}^{\oplus}$ obtained in [11] can be generalized for $\mathrm{adp}_k^{\oplus}$. Note that all our further results will use them.

**Theorem 2.** For all $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, $k \geqslant 2$, and a vector of the least significant bits $A \in \mathbb{Z}_2^{k+1}$ the following holds:

1) if $\mathrm{wt}(A)$ is odd, then

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0; \tag{2}$$

2) if $k$ is odd and $A = (1, \ldots, 1) = 2^{k+1} - 1$, then

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^k} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}); \tag{3}$$

3) otherwise

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ B \preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}). \tag{4}$$

Note that $\alpha^i \boxplus B_i$ is the addition modulo $2^n$, i.e., $\alpha^i$ determines $n$, $1 \leqslant i \leqslant k+1$.

***Proof.***

1) Let us prove that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0$ if $\mathrm{wt}(A)$ is odd. First of all, we define $odd(x) = x_{n+1}$ for $x \in \mathbb{Z}_2^{n+1}$, i.e., $odd(x) = 1$ if and only if $x$ is odd as integer. It is clear that $odd(x \boxplus y) = odd(x \oplus y) = odd(x) \oplus odd(y)$. By definition,

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{(n+1)k}} \left| \left\{ x^1, \ldots, x^k \in \mathbb{Z}_2^{n+1} : \bigoplus_{i=1}^{k} (x^i \boxplus \alpha^i A_i) = \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1} A_{k+1} \right\} \right|.$$

Since $\mathrm{wt}(A)$ is odd,

$$odd(\left(\bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i A_i)\right) \oplus \left(\bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1} A_{k+1}\right)) = \bigoplus_{i=1}^{k} odd(x^i) \oplus \bigoplus_{i=1}^{k} odd(x^i) \oplus \bigoplus_{i=1}^{k+1} A_i = 1.$$

It implies that for any $x^1, \ldots, x^k \in \mathbb{Z}_2^{n+1}$

$$\bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i A_i) \neq \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1} A_{k+1}.$$

In other words, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0$ since the condition from its definition cannot be satisfied.

2) Let us prove the equality (3). We rewrite the definition of $\mathrm{adp}_k^{\oplus}$ as

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^{(n+1)k}} \left| \left\{ x^1, \ldots, x^k \in \mathbb{Z}_2^n,\ a_1, \ldots, a_k \in \mathbb{Z}_2 : \bigoplus_{i=1}^{k}(\alpha^i 1 \boxplus x^i a_i) = \left(\bigoplus_{i=1}^{k} x^i a_i\right) \boxplus \alpha^{k+1} 1 \right\} \right|.$$

We fix a tuple $a_1, \ldots, a_k$. Using Proposition 1, we rearrange the $\mathrm{adp}_k^{\oplus}$ arguments so that $a_1 = a_2 = \ldots = a_j = 0$ and $a_{j+1} = \ldots = a_k = 1$ for some $j \leqslant k$. Then we rewrite the condition from the definition:

$$\bigoplus_{i=1}^{j}(\alpha^i 1 \boxplus x^i 0) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i 1 \boxplus x^i 1) = \left(\bigoplus_{i=1}^{j} x^i 0 \oplus \bigoplus_{i=j+1}^{k} x^i 1\right) \boxplus \alpha^{k+1} 1 =$$
$$= \left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i) 1\right) \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1) 0\right) = \left(\bigoplus_{i=1}^{j} x^i 0 \ \oplus \bigoplus_{i=j+1}^{k} x^i 1\right) \boxplus \alpha^{k+1} 1.$$

In the case of even $j$, we can rewrite the condition from the definition as

$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 0 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\bigoplus_{i=1}^{j} x^i \ \oplus \bigoplus_{i=j+1}^{k} x^i\right) 1 \boxplus \alpha^{k+1} 1,$$
$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 0 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1} \boxplus 1\right) 0.$$

Now look at the corresponding condition from the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^j, \alpha^{j+1} \boxplus 1, \ldots, \alpha^k \boxplus 1 \to \alpha^{k+1} \boxplus 1)$:

$$\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1) = \left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1} \boxplus 1.$$

It is easy to see that if a tuple $x^1, \ldots, x^k$ satisfies one of these conditions, then it must also satisfy the other.

In the case of odd $j$, we can rewrite the condition from the definition as

$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 1 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\bigoplus_{i=1}^{j} x^i \ \oplus \bigoplus_{i=j+1}^{k} x^i\right) 0 \boxplus \alpha^{k+1} 1,$$
$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 1 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1}\right) 1.$$

Now look at the corresponding condition from the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^j, \alpha^{j+1} \boxplus 1, \ldots, \alpha^k \boxplus 1 \to \alpha^{k+1})$:

$$\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1) = \left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1}.$$

It is easy to see that if a tuple $x^1, \ldots, x^k$ satisfies one of these conditions, then it must also satisfy the other.

The total number of tuples satisfying the conditions from the definitions for vectors of dimension $n+1$ is $2^{(n+1)k}\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1}1)$, and for vectors of dimension $n$ it is equal to $2^{nk}\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$. For every fixed tuple $a_1, \ldots, a_k$, there is a unique $\mathrm{adp}_k^{\oplus}$ such that $x^i a_i$ and $x^i$, $1 \leqslant i \leqslant k$, satisfy the corresponding conditions. Choosing all possible combinations of $a_1, \ldots, a_k$, we obtain that

$$\begin{aligned} &2^{(n+1)k}\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = \\ = \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} &2^{nk}\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}). \end{aligned}$$

We recall that after the rearranging $a_1, \ldots, a_k$ we have the following: $B_1, \ldots, B_j$ must be zero, $B_{j+1}, \ldots, B_k$ must be one, and $B_{k+1} = 1$ if and only if $j$ is even. That is why we consider only $B$ of even weight. The equality (3) is proven.

3) Now, we prove the equality (4). Since we exclude the previous cases, $\mathrm{wt}(A)$ is even and there exists $i$, $1 \leqslant i \leqslant k+1$, such that $A_i = 0$. Using Proposition 1, we rearrange the arguments of $\mathrm{adp}_k^{\oplus}$ so that $A_{j+1} = A_{j+2} = \ldots = A_{k+1} = 0$, where $j \leqslant k$, and $A_1 = \ldots = A_j = 1$. We rewrite the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^j 1, \alpha^{j+1}0, \ldots, \alpha^k 0 \to \alpha^{k+1}0)$:

$$\begin{aligned} &\frac{1}{2^{n(k+1)}}\Big|\Big\{x^1, \ldots, x^k \in \mathbb{Z}_2^n,\ a_1, \ldots, a_k \in \mathbb{Z}_2^1 : \\ &\bigoplus_{i=1}^{j}(\alpha^i 1 \boxplus x^i a_i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i 0 \boxplus x^i a_i) = \Big(\bigoplus_{i=1}^{j} x^i a_i \ \oplus \bigoplus_{i=j+1}^{k} x^i a_i\Big) \boxplus \alpha^{k+1}0\Big\}\Big|. \end{aligned}$$

We also fix the first $j$ elements from the tuple $a_1, \ldots, a_k$. Using Proposition 1, we rearrange the arguments of $\mathrm{adp}_k^{\oplus}$ so that $a_1 = \ldots = a_q = 1$ and $a_{q+1} = \ldots = a_j = 0$ for some $q \leqslant j$. Then we can rewrite the condition from the definition as

$$\begin{aligned} &\bigoplus_{i=1}^{q}(\alpha^i 1 \boxplus x^i 1) \oplus \bigoplus_{i=q+1}^{j}(\alpha^i 1 \boxplus x^i 0) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i 0 \boxplus x^i a_i) = \\ &\quad = \left(\bigoplus_{i=1}^{q} x^i 1 \ \oplus \bigoplus_{i=q+1}^{j} x^i 0 \ \oplus \bigoplus_{i=j+1}^{k} x^i a_i\right) \boxplus \alpha^{k+1}0, \\ &\bigoplus_{i=1}^{q}(\alpha^i \boxplus x^i \boxplus 1)0 \oplus \bigoplus_{i=q+1}^{j}(\alpha^i \boxplus x^i)1 \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i)a_i = \\ &= \left(\bigoplus_{i=1}^{q} x^i \ \oplus \bigoplus_{i=q+1}^{j} x^i \ \oplus \bigoplus_{i=j+1}^{k} x^i\right)\left(\bigoplus_{i=1}^{q} 1 \oplus \bigoplus_{i=j+1}^{k} a_i\right) \boxplus \alpha^{k+1}0. \end{aligned}$$

Next, we rewrite it in the following way:

$$\left(\bigoplus_{i=1}^{q}(\alpha^i \boxplus x^i \boxplus 1) \oplus \bigoplus_{i=q+1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i)\right)\left(\bigoplus_{i=q+1}^{j} 1 \oplus \bigoplus_{i=j+1}^{k} a_i\right) =$$
$$= \left(\bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1}\right)\left(\bigoplus_{i=1}^{q} 1 \oplus \bigoplus_{i=j+1}^{k} a_i\right).$$

Let us extract the condition for the least significant bit:

$$\bigoplus_{i=q+1}^{j} 1 \oplus \bigoplus_{i=j+1}^{k} a_i = \bigoplus_{i=1}^{q} 1 \oplus \bigoplus_{i=j+1}^{k} a_i, \text{which is equivalent to } \bigoplus_{i=1}^{j} 1 = 0.$$

It is always satisfied since $j = \mathrm{wt}(A)$ is even. Now we consider the transformed condition without the least significant bit:

$$\bigoplus_{i=1}^{q}(\alpha^i \boxplus x^i \boxplus 1) \oplus \bigoplus_{i=q+1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i) = \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1}.$$

It obviously matches the condition from the definition of

$$\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \ldots, \alpha^q \boxplus 1, \alpha^{q+1}, \ldots, \alpha^k \to \alpha^{k+1}).$$

If the tuple $x^1, \ldots, x^k$ satisfies the condition from the definition, then the tuple consisting of vectors $x^i 1$ for all $i$, $i \leqslant q$, vectors $x^i 0$ for all $i$, $q < i \leqslant j$ and vectors $x^i a_i$ for all $i$, $j < i \leqslant k$, also satisfies the condition from the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to$ $\to \alpha^{k+1} A_{k+1})$ for all $a_i$, $j < i \leqslant k$. There are $2^{k-j}$ such solutions. We can also see that $\alpha_i \boxplus 1$ can occur only when $A_i = 1$. The total number of solutions of the conditions from the definitions for vectors of dimension $n+1$ is $2^{(n+1)k}\,\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1})$, and for vectors of dimension $n$ it is equal to $2^{nk}\,\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$. Choosing all possible combinations of $a_i$, we obtain

$$2^{(n+1)k}\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \sum_{\substack{B \in \mathbb{Z}_2^{k+1},\\ B \preceq A}} 2^{nk} 2^{k-j} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

Since $j = \mathrm{wt}(A)$, the equality (4) is proven. ■

**Remark 1.** We can extend the recurrence formulas for "empty" $\alpha^1, \ldots, \alpha^{k+1}$, i.e., for $\alpha^i A_i \in \mathbb{Z}_2^1$. It is sufficient to assume that $\mathrm{adp}_k^{\oplus}(\varnothing, \ldots, \varnothing \to \varnothing) = 1$. Indeed, we obtain by the recurrence formulas exactly that $\mathrm{adp}_k^{\oplus}(A_1, \ldots, A_k \to A_{k+1}) = 1 \iff \mathrm{wt}(A_1, \ldots, A_{k+1})$ is even and $\mathrm{adp}_k^{\oplus}(A_1, \ldots, A_k \to A_{k+1}) = 0 \iff \mathrm{wt}(A_1, \ldots, A_{k+1})$ is odd.

**Remark 2.** Using symmetries from Section 3 and the equality

$$\alpha \boxplus 1 = (2^n - 1) \boxplus -\overline{\alpha} \boxplus 1 = 2^n \boxplus -\overline{\alpha} \boxplus -1 \boxplus 1 = 2^n \boxplus -\overline{\alpha} = -\overline{\alpha},$$

we can replace $\alpha \boxplus 1$ with $\overline{\alpha}$ for a pair of arguments in the recurrence formulas (and for any argument if $k$ is even). For instance,

$$\mathrm{adp}_3^{\oplus}(\alpha 1, \alpha 1, \alpha 1 \to \alpha 1) =$$
$$= \frac{1}{8}\mathrm{adp}_3^{\oplus}(\alpha, \alpha, \alpha \to \alpha) + \frac{3}{4}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \alpha \to \alpha) + \frac{1}{8}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \overline{\alpha} \to \overline{\alpha}).$$

## 5. Zeros and ones of the $\mathrm{adp}_k^{\oplus}$

For the purposes of cryptanalysis, it is important to distinguish the set of arguments on which $\mathrm{adp}_k^{\oplus}$ is equal to zero.

**Theorem 3.** For any $k \geqslant 2$ and any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, the equality $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 0$ holds if and only if there exists $i$, $1 \leqslant i \leqslant n$, such that $(\alpha_i^1, \ldots, \alpha_i^{k+1}) \neq (0, \ldots, 0)$, $(\alpha_j^1, \ldots, \alpha_j^{k+1}) = (0, \ldots, 0)$ for all $j$, $i < j \leqslant n$, and one of the following conditions is true:

1) the vector $(\alpha_i^1, \ldots, \alpha_i^{k+1})$ has odd weight;
2) $(\alpha_i^1, \ldots, \alpha_i^{k+1}) = (1, \ldots, 1)$, $k$ is odd, $i > 1$, and $(\alpha_{i-1}^1, \ldots, \alpha_{i-1}^{k+1})$ is of odd weight.

***Proof.*** Let us use induction by $n$. For $n = 1$, $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2$, is equal to 0 if and only if $(\alpha^1, \ldots, \alpha^{k+1})$ is of odd weight. It is the base of the induction. Suppose that the statement holds for $n$. Let us prove that it is true for $n+1$. We represent elements from $\mathbb{Z}_2^{n+1}$ as $\alpha^1 A_1, \ldots, \alpha^{k+1} A_{k+1}$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $A = (A_1, \ldots, A_{k+1}) \in \mathbb{Z}_2^{k+1}$. First of all, we can assume that $A \neq (0, \ldots, 0)$. Indeed, $\mathrm{adp}_k^{\oplus}(\alpha^1 0, \ldots, \alpha^k 0 \to \alpha^{k+1} 0) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ by Theorem 2. Moreover, the statement of the theorem takes it into account. Next, we need to consider three cases.

1) $\mathrm{wt}(A)$ is odd. According to Theorem 2, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0$. It proves that the first condition is sufficient.

2) $A = (1, \ldots, 1)$ and $k$ is odd. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^k} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

The least significant bits of $\alpha^1 \boxplus B_1, \ldots, \alpha^{k+1} \boxplus B_{k+1}$ are $\alpha_n^1 \oplus B_1, \ldots, \alpha_n^{k+1} \oplus B_{k+1}$. Moreover, $\mathrm{wt}(B)$ is even. Thus, if $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ is odd, then $\mathrm{wt}(\alpha_n^1 \oplus B_1, \ldots, \alpha_n^{k+1} \oplus B_{k+1})$ is odd as well. It means that any of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1})$ is equal to zero by induction.

Let $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ be even. Choosing $(0, \ldots, 0)$ or $(1, 1, 0, \ldots, 0)$ as $B$ and taking into account that $k \geqslant 2$, we obtain that at least one of $(\alpha_n^1, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ does not belong to $\{(0, \ldots, 0), (1, \ldots, 1)\}$. Moreover, both of them are of even weight. It means that at least one of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \alpha^2 \boxplus 1, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1})$ is not zero by induction. Therefore, $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1)$ is not zero as well.

Thus, in this case $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1)$ is zero if and only if $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ is odd. It proves the correctness of the second condition.

3) $\mathrm{wt}(A)$ is even and $A \notin \{(0, \ldots, 0), (1, \ldots, 1)\}$. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ B \preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

Without loss of generality we assume that $A_1 = A_2 = 1$, otherwise we can rearrange arguments by Theorem 1. Similarly to the previous point, at least one of $(\alpha_n^1, \alpha_n^2, \alpha_n^3, \ldots, \alpha_n^{k+1})$, $(\alpha_n^1 \oplus 1, \alpha_n^2, \alpha_n^3, \ldots, \alpha_n^{k+1})$, $(\alpha_n^1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ is of even weight and does not belong to $\{(0, \ldots, 0), (1, \ldots, 1)\}$. Thus, the corresponding

$\mathrm{adp}_k^{\oplus}$ is not zero by induction. Therefore, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \dots, \alpha^k A_k \to \alpha^{k+1} A_{k+1})$ is not zero as well.

It proves that the first condition is necessary, except for the cases $A = (0, \dots, 0)$ and $A = (1, \dots, 1)$ for odd $k$. ■

Note that the zeros of the function in the case of even $k$ look similar to the zeros for $\mathrm{adp}^{\oplus}$. The second point appears only for odd $k$ and generates an additional set of zeros.

The arguments on which $\mathrm{adp}_k^{\oplus}$ is equal to 1 are also interesting.

**Theorem 4.** For any $k \geqslant 2$ and any $\alpha^1, \dots, \alpha^{k+1} \in \mathbb{Z}_2^n$, the equality $\mathrm{adp}_k^{\oplus}(\alpha^1, \dots, \alpha^k \to \alpha^{k+1}) = 1$ holds if and only if the vector $(\alpha_1^1, \dots, \alpha_1^{k+1})$ has even weight, and one of the following conditions is true:

1) $(\alpha_i^1, \dots, \alpha_i^{k+1}) = (0, \dots 0)$ for all $i$, $2 \leqslant i \leqslant n$;
2) $(\alpha_2^1, \dots, \alpha_2^{k+1}) = (1, \dots, 1)$, $k$ is odd, $n \geqslant 2$, and $(\alpha_i^1, \dots, \alpha_i^{k+1}) = (0, \dots 0)$ for all $i$, $3 \leqslant i \leqslant n$.

***Proof.*** Let us use induction by $n$. For $n = 1$, $\mathrm{adp}_k^{\oplus}(\alpha^1, \dots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \dots, \alpha^{k+1} \in \mathbb{Z}_2$, is equal to 1 if and only if $(\alpha^1, \dots, \alpha^{k+1})$ is of even weight. It is the base of the induction. Suppose that the statement holds for $n$. Let us prove that it is true for $n+1$. We represent elements from $\mathbb{Z}_2^{n+1}$ as $\alpha^1 A_1, \dots, \alpha^{k+1} A_{k+1}$, where $\alpha^1, \dots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $A = (A_1, \dots, A_{k+1}) \in \mathbb{Z}_2^{k+1}$. Similarly to the proof of Theorem 3, we assume that $A \neq (0, \dots, 0)$ (otherwise the statement is true by induction) and consider three cases.

1) $\mathrm{wt}(A)$ is odd, which means that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \dots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0 \neq 1$.

2) $A = (1, \dots, 1)$ and $k$ is odd. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \dots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^k} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \dots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}),$$

which implies that $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \dots, \alpha^k 1 \to \alpha^{k+1} 1) = 1$ if and only if $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \dots, \alpha^k \boxplus \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = 1$ for all $B \in \mathbb{Z}_2^{k+1}$ of even weight.

The least significant bits of $\alpha^1 \boxplus B_1, \dots, \alpha^{k+1} \boxplus B_{k+1}$ are $\alpha_n^1 \oplus B_1, \dots, \alpha_n^{k+1} \oplus B_{k+1}$. Choosing $(0, \dots, 0)$ or $(1, 1, 0, \dots, 0)$ as $B$ and taking into account that $k \geqslant 2$, we obtain that at least one of $(\alpha_n^1, \dots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \dots, \alpha_n^{k+1})$ does not belong to $\{(0, \dots, 0), (1, \dots, 1)\}$. In other words, at least one of $\mathrm{adp}_k^{\oplus}(\alpha^1, \dots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \alpha^2 \boxplus 1, \alpha^3, \dots, \alpha^k \to \alpha^{k+1})$ is not equal to 1 if $n > 1$ by induction. If $n = 1$, then all $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \dots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha_1^1 \oplus B_1, \dots, \alpha_1^k \oplus B_k \to$ $\to \alpha_1^{k+1} \oplus B_{k+1}) = 1$ if and only if $\mathrm{wt}(\alpha_1^1, \dots, \alpha_1^{k+1})$ is even.

Thus, in this case $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \dots, \alpha^k 1 \to \alpha^{k+1} 1) = 1$ if and only if $n = 1$ and $\mathrm{wt}(\alpha_1^1, \dots, \alpha_1^{k+1})$ is even. It proves the correctness of the second condition.

3) $\mathrm{wt}(A)$ is even and $A \notin \{(0, \dots, 0), (1, \dots, 1)\}$. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \dots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ B \preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \dots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

This means that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \dots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 1$ if and only if $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus \boxplus B_1, \dots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = 1$ for all $B \in \mathbb{Z}_2^{k+1}$ such that $B \preceq A$.

Without loss of generality we assume that $A_1 = 1$, otherwise we can rearrange arguments by Theorem 1. Next, one of $(\alpha_n^1, \alpha_n^2, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2, \ldots, \alpha_n^{k+1})$ is of odd weight. Thus, one of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \alpha^2, \ldots, \alpha^k \to \alpha^{k+1})$ is zero by Theorem 2 and $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) \neq 1$.

Together with the first point, it proves the correctness of the first condition. ■

**Remark 3.** The conditions from Theorems 3 and 4 for $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ can be simplified. Let us define the following pattern symbols for elements of $\mathbb{Z}_2^{k+1}$:

— $*$ means any $x \in \mathbb{Z}_2^{k+1}$,
— $\mathtt{e}$ and $\mathtt{d}$ mean any $x \in \mathbb{Z}_2^{k+1}$ of even and odd weight respectively,
— $\mathbf{0}$ and $\mathbf{1}$ mean $(0, \ldots, 0)$ and $(1, \ldots, 1)$ from $\mathbb{Z}_2^{k+1}$ respectively.

Then $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 0$ if and only if the vector

$$\big((\alpha_1^1, \ldots, \alpha_1^{k+1}), \ldots, (\alpha_n^1, \ldots, \alpha_n^{k+1})\big) \tag{5}$$

matches

$$(*, \ldots, *, \mathtt{d}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for any } k \text{ or}$$
$$(*, \ldots, *, \mathtt{d}, \mathbf{1}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for odd } k.$$

Similarly, $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 1$ if and only if the vector (5) matches

$$(\mathtt{e}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for any } k \text{ or}$$
$$(\mathtt{e}, \mathbf{1}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for odd } k.$$

## 6. Maximums of the $\mathrm{adp}_k^{\oplus}$

Also, for the purposes of cryptanalysis, the maximum values of $\mathrm{adp}_k^{\oplus}$ are of interest, where some argument (or arguments) is fixed. In the case of even $k$, it is not difficult to show that the maximum of the characteristic, where one its argument is fixed, is similar to the maximum for $k = 2$.

**Theorem 5.** Let $k \geqslant 2$ be even and $\gamma \in \mathbb{Z}_2^n$. Then

$$\max_{x^1, \ldots, x^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(x^1, \ldots, x^k \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

***Proof.*** Let us use induction by $n$. If $n = 1$, $\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) = 1$ for any $\gamma \in \mathbb{Z}_2$, see Theorem 4. It is the base of the induction.

Next, we assume that $\mathrm{adp}_k^{\oplus}(\beta^1, \ldots, \beta^k \to \gamma) \leqslant \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma)$ for any $\beta^1, \ldots, \beta^k, \gamma \in \mathbb{Z}_2^n$. Let $\alpha^1, \ldots, \alpha^k, \gamma \in \mathbb{Z}_2^n$, $A \in \mathbb{Z}_2^{k+1}$. We need to prove that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) \leqslant \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1})$. We divide the proof into the following cases.

C a s e 1 . $A = (0, \ldots, 0)$. According to Theorem 2, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \gamma)$ and $\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1}) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma)$. Thus, the induction hypothesis provides that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) \leqslant \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1})$.

C a s e 2 . $\mathrm{wt}(A)$ is odd. According to Theorem 2, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) = 0$. It proves the induction step.

C a s e 3 . $\mathrm{wt}(A)$ is even and $A_{k+1} = 0$. Without loss of generality, we can assume that $A_1 = \ldots = A_w = 1$ and $A_{w+1} = \ldots = A_k = 0$, where $w = \mathrm{wt}(A)$. Indeed,

Proposition 1 allows us to rearrange the arguments of $\mathrm{adp}_k^{\oplus}$. Then, Theorem 2 and the induction hypothesis give us that

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma 0) = 2^{-w} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) \leqslant$$
$$\leqslant 2^{-w} \cdot 2^w \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 0 \to \gamma 0).$$

C a s e 4 . $\mathrm{wt}(A)$ is even and $A_{k+1} = 1$. Similarly to the previous case, we assume without loss of generality that $A_1 = \ldots = A_w = 1$ and $A_{w+1} = \ldots = A_k = 0$, where $w = \mathrm{wt}(A) - 1$. According to Theorem 2,

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) =$$
$$= 2^{-w-1} \sum_{c \in \mathbb{Z}_2} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus c) =$$
$$= 2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) +$$
$$+ 2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1).$$

Also, if the vector of the least significant coordinates has odd weight, i.e., $\mathrm{wt}(B) + c + \mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^k, \gamma_n)$ is odd, then $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus c) = 0$. It means that at least half of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma)$ are zero and at least half of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1)$ are zero. At the same time,

$$\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 1 \to \gamma 1) = \frac{1}{4} \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) + \frac{1}{4} \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1),$$

since $\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma \boxplus 1) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma) = 0$. Finally, by the induction hypothesis and due to the least significant vectors of odd weight, we obtain that

$$2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) \leqslant$$
$$\leqslant 2^{-w-1} \cdot 2^{w-1} \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) = \frac{1}{4} \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

Similarly,

$$2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1) \leqslant$$
$$\leqslant 2^{-w-1} \cdot 2^{w-1} \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1) = \frac{1}{4} \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1).$$

Thus, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma 1) \leqslant \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 1 \to \gamma 1)$. ■

For odd $k$ the maximum looks different.

**Corollary 1.** For any odd $k \geqslant 3$ and $\gamma = 2^{n-1} + 2^{n-2} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\gamma, \gamma, 0, \ldots, 0 \to 0) < 1 = \mathrm{adp}_k^{\oplus}(\gamma, \ldots, \gamma \to \gamma).$$

It directly follows from Theorem 4. However, for some cases we can generalize results of Theorem 5.

**Corollary 2.** Let $k \geqslant 3$ be odd. Then for any $\gamma \in \mathbb{Z}_2^n$ the following holds:

$$\max_{x^1,\ldots,x^{k-1} \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(0, x^1, \ldots, x^{k-1} \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

Indeed, the proof of Theorem 5 is correct for this case since the first argument is zero. Thus, we will never use the case $(1, \ldots, 1)$ in the recurrence formulas which is the only difference between even and odd $k$. At the same time, we believe that for an arbitrary odd $k$ the following holds.

**Hypothesis 1.** Let $k \geqslant 3$ be odd and $\gamma \in \mathbb{Z}_2^n$. Then

$$\max_{x^1,\ldots,x^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(x^1, \ldots, x^k \to \gamma) = \mathrm{adp}_k^{\oplus}(\gamma, \ldots, \gamma \to \gamma).$$

Note that a problem connected with the values $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ can be found in [16]. NSUCRYPTO-2014 [17] also included a problem related to ARX constructions.

## 7. A matrix approach for calculating $\mathrm{adp}_k^{\oplus}$

The section is devoted to a generalization of the approach proposed in [14] for calculating $\mathrm{adp}^{\oplus}$, i.e., $\mathrm{adp}_2^{\oplus}$. There is also the S-function technique [15], which provides a matrix calculation algorithm that help to compute values of any S-function (including $\mathrm{adp}_k^{\oplus}$). However, it does not allow us to obtain analytic expressions for the matrix elements, as well as relationship between matrices.

In this section, we will consider a vector space $\widehat{\mathbb{Q}}^{2^{k+1}}$ over rationals. We assume that the coordinates of the vectors from $\widehat{\mathbb{Q}}^{2^{k+1}}$ start with zero and for coordinate $x_1 2^k + x_2 2^{k-1} + \ldots + x_{k+1}$ we use both integer and binary vectors $(x_1, \ldots, x_{k+1})$ representations, $x \in \mathbb{Z}_2^{k+1}$. Let $A \in \mathbb{Z}_2^{k+1}$ and $k \geqslant 2$. We define matrices $M_A^k$ of size $2^{k+1} \times 2^{k+1}$ in the following way:

$$(M_A^k)_{y,x} = \begin{cases} 2^{-k}, & \text{if } x = \overline{A}, k \text{ is odd and } \mathrm{wt}(y) \text{ is even,} \\ 2^{-\mathrm{wt}(x \oplus A)}, & \text{if } \mathrm{wt}(x \oplus A) \text{ is even and } y \oplus A \preceq x \oplus A, \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$

where $x, y \in \mathbb{Z}_2^{k+1}$. Similarly to the elements of $\widehat{\mathbb{Q}}^{2^{k+1}}$, we use both integer (starting with 0) and binary vector notations for the matrix indexes.

The next theorem follows from the Theorem 2 and gives us a way to calculate $\mathrm{adp}_k^{\oplus}$.

**Theorem 6.** Let $k \geqslant 2$ and $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$. Then

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = (1, \ldots, 1) M^k_{(\alpha_1^1, \ldots, \alpha_1^{k+1})} \cdot \ldots \cdot M^k_{(\alpha_n^1, \ldots, \alpha_n^{k+1})} (1, 0, \ldots, 0)^{\mathrm{T}}.$$

***Proof.*** We use the recurrence formulas obtained in Theorem 2. First of all, we define $[\beta]_m = (\beta_1, \ldots, \beta_m)$ for any $\beta \in \mathbb{Z}_2^n$ and $1 \leqslant m \leqslant n$. Also, $[\beta]_m \boxplus a$ means $[\beta]_m + a \bmod 2^m$, where $a \in \mathbb{Z}_2$. Let $x \in \mathbb{Z}_2^{k+1}$. We apply Theorem 2 to $\mathrm{adp}_k^{\oplus}([\alpha^1]_{m+1} \boxplus x_1, \ldots, [\alpha^k]_{m+1} \boxplus x_k \to \to [\alpha^{k+1}]_{m+1} \boxplus x_{k+1})$. Let $A = (\alpha^1_{m+1}, \ldots, \alpha^{k+1}_{m+1})$. Then the vector of the least significant bits of the arguments is $x \oplus A$. After applying the recurrence formulas, we obtain a sum of

$$\mathrm{adp}_k^{\oplus}([[\alpha^1]_{m+1} \boxplus x_1]_m \boxplus y_1, \ldots, [[\alpha^k]_{m+1} \boxplus x_k]_m \boxplus y_k \to [[\alpha^{k+1}]_{m+1} \boxplus x_{k+1}]_m \boxplus y_{k+1})$$

for some $y \in \mathbb{Z}_2^{k+1}$, $y \preceq x \oplus A$. Let us show that

$$[[\alpha^i]_{m+1} \boxplus x_i]_m \boxplus y_i = [\alpha^i]_m \boxplus (y_i \oplus x_i \cdot A_i), \tag{7}$$

where $i = 1, \dots, k+1$ and $y \preceq x \oplus A$. Indeed, if $(A_i, x_i) = (\alpha^i_{m+1}, x_i) \neq (1,1)$, i.e., $x_i \cdot A_i = 0$, then the addition of $x_i$ to $[\alpha^i]_{m+1}$ may change only its least significant bit. Thus, $[[\alpha^i]_{m+1} \boxplus x_i]_m = [\alpha^i]_m$. If $(A_i, x_i) = (1,1)$, then $y_i = 0$ since $x_i \oplus A_i = 0$ and $y \preceq x \oplus A$. Thus, $[[\alpha^i]_{m+1} \boxplus x_i]_m \boxplus y_i = [[\alpha^i]_{m+1} \boxplus 1]_m = [\alpha^i]_m \boxplus 1 = [\alpha^i]_m \boxplus (y_i \oplus x_i \cdot A_i)$.

Next, we denote by $x \cdot A$ the vector $(x_1 \cdot A_1, \dots, x_{k+1} \cdot A_{k+1})$. Let us show that

$$\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1} \text{ and } y \preceq x \oplus A\} = \{z \in \mathbb{Z}_2^{k+1} : z \oplus A \preceq x \oplus A\}. \tag{8}$$

Indeed, $\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1} \text{ and } y \preceq x \oplus A\} = \{z \in \mathbb{Z}_2^{k+1} : z \oplus (x \cdot A) \preceq x \oplus A\}$. At the same time, $z \oplus (x \cdot A) \preceq x \oplus A \iff z \oplus A \preceq x \oplus A$ since for any $i = 1, \dots, k+1$ we have the following: $x_i \neq A_i$ (i.e., $x_i \oplus A_i = 1$) implies that both $z_i \oplus (x_i \cdot A_i) \leqslant 1$ and $z_i \oplus A_i \leqslant 1$ always hold for any $z_i \in \mathbb{Z}_2$; also, $x_i = A_i$ implies that $z_i \oplus (x_i \cdot A_i) = z_i \oplus A_i$.

Moreover, the following holds for $x = \overline{A}$:

$$\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1},\ \mathrm{wt}(y) \text{ is even}\} = \{z \in \mathbb{Z}_2^{k+1} : \mathrm{wt}(z) \text{ is even}\}. \tag{9}$$

It is straightforward since in this case $x \oplus A = (1, \dots, 1)$ and $x \cdot A = (0, \dots, 0)$.

Theorem 2 allows us to express $r = \mathrm{adp}^{\oplus}_k([\alpha^1]_{m+1} \boxplus x_1, \dots, [\alpha^k]_{m+1} \boxplus x_k \to [\alpha^{k+1}]_{m+1} \boxplus \boxplus x_{k+1})$ in the following way:

1) If $\mathrm{wt}(x \oplus A)$ is odd, then $r = 0$.
2) If $x \oplus A = (1, \dots, 1)$ and $k$ is odd, then according to (7) and (9) the following holds:

$$r = 2^{-k} \sum_{z:\, \mathrm{wt}(z) \text{ is even}} \mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus z_1, \dots, [\alpha^k]_m \boxplus z_k \to [\alpha^{k+1}]_m \boxplus z_{k+1}).$$

3) Otherwise, due to (7) and (8) we have that

$$r = 2^{-\mathrm{wt}(x \oplus A)} \sum_{z:\, z \oplus A \preceq x \oplus A} \mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus z_1, \dots, [\alpha^k]_m \boxplus z_k \to [\alpha^{k+1}]_m \boxplus z_{k+1}).$$

At the same time, we know how the matrix $M^k_A$ transforms the standard basis $\widehat{e}^{\,\mathrm{T}}_x$ (it has 1 in the coordinate $x$ and 0 in all other coordinates) for all $x \in \mathbb{Z}_2^{k+1}$: $(M^k_A)_{y,x}$ is the $y$-th coordinate of $M^k_A \widehat{e}^{\,\mathrm{T}}_x$, where $y \in \mathbb{Z}_2^{k+1}$, which is equal to

$$\begin{cases} 2^{-k}, & \text{if } x = \overline{A},\ k \text{ is odd and } \mathrm{wt}(y) \text{ is even,} \\ 2^{-\mathrm{wt}(x \oplus A)}, & \text{if } \mathrm{wt}(x \oplus A) \text{ is even and } y \oplus A \preceq x \oplus A, \\ 0 & \text{otherwise.} \end{cases}$$

It is not difficult to see that the mapping $M^k_A$ completely corresponds to the points 1, 2, and 3. It other words, we can consider it as a "state" transformation: it maps all multipliers of $\mathrm{adp}^{\oplus}_k([\alpha^1]_{m+1} \boxplus x_1, \dots, [\alpha^k]_{m+1} \boxplus x_k \to [\alpha^{k+1}]_{m+1} \boxplus x_{k+1})$ (for all $x \in \mathbb{Z}_2^{k+1}$) to all multipliers of $\mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus y_1, \dots, [\alpha^k]_m \boxplus y_k \to [\alpha^{k+1}]_m \boxplus y_{k+1})$ (for all $y \in \mathbb{Z}_2^{k+1}$). Since we start with $\mathrm{adp}^{\oplus}_k(\alpha^1, \dots, \alpha^k \to \alpha^{k+1})$, it corresponds to the "state" $\widehat{e}^{\,\mathrm{T}}_0$. Thus, the final multipliers are

$$s = M^k_{(\alpha^1_1, \dots, \alpha^{k+1}_1)} \dots M^k_{(\alpha^1_n, \dots, \alpha^{k+1}_n)} \widehat{e}^{\,\mathrm{T}}_0,$$

see Remark 1 for the case $n = 1$. Finally, $\mathrm{adp}^{\oplus}_k(\alpha^1, \dots, \alpha^k \to \alpha^{k+1}) = (1, \dots, 1) \cdot s$. ■

**Corollary 3.** If $k$ is even, then $(M^k_A)_{y,x} = (M^k_0)_{y \oplus A, x \oplus A}$, $A, x, y \in \mathbb{Z}_2^{k+1}$. It means that all $M^k_A$ can be obtained from each other using some permutations of rows and columns.

This does not hold for odd $k$. However, almost the same thing is true: we swap $x$ and $x \oplus A$ columns, after that we swap $y$ and $y \oplus A$ rows of $M^k_0$ except for the rows $\overline{A}$ and $(1, \dots, 1)$.

The proof follows directly from the definition of $M_A^k$. Thus, the difference in recurrence formulas gives us some difference in the calculation of the $\mathrm{adp}_k^{\oplus}$ for odd and even $k$.

Some matrices for $k = 3$ are presented bellow:

$$8 \cdot M^3_{(0,0,0,0)} = \begin{pmatrix}
8&0&0&2&0&2&2&0&0&2&2&0&2&0&0&1\\
0&0&0&2&0&2&0&0&0&2&0&0&0&0&0&0\\
0&0&0&2&0&0&2&0&0&0&2&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&2&2&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&2&2&0&2&0&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix},$$

$$8 \cdot M^3_{(0,0,0,1)} = \begin{pmatrix}
0&0&2&0&2&0&0&0&2&0&0&0&0&0&1&0\\
0&8&2&0&2&0&0&2&2&0&0&2&0&2&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&2&0&0&0&0&2&0&0&0&2&0&0&1&0\\
0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&2&0&0&2&0&0&0&0&0&2&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&2&0&0&2&0&2&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0
\end{pmatrix},$$

$$8 \cdot M^3_{(1,1,1,1)} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0\\
0&0&0&2&0&2&2&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&2&2&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&2&0&0&0&2&0&0&2&0&0&0\\
0&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0\\
1&0&0&2&0&2&2&0&0&2&2&0&2&0&0&8
\end{pmatrix}.$$

For instance, if $\alpha^1 = (0, 0, 1)$, $\alpha^2 = (0, 0, 1)$, $\alpha^3 = (0, 0, 1)$, and $\alpha^4 = (0, 1, 1)$, we obtain that

$$\mathrm{adp}_3^{\oplus}(\alpha^1, \alpha^2, \alpha^3 \to \alpha^4) = (\underbrace{1, \ldots, 1}_{16}) M^3_{(0,0,0,0)} M^3_{(0,0,0,1)} M^3_{(1,1,1,1)} (\underbrace{1, 0, \ldots, 0}_{16})^{\mathrm{T}}.$$

## 8. Conclusion

We have generalized some properties of $\mathrm{adp}^{\oplus}$ to $\mathrm{adp}_k^{\oplus}$. The results obtained show us that there is the difference between odd and even $k$, it looks like the case of odd $k$ is more complicated. A generalization of other properties such as maximum for odd $k$ is a topic for future research.

The authors would like to thank Nicky Mouha for interesting discussions and valuable advice.

REFERENCES

1. *Shimizu A. and Miyaguchi S.* Fast Data Encipherment Algorithm (FEAL). LNCS, 1988, vol. 304, pp. 267–278.
2. *Ferguson N., Lucks S., Schneier B., et al.* `http://www.skein-hash.info` — The Skein Hash Function Family, 2009.
3. *Bernstein D. J.* `https://cr.yp.to/snuffle/spec.pdf` — Salsa20 specification, 2005.
4. *Bernstein D. J.* `https://cr.yp.to/chacha/chacha-20080128.pdf` — ChaCha, a variant of Salsa20, 2008.
5. *Aumasson J.-P., Meier W., Phan R. C.-W., and Henzen L.* The Hash Function BLAKE. Berlin; Heidelberg, Springer, 2014.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. J. Cryptology, 1991, vol. 4, no. 1, pp. 3–72.
7. *Malyshev F. M.* Veroyatnostnye kharakteristiki raznostnykh sootnosheniy dlya neodnorodnoy lineynoy sredy [Probabilistic characteristics of differential and linear relations for nonhomogeneous linear medium]. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, no.1, pp. 41–72. (in Russian)
8. *Malyshev F. M.* Raznostnye kharakteristiki osnovnykh operatsiy ARX-shifrov [Differential characteristics of base operations in ARX-ciphers]. Matematicheskie Voprosy Kriptografii, 2020, vol. 11, no.4, pp. 97–105. (in Russian)
9. *Leurent G.* Analysis of differential attacks in ARX constructions. LNCS, 2012, vol. 7658, pp. 226–243.

10. *Leurent G.* Construction of differential characteristics in ARX designs application to Skein. LNCS, 2013, vol. 8042, pp. 241–258.
11. *Mouha N., Kolomeec N., Tokareva N., et al.* Maximums of the additive differential probability of exclusive-or with one fixed argument. IACR Trans. Symmetric Cryptology, 2021, vol. 2021, no. 2, pp. 292–313.
12. *Velichkov V., Mouha N., De Canniére C., and Preneel B.* The additive differential probability of ARX. LNCS, 2011, vol. 6733, pp. 342–358.
13. *Gligoroski D., Ødegård R. S., Mihova M., et al.* Cryptographic hash function Edon-R'. Proc. 1st Intern. Workshop on Security and Communication Networks, Trondheim, Norway, 2009, pp. 1–9.
14. *Lipmaa H., Wallén J., and Dumas P.* On the additive differential probability of Exclusive-Or. LNCS, 2004, vol. 3017, pp. 317–331.
15. *Mouha N., Velichkov V., De Canniére C., and Preneel B.* The differential analysis of S-functions. LNCS, 2011, vol. 6544, pp. 36–56.
16. *Gorodilova A., Tokareva N., Agievich S., et al.* An overview of the eight international olympiad in cryptography "Non-Stop University Crypto". Siberian Electronic Math. Reports, 2022, vol. 19, no. 1, pp. A9–A37.
17. *Agievich S. V., Gorodilova A. A., Tokareva N. N., et al.* Problems, solutions and experience of the first international student's Olympiad in cryptography. Prikladnaya Diskretnaya Matematika, 2015, no. 3, pp. 41–62.

# ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.1, 519.8 DOI 10.17223/20710410/60/6

## О СЛОЖНОСТИ КЛАСТЕРИЗАЦИИ ГРАФА В ЗАДАЧЕ С ОГРАНИЧЕНИЯМИ НА РАЗМЕРЫ КЛАСТЕРОВ[1]

Р. В. Балджанова*, А. В. Ильев**, В. П. Ильев*,**

*Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия,
**Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

**E-mail:** baldzhanova@mail.ru, artyom_iljev@mail.ru, iljev@mail.ru

В задачах кластеризации на графах для данного графа $G$ требуется найти ближайший к нему кластерный граф на том же множестве вершин. Граф называется кластерным, если каждая его компонента связности является полным графом. Расстояние между двумя графами понимается как число несовпадающих рёбер. Рассматривается задача кластеризации на графах, в которой размеры кластеров ограничены сверху числом $s$. Доказана верхняя оценка сложности кластеризации произвольного графа для случая $s = 2$. Предложен приближённый полиномиальный алгоритм решения задачи кластеризации на графах для случая $s = 3$ и доказана верхняя оценка сложности кластеризации произвольного графа для этого случая.

**Ключевые слова:** *граф, кластеризация, сложность кластеризации.*

## ON THE COMPLEXITY OF GRAPH CLUSTERING IN THE PROBLEM WITH BOUNDED CLUSTER SIZES

R. V. Baldzhanova*, A. V. Ilev**, V. P. Il'ev*,**

*Dostoevsky Omsk State University, Omsk, Russia
**Institute of Mathematics SB RAS, Omsk, Russia

In the graph clustering problems, for a given graph $G$, one has to find a nearest cluster graph on the same vertex set. A graph is called cluster graph if all its connected components are complete graphs. The distance between two graphs is equal to the number of non-coincide edges. In the paper, we consider the graph clustering problem with bounded size $s$ of clusters. The clustering complexity of a graph $G$ is the distance from $G$ to a nearest cluster graph. In the case of $s = 2$, we prove that the clustering complexity of an arbitrary $n$-vertex graph doesn't exceed $\lfloor (n-1)^2/2 \rfloor$ for $n \geqslant 2$. In the case of $s = 3$, we propose a polynomial time approximation algorithm for solving the graph clustering problem and use this algorithm to prove that clustering complexity of an arbitrary $n$-vertex graph doesn't exceed $(n(n-1)/2 - 3\lfloor n/3 \rfloor)$ for $n \geqslant 4$.

**Keywords:** *graph, clustering, clustering complexity.*

[1]Работа А. В. Ильева выполнена при поддержке гранта РНФ № 22-11-20019.

## Введение

В работе изучаются задачи кластеризации, в которых заданное множество объектов требуется разбить на несколько попарно непересекающихся подмножеств — кластеров, принимая во внимание только сходство объектов друг с другом.

Задачи кластеризации вершин графов являются наиболее наглядными формализациями задач кластеризации [1]. В этих задачах вершины неориентированного графа взаимно однозначно соответствуют рассматриваемым объектам и группируются в кластеры так, чтобы минимизировать число рёбер между кластерами и число пар несмежных вершин внутри кластеров.

Будем рассматривать *обыкновенные графы*, т. е. графы без петель и кратных рёбер. Обыкновенный граф называется *кластерным*, если каждая его компонента связности является полным графом.

Существуют различные постановки задачи кластеризации вершин графа. Например, возможны варианты, при которых не накладываются никакие ограничения на кластерный граф. В других вариантах ограничивается число компонент связности или их размер. Рассматриваются также взвешенные версии задачи. Постановки и различные интерпретации задачи кластеризации вершин графов можно найти в [2–9].

## 1. Известные результаты

Пусть $V$ — конечное множество. Обозначим через $\mathcal{M}(V)$ множество всех кластерных графов на множестве вершин $V$; $\mathcal{M}_k(V)$ — множество всех кластерных графов, имеющих ровно $k$ компонент связности; $\mathcal{M}_{\leqslant k}(V)$ — множество всех кластерных графов, имеющих не более $k$ компонент связности; $\mathcal{M}^{\leqslant s}(V)$ — множество всех кластерных графов, в которых размер любой компоненты связности не превосходит $s$.

Если $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ — обыкновенные графы на одном и том же множестве вершин $V$, то расстояние $d(G_1, G_2)$ между ними определяется как

$$d(G_1, G_2) = |E_1 \setminus E_2| + |E_2 \setminus E_1|.$$

Изучение кластеризации графов началось с задач без ограничений и с ограничением на количество кластеров [3, 4, 8–11]. Рассмотрим данные постановки, известные как задачи аппроксимации графов.

**Задача GC.** Дан граф $G = (V, E)$. Требуется найти такой кластерный граф $M^* \in \mathcal{M}(V)$, что

$$d(G, M^*) = \min_{M \in \mathcal{M}(V)} d(G, M) \stackrel{\text{def}}{=} \tau(G).$$

**Задача $\mathbf{GC_k}$.** Дан граф $G = (V, E)$ и целое число $k$, $2 \leqslant k \leqslant |V|$. Требуется найти такой кластерный граф $M^* \in \mathcal{M}_k(V)$, что

$$d(G, M^*) = \min_{M \in \mathcal{M}_k(V)} d(G, M) \stackrel{\text{def}}{=} \tau_k(G).$$

**Задача $\mathbf{GC_{\leqslant k}}$.** Дан граф $G = (V, E)$ и целое число $k$, $2 \leqslant k \leqslant |V|$. Требуется найти такой кластерный граф $M^* \in \mathcal{M}_{\leqslant k}(V)$, что

$$d(G, M^*) = \min_{M \in \mathcal{M}_{\leqslant k}(V)} d(G, M) \stackrel{\text{def}}{=} \tau_{\leqslant k}(G).$$

Будем рассматривать только задачи кластеризации с ограничением размеров компонент связности кластерного графа.

**Задача $\mathbf{GC}^{\leqslant \mathbf{s}}$.** Дан граф $G = (V, E)$ и целое число $s$, $2 \leqslant s \leqslant |V|$. Требуется найти такой кластерный граф $M^* \in \mathcal{M}^{\leqslant s}(V)$, что

$$d(G, M^*) = \min_{M \in \mathcal{M}^{\leqslant s}(V)} d(G, M) \stackrel{\text{def}}{=} \tau^{\leqslant s}(G).$$

Величины $\tau(G)$, $\tau_k(G)$, $\tau_{\leqslant k}(G)$ и $\tau^{\leqslant s}(G)$ называются *сложностью кластеризации графа* $G$ в задачах $\mathbf{GC}$, $\mathbf{GC_k}$, $\mathbf{GC}_{\leqslant \mathbf{k}}$ и $\mathbf{GC}^{\leqslant \mathbf{s}}$ соответственно. Для любого $n$-вершинного графа $G$ и $s \geqslant 2$ справедливо неравенство $\tau(G) \leqslant \tau^{\leqslant s+1}(G) \leqslant \tau^{\leqslant s}(G)$.

В 70-е гг. XX в. Г. Ш. Фридманом и И. Томеску были установлены точные верхние оценки сложности кластеризации графов в задачах $\mathbf{GC}$ и $\mathbf{GC}_{\leqslant \mathbf{k}}$. В 1974 г. Г. Ш. Фридманом доказана следующая теорема:

**Теорема 1** [4]. Для любого $n$-вершинного графа $G$

$$\tau(G) \leqslant \left\lfloor \frac{(n-1)^2}{4} \right\rfloor.$$

Независимо И. Томеску получил аналогичный результат для задачи $\mathbf{GC}_{\leqslant \mathbf{k}}$:

**Теорема 2** [8]. Для любого $k \geqslant 2$ и любого $n$-вершинного графа $G$

$$\tau_{\leqslant k}(G) \leqslant \left\lfloor \frac{(n-1)^2}{4} \right\rfloor.$$

Позже В. П. Ильев и Г. Ш. Фридман доказали следующую теорему:

**Теорема 3** [10]. Для любого $k \geqslant 2$ и любого $n$-вершинного графа $G$ при $n \geqslant 5(k-1)$

$$\tau_k(G) \leqslant \left\lfloor \frac{(n-1)^2}{4} \right\rfloor.$$

Что касается величины $\tau^{\leqslant s}(G)$, то она в общем случае не поддаётся такой же оценке. Например, для полного 10-вершинного графа $\tau^{\leqslant 2}(G) = 40 > \lfloor (n-1)^2/4 \rfloor = 20$ и $\tau^{\leqslant 3}(G) = 36 > \lfloor (n-1)^2/4 \rfloor = 20$.

## 2. Оценка сложности кластеризации в задаче $\mathbf{GC}^{\leqslant \mathbf{2}}$

**Теорема 4.** При $n \geqslant 2$ для любого $n$-вершинного графа $G$

$$\tau^{\leqslant 2}(G) \leqslant \frac{n(n-1)}{2} - \left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{(n-1)^2}{2} \right\rfloor.$$

***Доказательство.*** Воспользуемся индукцией по числу вершин.

О с н о в а н и е  и н д у к ц и и при $n = 2$. Нетрудно убедиться, что утверждение верно для 1-вершинного и 2-вершинных графов.

Пусть $n \geqslant 3$; предположим, что утверждение теоремы верно для всех графов с числом вершин, меньшим $n$.

Ш а г  и н д у к ц и и. Рассмотрим произвольный $n$-вершинный граф $G = (V, E)$. Если $G$ — полный или пустой граф, то неравенство верно, поэтому без ограничения общности считаем, что $G$ отличен от полного или пустого.

Выберем любую вершину $v \in V$ степени $d_G(v) \leqslant n - 2$ и рассмотрим подграф $G' = (V \setminus \{v\}, E')$, полученный из $G$ удалением вершины $v$ вместе со всеми инцидентными ей рёбрами.

По предположению индукции

$$d(G', M^*) \leqslant \frac{(n-1)(n-2)}{2} - \left\lfloor \frac{n-1}{2} \right\rfloor,$$

где $M^*$ — оптимальное решение задачи $\mathbf{GC}^{\leqslant \mathbf{2}}$ на графе $G'$, т. е. подграф графа $G$, представляющий собой наибольшее паросочетание в графе $G'$ плюс (возможно) какие-то изолированные вершины.

Вернём назад вершину $v$. Рассмотрим подграф $M$ графа $G$, полученный из $M^*$ добавлением к паросочетанию нового независимого ребра, инцидентного вершине $v$ (если такое ребро получится при возврате вершины $v$), или изолированной вершины $v$. Таким образом, в графе $M$ либо на одно ребро больше, либо столько же рёбер, как и в $M^*$. Тогда

$$d(G, M) \leqslant d(G'M^*) + d_G(v) \text{ или } \ d(G, M) \leqslant d(G'M^*) + d_G(v) - 1.$$

В любом случае $d(G, M) \leqslant d(G'M^*) + d_G(v)$. Следовательно,

$$d(G, M) \leqslant \frac{(n-1)(n-2)}{2} - \left\lfloor \frac{n-1}{2} \right\rfloor + d_G(v) \leqslant \frac{(n-1)(n-2)}{2} - \left\lfloor \frac{n-1}{2} \right\rfloor + n - 2 =$$
$$= \frac{n^2 - 3n + 2}{2} + n - 1 - \left\lfloor \frac{n-1}{2} \right\rfloor - 1 = \frac{n^2 - n}{2} - \left\lfloor \frac{n-1}{2} \right\rfloor - 1 \leqslant \frac{n(n-1)}{2} - \left\lfloor \frac{n}{2} \right\rfloor,$$

так как $\lfloor (n-1)/2 \rfloor + 1 = \lfloor (n+1)/2 \rfloor \geqslant \lfloor n/2 \rfloor$. Поэтому

$$\tau^{\leqslant 2}(G) \leqslant d(G, M) \leqslant \frac{n(n-1)}{2} - \left\lfloor \frac{n}{2} \right\rfloor.$$

Теорема 4 доказана. ■

## 3. Приближённый алгоритм решения задачи $\mathbf{GC}^{\leqslant \mathbf{3}}$

Приведём алгоритм 1 нахождения приближённого решения в задаче $\mathbf{GC}^{\leqslant \mathbf{3}}$.

**Алгоритм 1.**

**Вход:** произвольный граф $G = (V, E)$.
**Выход:** кластерный граф $M \in \mathcal{M}^{\leqslant 3}(V)$.

1: В графе $G$ находим максимальную $K_3$-упаковку, т. е. максимальное по включению множество попарно непересекающихся треугольников. Для каждого найденного треугольника удаляем из $G$ все рёбра, которые связывают вершины треугольника с вершинами вне данного треугольника. Получаем граф $M_1 \cup G_1$, в котором подграф $M_1$ содержит только найденные треугольники, а $G_1$ — оставшиеся неудалённые рёбра графа $G$, не образующие треугольников.
2: В графе $G_1$ находим наибольшее паросочетание $M_2$. Множество вершин, не вошедших в паросочетание, обозначим $M_3$.
3: Строим кластерный граф $M \in \mathcal{M}^{\leqslant 3}(V)$: $M = M_1 \cup M_2 \cup M_3$.

**Утверждение 1.** Алгоритм 1 имеет трудоёмкость $O(n^3)$.

***Доказательство.*** Рассмотрим операции, проводимые алгоритмом, и их трудоёмкости.

Обход в глубину находит цикл в графе за время $O(n+m)$, где $m$ — количество рёбер графа. Следовательно, чтобы найти все треугольники, необходимо затратить $O(n(n+m))$ операций. Для поиска наибольшего паросочетания применяется алгоритм Эдмондса, известный как алгоритм сжатия цветков, трудоёмкость которого — $O(n^3)$ [12]. Объединение $M = M_1 \cup M_2 \cup M_3$ выполняется за один проход, т. е. за время $O(n)$.

Таким образом, итоговая трудоёмкость алгоритма 1 равна $O(n(n+m)+n^3+n) = O(n^3)$. ■

**Замечание 1.** В полном графе $G$ алгоритм 1 находит оптимальное решение.

## 4. Оценка сложности кластеризации в задаче $\mathbf{GC}^{\leqslant 3}$

**Теорема 5.** При $n \geqslant 4$ для любого $n$-вершинного графа $G$

$$\tau^{\leqslant 3}(G) \leqslant \frac{n(n-1)}{2} - 3\left\lfloor \frac{n}{3} \right\rfloor. \tag{1}$$

Доказательство проведём в три этапа:

1) Пусть для данного $n$-вершинного графа $G$ алгоритмом 1 найден кластерный граф $M \subseteq G$. В этом графе обозначим: $m_3$ — количество клик $K_3$, $m_2$ — количество клик $K_2$, $m_1$ — количество изолированных вершин. Заметим, что $n = 3m_3 + 2m_2 + m_1$.
2) Проверим, выполняется ли для графа $M$ неравенство

$$\frac{n(n-1)}{2} - 3\left\lfloor \frac{n}{3} \right\rfloor - d(G,M) \geqslant 0. \tag{2}$$

3) Если для графов $G$ и $M$ неравенство (2) нарушается, то докажем, что в каждом из таких случаев для графа $G$ существует другой кластерный граф $M' \subseteq G$, такой, что $d(G,M') < d(G,M)$, причём для $M'$ неравенство (2) выполнено.

***Доказательство.***

1) Заметим, что в найденном алгоритмом 1 кластерном подграфе $M$ графа $G$ количество удалённых алгоритмом рёбер между кластерами имеет разные ограничения в каждом из возможных случаев:

- $K_3$ и $K_3$ могут иметь между собой не более 9 соединяющих рёбер;
- $K_3$ и $K_2$ могут иметь между собой не более 6 соединяющих рёбер;
- $K_3$ и $K_1$ могут иметь между собой не более 3 соединяющих рёбер;
- $K_2$ и $K_2$ могут иметь между собой не более 2 соединяющих рёбер;
- $K_2$ и $K_1$ могут иметь между собой не более 1 соединяющего ребра;
- $K_1$ и $K_1$ не должны иметь между собой соединяющих ребер.

Ограничения на количество рёбер для кластеров $K_3$ определены для каждого такого случая как максимально возможное количество рёбер, соединяющих эти кластеры с другими в обыкновенном графе. Для всех прочих случаев действуют следующие рассуждения. Если бы, например, кластеры $K_2$ и $K_2$ имели больше двух соединяющих рёбер, то вместо первого из них алгоритм 1 нашёл бы клику $K_3$. Если бы кластеры $K_2$ и $K_1$ имели больше одного соединяющего ребра, то вместо $K_2$ алгоритм 1 нашёл бы клику $K_3$. Аналогично, если бы кластеры $K_1$ и $K_1$ были соединены ребром, то вместо них алгоритм 1 нашёл бы клику $K_2$.

Следовательно,

$$d(G,M) \leqslant \frac{9m_3(m_3-1)}{2} + 6m_3m_2 + 3m_3m_1 + \frac{2m_2(m_2-1)}{2} + m_2m_1 =$$
$$= \frac{9}{2}m_3^2 + m_2^2 + 6m_3m_2 + 3m_3m_1 + m_2m_1 - \frac{9}{2}m_3 - m_2.$$

Отметим, что

$$\frac{n(n-1)}{2} - 3\left\lfloor\frac{n}{3}\right\rfloor = \frac{(3m_3+2m_2+m_1)(3m_3+2m_2+m_1-1)}{2} - 3\left\lfloor\frac{3m_3+2m_2+m_1}{3}\right\rfloor =$$
$$= \frac{9m_3^2+4m_2^2+m_1^2+12m_3m_2+6m_3m_1+4m_2m_1}{2} - \frac{9m_3+2m_2+m_1}{2} - 3\left\lfloor\frac{2m_2+m_1}{3}\right\rfloor =$$
$$= \frac{9}{2}m_3^2 + 2m_2^2 + \frac{1}{2}m_1^2 + 6m_3m_2 + 3m_3m_1 + 2m_2m_1 - \frac{9}{2}m_3 - m_2 - \frac{1}{2}m_1 - 3\left\lfloor\frac{2m_2+m_1}{3}\right\rfloor.$$

Поэтому

$$\frac{n(n-1)}{2} - 3\left\lfloor\frac{n}{3}\right\rfloor - d(G,M) \geqslant$$
$$\geqslant \frac{9}{2}m_3^2 + 2m_2^2 + \frac{1}{2}m_1^2 + 6m_3m_2 + 3m_3m_1 + 2m_2m_1 - \frac{9}{2}m_3 - m_2 - \frac{1}{2}m_1 - 3\left\lfloor\frac{2m_2+m_1}{3}\right\rfloor -$$
$$- \left(\frac{9}{2}m_3^2 + m_2^2 + 6m_3m_2 + 3m_3m_1 + m_2m_1 - \frac{9}{2}m_3 - m_2\right) =$$
$$= m_2^2 + \frac{1}{2}m_1^2 + m_2m_1 - \frac{1}{2}m_1 - 3\left\lfloor\frac{2m_2+m_1}{3}\right\rfloor.$$

Таким образом, неравенство (2) будет выполнено, если

$$m_2^2 + \frac{1}{2}m_1^2 + m_2m_1 - \frac{1}{2}m_1 - 3\left\lfloor\frac{2m_2+m_1}{3}\right\rfloor \geqslant 0. \tag{3}$$

2) В свою очередь, неравенство (3) будет выполнено, если

$$m_2^2 + \frac{1}{2}m_1^2 + m_2m_1 - 2m_2 - \frac{3}{2}m_1 \geqslant 0. \tag{4}$$

Выясним, при каких $m_2, m_1 \in \mathbb{Z}_+$ неравенство (4) будет выполнено. Для этого воспользуемся методом выделения полных квадратов в левой части этого неравенства:

$$\left(m_2^2 + m_2m_1 + \frac{1}{4}m_1^2\right) - \frac{1}{4}m_1^2 + \frac{1}{2}m_1^2 - 2m_2 - \frac{3}{2}m_1 = \left(m_2 + \frac{1}{2}m_1\right)^2 + \frac{1}{4}m_1^2 - 2m_2 - \frac{3}{2}m_1 \circledcirc$$

Делаем замену переменных $m_2' = m_2 + m_1/2$:

$$\circledcirc (m_2')^2 + \frac{1}{4}m_1^2 - 2m_2' + m_1 - \frac{3}{2}m_1 = (m_2')^2 + \frac{1}{4}m_1^2 - 2m_2' - \frac{1}{2}m_1 =$$
$$= \left((m_2')^2 - 2m_2' + 1\right) - 1 + \left(\frac{1}{4}m_1^2 - \frac{1}{2}m_1 + \frac{1}{4}\right) - \frac{1}{4} = (m_2'-1)^2 + \left(\frac{1}{2}m_1 - \frac{1}{2}\right)^2 - \frac{5}{4} \circledcirc$$

Делаем замену переменных $m_2'' = m_2' - 1$, $m_1' = m_1/2 - 1/2$:

$$\ominus (m_2'')^2 + (m_1')^2 - \frac{5}{4} \geqslant 0.$$

Нетрудно заметить, что это неравенство задаёт внешность круга:

$$\frac{4}{5}(m_2'')^2 + \frac{4}{5}(m_1')^2 \geqslant 1.$$

При этом точка с координатами $(m_1', m_2'')$ будет гарантированно лежать вне круга и, таким образом, удовлетворять неравенству (4), если

$$\frac{4}{5}(m_1')^2 \geqslant 1 \quad \text{или} \quad \frac{4}{5}(m_2'')^2 \geqslant 1.$$

Рассмотрим каждый из этих случаев с учётом того, что

$$\begin{cases} m_2'' = m_2 + m_1/2 - 1; \\ m_1' = m_1/2 - 1/2. \end{cases}$$

Неравенство $4/5\,(m_1')^2 \geqslant 1$ выполнено, если $(m_1/2 - 1/2)^2 \geqslant 5/4$. Наименьшее такое значение $m_1 \in \mathbb{Z}_+$ равно 4, т. е. возьмём $m_1 \geqslant 4$.

Неравенство $4/5\,(m_2'')^2 \geqslant 1$ выполнено, если $(m_2 + m_1/2 - 1)^2 \geqslant 5/4$. При $m_1 = 0$ наименьшее такое значение $m_2 \in \mathbb{Z}_+$ равно 3, т. е. возьмём $m_2 \geqslant 3$.

Таким образом, при $m_2 \geqslant 3$ либо $m_1 \geqslant 4$ неравенство (4), а значит, и неравенство (3) всегда будут выполнены.

3) Выясним, при каких $m_2 \leqslant 2$, $m_1 \leqslant 3$ неравенство (3) может нарушаться, т. е. алгоритм находит кластерный граф $M$, такой, что $d(G, M)$ превосходит оценку сложности кластеризации $\tau^{\leqslant 3}(G)$. Построим таблицу соответствующих значений левой части неравенства и посмотрим на его выполнимость.

| $m_2$ | $m_1$ | Левая часть | Неравенство |
|---|---|---|---|
| 0 | 0 | 0 | ИСТИНА |
| 0 | 1 | 0 | ИСТИНА |
| 0 | 2 | 1 | ИСТИНА |
| 0 | 3 | 0 | ИСТИНА |
| 1 | 0 | 1 | ИСТИНА |
| 1 | 1 | −1 | ЛОЖЬ |
| 1 | 2 | 1 | ИСТИНА |
| 1 | 3 | 4 | ИСТИНА |
| 2 | 0 | 1 | ИСТИНА |
| 2 | 1 | 3 | ИСТИНА |
| 2 | 2 | 3 | ИСТИНА |
| 2 | 3 | 7 | ИСТИНА |

Рассмотрим случай $m_2 = m_1 = 1$, когда неравенство (3) может нарушаться.

Так как $n \geqslant 4$, то в этом случае в графе $G$ должна содержаться хотя бы одна клика $K_3$, т. е. в найденном алгоритмом 1 кластерном графе $M$ обязательно $m_3 \geqslant 1$.

Рассмотрим 6-вершинный подграф $G'$ графа $G$, вершины которого разбиваются алгоритмом 1 на кластеры на последних шагах. Поскольку ранее обнаруженные подграфы $K_3$ не влияют на выполнение неравенства (3), его нарушение на единицу (как

показано в таблице) может произойти именно на этапе работы с графом $G'$, если количество удаляемых в нём рёбер между кластерами максимально возможное — 10. Напомним, что в случае нарушения этого ограничения алгоритм 1 непременно нашёл бы другие кластеры большего размера.

Однако если граф $G'$ имеет ровно 10 рёбер, то каждая из вершин его клики $K_3 = \{v_1, v_2, v_3\}$ должна быть смежна с обеими вершинами его клики $K_2 = \{v_4, v_5\}$ и изолированной вершиной $v_6$. Но тогда в графе $G'$ существуют другие кластеры: $K_3 = \{v_1, v_4, v_5\}$ и $K_3 = \{v_2, v_3, v_6\}$, для выделения которых в $G'$ нужно удалить на два ребра меньше, чем для выделения кластеров графа $M$.

Таким образом, в графе $G$ существует другой кластерный подграф $M'$, такой, что $d(G, M) = d(G, M') + 2$; для графа $M'$ неравенство (3) выполнено, а значит, оценка сложности кластеризации $\tau^{\leqslant 3}(G)$ в этом случае остаётся верна.

Следовательно, для любого $n$-вершинного графа $G$ ($n \geqslant 4$) существует кластерный граф $M$, такой, что

$$\frac{n(n-1)}{2} - 3\left\lfloor \frac{n}{3} \right\rfloor - d(G, M) \geqslant 0.$$

Поэтому

$$\tau^{\leqslant 3}(G) \leqslant d(G, M) \leqslant \frac{n(n-1)}{2} - 3\left\lfloor \frac{n}{3} \right\rfloor.$$

Теорема 5 доказана. ■

**Замечание 2.** Поскольку для любого $s \geqslant 3$ и любого $n$-вершинного графа $G$ $\tau^{\leqslant s}(G) \leqslant \tau^{\leqslant 3}(G)$, то при $n \geqslant 4$

$$\tau^{\leqslant s}(G) \leqslant \frac{n(n-1)}{2} - 3\left\lfloor \frac{n}{3} \right\rfloor.$$

## Заключение

Исследована задача кластеризации на графах, в которой размеры кластеров не превосходят числа $s$. Доказаны оценки сложности кластеризации для задач $\mathbf{GC}^{\leqslant 2}$ и $\mathbf{GC}^{\leqslant 3}$. Предложен приближённый полиномиальный алгоритм для задачи $\mathbf{GC}^{\leqslant 3}$, который используется при доказательстве оценки сложности кластеризации произвольного графа. Аналогичный подход может быть применён для получения оценок сложности кластеризации в отдельных случаях при $s > 3$, однако вопрос о его перспективности для доказательства оценки в случае произвольного $s$ пока остаётся открытым.

## ЛИТЕРАТУРА


1. *Schaeffer S. E.* Graph clustering // Comput. Sci. Rev. 2005. V. 1. No. 1. P. 27–64.
2. *Ляпунов А. А.* О строении и эволюции управляющих систем в связи с теорией классификации // Проблемы кибернетики. Вып. 27. М.: Наука, 1973. С. 7–18.
3. *Фридман Г. Ш.* Одна задача аппроксимации графов // Управляемые системы. 1971. Вып. 8. С. 73–75.
4. *Фридман Г. Ш.* Об одном неравенстве в задаче аппроксимации графов // Кибернетика. 1974. № 3. С. 151.
5. *Bansal N., Blum A., and Chawla S.* Correlation clustering // Machine Learning. 2004. V. 56. P. 89–113.
6. *Ben-Dor A., Shamir R., and Yakhimi Z.* Clustering gene expression patterns // J. Comput. Biol. 1999. V. 6. No. 3–4. P. 281–297.

7. *Shamir R., Sharan R., and Tsur D.* Cluster graph modification problems // Discrete Appl. Math. 2004. V. 144. No. 1–2. P. 173–182.
8. *Tomescu I.* La reduction minimale d'un graphe a une reunion de cliques // Discrete Math. 1974. V. 10. No. 1–2. P. 173–179.
9. *Zahn C. T.* Approximating symmetric relations by equivalence relations // J. SIAM. 1964. V. 12. No. 4. P. 840–847.
10. *Ильев В. П., Фридман Г. Ш.* К задаче аппроксимации графами с фиксированным числом компонент // Докл. АН СССР. 1982. Т. 264. № 3. С. 533–538.
11. *Фридман Г. Ш.* Исследование одной задачи классификации на графах // Методы моделирования и обработки информации. Новосибирск: Наука, 1976. С. 147–177.
12. *Пападимитриу Х., Стайглиц К.* Комбинаторная оптимизация. Алгоритмы и сложность. М.: Мир, 1984. 510 с.

## REFERENCES

1. *Schaeffer S. E.* Graph clustering. Computer Science Review, 2005, vol. 1, no. 1, pp. 27–64.
2. *Lyapunov A. A.* O stroenii i evolyutsii upravlyayushchikh sistem v svyazi s teoriey klassifikatsii [On the structure and evolution of control systems in connection with the theory of classification]. Problemy Kibernetiki, iss. 27, Moscow, Nauka Publ., 1973, pp. 7–18. (in Russian)
3. *Fridman G. Sh.* Odna zadacha approksimatsii grafov [A graph approximation problem]. Upravlyaemye Sistemy, 1971, vol. 8, pp. 73–75. (in Russian)
4. *Fridman G. Sh.* On an inequality in the graph approximation problem. Cybern. Syst. Anal., 1974, no. 10, p. 554.
5. *Bansal N., Blum A., and Chawla S.* Correlation clustering. Machine Learning, 2004, vol. 56, pp. 89–113.
6. *Ben-Dor A., Shamir R., and Yakhimi Z.* Clustering gene expression patterns. J. Comput. Biol, 1999, vol. 6, no. 3–4, pp. 281–297.
7. *Shamir R., Sharan R., and Tsur D.* Cluster graph modification problems. Discrete Appl. Math., 2004, vol. 144, no. 1–2, pp. 173–182.
8. *Tomescu I.* La reduction minimale d'un graphe a une reunion de cliques. Discrete Math., 1974, vol. 10, no. 1–2, pp. 173–179.
9. *Zahn C. T.* Approximating symmetric relations by equivalence relations. J. SIAM, 1964, vol. 12. no. 4, pp. 840–847.
10. *Il'ev V. P. and Fridman G. Sh.* On the problem of approximation by graphs with a fixed number of components. Sov. Math. Dokl., 1982, vol. 25, no. 3, pp. 666–670.
11. *Fridman G. Sh.* Issledovanie odnoy zadachi klassifikatsii na grafakh [Study of a classifying problem on graphs]. Metody Modelirovaniya i Obrabotki Informatsii, Novosibirsk, Nauka Publ., 1976, pp. 147–177. (in Russian)
12. *Papadimitriou C. H. and Steiglitz K.* Combinatorial Optimization: Algorithms and Complexity. NJ, Prentice-Hall Inc., 1982, 496 p.

УДК 519.176 DOI 10.17223/20710410/60/7

# ПОИСК СЕМЕЙСТВА ПРОСТЫХ ЦИКЛОВ В ГРАФАХ С ПОЛУСТЕПЕНЯМИ ВЕРШИН, НЕ ПРЕВОСХОДЯЩИМИ $k$

А. А. Медведев

*Московский государственный технический университет им. Н. Э. Баумана, г. Москва, Россия*

**E-mail:** medvedevaa@student.bmstu.ru

Исследована алгоритмическая сложность задачи о поиске семейства простых циклов, обходящих каждую вершину орграфа с полустепенями вершин, не превосходящими $k$, при наличии дополнительных ограничений на вид списка смежности. Рассмотрены поисковый и оптимизационный её варианты. Показана параметрически полиномиальная разрешимость задачи в обоих вариантах, предложены алгоритмы со временем работы $O(nk^2 + n\log_2 n)$, $O(n(k^2 + k) + n\log_2 n)$ и $O(n)$ для различных типов ограничений; $n$ — количество вершин орграфа.

**Ключевые слова:** *ориентированные графы, простые циклы, задачи поиска, оптимизация, класс P, параметрическая сложность, полиномиальная разрешимость.*

# FINDING A FAMILY OF SIMPLE CIRCUITS IN GRAPHS WITH VERTEX SEMIDEGREES BOUNDED BY $k$

A. A. Medvedev

*Bauman Moscow State Technical University, Moscow, Russia*

We study the algorithmic complexity of finding a family of simple circuits passing every vertice of a digraph with semidegree bounded by $k$. The problem is considered in two variants: as a search and as an optimization problem. Parametrically polynomial solvability of the problem is proved in both variants, Algorithms with complexity $O(nk^2 + n\log_2 n)$, $O(n(k^2 + k) + n\log_2 n)$ and $O(n)$ for various types of constraints are proposed, where $n$ is the number of digraph vertices.

**Keywords:** *digraphs, simple circuits, search problems, optimization, P class, parametrical complexity, polynomial solvability.*

## Введение

Рассматриваются задачи о поиске в орграфах некоторых специальных классов остовного подграфа, состоящего из непересекающихся простых циклов. Эта задача представляет собой обобщение задачи о поиске гамильтонова цикла и исследуется как в разрешимостном, так и в оптимизационном вариантах. К настоящему времени доказано, что разрешимостная задача о гамильтоновом цикле является NP-полной в общей постановке [1], на трёхсвязных 3-регулярных двудольных графах [2], подграфах квадратных решёток [3] и кубических подграфах квадратных решёток [4], а также орграфах с полустепенями вершин, не превосходящими 2 [5], но принадлежит к классу полиномиально разрешимых в постановке на четырёхсвязных планарных графах [6];

выведены проверяемые за полиномиальное время достаточные условия гамильтоновости: Дирака — Оре [7, 8], Гуйя — Ури [9], Woodall [10], Christofides [11], Keevash [12], Kelly [13]. В работах [14–16] исследуются вопросы поиска простых циклов вообще и гамильтоновых в частности.

## 1. Определения

Определения из теории графов приводятся в соответствии с [17].

**Определение 1.** Ориентированным графом $G$ называется пара множеств $V$ и $E$, $V$ — множество вершин орграфа $G$, $E$ — множество дуг, т. е. упорядоченных пар вида $(v_i, v_j)$, $v_i, v_j \in V$, $i \neq j$.

**Определение 2.** Неориентированным графом (или просто графом) $G$ называется пара множеств $V$ и $E$, $V$ — множество вершин, $E$ — множество рёбер, т. е. неупорядоченных пар вида $\{v_i, v_j\}$, $v_i, v_j \in V$, $i \neq j$.

**Определение 3.** Вершинно-простая цепь в ориентированном графе $G = (V, E)$ — последовательность из $m$ вершин и $m-1$ дуг $v_1, e_1, v_2, e_2, \ldots, v_{m-1}, e_{m-1}, v_m$, где $e_i = (v_i, v_{i+1})$ для всех $i = 1, \ldots, m-1$ и если $i \neq j$, то $v_i \neq v_j$, то есть все вершины различны.

**Определение 4.** Вершинно-простой цикл в ориентированном графе $G = (V, E)$ — последовательность из $(m+1)$ вершин и $m$ дуг $v_1, e_1, v_2, e_2, \ldots, v_m, e_m, v_1$, где $e_i = (v_i, v_{i+1})$ для всех $i = 1, \ldots, m-1$, $e_m = (v_m, v_1)$ и если $i \neq j$ и $i, j \leqslant m$, то $v_i \neq v_j$, то есть все вершины, за исключением первой и последней, различны.

**Определение 5.** Вершинно-простые цепи и циклы называются неориентированными, если элементы $e_i$ в них представляют собой неупорядоченные пары вида $\{v_p, v_q\}$.

**Определение 6.** Ориентированный (неориентированный) граф $G = (V, E)$ называется взвешенным, если для него определена функция $w(v, u)$, $v, u \in V$, равная некоторому значению из $\mathbb{R} \setminus \{0\}$, если $(v, u) \in E$, и 0 в противном случае.

**Определение 7.** Пусть элементы множества вершин $V$ пронумерованы. Матрицей весов $W$ взвешенного орграфа (графа) называется такая таблица размера $|V| \times |V|$, что $W_{ij} = w(v_i, v_j)$.

**Определение 8.** Пусть элементы множества вершин $V$ пронумерованы. Матрицей смежности $A$ взвешенного орграфа называется такая таблица размера $|V| \times |V|$, что $A_{ij} = 1$, если $(v_i, v_j) \in E$, и $A_{ij} = 0$ в противном случае.

**Определение 9.** Пусть множество $V$ графа $G = (V, E)$ упорядочено. Списком смежности этого графа называется набор из $|V|$ списков, по одному для каждой вершины из $V$; список, соответствующий вершине $v \in V$, состоит из номеров всех вершин $u$, для которых $(v, u) \in E$.

**Определение 10** (орграф класса kRS). Ориентированным графом $G = (V, E)$ класса kRS назовём всякий орграф, представимый в виде списка смежности следующего вида: для каждой вершины существует лишь $k-1$, за исключением её самой, имеющих в точности такой же список смежности, и ни одна другая вершина, кроме этих $k$, не смежна по исходящей дуге с теми же вершинами, с которыми смежны они; полустепени всех вершин орграфа, как входящие, так и исходящие, равны $k$. То есть список смежности такого орграфа имеет структуру

$$\begin{aligned} &u_{1,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \\ &u_{2,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \\ &\ldots \\ &u_{k,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \end{aligned} \tag{1}$$

где $|V|$ кратно $k$; $V \geqslant 2k$; $i = 1, \ldots, |V|/k$; если $p \neq q$, то $u_{p,i} \neq u_{q,i}$ и $v_{p,i} \neq v_{q,i}$, $p, q = 1, \ldots, k$; если $i \neq j$, то $\{u_{1,i}, \ldots, u_{k,i}\} \cap \{u_{1,j}, \ldots, u_{k,j}\} = \varnothing$ и $\{v_{1,i}, \ldots, v_{k,i}\} \cap \cap \{v_{1,j}, \ldots, v_{k,j}\} = \varnothing$.

**Определение 11** (граф класса kRS). Неориентированным графом $G = (V, E)$ класса kRS назовём всякий граф, компоненты связности которого являются полными двудольными графами $K_{k,k}$, или, иначе, граф, представимый в виде списка смежности следующего вида:

$$\begin{aligned} &u_{1,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \\ &u_{2,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \\ &\ldots \\ &u_{k,i} : v_{1,i}, v_{2,i}, \ldots, v_{k,i}, \\ \\ &v_{1,i} : u_{1,i}, u_{2,i}, \ldots, u_{k,i}, \\ &v_{2,i} : u_{1,i}, u_{2,i}, \ldots, u_{k,i}, \\ &\ldots \\ &v_{k,i} : u_{1,i}, u_{2,i}, \ldots, u_{k,i}. \end{aligned} \tag{2}$$

Здесь $|V|$ кратно $2k$; $i = 1, \ldots, |V|/(2k)$; если $p \neq q$, то $u_{p,i} \neq u_{q,i}$ и $v_{p,i} \neq v_{q,i}$, $p, q = 1, \ldots, k$; если $i \neq j$, то $\{u_{1,i}, \ldots, u_{k,i}\} \cap \{u_{1,j}, \ldots, u_{k,j}\} = \varnothing$ и $\{v_{1,i}, \ldots, v_{k,i}\} \cap \cap \{v_{1,j}, \ldots, v_{k,j}\} = \varnothing$.

**Определение 12.** Исходящей полустепенью (полустепенью исхода) $\deg^{\text{out}} u$ вершины $u \in V$ орграфа $G = (V, E)$ назовём количество дуг вида $(u, v) \in E$, $v \in V$. Входящей степенью (полустепенью захода) $\deg^{\text{in}} u$ будем называть количество дуг вида $(v, u) \in E$, $v \in V$.

**Определение 13** (орграф класса kS). Орграфом $G = (V, E)$ класса kS назовём всякий орграф, такой, что:

1) $|V|$ кратно $k$, $V \geqslant 2k$;
2) $\forall v \in V(\deg^{\text{out}} v \leqslant k \;\&\; \deg^{\text{in}} v \leqslant k)$;
3) $V = V_1 \cup \ldots \cup V_{|V|/k} \;\wedge\; \forall i, j \in \{1, \ldots, |V|/k\}(i \neq j \Rightarrow V_i \cap V_j = \varnothing) \;\wedge\; \exists i \in \in \{1, \ldots, |V|/k\}(|V_i| = k)$;
4) $V = U_1 \cup \ldots \cup U_{|V|/k} \;\wedge\; \forall i, j \in \{1, \ldots, |V|/k\}(i \neq j \Rightarrow U_i \cap U_j = \varnothing) \;\wedge\; \exists i \in \in \{1, \ldots, |V|/k\}(|U_i| = k)$;
5) $\forall i \in \{1, \ldots, |V|/k\}\,(V_i \cap U_i = \varnothing)$;
6) $\forall v, u \in V\big((v, u) \in E \Rightarrow \exists i\,(v \in V_i \wedge u \in U_i)\big)$;
7) $\forall i \in \{1, \ldots, |V|/k\}\,\exists v \in V_i\,(\deg^{\text{out}} v = k)$.

Пример kS-графа приведён на рис. 1.

**Определение 14** (задача НСЦ-k, неоптимизационная). Пусть дан взвешенный ориентированный или неориентированный граф $G = (V, E)$ класса kRS или kS. Требуется найти такой набор вершинно-простых циклов, чтобы каждая вершина из $V$ содержалась ровно в одном из них.

**Определение 15** (задача ОНСЦ-k, оптимизационная). Пусть дан взвешенный ориентированный или неориентированный граф $G = (V, E)$ класса kRS или kS и вещественное число $q$. Требуется найти такой набор вершинно-простых циклов, чтобы

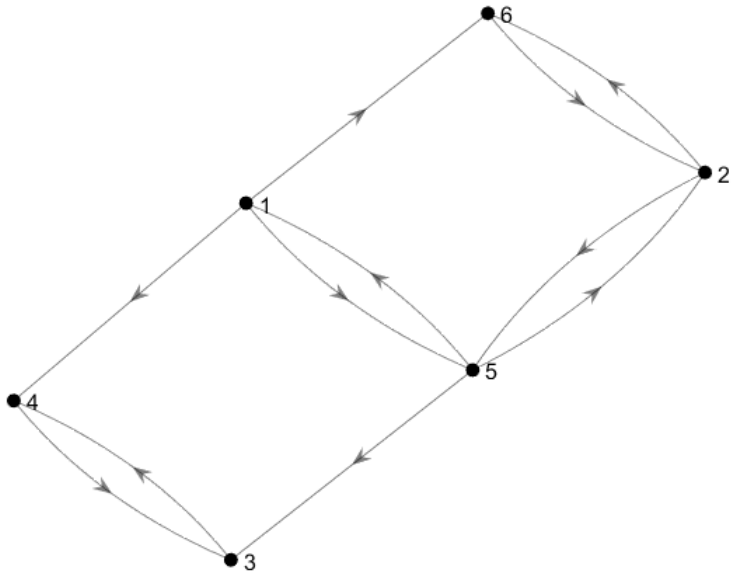


Рис. 1. Пример kS-орграфа: $k = 3$, $V_1 = \{1, 2, 3\}$, $V_2 = \{4, 5, 6\}$, $U_1 = \{4, 5, 6\}$, $U_2 = \{1, 2, 3\}$

каждая вершина из $V$ содержалась ровно в одном из них, а суммарный вес всех дуг, содержащихся в циклах набора, превосходил $q$.

**Определение 16.** Ориентированный или неориентированный граф $G = (V, E)$ называется двудольным, если множество $V$ можно разбить на две части $U_1$ и $U_2$, такие, что $U_1 \cup U_2 = V$, $U_1 \cap U_2 = \varnothing$ и ни одна вершина из $U_1$ не смежна никакой другой вершине из $U_1$, равно как ни одна вершина из $U_2$ не смежна никакой другой вершине из $U_2$.

**Определение 17.** Паросочетанием в ориентированном или неориентированном графе $G$ называется набор попарно несмежных дуг (рёбер).

**Определение 18** (задача о назначениях, или о паросочетаниях). Имеется неположительная (или неотрицательная) матрица весов двудольного орграфа (графа). Требуется найти максимальное совершенное паросочетание, то есть такое паросочетание, чтобы вес его был наибольшим возможным и каждая вершина орграфа (графа) являлась началом или концом какой-либо дуги (ребра) этого паросочетания.

## 2. Задача о семействе циклов в kRS-орграфе

**Лемма 1** [18]. Пусть дан взвешенный ориентированный граф $G$; всякий его остовный подграф, имеющий для каждой вершины ровно одну исходящую и одну входящую дугу, является семейством вершинно-простых циклов, обходящим все вершины графа $G$. Если такого семейства граф $G$ не содержит, то нет и остовного подграфа, обладающего указанным свойством.

**Теорема 1.** Задача ОНСЦ-k на kRS-орграфе может быть решена за время $O(nk^2 + n \log_2 n)$.

***Доказательство.*** Примем за элементарные операции (выполняемые за время $O(1)$) просмотр элемента в списке смежности и сложение двух чисел. Пусть $|V| = n$. Матрица весов орграфа имеет $n/k$ групп по $k$ строк, причём в строках из разных групп нет ни одного ненулевого элемента на одной и той же позиции.

При поиске семейства циклов, являющегося решением, в каждой группе строк надо выбрать $k$ элементов с наибольшей суммой из разных строк и столбцов. Получаем задачу о паросочетаниях, которая может быть решена с помощью венгерского алгоритма [19] за время $O(k^3)$. В результате получим семейство циклов с наибольшим возможным весом. Если этот вес превосходит $q$, то полученное семейство есть решение задачи.

Группировка строк по блокам простой сортировкой потребует $O(n\log_2 n)$ операций, поиск решений для всех блоков — $O((n/k)k^3) = O(nk^2)$ операций. Итого для решения необходимо время $O(n\log_2 n) + O(nk^2) = O(nk^2 + n\log_2 n)$. ■

**Следствие 1.** Задача НСЦ-k на kRS-орграфе может быть решена за время $O(nk^2 + n\log_2 n)$.

***Доказательство.*** Чтобы найти решение задачи НСЦ-k, достаточно решить на том же орграфе задачу ОНСЦ-k при $q = -\infty$. ■

**Теорема 2.** Задача НСЦ-k на kRS-орграфе может быть решена за время $O(n)$.

***Доказательство.*** Рассмотрим граф класса kRS. Для каждой группы строк вида (1) (для каждого $i$) выберем дуги $(u_{p,i}, v_{p,i})$, $p = 1,\ldots,k$, $i = 1,\ldots,k$. Получим подграф, в котором $\deg^{\text{in}} v = \deg^{\text{out}} v = 1$. Такой подграф, согласно лемме 1, является семейством вершинно-простых циклов, обходящим единожды все вершины рассматриваемого орграфа.

Выбор $k$ дуг требует времени $O(k)$, количество групп, в которых он проводится, равно $n/k$. Таким образом, поиск решения потребует времени $O(n)$. ■

**Пример 1.** Пусть $q = 26$. Рассмотрим орграф, заданный следующим списком смежности (вес соответствующей дуги указан в фигурных скобках):

$$\begin{array}{ll} 4: & 1\{1\}, 2\{1\}, 3\{1\}; \\ 5: & 1\{-1\}, 2\{-2\}, 3\{5\}; \\ 6: & 1\{1\}, 2\{-7\}, 3\{3\}; \\ 1: & 4\{1\}, 5\{-1\}, 6\{10\}; \\ 2: & 4\{5\}, 5\{7\}, 6\{-8\}; \\ 3: & 4\{3\}, 5\{2\}, 6\{2\}. \end{array}$$

Имеем разбиение строк на группы $\{4,5,6\}$ и $\{1,2,3\}$. Для каждой найдём паросочетание с максимальной суммой весов с помощью венгерского алгоритма:

$$\begin{array}{ll} 1) & \max S_1 = w(4,2) + w(5,3) + w(6,1) = 7; \\ 2) & \max S_2 = w(1,6) + w(2,5) + w(3,4) = 20. \end{array}$$

Таким образом, максимальное семейство циклов задаётся набором дуг $\{(4,2),(5,3),(6,1),(1,6),(2,5),(3,4)\}$. Оно состоит из двух циклов: 1) $1-6-1$ и 2) $2-5-3-4-2$; их общий вес равен 27.

Проверим решение, найдя максимальное семейство циклов поиском в глубину. Имеем следующие семейства (в скобках указан общий вес):

$$\begin{array}{llll} \{1-4-1, 2-5-2, 3-6-3\} & (12); & \{1-4-1, 2-5-3-6-2\} & (9); \\ \{1-4-2-5-1, 3-6-3\} & (13); & \{1-4-2-5-3-6-1\} & (17); \\ \{1-4-3-6-2-5-1\} & (3); & \{1-4-3-6-1, 2-5-2\} & (10); \\ \{1-4-1, 2-6-3-5-2\} & (-3); & \{1-4-1, 2-6-2, 3-5-3\} & (-6); \\ \{1-4-2-6-3-5-1\} & (-2); & \{1-4-2-6-1, 3-5-3\} & (2); \end{array}$$

| | | | |
|---|---|---|---|
| $\{1-4-3-5-1, 2-6-2\}$ | $(-12)$; | $\{1-4-3-5-2-6-1\}$ | $(-5)$; |
| $\{1-5-2-4-1, 3-6-3\}$ | $(8)$; | $\{1-5-3-6-2-4-1\}$ | $(5)$; |
| $\{1-5-1, 2-4-2, 3-6-3\}$ | $(9)$; | $\{1-5-3-6-1, 2-4-2\}$ | $(13)$; |
| $\{1-5-1, 2-4-3-6-2\}$ | $(-1)$; | $\{1-5-2-4-3-6-1\}$ | $(6)$; |
| $\{1-5-2-6-3-4-1\}$ | $(-4)$; | $\{1-5-3-4-1, 2-6-2\}$ | $(-7)$; |
| $\{1-5-1, 2-6-3-4-2\}$ | $(-3)$; | $\{1-5-3-4-2-6-1\}$ | $(1)$; |
| $\{1-5-1, 2-6-2, 3-4-3\}$ | $(-13)$; | $\{1-5-2-6-1, 3-4-3\}$ | $(-6)$; |
| $\{1-6-3-5-2-4-1\}$ | $(19)$; | $\{1-6-2-4-1, 3-5-3\}$ | $(16)$; |
| $\{1-6-3-5-1, 2-4-2\}$ | $(20)$; | $\{1-6-1, 2-4-2, 3-5-3\}$ | $(24)$; |
| $\{1-6-2-4-3-5-1\}$ | $(10)$; | $\{1-6-1, 2-4-3-5-2\}$ | $(17)$; |
| $\{1-6-3-4-1, 2-5-2\}$ | $(22)$; | $\{1-6-2-5-3-4-1\}$ | $(19)$; |
| $\{1-6-3-4-2-5-1\}$ | $(23)$; | $\{1-6-1, 2-5-3-4-2\}$ | $(27)$; |
| $\{1-6-2-5-1, 3-4-3\}$ | $(13)$; | $\{1-6-1, 2-5-2, 3-4-3\}$ | $(20)$. |

Максимальным является семейство $\{1-6-1, 2-5-3-4-2\}$ с весом 27, что совпадает с решением, полученным на основании теоремы 1.

## 3. Задача о семействе циклов в kRS-графе

**Теорема 3.** Задача НСЦ-k на kRS-графе может быть решена за время $O(n)$.

***Доказательство.*** Рассмотрим список смежности (2) произвольного kRS-графа. Для каждого $i = 1, \ldots, n/(2k)$ выберем рёбра $\{u_{p,i}, v_{p,i}\}$, $\{u_{p,i}, v_{p+1,i}\}$, $p = 1, \ldots, k-1$, а также рёбра $\{u_{k,i}, v_{1,i}\}$ и $\{u_{k,i}, v_{k,i}\}$. Вместе с инцидентными им вершинами они составляют неориентированный цикл $u_{1,i}$, $\{u_{1,i}, v_{2,i}\}$, $v_{2,i}$, $\{v_{2,i}, u_{2,i}\}$, $u_{2,i}$, $\{u_{2,i}, v_{3,i}\}$, $\ldots$, $v_{k,i}$, $\{v_{k,i}, u_{k,i}\}$, $u_{k,i}$, $\{u_{k,i}, v_{1,i}\}$, $v_{1,i}$, $\{v_{1,i}, u_{1,i}\}$, $u_{1,i}$.

Таким образом, получаем $n/(2k)$ циклов по $2k$ вершин, причём вершины различны как в пределах каждого цикла, так и между циклами, т. е. имеем семейство вершинно-простых неориентированных циклов, обходящих единожды все вершины графа — решение задачи НСЦ-k.

Выбор $2k$ рёбер при фиксированном $i$ (каждому ребру соответствуют два элемента списка смежности) потребует времени $O(k)$. Различных значений $i$ всего $n/(2k)$, значит, для построения всего решения нужно время $O(n)$. ■

Таким образом, для всякого kRS-графа задача НСЦ-k имеет решение.

**Пример 2.** Рассмотрим граф, заданный следующим списком смежности:

$$
\begin{array}{ll}
4: & 1, 2, 3; \\
5: & 1, 2, 3; \\
6: & 1, 2, 3; \\
1: & 4, 5, 6; \\
2: & 4, 5, 6; \\
3: & 4, 5, 6.
\end{array}
$$

В соответствии с процедурой, описанной в доказательстве теоремы 3, выберем рёбра $\{4, 1\}$, $\{4, 2\}$, $\{5, 2\}$, $\{5, 3\}$, $\{6, 1\}$ и $\{6, 3\}$. Получим вершинно-простой цикл $\{1-4-2-5-3-6-1\}$, который обходит все вершины графа.

## 4. Задача о семействе циклов в kS-орграфе

**Теорема 4.** Задача ОНСЦ-k на kS-орграфе может быть решена за время $O(n(k^2 + k) + n \log_2 n)$.

***Доказательство.*** В силу определения kS-орграфа на нём заданы два разбиения $\{U_1, \ldots, U_{n/k}\}$ и $\{V_1, \ldots, V_{n/k}\}$ множества вершин на $n/k$ подмножеств мощностью $k$ и все дуги, исходящие из вершин подмножества $V_i$, приходят только в вершины подмножества $U_i$, $i = 1, \ldots, n/k$. Таким образом, можно без ограничения общности утверждать, что список смежности орграфа состоит из $n/k$ блоков, обладающих структурой

$$\begin{aligned} &v_{i_1} : u_{i_{11}}, \ldots, u_{i_{1k_1}}, \\ &v_{i_2} : u_{i_{21}}, \ldots, u_{i_{2k_2}}, \\ &\ldots \\ &v_{i_k} : u_{i_{k1}}, \ldots, u_{i_{kk_k}}, \end{aligned}$$

где $i_{ab}$ — номера вершин подмножества $U_i$ (среди них могут быть и равные, количество вершин в строке не превосходит $k$); $i_j$ — номера вершин подмножества $V_i$ (попарно различные).

Так как из определения kS-орграфа следует, что в каждом таком блоке есть хотя бы одна строка, содержащая $k$ элементов, то есть все элементы подмножества $U_i$, можно ввести операцию дополнения kS-орграфа до kRS-орграфа. Для этого в каждой строке блока длиной меньше $k$ добавляются фиктивные дуги, приходящие в вершины, номера которых есть в подмножестве $U_i$, но отсутствуют в данной строке. Данное преобразование осуществимо за время $n/k(O(k^2)) = O(kn)$, где $O(k^2)$ — наибольшее возможное количество дуг в блоке.

Далее будем решать на полученном kRS-орграфе задачу ОНСЦ-k с помощью алгоритма, описанного в доказательстве теоремы 1, при следующем ограничении: паросочетания не должны содержать фиктивных дуг. Назначим этим дугам вес $-n \max\limits_{(v,u)\in E} |w(v,u)|$, тогда вес любого паросочетания, не содержащего фиктивных дуг, будет заведомо больше веса любого паросочетания, включающего хотя бы одну такую дугу. К времени выполнения алгоритма добавляется время преобразования орграфа, итого получим $O(nk^2 + n\log_2 n) + O(kn) = O(n(k^2 + k) + n\log_2 n)$. ■

**Пример 3.** Пусть $q = 10$. Рассмотрим орграф, заданный следующим списком смежности (вес соответствующей дуги указан в фигурных скобках):

$$\begin{aligned} 4: &\ 2\{1\}; \\ 5: &\ 1\{9\}, 3\{-2\}; \\ 6: &\ 1\{2\}, 2\{3\}, 3\{-8\}; \\ 1: &\ 6\{1\}; \\ 2: &\ 4\{-7\}, 5\{-1\}, 6\{10\}; \\ 3: &\ 4\{5\}. \end{aligned}$$

Произведём дополнение до kRS-орграфа. Пометим фиктивные дуги штрихом и назначим им вес, равный наибольшему по модулю весу дуги в исходном орграфе, взятому со знаком «минус» и умноженному на число вершин:

$$\begin{aligned} 4: &\ 1'\{-60\}, 2\{1\}, 3'\{-60\}; \\ 5: &\ 1\{9\}, 2'\{-60\}, 3\{-2\}; \\ 6: &\ 1\{2\}, 2\{3\}, 3\{-8\}; \\ 1: &\ 4'\{-60\}, 5'\{-60\}, 6\{1\}; \\ 2: &\ 4\{-7\}, 5\{-1\}, 6\{10\}; \\ 3: &\ 4\{5\}, 5'\{-60\}, 6'\{-60\}. \end{aligned}$$

Приведём решение задачи о назначениях для каждого блока венгерским алгоритмом:

$$\begin{array}{ll} 1) & \max S_1 = w(4,2) + w(5,1) + w(6,3) = 2; \\ 2) & \max S_2 = w(1,6) + w(2,5) + w(3,4) = 5. \end{array}$$

Таким образом, семейство циклов с максимальным весом задаётся набором дуг $\{(4,2),(5,1),\ (6,3),(1,6),(2,5),(3,4)\}$. Оно состоит из цикла $1-6-3-4-2-5-1$; общий вес равен 7. Это меньше $q$, следовательно, задача не имеет решения.

Проверим решение, найдя максимальное семейство циклов поиском в глубину. Имеем следующие циклы:

$$\begin{array}{lll} \{1-6-1\}; & \{1-6-2-5-1\}; & \{1-6-3-4-2-5-1\}; \\ \{2-4-2\}; & \{2-5-3-4-2\}; & \{2-6-2\}; \\ \{2-6-3-4-2\}. & & \end{array}$$

Из них могут быть составлены семейства (указан общий вес):

$$\begin{array}{ll} \{1-6-3-4-2-5-1\} & (7); \\ \{1-6-1, 2-5-3-4-2\} & (6). \end{array}$$

**Следствие 2.** Задача НСЦ-k на kS-орграфе может быть решена за время $O(n(k^2+k) + n\log_2 n)$.

***Доказательство.*** Дополним kS-орграф до kRS-орграфа. Применим алгоритм для решения задачи ОНСЦ-k с модификацией для учёта фиктивных дуг, при этом примем $q = -\infty$. Таким образом, получаем время $O(n(k^2+k) + n\log_2 n)$. ■

**Пример 4.** Рассмотрим орграф, заданный списком смежности:

$$\begin{array}{ll} 4: & 2; \\ 5: & 1,3; \\ 6: & 1,2,3; \\ 1: & 6; \\ 2: & 4,5,6; \\ 3: & 4. \end{array}$$

Произведём дополнение до kRS-орграфа; фиктивные дуги отмечены штрихом:

$$\begin{array}{ll} 4: & 1', 2, 3'; \\ 5: & 1, 2', 3; \\ 6: & 1, 2, 3; \\ 1: & 4', 5', 6; \\ 2: & 4, 5, 6; \\ 3: & 4, 5', 6'. \end{array}$$

Допустимые наборы дуг в первом и во втором блоке следующие:

$$\begin{array}{lll} 1) & (4,2),(5,1),(6,3); & (4,2),(5,3),(6,1); \\ 2) & (1,6),(2,5),(3,4). & \end{array}$$

Выберем любой из наборов первого блока (например, второй) и совместим с единственным набором из второго, получим семество циклов $\{1-6-1, 2-5-3-4-2\}$. Задача решена.

## Заключение

Рассмотрены поисковый и оптимизационный варианты задачи о поиске такого семейства непересекающихся простых циклов в орграфах класса kRS и kS, которое покрывает все вершины орграфа. Показана принадлежность задачи в обоих вариантах классу полиномиально разрешимых задач P, предложены алгоритмы, находящие решение поисковой и оптимизационной задач о максимизации веса семейства циклов за время $O(nk^2 + n\log_2 n)$ и $O(n(k^2 + k) + n\log_2 n)$ соответственно; показано, что на kRS-графах и kRS-орграфах поисковая задача может быть решена за линейное время вне зависимости от значения параметра $k$, а на kS-орграфах задача является полиномиальной со сложностью $O(n(k^2+k)+n\log_2 n)$. Поскольку решение оптимизационной задачи осуществляется путём сокращённого перебора по экспоненциальному пространству поиска, можно сделать предположение о существовании параметрически полиномиального алгоритма поиска гамильтонова цикла на рассматриваемых классах орграфов, так как среди решений задач НСЦ-k и ОНСЦ-k могут быть гамильтоновы циклы.

## ЛИТЕРАТУРА


1. *Karp R. M.* Reducibility among combinatorial problems // R. E. Miller, J. W. Thatcher, J. D. Bohlinger (eds). Complexity of Computer Computations. The IBM Research Symposia Series. Boston: Springer, 1972. P. 85–103.
2. *Akiyama T., Nisizeki T., and Saito N.* NP-completeness of the Hamiltonian cycle problem for bipartite graphs // J. Inform. Processing. 1981. V. 3. No. 2. P. 73–76.
3. *Itai A., Papadimitiou Ch., and Szwarcfiter J.* Hamiltonian paths in grid graphs // SIAM J. Computing. 1982. V. 4. No. 11. P. 676–686.
4. *Buro M.* Simple Amazons endgames and their connection to Hamilton circuits in cubic subgrid graphs // LNCS. 2000. V. 2063. P. 250–261.
5. *Plesńik J.* The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two // Inform. Process. Lett. 1979. V. 8. No. 4. P. 199–201.
6. *Chiba N. and Nishizeki T.* The Hamiltonian cycle problem is linear-time solvable for 4-connected planar graphs // J. Algorithms. 1989. V. 10. No. 2. P. 187–211.
7. *Dirac G. A.* Some theorems on abstract graphs // Proc. London Math. Soc. 1952. V. 2. No. 3. P. 69–81.
8. *Ore O.* Note on Hamiltonian circuits // American Math. Monthly. 1960. V. 67. P. 55.
9. *Ghouila-Houri A.* Une condition suffisante d'existence d'un circuit Hamiltonien // Comptes Rendus de l'Académie des Science Paris. 1960. V. 251. P. 495–497.
10. *Woodall D.* Sufficient conditions for cycles in digraphs // Proc. London Math. Soc. 1972. V. 24. P. 739–755.
11. *Christofides D., Keevash P., Kühn D., and Osthus D.* A semi-exact degree condition for Hamiltonian cycles in digraphs // SIAM J. Discrete Math. 2010. V. 24. No. 3. P. 709–756.
12. *Keevash P., Kühn D., and Osthus D.* An exact minimum degree condition for Hamiltonian cycles in oriented graphs // J. London Math. Soc. 2009. V. 79. No. 1. P. 144–166.
13. *Kelly L., Kühn D., and Osthus D.* A Dirac-type result on Hamiltonian cycles in oriented graphs // Combinatorics, Probability and Computing. 2008. V. 17. No. 5. P. 689–709.
14. *Björklund A., Husfeldt T., and Khanna S.* Approximating longest directed paths and cycles // Automata, Languages and Programming. 2004. V. 3142. P. 222–233.
15. *Gabow H. N. and Nie S.* Finding long paths, cycles and circuits // LNCS. 2008. V. 5369. P. 752–763.
16. *Zamfirescu T.* On longest paths and circuits in graphs // Mathematica Scandinavica. 1976. V. 38. P. 211–239.

17. *Харари Ф.* Теория графов. М.: Едиториал УРСС, 2003. 296 с.
18. *Медведев А. А.* Поиск семейства простых циклов в орграфе с полустепенями вершин, не превосходящими 2 // Интеллектуальные системы. Теория и приложения. 2022. Т. 26. № 3. С. 150–164.
19. *Kuhn H. W.* Variants of the Hungarian method for assignment problems // Naval Research Logistics Quarterly. 1956. V. 3. P. 253–258.

REFERENCES

1. *Karp R. M.* Reducibility among combinatorial problems. R. E. Miller, J. W. Thatcher, J. D. Bohlinger (eds). Complexity of Computer Computations. The IBM Research Symposia Series. Boston, Springer, 1972, pp. 85–103.
2. *Akiyama T., Nisizeki T., and Saito N.* NP-completeness of the Hamiltonian cycle problem for bipartite graphs. J. Inform. Processing, 1981, vol. 3, no. 2, pp. 73–76.
3. *Itai A., Papadimitiou Ch., and Szwarcfiter J.* Hamiltonian paths in grid graphs. SIAM J. Computing, 1982, vol. 4, no. 11, pp. 676–686.
4. *Buro M.* Simple Amazons endgames and their connection to Hamilton circuits in cubic subgrid graphs. LNCS, 2000, vol. 2063, pp. 250–261.
5. *Plesńik J.* The NP-completeness of the Hamiltonian cycle problem in planar digraphs with degree bound two. Inform. Process. Lett., 1979, vol. 8, no. 4, pp. 199–201.
6. *Chiba N. and Nishizeki T.* The Hamiltonian cycle problem is linear-time solvable for 4-connected planar graphs. J. Algorithms, 1989, vol. 10, no. 2, pp. 187–211.
7. *Dirac G. A.* Some theorems on abstract graphs. Proc. the London Math. Soc., 1952, vol. 2, no. 3, pp. 69–81.
8. *Ore O.* Note on Hamiltonian circuits. American Math. Monthly, 1960, vol. 67, p. 55.
9. *Ghouila-Houri A.* Une condition suffisante d'existence d'un circuit Hamiltonien [A sufficient condition for existence of a Hamiltonian circuit]. Comptes Rendus de l'Académie des Science Paris, 1960, vol. 251, pp. 495–497. (in French)
10. *Woodall D.* Sufficient conditions for cycles in digraphs. Proc. London Math. Soc., 1972, vol. 24, pp. 739–755
11. *Christofides D., Keevash P., Kühn D., and Osthus D.* A semi-exact degree condition for Hamiltonian cycles in digraphs. SIAM J. Discrete Math., 2010, vol. 24, no. 3, pp. 709–756.
12. *Keevash P., Kühn D., and Osthus D.* An exact minimum degree condition for Hamiltonian cycles in oriented graphs. J. London Math. Soc., 2009, vol. 79, no. 1, pp. 144–166.
13. *Kelly L., Kühn D., and Osthus D.* A Dirac-type result on Hamiltonian cycles in oriented graphs. Combinatorics, Probability and Computing, 2008, vol. 17, no. 5, pp. 689–709.
14. *Björklund A., Husfeldt T., and Khanna S.* Approximating longest directed paths and cycles. Automata, Languages and Programming, 2004, vol. 3142, pp. 222–233.
15. *Gabow H. N. and Nie S.* Finding long paths, cycles and circuits. LNCS, 2008, vol. 5369, pp. 752–763.
16. *Zamfirescu T.* On longest paths and circuits in graphs. Mathematica Scandinavica, 1976, vol. 38, pp. 211–239.
17. *Harary F.* Graph Theory. N.Y., Addison-Wesley Publ., 1969. 283 p.
18. *Medvedev A. A.* Poisk semeystva prostykh tsiklov v orgrafe s polustepenyami vershin, ne prevoskhodyashchimi 2 [Finding a family of simple circuits in an digraph with semidegree bound 2]. Intellektual'nyye Sistemy. Teoriya i Prilozheniya, 2022, vol. 26. no. 3, pp. 150–164. (in Russian)
19. *Kuhn H. W.* Variants of the Hungarian method for assignment problems. Naval Research Logistics Quarterly, 1956, vol. 3, pp. 253–258.

# ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ ДИСКРЕТНЫХ АВТОМАТОВ

УДК 519.711 DOI 10.17223/20710410/60/8

## SYNTHESIS OF COMBINATIONAL CIRCUITS BY MEANS OF BI-DECOMPOSITION OF BOOLEAN FUNCTIONS

Yu. V. Pottosin

*United Institute of Informatics Problems, National Academy of Sciences of Belarus, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus*

**E-mail:** pott@newman.bas-net.by

The problem of combinational circuits synthesis in the basis of two-input gates is considered. Those gates are AND, OR, NAND and NOR. A method for solving this problem by means of Boolean functions bi-decomposition is suggested. The method reduces the problem to the search for a weighted two-block cover of the orthogonality graph of ternary matrice rows representing the given Boolean function by complete bipartite subgraphs (bi-cliques). Each bi-clique in the obtained cover is assigned in a certain way with a set of variables that are the arguments of the function. This set is the weight of the bi-clique. Each of those bi-cliques defines a Boolean function whose arguments are the variables assigned to it. The functions obtained in such a way constitute the required decomposition. The process of combinational circuit synthesis consists in successively applying bi-decomposition to the functions obtained. The method for two-block covering the orthogonality graph of ternary matrice rows is described.

**Keywords:** *synthesis of combinational circuits, Boolean function, decomposition of Boolean functions, ternary matrix, complete bipartite subgraph, two-block cover.*

## СИНТЕЗ КОМБИНАЦИОННЫХ СХЕМ ПУТЁМ АЛГЕБРАИЧЕСКОЙ ДЕКОМПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ

Ю. В. Поттосин

*Объединенный институт проблем информатики НАН Беларуси, Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь*

Рассматривается задача синтеза комбинационных схем в базисе двухвходовых элементов И, ИЛИ, И–НЕ и ИЛИ–НЕ. Предложен метод её решения с помощью применения алгебраической декомпозиции булевых функций. Метод сводит решение задачи к поиску взвешенного двублочного покрытия полными двудольными подграфами (бикликами) графа ортогональности строк троичной матрицы, представляющей заданную булеву функцию. Каждой биклике в полученном покрытии определённым образом приписывается в качестве веса множество переменных,

являющихся аргументами заданной функции. Каждая из этих двух биклик определяет булеву функцию с аргументами, приписанными соответствующей бикли-ке. Полученные таким образом функции составляют искомое разложение. Процесс синтеза комбинационной схемы состоит из последовательного применения алгебраической декомпозиции к получаемым функциям. Описан способ получения двублочного покрытия бикликами графа ортогональности строк троичной матрицы.

**Ключевые слова:** *синтез комбинационных схем, булева функция, декомпозиция булевых функций, троичная матрица, полный двудольный подграф, двублочное покрытие.*

## 1. Introduction

The problem of bi-decomposition of a Boolean function is set as follows. Given a Boolean function $y = f(\mathbf{x})$, where the components of the vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ are Boolean variables constituting a set $X$, a superposition $f(\mathbf{x}) = \varphi(g_1(\mathbf{z}_1), g_2(\mathbf{z}_2))$ must be obtained, where the components of the vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ are the variables from the sets $Z_1 \subset X$ and $Z_2 \subset X$ respectively. The kind of the function $\varphi$ in two variables is given as well. It can be any of the ten Boolean functions which essentially depend on both arguments and are represented by the operations of logic algebra. Usually, the sets $Z_1$ and $Z_2$ are given and $Z_1 \cap Z_2 = \varnothing$. Such a decomposition is called *disjoint*, otherwise it is called *non-disjoint*, where the condition $Z_1 \cap Z_2 = \varnothing$ is optional, but some restrictions on the cardinalities of $Z_1$ and $Z_2$ can be imposed.

There are known examples of applying methods for bi-decomposition to reduce the delay of combinational circuits [1, 2] and in the synthesis of circuits in the base of FPGA [3]. The problem of bi-decomposition with $\varphi$ expressed by XOR operation and given partition $(Z_1, Z_2)$ has been considered in [4], where the logical equations are used. The probability of existence of any decomposition of a completely specified Boolean function is very low, but there is another situation with incompletely specified (partial) functions, especially when the domain of their specification is a very small part of Boolean space of arguments. Therefore, the main attention is paid to the decomposition (including bi-decomposition) of partial Boolean functions. Such a case of disjoint bi-decomposition with a given partition $(Z_1, Z_2)$ has been investigated in detail in [5]. A method for bi-decomposition (disjoint or non-disjoint) of partial Boolean functions with non-given partition $(Z_1, Z_2)$ is described in [6], where only the demand is made that the numbers of arguments of $g_1$ and $g_2$ be less than the number of arguments of $f$. This method can be applied also for completely specified functions, but as it was said above, the probability that the mentioned demand can be fulfilled is very low. At the same time, if $\varphi$ is in the class of non-linear Boolean functions, then the functions $g_1$ and $g_2$ turn out to be simpler than $f$ in the sense that the amount of their dependence on some arguments is less than that of $f$. This parameter has been considered in [7]. The amount of dependence of $f$ on $x_i$ is the number of pairs $(\mathbf{x}^*, \mathbf{x}^{**})$ of adjacent values of the vector $\mathbf{x}$ with different values of $x_i$, where $f(\mathbf{x}^*) \neq f(\mathbf{x}^{**})$. Moreover, if $g_i$ $(i = 1, 2)$ has the same number of arguments as the completely specified function $f$, then $g_i$ will be partial in any case. This increases the probability of its decomposability.

In this paper, we propose a method for synthesizing combinational circuits based on two-input gates that implement nonlinear Boolean functions. These gates are NOR, NAND and OR, AND with variable complements available. The method is based on successive application of bi-decomposition to the functions using the approach described in [6].

## 2. The proposed approach

Let a Boolean function $f(\mathbf{x})$ (completely or partially specified) be given by two sets: $M^1$ is a domain of Boolean space, where it has value 1, and $M^0$ is a domain of Boolean space, where it has value 0. We represent these sets by ternary matrices $\mathbf{M}_1$ and $\mathbf{M}_0$, respectively, whose rows represent the intervals in $M^1$ and $M^0$, and columns correspond to arguments $x_1, x_2, \ldots, x_n$ of the given function.

Let us consider a complete bipartite graph $G = (V^1, V^0, E)$ whose vertices from $V^1$ correspond to the rows of $\mathbf{M}_1$ and vertices from $V^0$ correspond to the rows of $\mathbf{M}_0$. The edges of $G$ are all the pairs of vertices $v^1v^0$ ($v^1 \in V^1$, $v^0 \in V^0$) corresponding to orthogonal rows of the matrices. Two ternary vectors are orthogonal according to a component $x_i$ if $x_i = 1$ in one of them and $x_i = 0$ in the other [8]. Naturally, any row-vector $\mathbf{m}^1$ of $\mathbf{M}^1$ is orthogonal to any row-vector $\mathbf{m}^0$ of $\mathbf{M}^0$. So the bipartite graph $G$ is complete.

We assign the elementary disjunction $x_i \vee x_j \vee \ldots \vee x_k$ of the arguments of the given function to each edge $v^1v^0$ of $G$ if the row-vectors $\mathbf{m}^1$ and $\mathbf{m}^0$ of $\mathbf{M}^1$ and $\mathbf{M}^0$ corresponding to the vertices $v^1$ and $v^0$ are orthogonal according to the components $x_i$, $x_j$, …, $x_k$. Each complete bipartite subgraph (*bi-clique*) of the graph $G$ is assigned with conjunctive normal form (CNF) having, as its terms, the elementary disjunctions assigned to the edges from that bi-clique. After removing possibly absorbed terms, we transform the obtained CNF into disjunctive normal form (DNF) and assign a term of minimal rank from the DNF to the corresponding bi-clique.

Let a Boolean function $f(\mathbf{x})$ (completely or partially specified) must be expressed as $f(\mathbf{x}) \preceq \varphi(g_1(\mathbf{z}_1), g_2(\mathbf{z}_2))$, where $\varphi$ is a Boolean function in two variables, $g_1$ and $g_2$, that are a functions of vectorial variables $\mathbf{z}_1$ and $\mathbf{z}_2$ being parts of the vector $\mathbf{x}$, and symbol "$\preceq$" denotes the relation of realization. A Boolean function $\varphi$ (completely or partially specified) *realizes* a partial Boolean function $f$ if $\varphi$ takes the same values as $f$ in the entire domain of $f$ [9]. Further, it is convenient to consider the function equality relation as a special case of the realization, and so we use the equality symbol "$=$" for denoting realization as well.

The functions $g_1$ and $g_2$ are constructed in the following way. Choose two bi-cliques, $B_1 = (V_1^1, V_1^0, E_1)$ and $B_2 = (V_2^1, V_2^0, E_2)$, in the graph $G$ so that any edge of $G$ would be at least in one of the sets $E_1$ or $E_2$. In other words, the bi-cliques $B_1$ and $B_2$ must cover the entire set $E$ with their edges. It is sufficient to define bi-cliques $B_1$ and $B_2$ with pairs $(V_1^1, V_1^0)$ and $(V_2^1, V_2^0)$, because any vertex in one part of a bi-clique is connected to all the vertices in the other part with edges.

The arguments of the function $g_i$, $i \in \{1, 2\}$, are the variables that are assigned to the bi-clique $B_i$. The set $M_i^1$ of values of the vectorial variable $\mathbf{z}_i$ for which $g_i = 1$ consists of the parts of the vectors from $M^1$ or $M^0$ (depending on the kind of $\varphi$) that correspond to the vertices in $V_i^1$. The parts of these vectors are defined by the variables assigned to the bi-clique $B_i$, i.e., these variables are the components of the vector $\mathbf{z}_i$. Similarly, the set $M_i^0$ is formed from parts of the vectors that correspond to the vertices from $V_i^0$. Thus, each vector from $M^1$ or from $M^0$ corresponds to a pair of values of $g_1$ and $g_2$. If this pair corresponds to a vector in $M^1$, then it is an element of the set $M_\varphi^1$, where $\varphi = 1$. If it corresponds to a vector in $M^0$, then it is an element of the set $M_\varphi^0$. So the function $\varphi$ is defined. Note the pairs $(V_1^1, V_1^0)$ and $(V_2^1, V_2^0)$ should be considered as ordered because they are related to the values of $g_1$ and $g_2$.

The described method involves the similar decomposition of $g_1$, $g_2$ and the next obtained functions until obtaining functions in two variables from the set $X = \{x_1, x_2, \ldots, x_n\}$ of the arguments of the given function.

The method for bi-decomposition of Boolean functions described in [6] is based on the finding of a cover of the graph $G$ with two bi-cliques having the best weight that leads to the minimum sum of arguments of the superposition functions. The cover is searched for among possibly many maximal bi-cliques of $G$ [10] which takes much time without guarantee of obtaining an optimal circuit in our case. The synthesis of combinational circuits by the proposed method involves multiple application of performing the cover task. Therefore, a heuristic method for covering is used, which does not minimize that sum, but takes less time for its realization.

## 3. Covering the graph $G$ by two bi-cliques

The Table shows the values that $g_1$ and $g_2$ must have at the given values of the function $\varphi$ and at the given kinds of it. It is seen that there must be $V_1^1 = V_2^1 = V^1$ for AND operation, $V_1^0 = V_2^0 = V^0$ for OR operation, $V_1^1 = V_2^1 = V^0$ for NAND operation, and $V_1^0 = V_2^0 = V^1$ for NOR operation.

| AND | | | OR | | | NAND | | | NOR | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi$ | $g_1$ | $g_2$ | $\varphi$ | $g_1$ | $g_2$ | $\varphi$ | $g_1$ | $g_2$ | $\varphi$ | $g_1$ | $g_2$ |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | – | 0 | 1 | – | 1 | 1 | – | 0 | 0 | – | 1 |
| 0 | 0 | – | 1 | 1 | – | 1 | 0 | – | 0 | 1 | – |

So one of the bi-cliques is always defined by the kind of $\varphi$ as one of the parts of the complete bipartite graph $G$ and it is one of the parts of both $B_1$ and $B_2$. The other parts of $B_1$ and $B_2$ are formed as blocks of a partition of the other part of $G$. For instance, if $V_1^0 = V_2^0 = V^1$, then $B_1 = (V_1^1, V^1)$ and $B_2 = (V_2^1, V^1)$, where $V_1^1 \cup V_2^1 = V^0$ and $V_1^1 \cap V_2^1 = \varnothing$.

The initial information to obtain the desired cover of $G$ is the set of *starred graphs* that are subgraphs of $G$. A starred graph (or *a star*) is a complete bipartite graph $K_{1,n}$ [11]. Its one-element part is its *center*. In our case, the set of starred graphs is the set of all bi-cliques of $G$ having one part as one-element set with $v \in V^0$ or $v \in V^1$, and the other part as $V^1$ or $V^0$, respectively. We call them *starred bi-cliques*.

As it was said above, each bi-clique is assigned with CNF that is transformed into DNF. We choose a term $K$ of minimum rank from DNF and assign the set $X_i$ of variables from $K$ to the corresponding starred bi-clique $B_i$. Two starred bi-cliques, $B_i$ and $B_j$, with the intersection $X_i \cap X_j$ of minimal cardinality are chosen among all the pairs of starred bi-cliques under consideration. If there are several variants of such pairs, the preference is given to the sets $X_i$ and $X_j$ of maximal cardinality. Naturally, the variant $X_i \cap X_j = \varnothing$ is desirable. The pair $(B_i, B_j)$ is taken as the initial value of the pair of bi-cliques that must cover the graph $G$, and we denote it $(B_1, B_2)$.

The subsequent process is successive extending the parts of bi-cliques $B_1$ and $B_2$ that were one-element sets by means of adding the vertices which are the centers of the considered starred bi-cliques. The sets $X_1$ and $X_2$ change correspondingly. For example, let $B_1 = (V_1^1, V_1^0)$, $B_2 = (V_2^1, V_2^0)$, $V_1^1 \cup V_2^1 = V^0$ and the set $V'$ consists of the vertices of $G$ which do not belong to either $V_1^0$ or $V_2^0$. Let the vertex $v_k \in V'$ be the center of a starred bi-clique $B_k$ and $V_i^0$ $(i = 1, 2)$ be such a set that cardinality of $X_i \cup X_k$ differs from that of $X_i$ or $X_k$ minimally among all bi-cliques $B_k$ corresponding the vertices belonging to $V'$. The set $V_i^0$ changes to $V_i^0 \cup \{v_k\}$, and the vertex $v_k$ is removed from $V'$. The process comes to the end when $V' = \varnothing$. The pair $(B_1, B_2)$ will be the desired cover of $G$.

## 4. Synthesis of a combinational circuit in the NOR basis

Let's build a combinational circuit of NOR gates that implements the completely specified Boolean function $f(x_1, x_2, x_3, x_4, x_5)$. The function is given by the following matrices (through numeration is used):

$$\mathbf{M}^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{matrix} \\ \left[\begin{array}{ccccc} - & - & 1 & 1 & - \\ 0 & - & 1 & - & - \\ - & 1 & - & 1 & - \\ 0 & 0 & - & - & - \\ - & 1 & 0 & - & 0 \\ 1 & 1 & - & - & 1 \\ 1 & - & 0 & 0 & 1 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix}; \qquad \mathbf{M}^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{matrix} \\ \left[\begin{array}{ccccc} 0 & 1 & 0 & 0 & 1 \\ 1 & - & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & - \\ 1 & 0 & 1 & 0 & - \end{array}\right] \end{array} \begin{matrix} 8 \\ 9 \\ 10 \\ 11 \end{matrix}.$$

To reduce the size the bipartite graphs, it would be better to represent the domain of the function by the minimum number of intervals. The complete bipartite graph $G = (V^1, V^0, E)$ is given by matrix $\mathbf{G}$ similar to an adjacency matrix:

$$\mathbf{G} = \begin{array}{c} \begin{matrix} 8 & 9 & 10 & 11 \end{matrix} \\ \left[\begin{array}{cccc} x_3 \vee x_4 & x_4 & x_3 & x_4 \\ x_3 & x_1 & x_1 \vee x_3 & x_1 \\ x_4 & x_4 & x_2 & x_2 \vee x_4 \\ x_2 & x_1 & x_1 & x_1 \\ x_5 & x_3 & x_2 & x_2 \vee x_3 \\ x_1 & x_5 & x_2 & x_2 \\ x_1 & x_3 \vee x_5 & x_4 & x_3 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix}.$$

The rows of $\mathbf{G}$ correspond to the vertices in the set $V^1 = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ (to the rows of $\mathbf{M}^1$), and the columns — to the vertices in the set $V^0 = \{v_8, v_9, v_{10}, v_{11}\}$ (to the rows of $\mathbf{M}^0$). The elementary disjunction or single variable assigned to the edge $v_i v_j$ is at the $i$-th row and $j$-th column of $\mathbf{G}$.

The bi-cliques $B_1 = (V_1^1, V_1^0)$ and $B_2 = (V_2^1, V_2^0)$ covering the graph $G$ have a common part. According to Table on page 98, for the NOR basis, we have $V_1^0 = V_2^0 = V^1$. The starred bi-cliques with the assigned variables are the following:

$$\begin{array}{lcl} (\{v_8\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}) & - & x_1 x_2 x_3 x_4 x_5; \\ (\{v_9\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}) & - & x_1 x_3 x_4 x_5; \\ (\{v_{10}\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}) & - & x_1 x_2 x_3 x_4; \\ (\{v_{11}\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}) & - & x_1 x_2 x_3 x_4. \end{array}$$

The first step, decomposition into functions $g_1$ and $g_2$, can be easy made because to reduce the total number of arguments one should form bi-cliques $B_1 = (\{v_8, v_9\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\})$ and $B_2 = (\{v_{10}, v_{11}\}, \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\})$ with corresponding sets of variables $\{x_1, x_2, x_3, x_4, x_5\}$ and $\{x_1, x_2, x_3, x_4\}$. The given function $f(x_1, x_2, x_3, x_4, x_5)$ is decomposed into two functions, $g_1(x_1, x_2, x_3, x_4, x_5)$ and $g_2(x_1, x_2, x_3, x_4)$, linked by NOR operation (Pierce function): $f = \varphi = g_1 \uparrow g_2$. They can be given by the matrices $\mathbf{M}_1^1$, $\mathbf{M}_1^0$ and $\mathbf{M}_2^1$, $\mathbf{M}_2^0$, the lower indices of which coincide with the indices of the functions. The matrices look as follows, where $\mathbf{M}_2^0$ represents the minimum number of intervals with value 0 of $g_2$:

$$\mathbf{M}_1^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{matrix} \\ \left[\begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & - & 1 & 0 & 0 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \qquad \mathbf{M}_1^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{matrix} \\ \left[\begin{matrix} - & - & 1 & 1 & - \\ - & 1 & - & 1 & - \\ 0 & 0 & - & - & - \\ - & 1 & 0 & - & 0 \\ 1 & - & 0 & 0 & 1 \\ 0 & - & - & - & 0 \\ - & 1 & 1 & - & 1 \end{matrix}\right] \end{array} \begin{matrix} 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{matrix};$$

$$\mathbf{M}_2^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \qquad \mathbf{M}_2^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} - & - & 1 & 1 \\ - & - & 0 & 0 \\ 0 & - & - & - \\ - & 1 & - & - \end{matrix}\right] \end{array} \begin{matrix} 3 \\ 4 \\ 5 \\ 6 \end{matrix}.$$

The function $g_2$ is specified in the entire Boolean argument space, and $g_1$ is a partial one. The value of $g_1$ is not defined at $(x_1, x_2, x_3, x_4, x_5) = (1, 0, 1, 0, 1), (1, 0, 0, 0, 0)$ and the interval represented by vector $(1, 0, 0, 1, -)$. For the decomposition of $g_1$ and $g_2$, the complete bipartite graphs $G_1$ and $G_2$ are constructed with the parts $V^{11} = \{v_1^1, v_2^1\}$, $V^{01} = \{v_3^1, v_4^1, v_5^1, v_6^1, v_7^1, v_8^1, v_9^1\}$ and $V^{12} = \{v_1^2, v_2^2\}$, $V^{02} = \{v_3^2, v_4^2, v_5^2, v_6^2\}$, respectively. The graphs $G_1$ and $G_2$ are given by the matrices $\mathbf{G}_1$ and $\mathbf{G}_2$:

$$\mathbf{G}_1 = \begin{array}{c} \begin{matrix} 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{matrix} \\ \left[\begin{matrix} x_3 \vee x_4 & x_4 & x_2 & x_5 & x_1 & x_5 & x_3 \\ x_4 & x_4 & x_1 & x_3 & x_3 \vee x_5 & x_1 & x_5 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{G}_2 = \begin{array}{c} \begin{matrix} 3 & 4 & 5 & 6 \end{matrix} \\ \left[\begin{matrix} x_3 & x_4 & x_1 & x_2 \\ x_4 & x_3 & x_1 & x_2 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}.$$

The starred bi-cliques of $G_1$ (left) and $G_2$ (right) with assigned variables are

$$\begin{array}{lcl} (\{v_3^1\}, \{v_1^1, v_2^1\}) & - & x_4; \\ (\{v_4^1\}, \{v_1^1, v_2^1\}) & - & x_4; \\ (\{v_5^1\}, \{v_1^1, v_2^1\}) & - & x_1x_2; \\ (\{v_6^1\}, \{v_1^1, v_2^1\}) & - & x_3x_5; \\ (\{v_7^1\}, \{v_1^1, v_2^1\}) & - & x_1(x_3 \vee x_5); \\ (\{v_8^1\}, \{v_1^1, v_2^1\}) & - & x_1x_5; \\ (\{v_9^1\}, \{v_1^1, v_2^1\}) & - & x_3x_5; \end{array} \qquad \begin{array}{lcl} (\{v_3^2\}, \{v_1^2, v_2^2\}) & - & x_3x_4; \\ (\{v_4^2\}, \{v_1^2, v_2^2\}) & - & x_3x_4; \\ (\{v_5^2\}, \{v_1^2, v_2^2\}) & - & x_1; \\ (\{v_6^2\}, \{v_1^2, v_2^2\}) & - & x_2. \end{array}$$

The function $g_2$ is decomposed trivially as the given function $f$. The bi-cliques $(\{v_3^2, v_4^2\}, \{v_1^2, v_2^2\})$ with variables $x_3, x_4$ and $(\{v_5^2, v_6^2\}, \{v_1^2, v_2^2\})$ with variables $x_1, x_2$ cover the graph $G_2$. So $g_2 = g_3(x_3, x_4) \uparrow g_4(x_1, x_2)$, and $g_3$ and $g_4$ are given by the following matrices obtained from $\mathbf{M}_2^1$ and $\mathbf{M}_2^0$:

$$\mathbf{M}_3^1 = \begin{array}{c} \begin{matrix} x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix}\right] \end{array}; \qquad \mathbf{M}_3^0 = \begin{array}{c} \begin{matrix} x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}\right] \end{array}; \qquad \mathbf{M}_4^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 \end{matrix} \\ \left[\begin{matrix} 0 & - \\ - & 1 \end{matrix}\right] \end{array}; \qquad \mathbf{M}_4^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 \end{matrix} \\ \left[\begin{matrix} 1 & 0 \end{matrix}\right] \end{array}.$$

Finally, for $g_2$, we have $g_3 = x_3x_4 \vee \overline{x}_3\overline{x}_4 = (x_3 \uparrow \overline{x_4}) \uparrow (\overline{x}_3 \uparrow x_4)$ and $g_4 = \overline{x}_1 \vee x_2 = (\overline{x}_1 \uparrow x_2) \uparrow (\overline{x}_1 \uparrow x_2)$.

To decompose $g_1$, the way to cover graph $G_1$ by two bi-cliques described in Section 3 can be applied. The initial meanings of bi-cliques $B_1$ and $B_2$ are $(\{v_5^1\}, \{v_1^1, v_2^1\})$ and $(\{v_6^1\}, \{v_1^1, v_2^1\})$, because the intersection of $X_1 = \{x_1, x_2\}$ and $X_2 = \{x_3, x_5\}$ is empty and these sets have the maximum cardinality. As a result of the next step, we have

$$(\{v_5^1\}, \{v_1^1, v_2^1\}) - x_1x_2, \qquad (\{v_6^1, v_9^1\}, \{v_1^1, v_2^1\}) - x_3x_5.$$

The sequence of transformations of $B_1$ and $B_2$ is presented below, where the last row presents the desired cover of $G$:

$$
\begin{array}{llll}
(\{v_3^1, v_5^1\}, \{v_1^1, v_2^1\}) & - & x_1x_2x_4; & (\{v_6^1, v_9^1\}, \{v_1^1, v_2^1\}) \quad - \quad x_3x_5; \\
(\{v_3^1, v_5^1\}, \{v_1^1, v_2^1\}) & - & x_1x_2x_4; & (\{v_6^1, v_7^1, v_9^1\}, \{v_1^1, v_2^1\}) \quad - \quad x_1x_3x_5; \\
(\{v_3^1, v_4^1, v_5^1\}, \{v_1^1, v_2^1\}) & - & x_1x_2x_4; & (\{v_6^1, v_7^1, v_8^1, v_9^1\}, \{v_1^1, v_2^1\}) \quad - \quad x_1x_3x_5.
\end{array}
$$

The $g_1(x_1, x_2, x_3, x_4, x_5)$ is decomposed into two functions, $g_5(x_1, x_2, x_4)$ and $g_6(x_1, x_3, x_5)$, linked by NOR operation: $g_1 = g_5 \uparrow g_6$. They can be given by the matrices $\mathbf{M}_5^1$, $\mathbf{M}_5^0$ and $\mathbf{M}_6^1$, $\mathbf{M}_6^0$:

$$
\mathbf{M}_5^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_4 \end{matrix} \\ \left[\begin{array}{ccc} - & - & 1 \\ 0 & 0 & - \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad
\mathbf{M}_5^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_4 \end{matrix} \\ \left[\begin{array}{ccc} 0 & 1 & 0 \\ 1 & - & 0 \end{array}\right] \end{array} \begin{matrix} 3 \\ 4 \end{matrix}; \quad
\mathbf{M}_6^1 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 1 & 0 & - \\ 0 & - & 0 \\ - & 1 & 1 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}; \quad
\mathbf{M}_6^0 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}\right] \end{array} \begin{matrix} 4 \\ 5 \end{matrix}.
$$

The corresponding graphs $G_5$ and $G_6$ are given by the matrices $\mathbf{G}_5$ and $\mathbf{G}_6$:

$$
\mathbf{G}_5 = \begin{array}{c} \begin{matrix} 3 & 4 \end{matrix} \\ \left[\begin{array}{cc} x_4 & x_4 \\ x_2 & x_1 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad
\mathbf{G}_6 = \begin{array}{c} \begin{matrix} 4 & 5 \end{matrix} \\ \left[\begin{array}{cc} x_1 & x_3 \\ x_5 & x_1 \\ x_3 & x_5 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}.
$$

Graph $G_5$ is covered by bi-cliques $(\{v_3^5\}, \{v_1^5, v_2^5\})$ with variables $x_2, x_4$ and $(\{v_4^5\}, \{v_1^5, v_2^5\})$ with variables $x_1, x_4$. Then $g_5 = g_7(x_2, x_4) \uparrow g_8(x_1, x_4)$ and $g_7$ and $g_8$ are given by the following matrices:

$$
\mathbf{M}_7^1 = \begin{array}{c} \begin{matrix} x_2 & x_4 \end{matrix} \\ \left[\begin{array}{cc} 1 & 0 \end{array}\right] \end{array}; \quad
\mathbf{M}_7^0 = \begin{array}{c} \begin{matrix} x_2 & x_4 \end{matrix} \\ \left[\begin{array}{cc} - & 1 \\ 0 & - \end{array}\right] \end{array}; \quad
\mathbf{M}_8^1 = \begin{array}{c} \begin{matrix} x_1 & x_4 \end{matrix} \\ \left[\begin{array}{cc} 1 & 0 \end{array}\right] \end{array}; \quad
\mathbf{M}_8^0 = \begin{array}{c} \begin{matrix} x_1 & x_4 \end{matrix} \\ \left[\begin{array}{cc} - & 1 \\ 0 & - \end{array}\right] \end{array}.
$$

Hence, $g_7 = \overline{x}_2 \uparrow x_4$ and $g_8 = \overline{x}_1 \uparrow x_4$.

Graph $G_6$ is covered by bi-cliques $(\{v_4^6\}, \{v_1^6, v_2^6, v_3^6\})$ with variables $x_1, x_3, x_5$ and $(\{v_5^6\}, \{v_1^6, v_2^6, v_3^6\})$ with the same variables. Then $g_6 = g_9(x_1, x_3, x_5) \uparrow g_{10}(x_1, x_3, x_5)$ and $g_9$ and $g_{10}$ are given by the following matrices:

$$
\mathbf{M}_9^1 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 0 & 0 & 1 \end{array}\right] \end{array} 1; \quad
\mathbf{M}_9^0 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 1 & 0 & - \\ 0 & - & 0 \\ - & 1 & 1 \end{array}\right] \end{array} \begin{matrix} 2 \\ 3 \\ 4 \end{matrix}; \quad
\mathbf{M}_{10}^1 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 1 & 1 & 0 \end{array}\right] \end{array} 1; \quad
\mathbf{M}_{10}^0 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{ccc} 1 & 0 & - \\ 0 & - & 0 \\ - & 1 & 1 \end{array}\right] \end{array} \begin{matrix} 2 \\ 3 \\ 4 \end{matrix}.
$$

The corresponding graphs $G_9$ and $G_{10}$ are given by the matrices

$$
\mathbf{G}_9 = \begin{array}{c} \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \left[\begin{array}{ccc} x_1 & x_5 & x_3 \end{array}\right] \end{array} 1; \quad
\mathbf{G}_{10} = \begin{array}{c} \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \left[\begin{array}{ccc} x_3 & x_1 & x_5 \end{array}\right] \end{array} 1.
$$

Graph $G_9$ is covered by bi-cliques $(\{v_2^9, v_4^9\}, \{v_1^9\})$ with variables $x_1, x_3$ and $(\{v_3^9\}, \{v_1^9\})$ with $x_5$ that define $g_9 = g_{11} \uparrow \overline{x}_5$ and $g_{11} = x_1 \vee x_3 = (x_1 \uparrow x_3) \uparrow (x_1 \uparrow x_3)$. Graph $G_{10}$ is covered by bi-cliques $(\{v_2^{10}, v_3^{10}\}, \{v_1^{10}\})$ and $(\{v_4^{10}\}, \{v_1^{10}\})$ with the same variables. Those bi-cliques define $g_{10} = g_{12} \uparrow x_5$ and $g_{12} = \overline{x}_1 \vee \overline{x}_3 = (\overline{x}_1 \uparrow \overline{x}_3) \uparrow (\overline{x}_1 \uparrow \overline{x}_3)$.

Now, the given function $f$ is completely decomposed into superposition of Pierce functions in two variables. The system of functions $f, g_1, \ldots, g_{12}$ gives the circuit with NOR gates and inverters shown in Fig. 1.

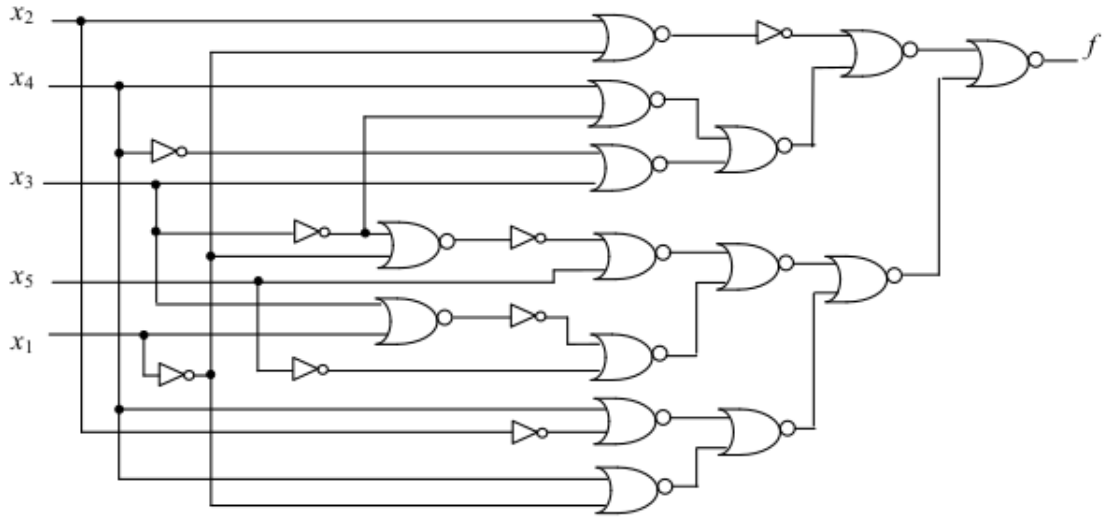


Fig. 1. Circuit with NOR gates and inverters

## 5. Synthesis of a combinational circuit in the AND, OR basis

We now obtain a combinational circuit that implements the same function in the basis of AND, OR gates with accessible variable complements. According to the Table in Section 3, the bi-cliques $B_1 = (V_1^1, V_1^0)$ and $B_2 = (V_2^1, V_2^0)$ covering the graph $G$ have $V_1^1 = V_2^1 = V^1$ for AND operation and $V_1^0 = V_2^0 = V_0$ for OR operation. It can be noted in the matrix $\mathbf{G}$ that the AND operation for $\varphi$ is desirable for the best variant of superposition $f = \varphi(g_1, g_2)$ if the matrix $\mathbf{M}^0$ has more rows than the matrix $\mathbf{M}^1$ has. Vice versa, the OR operation is desirable if the matrix $\mathbf{M}^1$ has more rows than the matrix $\mathbf{M}^0$ has. A variant is considered better if $g_1$ and $g_2$ have the less number of essential arguments. We choose OR operations for the output function ($f = g_1 \vee g_2$). Then, the starred bi-cliques, from which the initial meanings of $B_1$ and $B_2$ must be chosen, look as follows:

$$
\begin{array}{llll}
(\{v_1\},\{v_8,v_9,v_{10},v_{11}\}) & - & x_3x_4; & (\{v_2\},\{v_8,v_9,v_{10},v_{11}\}) \quad - \quad x_1x_3;\\
(\{v_3\},\{v_8,v_9,v_{10},v_{11}\}) & - & x_2x_4; & (\{v_4\},\{v_8,v_9,v_{10},v_{11}\}) \quad - \quad x_1x_2;\\
(\{v_5\},\{v_8,v_9,v_{10},v_{11}\}) & - & x_2x_3x_5; & (\{v_6\},\{v_8,v_9,v_{10},v_{11}\}) \quad - \quad x_1x_2x_5;\\
(\{v_7\},\{v_8,v_9,v_{10},v_{11}\}) & - & x_1x_3x_4. &
\end{array}
$$

The bi-cliques $B_1 = (\{v_1, v_2, v_3, v_7\}, \{v_8, v_9, v_{10}, v_{11}\})$ with variables $x_1, x_2, x_3, x_4$ and $B_2 = (\{v_4, v_5, v_6\}, \{v_8, v_9, v_{10}, v_{11}\})$ with variables $x_1, x_2, x_3, x_5$ are obtained by the same way as in the case of NOR operation. To decompose the function $f$ in the form $f = g_1 \vee g_2$, the following matrices are used:

$$
\mathbf{M}_1^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{array}{cccc} - & - & 1 & 1 \\ 0 & - & 1 & - \\ - & 1 & - & 1 \\ 1 & - & 0 & 0 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix}; \quad \mathbf{M}_1^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & - & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right] \end{array} \begin{matrix} 5 \\ 6 \\ 7 \end{matrix};
$$

$$
\mathbf{M}_2^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{cccc} 0 & 0 & - & - \\ - & 1 & 0 & 0 \\ 1 & 1 & - & 1 \end{array}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}; \quad \mathbf{M}_2^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_5 \end{matrix} \\ \left[\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & - & 1 & 0 \\ 1 & 0 & - & - \end{array}\right] \end{array} \begin{matrix} 4 \\ 5 \\ 6 \end{matrix}.
$$

The graphs $G_1$ and $G_2$ corresponding to the functions $g_1$ and $g_2$ are given by the matrices $\mathbf{G}_1$ and $\mathbf{G}_2$:

$$\mathbf{G}_1 = \begin{array}{c} \begin{matrix} 5 & 6 & 7 \end{matrix} \\ \left[\begin{matrix} x_3 \vee x_4 & x_4 & x_3 \\ x_3 & x_1 & x_1 \vee x_3 \\ x_4 & x_4 & x_2 \\ x_1 & x_3 & x_4 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix}; \quad \mathbf{G}_2 = \begin{array}{c} \begin{matrix} 4 & 5 & 6 \end{matrix} \\ \left[\begin{matrix} x_2 & x_1 & x_1 \\ x_5 & x_3 & x_2 \\ x_1 & x_5 & x_2 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}.$$

For decomposition $g_1 = g_3 \vee g_4$ and $g_2 = g_5 \vee g_6$, the starred bi-cliques of $G_1$ and $G_2$ are

$$\begin{array}{llll} (\{v_1^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_3x_4; & (\{v_1^2\},\{v_5^2,v_6^2,v_7^2\}) \quad - \quad x_1x_2; \\ (\{v_2^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_1x_3; & (\{v_2^2\},\{v_5^2,v_6^2,v_7^2\}) \quad - \quad x_2x_3x_5; \\ (\{v_3^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_2x_4; & (\{v_3^2\},\{v_5^2,v_6^2,v_7^2\}) \quad - \quad x_1x_2x_5; \\ (\{v_4^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_1x_3x_4. & \end{array}$$

From these bi-cliques, the pairs $(B_1^1, B_2^1)$ and $(B_1^2, B_2^2)$ covering $G_1$ and $G_2$ are obtained, where

$$\begin{array}{llll} B_1^1 = (\{v_1^1, v_3^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_2x_3x_4; & B_1^2 = (\{v_1^2, v_3^2\},\{v_5^2,v_6^2,v_7^2\}) \quad - \quad x_1x_2x_5; \\ B_2^1 = (\{v_2^1, v_4^1\},\{v_5^1,v_6^1,v_7^1\}) & - & x_1x_3x_4; & B_2^2 = (\{v_2^2\},\{v_5^2,v_6^2,v_7^2\}) \quad - \quad x_2x_3x_5. \end{array}$$

The incompletely specified functions $g_3$, $g_4$, $g_5$ and $g_6$ are given by the following matrices:

$$\mathbf{M}_3^1 = \begin{array}{c} \begin{matrix} x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} - & 1 & 1 \\ 1 & - & 1 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{M}_3^0 = \begin{array}{c} \begin{matrix} x_2 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 1 & 0 & 0 \\ - & 1 & 0 \\ 0 & 0 & 1 \end{matrix}\right] \end{array} \begin{matrix} 3 \\ 4 \\ 5 \end{matrix}; \quad \mathbf{M}_4^1 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 0 & 1 & - \\ 1 & 0 & 0 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{M}_4^0 = \begin{array}{c} \begin{matrix} x_1 & x_3 & x_4 \end{matrix} \\ \left[\begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{matrix}\right] \end{array} \begin{matrix} 3 \\ 4 \\ 5 \end{matrix};$$

$$\mathbf{M}_5^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_5 \end{matrix} \\ \left[\begin{matrix} 0 & 0 & - \\ 1 & 1 & 1 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{M}_5^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_5 \end{matrix} \\ \left[\begin{matrix} 0 & 1 & 1 \\ 1 & - & 0 \\ 1 & 0 & - \end{matrix}\right] \end{array} \begin{matrix} 3 \\ 4 \\ 5 \end{matrix}; \quad \mathbf{M}_6^1 = \begin{array}{c} \begin{matrix} x_2 & x_3 & x_5 \end{matrix} \\ \left[\begin{matrix} 1 & 0 & 0 \end{matrix}\right] \end{array} 1; \quad \mathbf{M}_6^0 = \begin{array}{c} \begin{matrix} x_2 & x_3 & x_5 \end{matrix} \\ \left[\begin{matrix} 1 & 0 & 1 \\ - & 1 & 0 \\ 0 & - & - \end{matrix}\right] \end{array} \begin{matrix} 2 \\ 3 \\ 4 \end{matrix}.$$

The corresponding graphs $G_3$, $G_4$, $G_5$ and $G_6$ are represented by the following matrices:

$$\mathbf{G}_3 = \begin{array}{c} \begin{matrix} 3 & 4 & 5 \end{matrix} \\ \left[\begin{matrix} x_3 \vee x_4 & x_4 & x_3 \\ x_4 & x_4 & x_2 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{G}_4 = \begin{array}{c} \begin{matrix} 3 & 4 & 5 \end{matrix} \\ \left[\begin{matrix} x_3 & x_1 & x_1 \vee x_3 \\ x_1 & x_3 & x_4 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix};$$

$$\mathbf{G}_5 = \begin{array}{c} \begin{matrix} 3 & 4 & 5 \end{matrix} \\ \left[\begin{matrix} x_2 & x_1 & x_1 \\ x_1 & x_5 & x_2 \end{matrix}\right] \end{array} \begin{matrix} 1 \\ 2 \end{matrix}; \quad \mathbf{G}_6 = \begin{array}{c} \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \left[\begin{matrix} x_5 & x_3 & x_2 \end{matrix}\right] \end{array} 1.$$

To implement the functions $g_3, g_4, g_5$ and $g_6$, take the AND operation. Then, the starred bi-cliques of the graphs $G_3, G_4, G_5$ and $G_6$ are

$$\begin{array}{llll} (\{v_1^3,v_2^3\},\{v_3^3\}) - x_4; & (\{v_1^4,v_2^4\},\{v_3^4\}) - x_1x_3; & (\{v_1^5,v_2^5\},\{v_3^5\}) - x_1x_2; & (\{v_1^6\},\{v_2^6\}) - x_5; \\ (\{v_1^3,v_2^3\},\{v_4^3\}) - x_4; & (\{v_1^4,v_2^4\},\{v_4^4\}) - x_1x_3; & (\{v_1^5,v_2^5\},\{v_4^5\}) - x_1x_5; & (\{v_1^6\},\{v_3^6\}) - x_3; \\ (\{v_1^3,v_2^3\},\{v_5^3\}) - x_2x_3; & (\{v_1^4,v_2^4\},\{v_5^4\}) - x_3x_4; & (\{v_1^5,v_2^5\},\{v_5^5\}) - x_1x_5; & (\{v_1^6\},\{v_4^6\}) - x_2. \end{array}$$

The covers of $G_3, G_4, G_5$ and $G_6$ are

$$\begin{array}{llll} B_1^3 = (\{v_1^3, v_2^3\},\{v_3^3, v_4^3\}) & - & x_4, & B_1^4 = (\{v_1^4, v_2^4\},\{v_3^4, v_2^4\}) \quad - \quad x_1x_3, \\ B_2^3 = (\{v_1^3, v_2^3\},\{v_5^3\}) & - & x_2x_3; & B_2^4 = (\{v_1^4, v_2^4\},\{v_5^4\}) \quad - \quad x_3x_4; \end{array}$$

$$\begin{array}{llll} B_1^5 = (\{v_1^5, v_2^5\},\{v_3^5, v_5^5\}) & - & x_1x_2, & B_1^6 = (\{v_1^6\},\{v_2^6, v_3^6\}) \quad - \quad x_3x_5, \\ B_2^5 = (\{v_1^5, v_2^5\},\{v_4^5\}) & - & x_1x_5; & B_2^6 = (\{v_1^6\},\{v_4^6\}) \quad - \quad x_2. \end{array}$$

These pairs define the following decompositions:

$$g_3(x_2, x_3, x_4) = g_7(x_2, x_3) \wedge x_4, \qquad g_4(x_2, x_3, x_4) = g_8(x_1, x_3) \wedge g_9(x_3, x_4),$$
$$g_5(x_1, x_2, x_5) = g_{10}(x_1, x_2) \wedge g_{11}(x_1, x_5), \qquad g_6(x_1, x_3, x_5) = g_{12}(x_3, x_5) \wedge x_2.$$

The functions $g_7, g_8, g_9, g_{10}, g_{11}$ and $g_{12}$ are given by the following matrices:

$$\mathbf{M}_7^1 = \begin{array}{c} \begin{matrix} x_2 & x_3 \end{matrix} \\ \begin{bmatrix} - & 1 \\ 1 & - \end{bmatrix} \end{array}; \quad \mathbf{M}_7^0 = \begin{array}{c} \begin{matrix} x_2 & x_3 \end{matrix} \\ \begin{bmatrix} 0 & 0 \end{bmatrix} \end{array}; \quad \mathbf{M}_8^1 = \begin{array}{c} \begin{matrix} x_1 & x_3 \end{matrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array}; \quad \mathbf{M}_8^0 = \begin{array}{c} \begin{matrix} x_1 & x_3 \end{matrix} \\ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \end{array};$$

$$\mathbf{M}_9^1 = \begin{array}{c} \begin{matrix} x_3 & x_4 \end{matrix} \\ \begin{bmatrix} 1 & - \\ - & 0 \end{bmatrix} \end{array}; \quad \mathbf{M}_9^0 = \begin{array}{c} \begin{matrix} x_3 & x_4 \end{matrix} \\ \begin{bmatrix} 0 & 1 \end{bmatrix} \end{array}; \quad \mathbf{M}_{10}^1 = \begin{array}{c} \begin{matrix} x_1 & x_2 \end{matrix} \\ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \end{array}; \quad \mathbf{M}_{10}^0 = \begin{array}{c} \begin{matrix} x_1 & x_2 \end{matrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array};$$

$$\mathbf{M}_{11}^1 = \begin{array}{c} \begin{matrix} x_1 & x_5 \end{matrix} \\ \begin{bmatrix} 0 & - \\ - & 1 \end{bmatrix} \end{array}; \quad \mathbf{M}_{11}^0 = \begin{array}{c} \begin{matrix} x_1 & x_5 \end{matrix} \\ \begin{bmatrix} 1 & 0 \end{bmatrix} \end{array}; \quad \mathbf{M}_{12}^1 = \begin{array}{c} \begin{matrix} x_3 & x_5 \end{matrix} \\ \begin{bmatrix} 0 & 0 \end{bmatrix} \end{array}; \quad \mathbf{M}_{12}^0 = \begin{array}{c} \begin{matrix} x_3 & x_5 \end{matrix} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array}.$$

These matrices are used to obtain the algebraic representations of the completely specified functions $g_7, g_8, g_9, g_{10}, g_{11}$ and the realization of the partial function $g_{12}$:

$$g_7 = x_2 \vee x_3, \qquad g_8 = x_1 \oplus x_3 = \overline{x}_1 x_3 \vee x_1 \overline{x}_3, \qquad g_9 = x_3 \vee \overline{x}_4,$$
$$g_{10} = x_1 \sim x_2 = \overline{x}_1 \overline{x}_2 \vee x_1 x_2, \qquad g_{11} = \overline{x}_1 \vee x_5, \qquad g_{12} = \overline{x}_3 \overline{x}_5.$$

The corresponding combinational circuit with AND and OR gates is shown in Fig. 2.

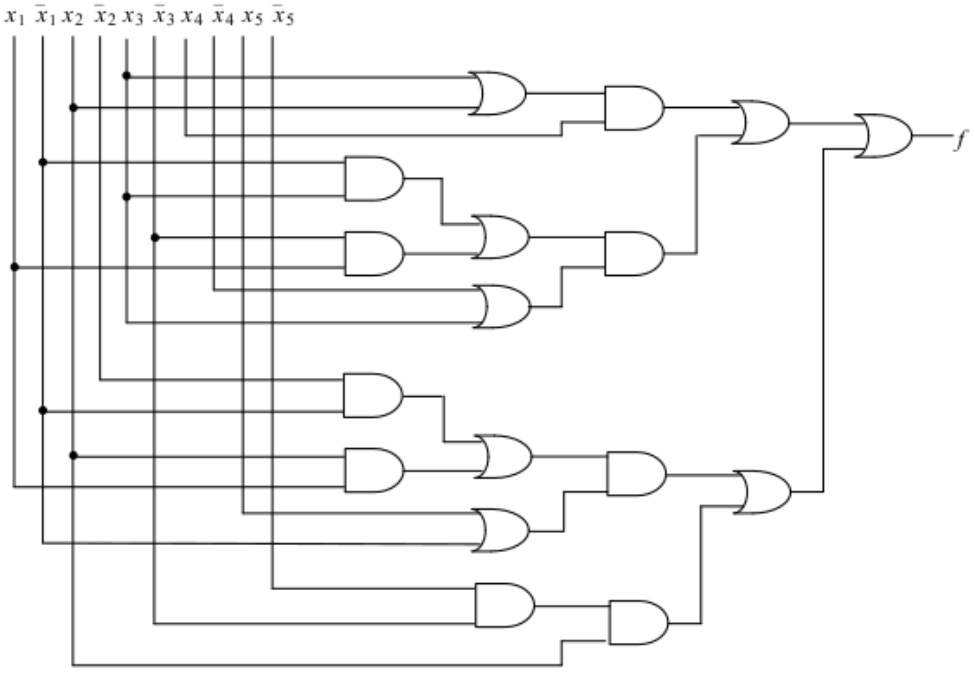


Fig. 2. Circuit with AND and OR gates

## 6. Conclusion

The paper shows how to apply the method for bi-decomposition in the synthesis of combinational circuits. The advantage of the suggested approach is the possibility of constructing circuits of short delay that is characterized by the number of levels in the

circuit. The method is convenient to be applied for incompletely specified Boolean functions, where the functions are given by two domains of Boolean space, as opposed to completely specified functions when the zero domains must be obtained. The "bottle-neck" of the proposed approach is transformation CNF into DNF which is a non-polynomial problem. Thus, the scope of application of the proposed method is limited. It would be established by computer experiment, which is an independent research. The joint implementation of a system of Boolean functions demands reveling the function coincidence at every level of decomposition.

REFERENCES

1. *Cortadella J.* Timing-driven logic bi-decomposition. IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, 2003, vol. 22, no. 6, pp. 675–685.
2. *Mishchenko A., Steinbach B., and Perkowski M.* An algorithm for bi-decomposition of logic functions. Proc. DAC'2001, 18–22 June 2001, Las Vegas, USA, pp. 103–108.
3. *Chang S.-C., Marek-Sadowska M., and Hwang T.* Technology mapping for TLU FPGAś based on decomposition of binary decision diagrams. IEEE Trans. Computer-Aided Design, 1996, vol. 15, no. 10, pp. 1226–1235.
4. *Bibilo P. N.* Dekompozitsiya bulevykh funktsiy na osnove resheniya logicheskikh uravneniy [Decomposition of Boolean Functions based on Solving Logical Equations]. Minsk, Belaruskaja Navuka, 2009. 211 p. (in Russian)
5. *Zakrevskiy A. D.* On a special kind decomposition of weakly specified Boolean functions. Proc. Second Int. Conf. CAD DD'97, Minsk, Belarus, 12–14 November 1997, National Academy of Sciences of Belarus, Institute of Engineering Cybernetics, Minsk, 1997, vol. 1, pp. 36–41.
6. *Pottosin Yu. V.* A method for bi-decomposition of partial Boolean functions. Prikladnaya Diskretnaya Matematika, 2020, no. 47, pp. 108–116.
7. *Pottosin Yu. V. and Shestakov E. A.* Parallel'no-posledovatel'naya kompozitsiya sistemy chastichnykh bulevykh funktsiy [Series parallel decomposition of a system of incompletely specified Boolean functions]. Prikladnaya Diskretnaya Matematika, 2010, no. 4(10), pp. 55–63. (in Russian)
8. *Zakrevskiy A. D., Pottosin Yu. V., and Cheremisinova L. D.* Combinatorial Algorithms of Discrete Mathematics. Tallinn, TUT Press, 2008. 194 p.
9. *Zakrevskiy A. D., Pottosin Yu. V., and Cheremisinova L. D.* Optimization in Boolean Space. Tallinn, TUT Press, 2009. 242 p.
10. *Pottosin Yu. V.* Kombinatornye zadachi v logicheskom proektirovanii diskretnykh ustroystv [Combinatorial Problems in Logical Design of Discrete Devices]. Minsk, Belaruskaja Navuka, 2021. 175 p. (in Russian)
11. *Harary F.* Graph Theory. Addison-Wesley, Reading, 1969.

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 512.626+519.682 DOI 10.17223/20710410/60/9

## О РЕШЕНИИ ОБЩЕГО АЛГЕБРАИЧЕСКОГО УРАВНЕНИЯ СТЕПЕННЫМИ РЯДАМИ И ПРИЛОЖЕНИИ В ТЕОРИИ ФОРМАЛЬНЫХ ГРАММАТИК

О. И. Егорушкин, И. В. Колбасина, К. В. Сафонов

*Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск, Россия*

**E-mail:** egorushkin.o@yandex.ru, kabaskina@yandex.ru, safonovkv@rambler.ru

Рассматривается общее алгебраическое уравнение и ставится задача найти его решение при помощи степенных рядов или рядов Лорана, зависящих от коэффициентов уравнения. Получено решение в виде ряда Лорана, коэффициенты которого выражаются через коэффициенты формулами в «замкнутом» виде, когда число слагаемых в формуле не растёт вместе с номером коэффициента. В прикладном аспекте общее алгебраическое уравнение рассматривается как коммутативный образ соответствующего уравнения с некоммутативными символами, которое, в свою очередь, интерпретируется в теории формальных грамматик как полиномиальная грамматика. Показано, что такая грамматика не порождает формального языка (не имеет решения в виде формального степенного ряда), поскольку её коммутативный образ имеет решение в виде ряда Лорана, содержащего отрицательные степени переменных, тогда как деление в теории формальных грамматик не определено.

**Ключевые слова:** *общее алгебраическое уравнение, степенной ряд, ряд Лорана, коммутативный образ, полиномиальная грамматика, формальный язык.*

## ON THE SOLUTION OF A GENERAL ALGEBRAIC EQUATION BY POWER SERIES AND APPLICATIONS IN THE THEORY OF FORMAL GRAMMARS

O. I. Egorushkin, I. V. Kolbasina, K. V. Safonov

*Reshetnev State University of Science and Technology, Krasnoyarsk, Russia*

A general algebraic equation is considered, and the problem is to find its solution using power series or Laurent series depending on the coefficients of the equation. A solution is obtained in the form of a Laurent series, the coefficients of which are expressed in terms of the coefficients by formulas in a “closed” form, when the number of terms in the formula does not increase with the number of the coefficient. In the applied aspect, a general algebraic equation is considered as a commutative image of the corresponding equation with non-commutative symbols, which, in turn, is interpreted in the theory of formal grammars as a polynomial grammar. It is shown that such a

grammar does not generate a formal language (it does not have a solution in the form of a formal power series), since its commutative image has a solution in the form of a Laurent series containing negative degrees of variables, while division in the theory of formal grammars is not defined.

**Keywords:** *general algebraic equation, power series, Laurent series, commutative image, polynomial grammar, formal language.*

## Введение

Рассмотрим общее алгебраическое уравнение

$$x_n z^n + x_{n-1} z^{n-1} + \ldots + x_1 z + x_0 = 0, \tag{1}$$

которое решается относительно символа $z$ в виде функции $z = z(x) = z(x_0, \ldots, x_n)$ от коэффициентов $x_0, \ldots, x_n$.

Конструктивное представление функции $z = z(x)$ является фундаментальной задачей математики с многовековой историей.

Как известно, после открытия формул Кардано и Феррари для решений уравнений третьей и четвёртой степени появилась надежда решать в радикалах алгебраическое уравнение произвольной степени. Прошло почти три века, прежде чем в 1824 г. Абель доказал невозможность этого, рассмотрев уравнения пятой степени [1]. Точнее, Абель доказал, что если существует формула, выражающая в радикалах корни уравнения пятой степени через его коэффициенты, то в случае действительных коэффициентов это уравнение имеет либо один действительный корень, либо пять [2]. Однако уравнение пятой степени с действительными коэффициентами может иметь три действительных и два комплексно сопряжённых корня, а значит, формулы в радикалах не существует.

После доказательства теоремы Абеля интересы математиков обратились к конструктивному представлению многозначной аналитической функции $z = z(x)$ с использованием более сложных, чем радикалы, инструментов, например степенных рядов, интегралов и специальных функций, поскольку они зачастую дают возможность осуществлять приближенные вычисления.

Так, в 1921 г. Я. Меллин предложил решать общее уравнение с помощью гипергеометрических функций, причём разложение в ряд получено на основе интегрального представления Меллина — Барнса [3]. В 1984 г. Умемура доказал разрешимость уравнения произвольной степени с помощью тэта-функций.

В принципе, получить разложение в степенной ряд или ряд Лорана неявной функции $z = z(x_0, \ldots, x_n)$, определяемой функциональным уравнением

$$F(x_0, \ldots, x_n, z) = 0,$$

не очень сложно. Как правило, такие разложения содержат оператор дифференцирования возрастающего порядка, либо коэффициенты разложения выражаются через коэффициенты исходной функции формулой с возрастающим числом слагаемых [4].

Наша цель — найти решение $z = z(x)$ общего алгебраического уравнения (1) в виде степенного ряда либо ряда Лорана, коэффициенты которого выражены формулой в «замкнутом виде»: когда число слагаемых в ней не растёт вместе с номером коэффициента, что позволяет более эффективно исследовать коэффициенты разложения.

Идея, реализуемая в настоящей работе, состоит в том, что решение $z(x)$ является алгебраической функцией от нескольких переменных — коэффициентов уравнения (1), и потому её степенной ряд является диагональю степенного ряда некоторой

рациональной функции, зависящей от этих переменных и ещё одной, дополнительной, переменной [5]. Далее указанная рациональная функция будет разложена в степенной ряд, наконец, после взятия его диагонали по паре переменных будет получена искомая формула в замкнутом виде.

Поскольку разложение аналитической функции в степенной ряд или ряд Лорана в фиксированной области единственно, то коэффициенты ряда функции $z = z(x)$ не зависят от способа их получения, остаётся лишь вопрос о простоте и удобстве соответствующих формул. Заметим, что полученное в настоящей работе разложение можно извлечь в несколько ином виде из более общей функции, найденной ранее с помощью интеграла Меллина — Барнса и гипергеометрических функций [3].

Решение уравнения (1) имеет приложение в теории формальных языков и грамматик, играющей ведущую роль как в лингвистике, так и в программировании. Приложение связано с тем, что наиболее важные классы формальных грамматик можно записать в виде системы полиномиальных уравнений с некоммутативными переменными [6, 7], а именно: под полиномиальной грамматикой понимается [8, 9] система полиномиальных уравнений

$$P_j(x, z) = 0, \quad P_j(0, 0) = 0, \quad j = 1, \ldots, k, \tag{2}$$

которая решается относительно символов $z = (z_1, \ldots, z_n)$ в виде формальных степенных рядов (ФСР), зависящих от символов $x = (x_0, \ldots, x_m)$.

Символы $x_0, \ldots, x_m$ называются терминальными и образуют словарь языка, а символы $z_1, \ldots, z_n$ — нетерминальными и участвуют в задании его грамматических правил. Над всеми символами определена некоммутативная операция конкатенации и коммутативные операции формального сложения и умножения на числа, что позволяет рассматривать ФСР с числовыми коэффициентами.

Если система ФСР $z_1 = z_1(x), \ldots, z_n = z_n(x)$ является решением системы уравнений (2), то первый ФСР $z_1(x)$ называется полиномиальным языком, порождённым полиномиальной грамматикой (2), что обусловлено особой ролью начального символа языка $z_1$. При этом мономы от терминальных символов интерпретируются как предложения языка, а язык $z_1(x)$ — как сумма всех «правильных» мономов (предложений) [8, 9].

В этом аспекте общее алгебраическое уравнение (1) можно рассматривать как полиномиальную грамматику, состоящую из одного уравнения, решение которого в виде ФСР $z = z(x) = z(x_0, \ldots, x_n)$, если оно существует, представляет собой формальный язык.

Исследовать системы с некоммутативными символами очень трудно ввиду некоммутативности переменных и отсутствия операции деления. Трудность, естественно, сохраняется и в случае полиномиальной грамматики, состоящей из одного уравнения

$$P_1(x, z) = 0,$$

относительно одного неизвестного $z = z_1$, и даже в частном случае некоммутативного общего алгебраического уравнения

$$P_1(x, z) = x_n z^n + x_{n-1} z^{n-1} + \ldots + x_1 z + x_0 = 0.$$

И всё же при исследовании грамматики можно использовать степенные ряды (ряды Лорана) с коммутативными переменными, если перейти от грамматики к её коммутативному образу.

## 1. Коммутативный образ ФСР

Для ФСР, являющегося в нашем случае кратным рядом, возникает вопрос об определении частичной суммы ряда. Поскольку ряд формальный, его частичную сумму можно определять произвольным образом. Один из возможных способов состоит в том, чтобы перенумеровать члены кратного ФСР в одномерную последовательность, что естественным образом определит порядок суммирования.

Можно упорядочить члены ФСР следующим образом: сгруппировать все возможные мономы от $x_0, \ldots, x_m$ в однородные многочлены, расположенные по возрастанию степеней, затем перенумеровать мономы каждого из однородных многочленов в лексикографическом порядке в одну последовательность, переходя от многочлена меньшей степени к большей [6, 7]. При таком упорядочивании все мономы от символов $x_0, \ldots, x_m$ единственным образом записываются в виде последовательности $\{u_i\}_{i=0}^{\infty}$, играющей роль базиса ФСР. Теперь каждый ряд $s$ можно однозначно записать в виде разложения по этому базису

$$s = \sum_{i=0}^{\infty} \langle s, u_i \rangle \; u_i, \tag{3}$$

где $\langle s, u_i \rangle$ — числовой коэффициент при мономе $u_i$. Можно также ещё раз перенумеровать члены ФСР, пропуская мономы с нулевыми коэффициентами.

Поставим в соответствие ФСР (3) его коммутативный образ $\mathrm{ci}(s)$ — степенной ряд, который получается из $s$ в предположении, что символы $x_0, \ldots, x_m$ (равно как и $z_1, \ldots, z_n$) обозначают коммутативные переменные, принимающие значения из поля комплексных чисел. При этом гомоморфизм, отображающий кольцо степенных рядов, задаётся отображением множества терминальных символов на множество образующих свободной коммутативной полугруппы и считается фиксированным [10].

В этом предположении любой моном $u_i$ от символов $x_1, \ldots, x_m$ можно записать в виде $x_0^{\alpha_0} \ldots x_m^{\alpha_m}$, где $\alpha_j = \deg_{x_j}(u_i)$ — число вхождений (степень) символа $x_j$ в этот моном. Если обозначить мультииндекс $\alpha = (\alpha_0, \ldots, \alpha_m)$, то можно записать равенство $\alpha = \deg_x(u_i)$, с учётом которого получаются следующие равенства:

$$\mathrm{ci}(s) = \sum_{i=0}^{\infty} \langle s, u_i \rangle \cdot \mathrm{ci}(u_i) = \sum_{\alpha} \left( \sum_{\alpha = \deg_x(u_i)} \langle s, u_i \rangle \right) x^{\alpha} \stackrel{\text{def}}{=} \sum_{\alpha} c_{\alpha} x^{\alpha}.$$

Впервые коммутативный образ ФСР был рассмотрен и применён в работе [10], которая показала эффективность и перспективность аналитических методов в теории формальных грамматик.

## 2. Основной результат

Как отмечалось выше, функция $z = z(x)$ является многозначной аналитической функцией; она может иметь особенности лишь на дискриминантном множестве коммутативного многочлена $P_1(x, z)$, содержащем, в частности, гиперплоскость $\{x_n = 0\}$.

Вблизи точки $x = 0$, $z = 0$ может быть несколько ветвей решения уравнения (1). Рассмотрим ту ветвь $z = z(x)$ решения, которая при $x_1 \neq 0$ аналитична в достаточно малой окрестности точки $x = 0$ и, кроме того, для которой выполнено равенство $z(0, x_1, \ldots, x_n) = 0$; по теореме о неявной функции такая ветвь существует и единственна. Имеет место следующая

**Теорема 1.** Для указанной ветви решения общего алгебраического уравнения (1) имеет место разложение в ряд Лорана

$$z(x)=\sum_{k_2,\ldots,k_n\geqslant 0}(-1)^{2k_2+\ldots+nk_n+1}\frac{(2k_2+\ldots+nk_n)!}{(k_2+\ldots+(n-1)k_n+1)!\;k_2!\ldots k_n!}\times \\ \times x_0^{k_2+\ldots+(n-1)k_n+1}x_1^{-2k_2-\ldots-nk_n-1}x_2^{k_2}\ldots x_n^{k_n}, \tag{4}$$

который сходится абсолютно и равномерно на множестве $\{|x_k|\leqslant\rho,\ k\neq 1,\ |x_1|\geqslant 1\}$, где число $\rho$ достаточно мало.

Ряд Лорана (4) содержит мономы с отрицательными степенями переменной $x_1$, при этом решения в виде степенного ряда не существует, поскольку ряд Лорана получается заменой переменных из единственного решения уравнения (6). Отсюда следует, что решить соответствующее некоммутативное уравнение в виде ФСР также невозможно [6, 7]. Получаем следствие теоремы 1.

**Следствие 1.** Формальная грамматика, состоящая из одного уравнения с некоммутативными символами

$$x_nz^n+x_{n-1}z^{n-1}+\ldots+x_1z+x_0=0,$$

не порождает формального языка, поскольку не имеет решения в виде ФСР.

Для сравнения заметим, что грамматика (уравнение с некоммутативнными символами)

$$x_nz^n+\ldots+x_2z^2+z+x_0=0$$

порождает формальный язык (имеет решение в виде ФСР), который можно получить методом последовательных приближений:

$$z^{(k+1)}=-x_n(z^{(k)})^n-\ldots-x_2(z^{(k)})^2-x_0;\quad k=0,1,2,\ldots;\quad z^{(0)}=0.$$

***Доказательство*** теоремы 1. В уравнении (1) сделаем мономиальную замену переменных

$$x_1=x_1,\ x_k=x_1x_k,\ k\neq 1, \tag{5}$$

тогда после сокращения на $x_1$ получим уравнение

$$P_1(x[1],z)=x_nz^n+\ldots+x_2z^2+z+x_0=0, \tag{6}$$

где $x[1]=(x_0,1,x_2,\ldots,x_n)$. Рассмотрим ветвь решения уравнения (6), для которой $z(0,1,x_2,\ldots,x_n)=0$. При этом выполнены условия теоремы о неявной функции

$$P_1(0,0)=0,\qquad \frac{\partial P_1(0,0)}{\partial z}=1,$$

и потому в окрестности точки $x[1]=(0,1,0,\ldots,0)$ решение аналитическое и единственное. Следовательно, функция $z(x[1])$ раскладывается в степенной ряд

$$z(x[1])=\sum b_{\alpha[1]}x[1]^{\alpha[1]},$$

где $\alpha[1]=(\alpha_0,\alpha_2,\ldots,\alpha_n)$. Заметим также, что, удовлетворяя полиномиальному уравнению (6), она является алгебраической функцией.

Теперь можно утверждать [5], что, в силу алгебраичности функции $z(x[1])$, её степенной ряд является диагональю степенного ряда рациональной функции

$$R(x[1],y)=\left.\frac{z^2P'_{1z}(x[1],z)}{P_1(x[1],z)}\right|_{\substack{z=y\\ x_0=x_0y}}$$

по паре переменных $x_0,\ y$, что будем записывать так:

$$z(x[1])=\Delta_{x_0,y}(R(x[1],y)).$$

Итак, для того чтобы получить ряд для искомой ветви $z(x)$, следует: 1) разложить в ряд функцию $R(x[1],z)$; 2) сделать в этом ряде мономиальную замену переменных $z=y$, $x_0=x_0y$; 3) взять диагональ этого ряда по $x_0$ и $y$, т. е. выбрать те слагаемые, степень которых по $x_0$ равна степени по $y$, и заменить в них моном $(x_0y)^k$ на $x_0^k$. Эти действия выполнены ниже.

1. Для получения разложения функции $R$ заметим, что

$$\frac{z^2P'_{1z}(x[1],z)}{P(x[1],z)}=z^2\left[\ln P_1(x[1],z)\right]'_z.$$

Далее, используя разложение логарифма в ряд Маклорена и формулу бинома Ньютона, получим

$$\begin{gathered}\ln P_1(x[1],z)=\ln(z(1+x_nz^{n-1}+\ldots+x_2z+x_0z^{-1})=\\ =\ln z+\sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{k}(x_nz^{n-1}+\ldots+x_2z+x_0z^{-1})^k=\\ =\ln z+\sum_{k=1}^{\infty}\sum_{\substack{k_1,\ldots,k_n\geqslant 0\\ k_1+\ldots+k_n=k}}\frac{(-1)^{k-1}}{k}\,\frac{k!}{k_1!\ldots k_n!}(x_nz^{n-1})^{k_n}\ldots(x_2z)^{k_2}(x_0z^{-1})^{k_1}=\\ =\ln z+\sum_{\substack{k_1,\ldots,k_n\geqslant 0\\ k_1+\ldots+k_n\geqslant 1}}(-1)^{k_1+\ldots+k_n-1}\frac{(k_1+\ldots+k_n-1)!}{k_1!\ldots k_n!}x_0^{k_1}x_2^{k_2}\ldots x_n^{k_n}z^{-k_1+k_2+\ldots+(n-1)k_n}.\end{gathered}$$

Данные ряды сходятся абсолютно и равномерно, если $|x_nz^{n-1}+\ldots+x_2z+x_0z^{-1}|<1$, что, в свою очередь, имеет место, если $0<r_1\leqslant|z|\leqslant r_2$, $|x_k|\leqslant\rho$, $k\neq 1$, где число $r>0$ произвольное, а число $\rho$ достаточно малое.

Почленно дифференцируя последний ряд, получим разложение для функции $z^2[\ln P_1(x[1],z)]'_z$:

$$\begin{gathered}z+\sum_{\substack{k_1,\ldots,k_n\geqslant 0\\ k_1+\ldots+k_n\geqslant 1}}(-1)^{k_1+\ldots+k_n-1}\frac{(k_1+\ldots+k_n-1)!}{k_1!\ldots k_n!}(-k_1+k_2+\ldots+(n-1)k_n)\times\\ \times x_0^{k_1}x_2^{k_2}\ldots x_n^{k_n}z^{-k_1+k_2+\ldots+(n-1)k_n+1}.\end{gathered}$$

2. Заменив $z$ на $y$, а $x_0$ на $x_0y$, получим ряд

$$\begin{gathered}R(x[1],y)=y+\sum_{\substack{k_1,\ldots,k_n\geqslant 0\\ k_1+\ldots+k_n\geqslant 1}}(-1)^{k_1+\ldots+k_n-1}\,\frac{(k_1+\ldots+k_n-1)!}{k_1!\ldots k_n!}\times\\ \times(-k_1+k_2+\ldots+(n-1)k_n)x_0^{k_1}x_2^{k_2}\ldots x_n^{k_n}y^{k_2+\ldots+(n-1)k_n+1}.\end{gathered}$$

3. Выбирая диагональные члены ряда условием

$$k_1 = k_2 + \ldots + (n-1)k_n + 1$$

и заменяя $x_0 y$ на $x_0$, получаем степенной ряд

$$z(x[1]) = \sum_{\substack{k_2,\ldots,k_n \geqslant 0 \\ k_2+\ldots+k_n \geqslant 0}} (-1)^{2k_2+\ldots+nk_n} \frac{(2k_2+\ldots+nk_n)!}{(k_2+\ldots+(n-1)k_n+1)!\, k_2!\ldots k_n!} \times$$
$$\times (-1) x_0^{k_2+\ldots+(n-1)k_n+1} x_2^{k_2} \ldots x_n^{k_n} =$$
$$= \sum_{k_2,\ldots,k_n \geqslant 0} (-1)^{2k_2+\ldots+nk_n+1} \frac{(2k_2+\ldots+nk_n)!}{(k_2+\ldots+(n-1)k_n+1)!\, k_2!\ldots k_n!} \times$$
$$\times x_0^{k_2+\ldots+(n-1)k_n+1} x_2^{k_2} \ldots x_n^{k_n}.$$

Наконец, сделав в последнем степенном ряде замену переменных

$$x_1 = x_1,\ x_k = x_k/x_1,\ k \neq 1,$$

обратную к замене переменных (5), получим ряд Лорана (4), который сходится абсолютно и равномерно, если $|x_k/x_1| \leqslant \rho$, $k \neq 1$, что выполняется при $|x_1| \geqslant 1$. ■

**Пример 1.** Рассмотрим квадратное уравнение

$$x_2 z^2 + x_1 z + x_0 = 0$$

и его решение $z = z(x)$, такое, что $z(0, x_1, x_2) = 0$ при $|x_1| \neq 0$. Это решение равно

$$z(x) = \frac{-x_1 + \sqrt{x_1^2 - 4x_0x_2}}{2x_2} = -\frac{x_1}{2x_2} + \frac{x_1}{2x_2}\sqrt{1 - \frac{4x_0x_2}{x_1^2}}\ .$$

С одной стороны, используя разложение степенной функции в ряд Маклорена, получаем

$$z(x) = -\frac{x_1}{2x_2} + \frac{x_1}{2x_2}\left(1 - \frac{1}{2}\frac{4x_0x_2}{x_1^2} + \frac{1/2(1/2-1)}{1\cdot 2}\left(\frac{4x_0x_2}{x_1^2}\right)^2 -\right.$$
$$\left. -\frac{1/2(1/2-1)(1/2-2)}{1\cdot 2\cdot 3}\left(\frac{4x_0x_2}{x_1^2}\right)^3 + \ldots\right) = -\frac{x_0}{x_1} - \frac{x_0^2x_2}{x_1^3} - 2\,\frac{x_0^3x_2^2}{x_1^5} - 5\,\frac{x_0^4x_2^3}{x_1^7} - \ldots$$

С другой стороны, тот же результат даёт ряд (4), который при $n = 2$ имеет вид

$$z(x) = \sum_{k_2=0}^{\infty} (-1)^{2k_2+1} \frac{(2k_2)!}{(k_2+1)!\, k_2!}\, x_0^{k_2+1} x_1^{-2k_2-1} x_2^{k_2} = -\sum_{k_2=0}^{\infty} \frac{(2k_2)!}{(k_2+1)!\, k_2!}\, x_0^{k_2+1} x_1^{-2k_2-1} x_2^{k_2} =$$
$$= -\frac{x_0}{x_1} - \frac{x_0^2x_2}{x_1^3} - 2\,\frac{x_0^3x_2^2}{x_1^5} - 5\,\frac{x_0^4x_2^3}{x_1^7} - \ldots$$

В заключение заметим, что наличие у коммутативного образа полиномиальной грамматики (2) решения в виде рядов Лорана ещё не говорит о том, что грамматика не имеет решения в виде ФСР и не порождает формального языка, поскольку её коммутативный образ может иметь и другие решения, в том числе в виде степенного ряда.

## ЛИТЕРАТУРА


1. *Abel N. H.* Oeuvres completes, t. 1. Christiania: Grondahl, 1839. 294 p.
2. *Тихомиров В.* Абель и его великая теорема // Квант. 2003. № 1. С. 11–15.
3. *Семушева А. Ю., Цих А. К.* Продолжение исследований Меллина о решении алгебраических уравнений / Сб. «Комплексный анализ и дифференциальные операторы (К 150-летию С. В. Ковалевской)». Красноярск: Красноярский гос. ун–т, 2000. С. 122–134.
4. *Aizenberg L. A. and Yuzhakov A. P.* Integral Representations and Residues in Multidimensional Complex Analysis. Providence: AMS, 1983. 283 p.
5. *Safonov K. V.* On power series of algebraic and rational functions in $C^n$ // J. Math. Analys. Appl. 2000. V. 243. P. 261–277.
6. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журнал СФУ. Математика и физика. 2016. Т. 9. № 2. С. 166–172.
7. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* О применении многомерного комплексного анализа в теории формальных языков и грамматик // Прикладная дискретная математика. 2017. № 37. С. 76–89.
8. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978. 167 p.
9. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973. 319 с.
10. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Доклады АН СССР. 1973. Т. 212. С. 50–52.


## REFERENCES


1. *Abel N. H.* Oeuvres completes, t. 1. Christiania, Grondahl, 1839. 294 p.
2. *Tikhomirov V.* Abel' i ego velikaya teorema [Abel and his great theorem]. Kvant, 2003, no. 1, pp. 11–15. (in Russian)
3. *Semusheva A. Yu. and Tsikh A. K.* Prodolzhenie issledovaniy Mellina o reshenii algebraicheskikh uravneniy [Continuation of Mellin's research on the solving of algebraic equations]. Kompleksnyy Analiz i Differentsial'nye Operatory. Krasnoyarsk, Krasnoyarsk State University, 2000, pp. 122–134. (in Russian)
4. *Aizenberg L. A. and Yuzhakov A. P.* Integral Representations and Residues in Multidimensional Complex Analysis. Providence, AMS, 1983. 283 p.
5. *Safonov K. V.* On power series of algebraic and rational functions in $C^n$. J. Math. Analys. Appl., 2000, vol. 243, pp. 261–277.
6. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations. J. SFU, Mathematics and Physics, 2016, vol. 9, no. 2, pp. 166–172.
7. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* O primenenii mnogomernogo kompleksnogo analiza v teorii formal'nyh yazykov i grammatik [On the application of multidimensional complex analysis in the theory of formal languages and grammars]. Prikladnaya Diskretnaya Matematika, 2017, no. 37, pp. 76—89. (in Russian)
8. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y., Springer Verlag, 1978. 167 p.
9. *Glushkov V. M., Tseytlin G. E., and Yushchenko E. L.* Algebra. Yazyki. Programmirovanie [Algebra. Languages. Programming]. Kiev, Naukova Dumka, 1973. 319 p. (in Russian)
10. *Semenov A. L.* Algoritmicheskie problemy dlya stepennykh ryadov i kontekstno-svobodnykh grammatik [Algorithmic problems for power series and context-free grammars]. Reports of the Academy of Sciences of the USSR, 1973, vol. 212, pp. 50–52. (in Russian)

УДК 510.52 DOI 10.17223/20710410/60/10

# О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ КЛАСТЕРИЗАЦИИ ГРАФОВ С ОГРАНИЧЕНИЯМИ НА РАЗМЕР КЛАСТЕРОВ[1]

А. Н. Рыбалов

*Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия*

**E-mail:** alexander.rybalov@gmail.com

Изучается генерическая сложность проблемы кластеризации графов с ограничением $p$ на размеры кластеров при $p \geqslant 3$. В этой задаче структура взаимосвязей объектов задаётся с помощью графа, вершины которого соответствуют объектам, а рёбра соединяют похожие объекты. Требуется разбить множество объектов на попарно непересекающиеся группы (кластеры) ограниченного числом $p$ размера так, чтобы минимизировать число связей между кластерами и число недостающих связей внутри кластеров. Доказывается, что при условии $\mathrm{P} \neq \mathrm{NP}$ и $\mathrm{P} = \mathrm{BPP}$ для этой проблемы не существует полиномиального сильно генерического алгоритма. Сильно генерический алгоритм решает проблему не на всём множестве входов, а на подмножестве, последовательность частот которого при увеличении размера экспоненциально быстро сходится к 1.

**Ключевые слова:** *генерическая сложность, кластеризация графа.*

# ON GENERIC COMPLEXITY OF THE GRAPH CLUSTERING PROBLEM WITH BOUNDED CLUSTERS

A. N. Rybalov

*Sobolev Institute of Mathematics, Omsk, Russia*

In this paper, we study the generic complexity of the graph clustering problem with bounded sizes of clusters. In this problem, the structure of object relations is presented as a graph: vertices correspond to objects, and edges connect similar objects. It is required to divide a set of objects into disjoint groups (clusters) of bounded sizes to minimize the number of connections between clusters and the number of missing links within clusters. It is proved that, under the condition $\mathrm{P} \neq \mathrm{NP}$ and $\mathrm{P} = \mathrm{BPP}$, for this problem there is no polynomial strongly generic algorithm. A strongly generic algorithm solves a problem not on the entire set of inputs, but on a subset whose frequency sequence converges exponentially to 1 as the size increases. To prove this result, we use the method of generic amplification, which allows to construct generically hard problems from the problems hard in the classical sense. The main component of this method is the cloning technique, which combines the inputs of a problem together into sufficiently large sets of equivalent inputs. Equivalence is understood in the sense that the problem is solved similarly for them.

**Keywords:** *generic complexity, graph clustering.*

[1]Работа поддержана грантом РНФ № 22-11-20019.

## Введение

Одной из важных проблем машинного обучения является проблема кластеризации графов. В этой задаче структура взаимосвязей объектов задаётся с помощью графа, вершины которого соответствуют объектам, а рёбра соединяют похожие объекты. Требуется разбить множество объектов на попарно непересекающиеся группы (кластеры) так, чтобы минимизировать число связей между кластерами и число недостающих связей внутри кластеров. В работах [1–7] доказана NP-трудность проблемы кластеризации графа для различных её постановок. Кроме того, В. П. Ильев и А. А. Навроцкая доказали [8], что проблема кластеризации графов, в которой размер (то есть число вершин) каждого кластера ограничен фиксированным числом $p$, является NP-трудной при $p \geqslant 3$ и разрешимой за полиномиальное время при $p = 2$.

В работах [9, 10] исследована генерическая сложность общей проблемы кластеризации графов и проблемы кластеризации графов с ограничением на число кластеров. В рамках генерического подхода [11] алгоритмическая проблема изучается не на всём множестве входов, а на некотором естественном подмножестве «почти всех» входов. Здесь генерический алгоритм должен выдавать правильный ответ. Остальные «редкие» входы игнорируются, на них генерический алгоритм выдаёт ответ «не знаю». Понятие «почти все» уточняется введением асимптотической плотности на множестве входных данных. Отметим, что похожий подход для изучения проблем оптимизации предложен ранее в [12].

В исследованиях по генерической вычислимости и сложности вычислений можно выделить два основных направления. Первое связано с построением генерических (полиномиальных) алгоритмов для алгоритмических проблем, которые являются неразрешимыми или трудноразрешимыми в классическом смысле. Второе направление концентрируется на поиске алгоритмических проблем, которые остаются неразрешимыми или трудноразрешимыми и в генерическом смысле. Это второе направление имеет важное значение для современной криптографии, так как для построения криптосистем с открытым ключом не годятся алгоритмические проблемы, являющиеся легко разрешимыми для почти всех входов.

Данная работа посвящена изучению генерической сложности задачи кластеризации графов с ограничением $p$ на размеры кластеров при $p \geqslant 3$. Доказывается, что при условии $\mathrm{P} \neq \mathrm{NP}$ и $\mathrm{P} = \mathrm{BPP}$ для этой проблемы не существует полиномиального сильно генерического алгоритма. Отсюда, в частности, следует, что теоретически существует эффективная процедура генерации трудных входов данной проблемы, что указывает на потенциальную возможность её использования в криптографии. Здесь равенство $\mathrm{P} = \mathrm{BPP}$ означает, что любой вероятностный полиномиальный алгоритм можно эффективно дерандомизировать, то есть построить эквивалентный ему полиномиальный алгоритм, не использующий генератор случайных чисел. Эта гипотеза пока не доказана, однако имеются веские основания в пользу этого равенства [13].

## 1. Предварительные сведения

Определения сильно генерического полиномиального алгоритма можно найти в работах [9, 10]. С понятием вероятностного алгоритма можно познакомиться, например, в [14].

Здесь и далее будем рассматривать неориентированые графы без петель и кратных рёбер. Граф называется *кластерным*, если каждая его компонента связности является полным графом. Обозначим через $\mathcal{M}^{\leqslant p}(V)$ множество всех кластерных графов на множестве вершин $V$, у которых каждая компонента связности имеет не более $p$ вершин.

Если $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ — графы на одном и том же множестве вершин $V$, то *расстояние* $\rho(G_1, G_2)$ между ними есть число несовпадающих рёбер в графах $G_1$ и $G_2$, то есть

$$\rho(G_1, G_2) = |E_1 \triangle E_2| = |E_1 \setminus E_2| + |E_2 \setminus E_1|.$$

*Проблема p-кластеризации графа* состоит в следующем. Задан граф $G = (V, E)$. Найти такой граф $M^* \in \mathcal{M}^{\leqslant p}(V)$, что

$$\rho(G, M^*) = \min_{M \in \mathcal{M}^{\leqslant p}(V)} \rho(G, M).$$

**Лемма 1.** Пусть $G_1$ и $G_2$ — два графа с непересекающимися множествами вершин и $M^*$ — кластерный граф, являющийся решением проблемы $p$-кластеризации для графа $G_1 \cup G_2$. Тогда $M^* = M_1^* \cup M_2^*$, где $M_i^*$ — решение проблемы $p$-кластеризации для графа $G_i$, $i = 1, 2$.

***Доказательство.*** Пусть $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$. Допустим, что существует кластерный граф $M$, являющийся решением проблемы $p$-кластеризации для графа $G_1 \cup G_2$, такой, что

$$M = C_1 \cup C_2 \cup \ldots \cup C_m,$$

где $C_i$, $i = 1, \ldots, m$, — непересекающиеся полные компоненты связности с не более чем $p$ вершинами, причём среди них есть компонента $C_k = K(V_c)$, которая имеет непустое пересечение как с графом $G_1$, так и с графом $G_2$. Заменим в кластерном графе $M$ его компоненту $C_k$ на два полных графа $C_{k,i} = K(V_c \cap V_i)$, $i = 1, 2$. Очевидно, что число вершин каждого из этих графов не превосходит числа вершин $K(V_c)$, то есть оно не больше $p$. Вершины первого лежат в графе $G_1$, а второго — в $G_2$. Обозначим через $M'$ получившийся кластерный граф. Теперь заметим, что

$$\rho(G_1 \cup G_2, M') < \rho(G_1 \cup G_2, M),$$

так как в новых компонентах $C_{k,i}$, $i = 1, 2$, присутствуют все рёбра старой компоненты $C_k$, обе вершины которых лежат либо в $G_1$, либо в $G_2$, и отсутствуют все рёбра старой компоненты $C_k$, одна вершина которых лежит в $G_1$, а другая — в $G_2$. При этом последних рёбер нет и в графе $G_1 \cup G_2$.

Полученное противоречие показывает, что для кластерного графа $M^*$, являющегося решением проблемы $p$-кластеризации для графа $G_1 \cup G_2$, имеет место $M^* = M_1^* \cup M_2^*$, причём $M_i^*$ — решение проблемы $p$-кластеризации для графа $G_i$, $i = 1, 2$, так как иначе кластерный граф $M_i^*$ можно заменить на более подходящий, уменьшив тем самым расстояние $\rho(G_1 \cup G_2, M^*)$. ■

## 2. Основной результат

Будем использовать представление графов с помощью матриц смежности. Так как графы неориентированные, для кодирования графа с $n$ вершинами достаточно верхней части матрицы, состоящей из $n(n-1)/2$ бит. Таким образом, будем считать, что размер графа с $n$ вершинами равен $n(n-1)/2$. Обозначим через $\mathcal{G}$ множество всех графов с таким представлением.

**Теорема 1.** Не существует сильно генерического полиномиального алгоритма для решения проблемы $p$-кластеризации графов при $p \geqslant 3$, если $\mathrm{P} \neq \mathrm{NP}$ и $\mathrm{P} = \mathrm{BPP}$.

***Доказательство.*** Допустим, что существует сильно генерический полиномиальный алгоритм $\mathcal{A}$, решающий проблему $p$-кластеризации графа. Тогда существует

вероятностный полиномиальный алгоритм $\mathcal{B}$, разрешающий эту проблему на всём множестве входов. На графе $G$ с $n$ вершинами (размера $n(n-1)/2$) алгоритм $\mathcal{B}$ работает следующим образом:

1) генерирует случайный граф $H$ с $n^2-n$ вершинами;
2) запускает алгоритм $\mathcal{A}$ на графе $G \cup H$;
3) если $\mathcal{A}(G \cup H) \neq ?$, то по решению проблемы $p$-кластеризации для графа $G \cup H$, согласно лемме 1, выдаёт решение проблемы $p$-кластеризации для графа $G$;
4) если $\mathcal{A}(G \cup H) = ?$, то выдаёт ответ $K_n$.

Заметим, что полиномиальный вероятностный алгоритм $\mathcal{B}$ выдаёт правильный ответ на шаге 3, а на шаге 4 может выдать неправильный ответ. Нужно доказать, что вероятность того, что ответ выдаётся на шаге 4, меньше $1/3$.

Граф $G \cup H$ имеет $n^2$ вершин, то есть его размер равен $m = (n^4-n^2)/2$. Вероятность того, что для случайного графа $G \cup H$ имеет место $\mathcal{A}(G \cup H) = ?$, не больше

$$\frac{|\{G \in \mathcal{G} : \mathcal{A}(G) = ?\}_m|}{|\{G \cup H : H \in \mathcal{G}\}_m|} = \frac{|\{G \in \mathcal{G} : \mathcal{A}(G) = ?\}_m|}{|\mathcal{G}_m|} \frac{|\mathcal{G}_m|}{|\{G \cup H : H \in \mathcal{G}\}_m|}.$$

Так как множество $\{G \in \mathcal{G} : \mathcal{A}(G) = ?\}$ сильно пренебрежимое, то существует константа $\alpha > 0$, такая, что

$$\frac{|\{G \in \mathcal{G} : \mathcal{A}(G) = ?\}_m|}{|\mathcal{G}_m|} < \frac{1}{2^{\alpha m}} = \frac{1}{2^{\alpha(n^4-n^2)/2}}$$

для любого $n$.

С другой стороны, так как граф $H$ имеет $n^2-n$ вершин, то

$$|\{G \cup H : H \in \mathcal{G}\}_m| = |\{H : H \in \mathcal{G}\}_{((n^2-n)^2-(n^2-n))/2}| = 2^{(n^4-2n^3+n)/2}.$$

Отсюда

$$\frac{|\mathcal{G}_m|}{|\{G \cup H : H \in \mathcal{G}\}_m|} = \frac{2^{(n^4-n^2)/2}}{2^{(n^4-2n^3+n)/2}} = 2^{(2n^3-n^2+n)/2}.$$

Поэтому искомая вероятность не больше

$$\frac{2^{(2n^3-n^2+n)/2}}{2^{\alpha(n^4-n^2)/2}} < \frac{1}{3}$$

при больших $n$.

Теперь покажем, что при условиях P $\neq$ NP и P = BPP не существует полиномиального вероятностного алгоритма для решения проблемы $p$-кластеризации графов при $p \geqslant 3$. Действительно, пусть такой алгоритм существует. Так как проблема $p$-кластеризации графов при $p \geqslant 3$ является NP-трудной [8], существует полиномиально эквивалентная ей NP-полная проблема распознавания $A$. Из полиномиального вероятностного алгоритма для проблемы $p$-кластеризации графов легко получается полиномиальный вероятностный алгоритм для решения проблемы $A$. А так как P = BPP, то существует и детерминированный полиномиальный алгоритм для $A$, откуда P = NP. Противоречие. ■

## Заключение

В работе изучена генерическая сложность проблемы кластеризации графов с ограничением $p$ на размеры кластеров при $p \geqslant 3$. Доказано, что при условии $\mathrm{P} \neq \mathrm{NP}$ и $\mathrm{P} = \mathrm{BPP}$ для этой проблемы не существует полиномиального сильно генерического алгоритма. Этот результат показывает некоторый потенциал применения данной алгоритмической проблемы в криптографии, устанавливая, что существует возможность эффективно генерировать случайные трудные входы для этой задачи.

Автор выражает благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

## ЛИТЕРАТУРА

1. *Křivánek M. and Morávek J.* NP-hard problems in hierarchical-tree clustering // Acta Informatica. 1986. V. 23. P. 311–323.
2. *Bansal N., Blum A., and Chawla S.* Correlation clustering // Machine Learning. 2004. V. 56. P. 89–113.
3. *Shamir R., Sharan R., and Tsur D.* Cluster graph modification problems // Discrete Appl. Math. 2004. V. 144. No. 1–2. P. 173–182.
4. *Агеев А. А., Ильев В. П., Кононов А. В., Талевнин А. С.* Вычислительная сложность задачи аппроксимации графов // Дискретный анализ и исследование операций. Сер. 1. 2006. Т. 13. № 1. С. 3–11.
5. *Ильев В. П., Ильева С. Д.* О задачах кластеризации графов // Вестник Омского университета. 2016. № 2. С. 16–18.
6. *Ильев А. В., Ильев В. П.* Об одной задаче кластеризации графа с частичным обучением // Прикладная дискретная математика. 2018. № 42. С. 66–75.
7. *Талевнин А. С.* О сложности задачи аппроксимации графов // Вестник Омского университета. 2004. № 4. С. 22–24.
8. *Ильев В. П., Навроцкая А. А.* Вычислительная сложность задачи аппроксимации графами с компонентами связности ограниченного размера // Прикладная дискретная математика. 2011. № 3(13). С. 80–84.
9. *Рыбалов А. Н.* О генерической сложности проблемы кластеризации графов // Прикладная дискретная математика. 2019. № 46. С. 72–77.
10. *Рыбалов А. Н.* О генерической сложности ограниченной проблемы кластеризации графов // Прикладная дискретная математика. 2022. № 57. С. 91–97.
11. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
12. *Гимади Э. Х., Глебов Н. И., Перепелица В. А.* Алгоритмы с оценками для задач дискретной оптимизации // Проблемы кибернетики. 1975. Т. 31. С. 35–42.
13. *Impagliazzo R. and Wigderson A.* $\mathrm{P} = \mathrm{BPP}$ unless E has subexponential circuits: Derandomizing the XOR Lemma // Proc. 29th STOC. El Paso: ACM, 1997. P. 220–229.
14. *Вялый М., Китаев А., Шень А.* Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999. 192 с.

## REFERENCES

1. *Křivánek M. and Morávek J.* NP-hard problems in hierarchical-tree clustering. Acta Informatica, 1986, vol. 23, pp. 311–323.
2. *Bansal N., Blum A., and Chawla S.* Correlation clustering. Machine Learning, 2004, vol. 56, pp. 89–113.

3. *Shamir R., Sharan R., and Tsur D.* Cluster graph modification problems. Discrete Appl. Math., 2004, vol. 144, no. 1–2, pp. 173–182.
4. *Ageev A. A., Il'ev V. P., Kononov A. V., and Talevnin A. S.* Computational complexity of the graph approximation problem. J. Appl. Ind. Math., 2007, vol. 1, no. 1, pp. 1–8.
5. *Il'ev V. P. and Il'eva S. D.* O zadachakh klasterizatsii grafov [On problems of graph clustering]. Vestnik Omskogo Universiteta, 2016, no. 2, pp. 16–18. (in Russian)
6. *Il'ev A. V. and Il'ev V. P.* Ob odnoy zadache klasterizatsii grafa s chastichnym obucheniem [On a semi-superwized graph clustering problem]. Prikladnaya Diskretnaya Matematika, 2018, no. 42, pp. 66–75. (in Russian)
7. *Talevnin A. S.* O slozhnosti zadachi approksimatsii grafov [On the complexity of the graph approximation problem]. Vestnik Omskogo Universiteta, 2004, no. 4, pp. 22–24. (in Russian)
8. *Il'ev V. P. and Navrotskaya A. A.* Vychislitel'naya slozhnost' zadachi approksimatsii grafami s komponentami svyaznosti ogranichennogo razmera [Computational complexity of the problem of approximation by graphs with connected components of bounded size]. Prikladnaya Diskretnaya Matematika, 2011, no. 3(13), pp. 80–84. (in Russian)
9. *Rybalov A. N.* O generichеskoy slozhnosti problemy klasterizatsii grafov [On generic complexity of the graph clustering problem]. Prikladnaya Diskretnaya Matematika, 2019, no. 46, pp. 72–77. (in Russian)
10. *Rybalov A. N.* O generichеskoy slozhnosti ogranichennoy problemy klasterizatsii grafov [The generic complexity of the bounded problem of graphs clustering]. Prikladnaya Diskretnaya Matematika, 2022, no. 57, pp. 91–97. (in Russian)
11. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
12. *Gimadi E. X., Glebov N. I., and Perepelitsa V. A.* Algoritmy s otsenkami dlya zadach diskretnoy optimizatsii [Algorithms with bounds for problems of discrete optimization]. Problemy Kibernetiki, 1975, vol. 31, pp. 35–42. (in Russian)
13. *Impagliazzo R. and Wigderson A.* P = BPP unless E has subexponential circuits: Derandomizing the XOR Lemma. Proc. 29th STOC, El Paso, ACM, 1997, pp. 220–229.
14. *Vyalyy M., Kitaev A., and Shen' A.* Klassicheskie i kvantovye vychisleniya // Moscow, MCCME & CheRo Publ., 1999. 192 p. (in Russian)

# ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.8 DOI 10.17223/20710410/60/11

## РЕШЕНИЕ МАКСИ-СУММНОЙ ЗАДАЧИ РАЗМЕЩЕНИЯ НА СЕТИ С ОГРАНИЧЕНИЕМ НА ТРАНСПОРТНЫЕ ЗАТРАТЫ[1]

Г. Г. Забудский

*Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия*

**E-mail:** zabudsky@ofim.oscsbras.ru

Рассматривается задача оптимального размещения объекта на неориентированной взвешенной сети. Каждому ребру приписан положительный вес, а вершинам — два положительных параметра. Первый параметр отражает требование размещать объект как можно ближе к вершине, а второй — как можно дальше. Задано ограничение на суммарное взвешенное расстояние от объекта до вершин с учётом первого параметра. Необходимо найти допустимые места размещения объекта на рёбрах сети с максимальной суммой взвешенных расстояний от них до вершин с учётом второго параметра (локальные экстремумы). Предложен полиномиальный алгоритм поиска всех локальных экстремумов на рёбрах сети.

**Ключевые слова:** *задача размещения, макси-суммный критерий, опасный объект, сеть.*

## SOLVING OF THE MAXISUM LOCATION PROBLEM ON NETWORK WITH A RESTRICTION ON TRANSPORT COSTS

G. G. Zabudsky

*Sobolev Institute of Mathematics, Novosibirsk, Russia*

We consider the problem of the optimal location of a facility on an undirected weighted network. A positive weight is assigned to each edge. Two positive parameters are assigned to the vertices. The first parameter reflects the requirement to place the facility as close to the vertex as possible, and the second — as far as possible. There is a limit on the total weighted distance from the facility to the vertices, taking into account the first parameter. It is necessary to find acceptable locations of the facility on the edges of the network with the maximum sum of weighted distances from them to the vertices, taking into account the second parameter (local extremes). A polynomial algorithm is proposed to find all local extremums at the edges of the network.

**Keywords:** *location problem, maxisum criterion, undesirable facility, network.*

[1]Работа выполнена в рамках госзадания ИМ СО РАН, проект № FWNF-2022-0020.

## Введение

С развитием промышленного производства всё более актуальной становится проблема оптимального (рационального) размещения промышленных объектов. Увеличивается их влияние на природу, что может привести к экологическим проблемам. Растёт уровень жизни, и это повышает требования населения к окружающей среде. Поэтому необходимо размещать производства и другие объекты не только с учётом экономической эффективности, но при этом не ухудшать качество жизни для проживающего вблизи населения. Примерами объектов могут быть мусороперерабатывающие предприятия, свалки, аэропорты, хранилища опасных отходов. Они оказывают негативное влияние на жителей, проживающих вблизи. В то же время необходима доставка каких-либо материалов к этим объектам, например бытовых отходов населённых пунктов на мусороперерабатывающее предприятие. Транспортные расходы увеличиваются с удалением таких объектов от населения. Поэтому объекты должны размещаться как можно дальше от населённых пунктов, но не слишком далеко, чтобы расходы на обслуживание населения этими объектами не превышали некоторого бюджета. Исследования сложности решения задач такого класса можно найти в [1].

В теории оптимальных размещений ранее доминировали модели и методы определения размещений «желательных» объектов, таких, как магазины, больницы и пожарные депо, которые необходимо размещать вблизи населенных пунктов. Ситуация изменилась в 1970-х гг. с началом исследований по поиску размещений «нежелательных» (опасных) объектов. Позднее появление в литературе исследований таких задач имеет несколько причин, в частности то, что большинство нежелательных объектов являются побочными продуктами технологических достижений и индустриализации во второй половине XX века.

Критерием определения места размещения нежелательного объекта может быть максимизация некоторой возрастающей функции расстояний между объектом и клиентами. Критерии minisum (задача о медиане) и minimax (задача о центре) наиболее популярны для определения размещений желательных объектов. По аналогии, для нежелательных объектов часто применяются критерии maxisum и maximin [2–4]. Критерий maxisum применяется для максимизации суммы расстояний (среднего расстояния) между объектом и клиентами, в то время как цель maximin — максимизировать расстояние между объектом и ближайшим к нему клиентом. Клиентам могут быть приписаны параметры, чтобы отразить относительную несовместимость между клиентом и объектом. Критерии для нежелательных объектов часто называют критериями отталкивания (push), поскольку они отталкивают нежелательный объект от клиентов. Критерии для желательных объектов называют критериями притяжения (pull), поскольку они приближают объект к клиентам. Чтобы избежать размещения нежелательного объекта на бесконечном расстоянии от клиентов, что не имеет смысла в реальной задаче, рассматривается ограниченная область (сеть, многоугольник на плоскости). Задачи оптимизации размещения нежелательных объектов более трудные для решения. В отличие от задач размещения желательных объектов, они являются невыпуклыми с множеством локальных оптимумов.

Первой опубликованной работой о нахождении места размещения нежелательного объекта была работа [5]. Рассматривалась проблема поиска такой точки на общей сети, чтобы сумма взвешенных расстояний от неё до вершин сети была максимальной. Множество рассматриваемых решений было сокращено до конечного набора точек, которые представляют точки на рёбрах и висячие вершины сети. Впервые было показано, что задача с критерием maxisum — это невыпуклая задача, имеющая локальные опти-

мумы. Кроме того, не выполняется принцип оптимальности Хакими [6] (оптимальное решение можно искать в вершинах сети).

В данной работе рассматривается обобщение постановки задачи, предложенной в [5]. Заданы транспортная сеть, соединяющая населённые пункты, и бюджет на транспортные затраты по обслуживанию указанных пунктов некоторым объектом, оказывающим негативное влияние на население. Требуется разместить объект на сети таким образом, чтобы общие транспортные затраты не превышали бюджет и суммарное (среднее) отрицательное влияние объекта на население было минимальным. Предложен полиномиальный алгоритм поиска всех локальных экстремумов. Выбор конкретного места размещения из множества найденных локальных оптимумов может быть осуществлён лицом, принимающим решение, с учётом дополнительных требований к размещению.

## 1. Постановка задачи

Имеется некоторое число населенных пунктов (фиксированных объектов), соединённых между собой сетью дорог, и объект, который необходимо разместить на сети для обслуживания пунктов. Размещаемый объект оказывает негативное влияние на население. Влияние уменьшается с увеличением расстояния до объекта. Для каждого пункта заданы два параметра (веса). Первый отражает требование размещать объект ближе к пункту, например равен количеству населения в нем. Второй характеризует важность размещения объекта как можно дальше от пункта, например это величина, обратная количеству населения в пункте. Имеется бюджетное ограничение на общие транспортные затраты по обслуживанию объектом населённых пунктов. Требуется разместить объект на сети таким образом, чтобы общие транспортные затраты не превышали бюджет и суммарное отрицательное влияние на население было минимальным с учётом количества проживающих в пунктах (макси-суммный критерий).

Приведём математическую модель. Для этого введём обозначения: $G = (V, E)$ — неориентированная сеть, соответствующая населённым пунктам и дорогам; $V = \{v_1, \ldots, v_n\}$ — множество вершин, $N = \{1, \ldots, n\}$ — множество их номеров; $E = \{e_1, \ldots, e_m\}$ — множество рёбер, $M = \{1, \ldots, m\}$ — множество их номеров; $(w_i, \alpha_i)$, $w_i > 0$, $\alpha_i > 0$ — веса вершины $v_i$, $i \in N$; если $w_i > w_j$, то желательно, чтобы объект был размещен ближе к $v_i$, чем к $v_j$; если $\alpha_i < \alpha_j$, то желательно, чтобы объект находился на большем расстоянии от вершины $v_i$, чем от вершины $v_j$; $c(v_i, v_j) > 0$ — длина ребра $e_i = (v_i, v_j)$, $i, j \in M$; $z$ — размещаемый объект; $d(x, y)$ — длина кратчайшего пути между двумя точками $x$ и $y$ сети $G$; $S$ — бюджет на транспортные затраты по обслуживанию объектом населённых пунктов.

Необходимо найти такие точки на рёбрах сети $G$ для размещения объекта $z$, чтобы не нарушалось ограничение по бюджету и суммарное взвешенное расстояние до вершин сети было максимальным. Математическая модель задачи:

$$T_1(z) = \sum_{i=1}^{n} \alpha_i \, d(v_i, z) \to \max; \tag{1}$$

$$T_2(z) = \sum_{i=1}^{n} w_i \, d(v_i, z) \leqslant S. \tag{2}$$

Задача без ограничения на бюджет впервые была исследована в работе [5]. В отличие от задачи о медиане, в которой минимизируется суммарное взвешенное расстояние от медианы до вершин, в рассматриваемой задаче указанное расстояние максимизируется. При поиске медианы доказано, что оптимальное решение достаточно искать на

множестве вершин сети [6]. Переход от задачи минимизации к задаче максимизации приводит к тому, что оптимальное решение может находиться на рёбрах сети. Поиск максимума функции (1) на всей сети $G$ — это задача невыпуклого программирования. Основной результат работы [5] состоит в том, что нахождение оптимального решения сводится к анализу конечного множества точек. Для решения задачи (1) предложен полиномиальный алгоритм трудоёмкости $O(n^2)$. Позднее в работе [7] предложен алгоритм трудоёмкости $O(mn)$. Частный случай задачи (1)–(2) рассмотрен в [8]. Отметим, что для произвольного числа размещаемых объектов задача (1) является NP-трудной для сети, которая состоит из одного ребра [1].

Двухкритериальная задача размещения объекта на сети дорог, в которой один из критериев — это максимизация суммы взвешенных расстояний от объекта до вершин сети, рассмотрена в [9].

## 2. Алгоритм решения задачи (1)–(2)

Далее приведена общая схема алгоритма решения задачи (1)–(2), алгоритмы построения области допустимых решений и нахождения локальных оптимумов на рёбрах. Кроме того, предложен вариант вычисления верхней оценки значения целевой функции, который сокращает множество рассматриваемых рёбер сети в случае, когда ставится задача нахождения глобального оптимума.

### 2.1. Определения. Общая схема алгоритма

Для описания алгоритма решения задачи (1)–(2) введём некоторые обозначения [1]. Выберем произвольно ребро $(v_i, v_j)$. Через $z$ будем обозначать объект и расстояние от вершины $v_i$, $i < j$, на котором размещается объект $z$. Внутренняя точка $s$ на ребре $(v_i, v_j)$ делит его на два сегмента $(v_i, s)$ и $(v_j, s)$, длины которых обозначим $c(v_i, s) > 0$ и $c(v_j, s) > 0$ соответственно. Предполагается, что кратчайшие расстояния между вершинами известны. Они могут быть эффективно вычислены с помощью различных алгоритмов, например из [10]. Если существует вершина $v_k$, такая, что

$$d(v_k, v_i) + c(v_i, s) = d(v_k, v_j) + c(v_j, s),$$

то $s$ называется рёберной узкой точкой относительно вершины $v_k$. Через $B_A(v_k)$ обозначим множество указанных точек на сети по отношению к вершине $v_k$. Ребро $(v_i, v_j)$ содержит узкие точки по отношению к вершине $v_k$, когда выполняется неравенство

$$|d(v_k, v_i) - d(v_k, v_j| < c(v_i, v_j). \tag{3}$$

Аналогичное понятие узких точек можно определить для вершин. Если имеются рёбра $(v_i, v_j)$ и $(v_i, v_k)$, инцидентные вершине $v_i$, и вершина $v_l$, такая, что выполняется равенство

$$d(v_l, v_j) + c(v_i, v_j) = d(v_l, v_k) + c(v_k, v_i),$$

то вершина $v_i$ называется вершинной узкой точкой относительно вершины $v_l$. Множество таких точек обозначим через $B_N(v_l)$. Все рёберные и вершинные узкие точки принадлежат циклам в сети $G$.

Пусть $B_A = \bigcup\limits_{k \in N} B_A(v_k)$ — множество рёберных узких точек, $B_N = \bigcup\limits_{k \in N} B_N(v_k)$ — множество вершинных узких точек и $B = B_A \cup B_N$ — множество всех узких точек $G$. Через $D$ обозначим множество висячих вершин $G$. Очевидно, что $D \cap B = \varnothing$, поскольку

узкие точки связаны с циклами. В [1] сформулирована и доказана теорема, применение которой позволяет искать оптимальное решение задачи (1) на множестве $D \cup B$.

В [5] отмечается свойство вогнутости целевой функции (1) на ребре, на основании которого не надо рассматривать рёбра, в вершинах которых не выполняется бюджетное ограничение (2). Кроме того, можно предложить алгоритм поиска локальных экстремумов на ребре. Схематично это можно представить так. Решаем задачу о медиане на сети. Если значение целевой функции превосходит бюджет, то исходная задача не имеет решения. Если задача разрешима, убираем из рассмотрения рёбра, для вершин которых нарушается ограничение по бюджету. Затем на каждом из оставшихся рёбер находим все узкие точки, строим допустимое множество решений и определяем локальный оптимум. Приведём алгоритм решения задачи (1)–(2) на ребре $(v_i, v_j)$.

### 2.2. Нахождение узких точек

После удаления из рассмотрения рёбер, для вершин которых нарушается ограничение (2), на оставшихся рёбрах определяем область допустимых решений. Если в одной или обеих вершинах ребра выполняется неравенство (2), то покажем, что область допустимых решений задачи (1)–(2) на ребре может представлять всё ребро, отрезок или два отрезка. Для каждого такого отрезка одним из его концов является вершина ребра.

Для поиска узких точек предлагается следующий алгоритм. Фиксируем ребро $(v_i, v_j)$ и по очереди рассматриваем другие вершины сети $G$. Для текущей вершины $v_k$ проверяем справедливость неравенства (3).

Если неравенство не выполняется, то ребро $(v_i, v_j)$ не содержит рёберную узкую точку относительно $v_k$; переходим к другой вершине $G$.

Если неравенство выполняется, то ребро $(v_i, v_j)$ содержит рёберную узкую точку относительно вершины $v_k$. Это означает, что нет кратчайших путей от $v_i$ до $v_k$ и от $v_k$ до $v_j$, содержащих ребро $(v_i, v_j)$. Кратчайший путь от $v_k$ до $v_i$, ребро $(v_i, v_j)$ и кратчайший путь от $v_j$ до $v_k$ образуют цикл $C[v_k, (v_i, v_j)]$ в $G$. Расстояние $s$ от вершины $v_i$, на котором располагается узкая точка, равно

$$s = \big(|d(v_k, v_i) - d(v_k, v_j)| + c(v_i, v_j)\big)/2. \tag{4}$$

**Замечание 1.** Так как все кратчайшие пути от $v_k$ до $v_i$ и от $v_k$ до $v_j$ равны по длине, то им будет соответствовать одна узкая точка относительно вершины $v_k$. Перебирая все вершины сети $G$, найдём все рёберные узкие точки на ребре $(v_i, v_j)$.

**Замечание 2.** Любая вершина, входящая в цикл $C[v_k, (v_i, v_j)]$, образует узкую точку на ребре $(v_i, v_j)$.

**Замечание 3.** Вершинные узкие точки необходимо находить при поиске глобального оптимума.

**Замечание 4.** Рёберные и вершинные узкие точки определяются только длинами кратчайших путей в сети $G$, которые не зависят от весов вершин. Поэтому множество узких точек для функций $T_1$ и $T_2$ совпадают.

### 2.3. Построение области допустимых решений

Если в одной или обеих вершинах ребра $(v_i, v_j)$ выполняется ограничение по бюджету, то после построения всех узких точек на ребре определяем область допустимых решений. Так как функция (2) вогнутая и кусочно-линейная на ребре с точками перегиба в узких точках, находим узкие точки и упорядочиваем их по возрастанию

расстояний от вершины $v_i$: $s_1 < s_2 < \ldots < s_n$. Последовательно вычисляем значение функции (2) в найденных точках по формуле

$$T_2(s_i) = \sum_{i \in N} w_i \min\{d(v_k, v_i) + s_i; d(v_k, v_j) + c(v_i, v_j) - s_i\}.$$

Возможны следующие варианты:

1) $T_2(v_i) < S$, $T_2(v_j) < S$.

1.1. Последовательно просматриваем узкие точки. Найдётся пара точек $s_t$ и $s_{t+1}$, такая, что $T_2(s_t) < S$ и $T_2(s_{t+1}) > S$. Строим уравнение прямой $l(s_t, s_{t+1})$ через точки $(s_t, T_2(s_t))$ и $(s_{t+1}, T_2(s_{t+1}))$. Решаем уравнение $l(s_t, s_{t+1}) = S$ и находим точку $z_1$, в которой $T_2(z_1) = S$. Далее вычисляем значение функции $T_2$ в точках $s_{t+2}, s_{t+3}$ и т. д. Найдётся $k$, такое, что $T_2(s_k) > S$, а $T_2(s_{k+1}) < S$. Строим уравнение прямой $l(s_k, s_{k+1})$ через указанную пару точек. Решаем уравнение $l(s_k, s_{k+1}) = S$ и находим точку $z_2$, такую, для которой $T_2(z_2) = S$. Таким образом, на данном ребре найдены две точки $z_1$ и $z_2$, такие, что $T_2(z_1) = T_2(z_2) = S$. Область допустимых решений представляет два отрезка $[v_i, z_1]$ и $[v_j, z_2]$.

1.2. Если найдётся пара точек $s_t$ и $s_{t+1}$, такая, что $T_2(s_t) > T_2(s_{t+1})$ и $T_2(s_t) < S$, то все точки ребра образуют область допустимых решений.

2) $T_2(v_i) < S$, $T_2(v_j) > S$.

Найдётся пара точек $s_t$ и $s_{t+1}$, такая, что $T_2(s_t) < S$ и $T_2(s_{t+1}) > S$. Строим уравнение прямой $l(s_t, s_{t+1})$ через точки $(s_t, T_2(s_t))$ и $(s_{t+1}, T_2(s_{t+1}))$. Решаем уравнение $l(s_t, s_{t+1}) = S$ и находим точку $z_1$, в которой $T_2(z_1) = S$. Область допустимых решений представляет отрезок $[v_i, z_1]$.

3) $T_2(v_i) > S$, $T_2(v_j) < S$.

Найдётся пара точек $s_t$ и $s_{t+1}$, такая, что $T_2(s_t) > S$ и $T_2(s_{t+1}) < S$. Строим уравнение прямой $l(s_t, s_{t+1})$ через точки $(s_t, T_2(s_t))$ и $(s_{t+1}, T_2(s_{t+1}))$ и решаем уравнение $l(s_t, s_{t+1}) = S$. Находим точку $z_2$, такую, что $T_2(z_1) = S$. Область допустимых решений представляет отрезок $[z_2, v_j]$.

### 2.4. Локальные оптимумы на ребре. Верхняя оценка целевой функции

В случае 1.1 если $T_1(z_1) \geqslant T_1(z_2)$, то $z_1$ будет локальным максимумом на ребре, иначе $z_2$ — локальный максимум.

В случае 1.2 вычисляем значения функции $T_1$ в узких точках по формуле

$$T_1(s_t) = \sum_{k \in N} w_k \min\{d(v_k, v_i) + s_t; d(v_k, v_j) + c(v_i, v_j) - s_t\}$$

и выбираем узкую точку с максимальным значением. Если для пары точек $s_t$ и $s_{t+1}$ выполняется равенство $T_1(s_t) = T_1(s_{t+1})$, то локальный максимум на ребре представляет отрезок $[s_t, s_{t+1}]$.

В случае 2 $z_1$ — локальный максимум, а в случае 3 $z_2$ — локальный максимум.

В результате на ребре локальный максимум — это одна точка, две или отрезок. Трудоёмкость поиска узких точек равна $O(n^2)$. Тогда трудоёмкость алгоритма построения всех локальных оптимумов на сети оценивается как $O(mn^2)$.

Отметим, что глобальный оптимум можно найти, перебирая локальные оптимумы на рёбрах. При этом некоторые рёбра можно исключить из рассмотрения, используя верхнюю оценку значения функции $T_1$. Так как функция $T_1$ вогнутая кусочно-линейная, то для получения верхней оценки её значения на ребре $(v_i, v_j)$ можно найти ближайшую к $v_i$ узкую точку и максимально удалённую от неё точку. Расстояние $s$

от вершины $v_i$ до узкой точки определяется по формуле (4). Ближайшая узкая точка будет образована некоторой вершиной $v_k$, которой соответствует минимальная разность между длинами кратчайших путей от $v_k$ до вершин $v_i$ и $v_j$. Максимально удалённая от $v_i$ узкая точка будет образована вершиной сети, для которой аналогичная разность будет максимальной. Таким образом определяются узкие точки $s_1$ и $s_n$. Строятся уравнения прямых через точки $(0, T_1(v_i))$ и $(s_1, T_1(s_1))$ и через точки $(s_n, T_1(s_n))$ и $(c(v_i, v_j), T_1(v_j))$. Из свойств функции $T_1$ следует, что точка пересечения указанных прямых — это верхняя оценка целевой функции на ребре $(v_i, v_j)$.

## Заключение

Рассмотрена задача поиска всех локальных экстремумов оптимального размещения опасного объекта на сети дорог, соединяющих населённые пункты. Предложен полиномиальный алгоритм решения задачи.

## ЛИТЕРАТУРА


1. *Tamir A.* Obnoxious facility location on graphs // SIAM J. Discrete Math. 1991. V. 4. No.4. P. 550–567.
2. *Drezner Z.* Facility Location. A Survey of Applications and Methods. N.Y.: Springer, 1995. 571 p.
3. *Eiselt H. A. and Marianov V.* Foundations of Location Analysis. N.Y.: Springer, 2011. 509 p.
4. *Zabudsky G. G. and Lisina M. S.* Approximately algorithm for maximin location problem on network // Dynamics of Systems, Mechanisms and Machines. XII Intern. Conf. Omsk, Russia, 13–15 November 2018. https://ieeexplore.ieee.org/document/8601502.
5. *Church R. L. and Garfinkel R. S.* Locating an obnoxious facility on a network // Trans. Sci. 1978. V. 12. No. 2. P. 107–118.
6. *Hakimi S. L.* Optimal location of switching centers and the absolute centers and medians of a graph // Oper. Res. 1964. V. 12. No. 3. P. 450–459.
7. *Berman O. and Drezner Z.* A note on the location of an obnoxious facility on a network // Eur. J. Oper. Res. 2000. V. 120. No. 1. P. 215–217.
8. *Забудский Г. Г.* Размещение опасного объекта на сети с ограничением на транспортные затраты // Проблемы машиноведения. VI Междунар. науч.-техн. конф. Омск, 22–23 марта 2022. С. 162–165.
9. *Heydari R. and Melachrinoudis E.* Location of a semi-obnoxious facility with elliptic maxmin and network minisum objectives // Eur. J. Oper. Res. 2012. V. 223. No. 2. P. 452–460.
10. *Xy T.* Целочисленное программирование и потоки в сетях. М.: Мир, 1974. 519 с.


## REFERENCES


1. *Tamir A.* Obnoxious facility location on graphs. SIAM J. Discrete Math., 1991, vol. 4, no. 4, pp. 550–567.
2. *Drezner Z.* Facility Location. A Survey of Applications and Methods. N.Y., Springer, 1995. 571 p.
3. *Eiselt H. A. and Marianov V.* Foundations of Location Analysis. N.Y., Springer, 2011. 509 p.
4. *Zabudsky G. G. and Lisina M. S.* Approximately algorithm for maximin location problem on network. Dynamics of Systems, Mechanisms and Machines. XII Intern. Conf., Omsk, Russia, 13–15 November 2018, https://ieeexplore.ieee.org/document/8601502.
5. *Church R. L. and Garfinkel R. S.* Locating an obnoxious facility on a network. Trans. Sci., 1978, vol. 12, no. 2, pp. 107–118.

6. *Hakimi S. L.* Optimal location of switching centers and the absolute centers and medians of a graph. Oper. Res., 1964, vol. 12, no. 3, pp. 450–459.
7. *Berman O. and Drezner Z.* A note on the location of an obnoxious facility on a network . Eur. J. Oper. Res., 2000, vol. 120, no. 1, pp. 215–217.
8. *Zabudskiy G. G.* Razmeshchenie opasnogo ob"ekta na seti s ogranicheniem na transportnye zatraty [Location an undesirable facility on the network with a restriction on transportation costs]. Mechanical Science and Technology Update, VI Intern. Conf., Omsk, Russia, 22–23 March 2022, pp. 162–165. (in Russian)
9. *Heydari R., Melachrinoudis E.* Location of a semi-obnoxious facility with elliptic maxmin and network minisum objectives. Eur. J. Oper. Res., 2012, vol. 223, no. 2, pp. 452–460.
10. *Hu T. C.* Integer Programming and Network Flows. Addison-Wesley Publ., 1969. 452 p.

# СВЕДЕНИЯ ОБ АВТОРАХ

**БАЛДЖАНОВА Роза Вагиф кызы** — аспирантка Омского государственного университета им. Ф. М. Достоевского, г. Омск. E-mail: **baldzhanova@mail.ru**

**БЕЛОВ Александр Романович** — аспирант Ярославского государственного университета им. П. Г. Демидова, г. Ярославль. E-mail: **ashmedey@gmail.com**

**ГРУБА Андрей Алексеевич** — научный сотрудник ООО «Центр сертификационных исследований», г. Москва. E-mail: **andreyka7kc@gmail.com**

**ЕГОРУШКИН Олег Игоревич** — кандидат физико-математических наук, доцент кафедры прикладной математики Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **egorushkin.o@yandex.ru**

**ЗАБУДСКИЙ Геннадий Григорьевич** — доктор физико-математических наук, профессор, ведущий научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **zabudsky@ofim.oscsbras.ru**

**ИЛЬЕВ Артём Викторович** — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Омск.
E-mail: **artyom_iljev@mail.ru**

**ИЛЬЕВ Виктор Петрович** — доктор физико-математических наук, профессор, профессор Омского государственного университета им. Ф. М. Достоевского, г. Омск, ведущий научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Омск.
E-mail: **iljev@mail.ru**

**КОЛБАСИНА Ирина Валерьевна** — старший преподаватель кафедры прикладной математики Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **kabaskina@yandex.ru**

**КОЛОМЕЕЦ Николай Александрович** — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **kolomeec@math.nsc.ru**

**МАРТЫНЕНКОВ Игорь Владимирович** — АО «КВАНТ-ТЕЛЕКОМ», г. Москва.
E-mail: **mivpost@yandex.ru**

**МЕДВЕДЕВ Анатолий Александрович** — студент Московского государственного технического университета им. Н. Э. Баумана, г. Москва.
E-mail: **medvedevaa@student.bmstu.ru**

**ПОТТОСИН Юрий Васильевич** — кандидат физико-математических наук, доцент, ведущий научный сотрудник Объединенного института проблем информатики Национальной академии наук Беларуси, доцент Белорусского государственного университета информатики и радиоэлектроники, г. Минск.
E-mail: **pott@newman.bas-net.by**

**РЫБАЛОВ Александр Николаевич** — кандидат физико-математических наук, старший научный сотрудник лаборатории комбинаторных и вычислительных методов

алгебры и логики Института математики им. С. Л. Соболева СО РАН, г. Омск. E-mail: **alexander.rybalov@gmail.com**

**САФОНОВ Константин Владимирович** — доктор физико-математических наук, профессор, заведующий кафедрой прикладной математики Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **safonovkv@rambler.ru**

**СУТОРМИН Иван Александрович** — аспирант Новосибирского государственного университета, г. Новосибирск. E-mail: **ivan.sutormin@gmail.com**

**ТИССИН Александр Сергеевич** — ООО «Центр сертификационных исследований», г. Москва. E-mail: **at_science@mail.ru**

Журнал «Прикладная дискретная математика» входит в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание учёной степени кандидата и доктора наук по специальностям 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (технические науки), 2.3.6. Методы и системы защиты информации, информационная безопасность (физико-математические и технические науки), 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика (физико-математические науки), 1.2.3. Теоретическая информатика, кибернетика (физико-математические науки), а также в перечень журналов, рекомендованных ФУМО ВО ИБ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал индексируется в базах данных Web of Science (Emerging Sources Citation Index (ESCI) и Russian Science Citation Index (RSCI)), Scopus, MathSciNet и Zentralblatt MATH.

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также правила подготовки рукописей статей для публикации в журнале.

**Тематика публикаций журнала:**

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*