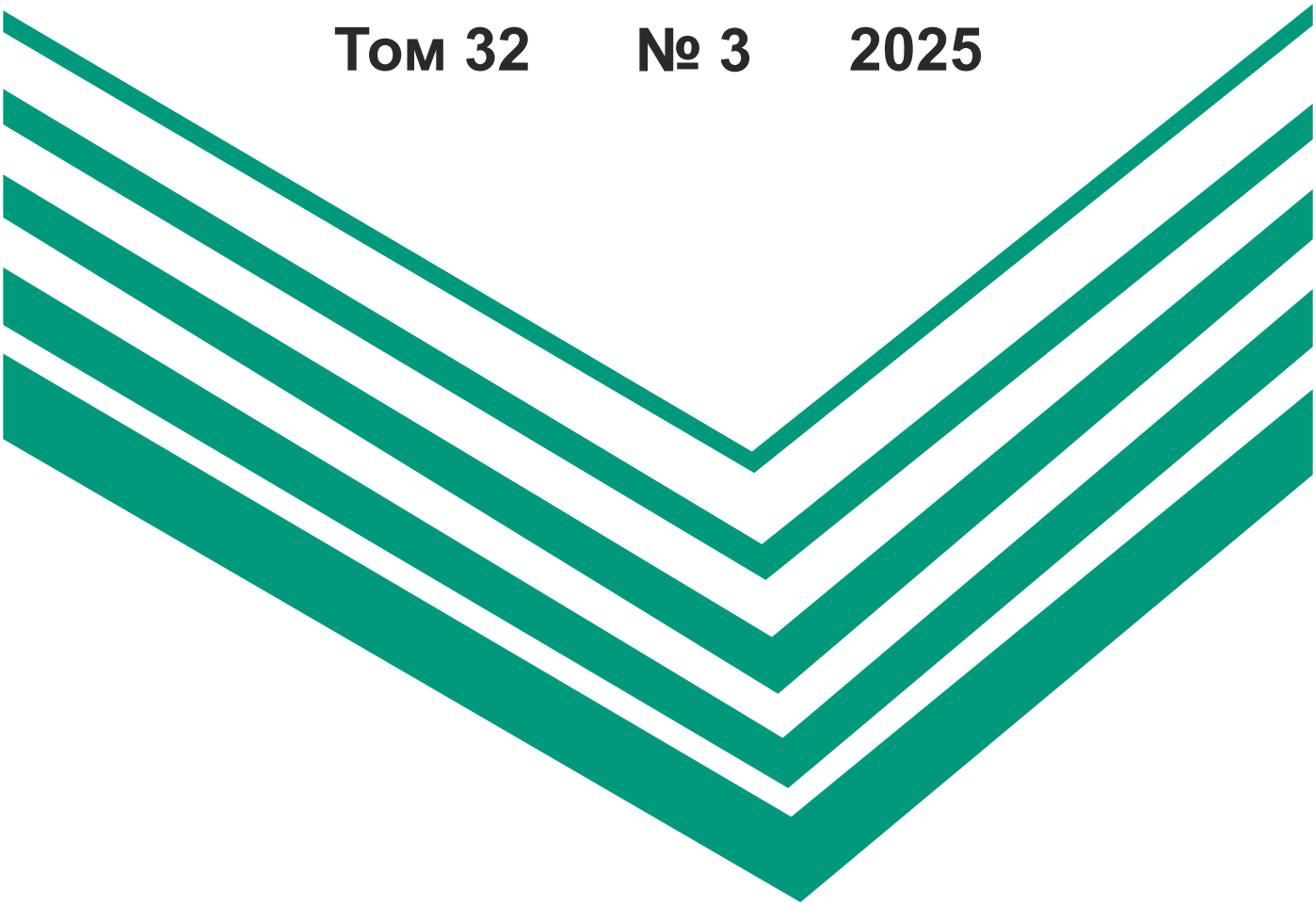
ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 32 № 3 2025



Новосибирск
Издательство Института математики

Учредители журнала Сибирское отделение РАН
Институт математики им. С. Л. Соболева СО РАН

Журнал включён в базу данных Russian Science Citation Index (RSCI) на платформе Web of Science. Переводы статей на английский язык публикуются в *Journal of Applied and Industrial Mathematics* и доступны по ссылке `www.springer.com/mathematics/journal/11754`.

СИБИРСКОЕ ОТДЕЛЕНИЕ РОССИЙСКОЙ АКАДЕМИИ НАУК
ИНСТИТУТ МАТЕМАТИКИ им. С. Л. СОБОЛЕВА СО РАН

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Выпускается с 1994 г. Научный журнал 4 номера в год

Том 32, № 3 (165) **Июль–сентябрь 2025**

СОДЕРЖАНИЕ

Быков Д. А., Коломеец Н. А. *О ближайших бент-функциях к заданной бент-функции Мэйорана — МакФарланда* **5**

Водян М. Е., Панин А. А., Плясунов А. В. *Максимизация радиуса пороговой устойчивости в модели размещения производства и фабричного ценообразования* **43**

Еремеев А. В. *О вычислительной сложности задачи синтеза антенной решётки* **71**

Лежнин М. В., Хвощевский Д. А. *Обобщённые централизаторы бинарного отношения* **84**

Монахова Э. А., Монахов О. Г. *Поиск и исследование идеальных двумерных циркулянтных сетей на основе графовых баз данных* **98**

Юськов А. Д., Кулаченко И. Н., Мельников А. А., Кочетов Ю. А. *Гибридный алгоритм для двухкритериальной задачи оптимизации трафика в сети* **117**

НОВОСИБИРСК
ИЗДАТЕЛЬСТВО ИНСТИТУТА МАТЕМАТИКИ

В журнале публикуются оригинальные научные статьи и обзоры теоретической и прикладной направленности по следующим разделам дискретного анализа, исследования операций и информатики:

- дискретная оптимизация
- комбинаторика
- контроль и надёжность дискретных устройств
- математические модели и методы принятия решений
- математическое программирование
- модели экономики
- моделирование процессов управления
- построение и анализ алгоритмов
- синтез и сложность управляющих систем
- теория автоматов
- теория графов
- теория игр и её приложения
- теория кодирования
- теория расписаний и размещений

Адрес редакции:
Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия
Телефон: +7 (383) 329–75–79
E-mail: discopr@math.nsc.ru

SIBERIAN BRANCH OF THE RUSSIAN ACADEMY OF SCIENCES
SOBOLEV INSTITUTE OF MATHEMATICS

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII

/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/

Published since 1994 | Scientific journal | 4 issues per year

Vol. 32, No. 3 (165) | **July–September, 2025**

CONTENTS

D. A. Bykov and **N. A. Kolomeec.** *On the bent functions closest to a given Maiorana–McFarland bent function* **5**

M. E. Vodyan, A. A. Panin, and **A. V. Plyasunov.** *Maximizing the threshold stability in the model of facility location and the mill pricing* . **43**

A. V. Eremeev. *On computational complexity of phased antenna array synthesis* **71**

M. V. Lezhnin and **D. A. Khvoshchevskiy.** *Generalized centralizers of a binary relation* **84**

E. A. Monakhova and **O. G. Monakhov.** *Search and research of ideal two-dimensional circulant networks based on graph databases* **98**

A. D. Yuskov, I. N. Kulachenko, A. A. Melnikov, and **Y. A. Kochetov.** *A hybrid algorithm for a two-objective traffic engineering problem* **117**

NOVOSIBIRSK
SOBOLEV INSTITUTE PRESS

In this journal we publish original research papers and survey papers of both theoretical and practical importance on the following topics of discrete analysis, operations research and informatics:

- discrete optimization
- combinatorics
- control and reliability of discrete devices
- decision making models and methods
- mathematical programming
- economic models
- management modeling
- design and analysis of algorithms
- synthesis and complexity of control systems
- automata theory
- graph theory
- game theory and its applications
- coding theory
- theory of scheduling and facility location

Editorial office address:
Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue,
630090 Novosibirsk, Russia
Phone: +7 (383) 329–75–79
E-mail: discopr@math.nsc.ru

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 5–42

УДК 519.7 DOI: 10.33048/daio.2025.32.811

О БЛИЖАЙШИХ БЕНТ-ФУНКЦИЯХ К ЗАДАННОЙ БЕНТ-ФУНКЦИИ МЭЙОРАНА — МАКФАРЛАНДА

Д. А. Быков [a], *Н. А. Коломеец* [b]

Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
E-mail: [a] den.bykov.2000i@gmail.com, [b] nkolomeec@gmail.com

Аннотация. Исследуются бент-функции от $2n$ переменных, ближайшие к заданной функции из класса Мэйорана — МакФарланда. Переформулирован критерий расположения таких бент-функций, и уточнён метод подсчёта их числа. Исследованы функции с числом ближайших бент-функций, близким к его нижней и точной верхней оценкам. Доказано существование бент-функций, у которых число ближайших бент-функций имеет ту же асимптотику, что и нижняя оценка. Приведены примеры функций из класса Мэйорана — МакФарланда, для которых рассчитанное число ближайших бент-функций близко к верхней оценке. Рассматривается также достижимость нижней оценки, а именно, усилены известные необходимые и достаточные условия. Показано, что нижняя оценка достигается при n, равном степени простого числа $p \geqslant 5$, а также при некоторых других n. Приведена полная классификация функций от 6 переменных из класса Мэйорана — МакФарланда по числу ближайших бент-функций. Табл. 1, библиогр. 40.

Ключевые слова: бент-функция, булева функция, аффинное подпространство, минимальное расстояние, класс Мэйорана — МакФарланда.

Введение

Бент-функции — булевы функции от чётного числа переменных, обладающие максимальной нелинейностью — впервые введены в рассмотрение в 1960-х гг. Их название появилось в работе Ротхауса [1], а в СССР В. А. Елисеев и О. П. Степченков называли их минимальными [2]. Бент-функции интересны своими приложениями в криптографии, алгебре, теории кодирования, теории символьных последовательностей и т. д. О них написаны обзоры и книги [2–7], а общую информацию о криптографических свойствах булевых функций можно найти в [8–14].

В данной работе рассматриваются метрические свойства бент-функций, а именно бент-функции, ближайшие относительно метрики Хэмминга к некоторой заданной бент-функции из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$ от $2n$ переменных, который независимо ввели Мэйорана и МакФарланд, аналогичную конструкцию предложил также В. А. Елисеев (см. [2, 15]). Этот класс состоит из бент-функций вида

$$f_{\pi,\varphi}(x,y) = \langle x, \pi(y)\rangle \oplus \varphi(y), \quad x,y \in \mathbb{F}_2^n,$$

где π — подстановка на $\mathbb{F}_2^n$, $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2$, и наряду с классом $\mathcal{PS}$ [16] является одной из базовых конструкций бент-функций. Известно [17], что все ближайшие к $f_{\pi,\varphi}$ бент-функции находятся на расстоянии 2^n и имеют вид

$$f_{\pi,\varphi} \oplus \mathrm{Ind}_L, \quad L \in \mathcal{LA}_n(f_{\pi,\varphi}), \tag{1}$$

где $\mathcal{LA}_n(f_{\pi,\varphi})$ — множество всех аффинных подпространств $L \subseteq \mathbb{F}_2^{2n}$ размерности n, на которых $f_{\pi,\varphi}$ аффинна. Конструкция (1), впервые описанная в [16] и применимая к любой бент-функции, позволяет строить бент-функции разных классов, поэтому она интересна и вне метрических свойств. На её основе построен класс $\mathcal{D}$ [18], выходящий за пределы замыканий $\mathcal{M}_{2n}$ и $\mathcal{PS}$ относительно EA-эквивалентности [18–20]. Свойства схожей с (1) конструкции для аффинных подпространств L произвольной размерности рассматривались в [18, 21–24], а построение бент-функций, не принадлежащих замыканию $\mathcal{M}_{2n}$, исследовалось также в [25–27]. Таким образом, мощность $\mathcal{LA}_n(f_{\pi,\varphi})$ характеризует как размер минимальной окрестности $f_{\pi,\varphi}$ (метрические свойства), так и число бент-функций, порождаемых конструкцией (1).

Для $|\mathcal{LA}_n(f_{\pi,\varphi})|$ справедливы оценки

$$\ell_{2n} = 2^{2n+1} - 2^n \leqslant |\mathcal{LA}_n(f_{\pi,\varphi})| \leqslant 2^n(2^1+1)(2^2+1)\dots(2^n+1) = \mathcal{U}_{2n}.$$

Верхняя оценка $\mathcal{U}_{2n}$ верна для произвольной бент-функции и точна: она достигается на всех квадратичных бент-функциях и только на них [29]. Нижняя оценка ℓ_{2n} впервые представлена в [28], она тесно связана и с пересечениями классов: все учтённые в ней бент-функции лежат в $\mathcal{M}_{2n}$, а все неучтённые — вне его [29]. Таким образом, её достижимость влечёт отсутствие ближайших к $f_{\pi,\varphi}$ бент-функций за пределами $\mathcal{M}_{2n}$. Этот вопрос исследуется в [30], где показано, что ℓ_{2n} достижима при простых $n \geqslant 5$. В то же время, для равенства $|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n}$ необходимо, чтобы π была APN-подстановкой [31]. Однако вопрос существования таких подстановок при чётных $n \geqslant 8$ является открытым (the big APN problem) [32].

В рамках данной работы мы предлагаем ещё одну формулировку критерия для $L \in \mathcal{LA}_n(f_{\pi,\varphi})$ в конструкции (1), используя отличное от [30]

представление аффинных подпространств $\mathbb{F}_2^n \times \mathbb{F}_2^n$, и демонстрируем подсчёт $|\mathcal{LA}_n(f_{\pi,\varphi})|$ для некоторых $f_{\pi,\varphi}$. Например, все функции из $\mathcal{M}_6$ классифицированы по значению $|\mathcal{LA}_3(f_{\pi,\varphi})|$. Результаты позволяют усилить как необходимое, так и достаточное условия достижимости ℓ_{2n}, а также выделить бент-функции с близким к ℓ_{2n} или $\mathcal{U}_{2n}$ размером $\mathcal{LA}_n(f_{\pi,\varphi})$, для которых при $n \to \infty$ имеет место одно из равенств

$$|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n} + o(\ell_{2n}), \quad |\mathcal{LA}_n(f_{\pi,\varphi})| = \frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n}).$$

Поскольку любая бент-функция $f_{\pi,\varphi} \in \mathcal{M}_{2n}$ «собрана» из 2^n аффинных ограничений на $\mathbb{F}_2^n \times \{y\}$ для $y \in \mathbb{F}_2^n$, функции с $|\mathcal{LA}_n(f_{\pi,\varphi})|$, близким к $\mathcal{U}_{2n}$ (ℓ_{2n}), можно считать наиболее «простыми» («сложными»).

Структура работы следующая. В разд. 1 приводятся необходимые определения. В разд. 2 переформулирован критерий из [30] расположения ближайших бент-функций к $f_{\pi,\varphi} \in \mathcal{M}_{2n}$ в более удобном для вычисления их числа виде (теорема 1). Отличие состоит в представлении аффинных подпространств $\mathbb{F}_2^n \times \mathbb{F}_2^n$, основанном на их пересечении с $\mathbb{F}_2^n \times \{0\}^n$ и проекции на $\{0\}^n \times \mathbb{F}_2^n$ (см. п. 2.1), и использовании специального линейного оператора $\mathcal{G}_\pi^L$ ($\mathcal{G}_\pi$) (п. 2.2), через образ и размер ядра которого выражается число ближайших к $f_{\pi,\varphi}$ бент-функций (следствие 1, см. также теорему 3). Его удобство обусловлено возможностью до определённой степени отделить свойства π от свойств φ. Важно, что допускается представление $f_{\pi,\varphi}$ как над $\mathbb{F}_2^n \times \mathbb{F}_2^n$, так и над $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$: во всех ключевых теоремах предполагается, что $f_{\pi,\varphi}(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y)$, где $\langle\cdot,\cdot\rangle_n$ — произвольная невырожденная симметричная билинейная форма на $\mathbb{F}_2^n$. Доказанная в п. 2.3 теорема 2 упрощает работу с $\mathcal{G}_\pi^L$ с помощью перехода к «естественной» билинейной форме, определённой на $\mathbb{F}_2^{\dim L} \times \mathbb{F}_2^{\dim L}$.

В разд. 3 найдены мощность ядра и образ оператора $\mathcal{G}_\pi$ для некоторых подстановок π: аффинных, зависящих от не более чем трёх переменных (п. 3.1), а также для функции инверсии элементов $\mathbb{F}_{2^n}$ (п. 3.2). Все полученные далее утверждения и теоремы демонстрируют применение результатов из разд. 2 и 3 к конкретным бент-функциям $f_{\pi,\varphi}$.

В разд. 4 изучается достижимость нижней оценки ℓ_{2n} числа ближайших к $f_{\pi,\varphi}$ бент-функций, для этого уточнена общая формула подсчёта их числа (теорема 3). Данная теорема позволила получить как следствие усиление результата [30] о необходимости для π быть APN-подстановкой при $|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n}$: L и его образ $\pi(L)$ не должны быть одновременно аффинными подпространствами $\mathbb{F}_2^n$ размерности 3 (следствие 2). Усилено и достаточное условие достижимости ℓ_{2n} из [30]: доказано, что оценка гарантированно достигается не только при простых $n \geqslant 5$, но и при любых степенях таких простых чисел (теорема 4 и следствие 3).

В разд. 5 теорема 3 применяется для подсчёта числа ближайших к $f_{\pi,\varphi}$ бент-функций, близкого к его нижней ℓ_{2n} или верхней $\mathcal{U}_{2n}$ оценкам. В п. 5.1 доказано существование функции $f_{\pi,\varphi} \in \mathcal{M}_{2n}$, для которой $|\mathcal{LA}_n(f_{\pi,\varphi})| < 2^{2n+1} + 81 \cdot 2^n - 82$, причём неравенство превращается в равенство $\ell_{2n} + o(\ell_{2n})$ при $n \to \infty$ (теорема 5). Следствием является достижимость оценки ℓ_{2n} при некоторых других n (следствие 5). В качестве π здесь используется функция инверсии элементов $\mathbb{F}_{2^n}$.

В п. 5.2 для $f_\varphi(x, y) = \langle x, y\rangle \oplus \varphi(y)$ приведена формула мощности $\mathcal{LA}_n(f_\varphi)$, использующая нетривиальные параметры φ (следствие 6). Далее для $\varphi_m(y_1, \ldots, y_n) = y_1 \ldots y_m$, где $3 \leqslant m \leqslant n$ дано явное выражение для $|\mathcal{LA}_n(f_{\varphi_m})|$ (следствие 7, см. также утверждение 11 и замечание 4 о расширении класса функций φ). В случаях $m = 3$ и $m = n$ получены краткие формулы, по виду близкие к оценке $\mathcal{U}_{2n}$; из них следует, что при $n \to \infty$ величина $|\mathcal{LA}_n(f_{\varphi_m})|$ имеет порядок $o(\mathcal{U}_{2n})$ и $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ соответственно (следствие 8). Показано также, что бент-функция f_τ, построенная с помощью транспозиции $\tau\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и тождественно нулевой φ, имеет $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_{\varphi_n})|$ (утверждение 12 и замечание 5). Выдвинута гипотеза, что это максимальное возможное число ближайших бент-функций для неквадратичной бент-функции (гипотеза 1).

В разд. 6 показано, что из теоремы 3 следует классификация всех $f \in \mathcal{M}_6$ по мощности $\mathcal{LA}_3(f)$, которая в данном случае является полным инвариантом относительно EA-эквивалентности (теорема 6).

1. Определения

1.1. Булевы функции. Пусть $\mathbb{F}_{2^k}$ — конечное поле, состоящее из 2^k элементов, и $\mathbb{F}_2^n = \{(x_1, x_2, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{F}_2\}$ — векторное пространство размерности n над полем $\mathbb{F}_2$, сложение в котором обозначено через $\oplus$. Функция $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных. Функция $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется *векторной булевой функцией* и представляет собой упорядоченный набор m булевых функций от n переменных, каждая из которых называется *координатной*, а их нетривиальная линейная комбинация — *компонентной* функцией. Булевы функции будем рассматривать в том числе как частный случай векторных булевых функций.

Любая векторная булева функция $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ единственным образом представляется в виде *полинома Жегалкина* (алгебраической нормальной формы, АНФ):

$$F(x_1, x_2, \ldots, x_n) = \bigoplus_{a \in \mathbb{F}_2^n} g_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}, \quad g_a \in \mathbb{F}_2^m,\ 0^0 = 1. \tag{2}$$

Степенью векторной булевой функции называется степень её полинома Жегалкина. Функция F *линейная*, если $F(x \oplus y) = F(x) \oplus F(y)$ для

всех $x, y \in \mathbb{F}_2^n$. Прибавляя константу из $\mathbb{F}_2^m$ к линейным функциям, получим множество *аффинных* функций (функций степени не более 1). *Образ* множества $S \subseteq \mathbb{F}_2^n$ будем обозначать через $F(S) = \{F(s) \mid s \in S\}$.

Производной F по направлению $a \in \mathbb{F}_2^n$ называется векторная булева функция $\mathcal{D}_a F(x) = F(x) \oplus F(x \oplus a)$. *Порядком дифференциальной равномерности* $\delta(F)$ называется минимальное t, для которого при любых параметрах $a \in \mathbb{F}_2^n \setminus \{0\}$ и $b \in \mathbb{F}_2^m$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более t решений. При $n = m$ функции с $\delta(F) = 2$ называются APN-*функциями*, а взаимно однозначные APN-функции — APN-*подстановками*.

Расстояние Хэмминга между булевыми функциями $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ равно числу векторов, на которых их значения различаются. *Вес Хэмминга* $\mathrm{wt}(f)$ функции (вектора $x \in \mathbb{F}_2^n$) — число векторов (координат) со значением 1. Булева функция называется *уравновешенной*, если она принимает значения 0 и 1 на одинаковом числе векторов.

Функции f и g EA-*эквивалентны*, если $f(x) = g(A(x)) \oplus h(x)$ для всех $x \in \mathbb{F}_2^n$, где $A\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — обратимое аффинное преобразование и $h\colon \mathbb{F}_2^n \to \mathbb{F}_2$ аффинна. Функция f при чётном n называется *бент-функцией*, если она находится на максимальном расстоянии от множества всех аффинных булевых функций. Множество всех бент-функций замкнуто относительно EA-эквивалентности.

Обратим внимание, что большинство приводимых определений и фактов можно найти в [8].

1.2. Подпространства и ограничения функций. *Линейным подпространством* $\mathbb{F}_2^n$ называется непустое подмножество $L \subseteq \mathbb{F}_2^n$ такое, что для любых $x, y \in L$ выполнено $x \oplus y \in L$. Для $a \in \mathbb{F}_2^n$ множество $U = a \oplus L = \{a \oplus x \mid x \in L\}$ называется *аффинным подпространством* $\mathbb{F}_2^n$. Положим $[U] = L = a \oplus U$. *Размерность* аффинного подпространства U полагаем равной $\dim U = \dim[U]$. Множества всех линейных и аффинных подпространств $\mathbb{F}_2^n$ размерности k обозначим через $\mathcal{S}_n^k$ и $\mathcal{AS}_n^k$ соответственно.

Ограничением функции $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ на множество $S \subseteq \mathbb{F}_2^n$ называется $F|_S\colon S \to \mathbb{F}_2^m$ такая, что $F|_S(y) = F(y)$ для всех $y \in S$.

Пусть U и V — аффинные подпространства $\mathbb{F}_2^n$ и $\mathbb{F}_2^m$ соответственно. Функция $A\colon U \to V$ называется *аффинной*, если $A = A'|_U$ для некоторой аффинной функции $A'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$. Через $[A]$ обозначим любую линейную функцию вида $\mathbb{F}_2^n \to \mathbb{F}_2^m$ такую, что $A = [A]|_U \oplus \mathrm{const}$. Например, подходящей является $[A] = A' \oplus A'(0)$. Введём следующие обозначения:

- $\mathcal{A}_U^V = \{f\colon U \to V \mid f \text{ аффинна}\}$ — множество всех аффинных функций из U в V;
- $\mathcal{A}_n^V = \mathcal{A}_{\mathbb{F}_2^n}^V$ и $\mathcal{A}_U^k = \mathcal{A}_U^{\mathbb{F}_2^k}$; в булевом случае $\mathcal{A}_n = \mathcal{A}_n^1$ и $\mathcal{A}_U = \mathcal{A}_U^1$.

Введём в рассмотрение также следующие фактор-пространства.

• $\widetilde{\mathcal{F}}_U = \mathcal{F}_U/\mathcal{A}_U$, где $\mathcal{F}_U = \{f\colon U \to \mathbb{F}_2\}$, $\mathcal{F}_n = \mathcal{F}_{\mathbb{F}_2^n}$. Соответствующее отношение эквивалентности обозначим через $\simeq$, так что $f \simeq g$ тогда и только тогда, когда $f \oplus g \in \mathcal{A}_U$, где $f, g \in \mathcal{F}_U$.

• $\mathcal{A}_U^n/\mathcal{A}_U^V$, где $V \subseteq \mathbb{F}_2^n$ — линейное подпространство. Соответствующее отношение эквивалентности обозначим через $\overset{V}{=}$, так что $F \overset{V}{=} G$ тогда и только тогда, когда $F \oplus G \in \mathcal{A}_U^V$, где $F, G \in \mathcal{A}_U^n$

С целью упрощения записи будем считать, что для $f \in \mathcal{F}_U$ также имеет место $f \in \widetilde{\mathcal{F}}_U$ (аналогично $F \in \mathcal{A}_U^n$ и $F \in \mathcal{A}_U^n/\mathcal{A}_U^V$), а для равенства в фактор-пространстве используем символ эквивалентности.

Характеристическую функцию множества S обозначим через Ind_S, где S может быть как подмножеством $\mathbb{F}_2^n$, так и $\widetilde{\mathcal{F}}_U$.

1.3. Алгебраическое представление булевых функций. Функцию $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ можно также рассмотреть как функцию $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, зафиксировав некоторый базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$. Многие свойства, например, алгебраическая степень, нахождение функций на определённом расстоянии, свойство быть бент-функцией и т. д., не зависят от выбора базиса. Любую такую функцию F можно однозначно представить в виде полинома над полем:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \quad \delta_0, \ldots, \delta_{2^n-1} \in \mathbb{F}_{2^n}.$$

Степень функции, отличной от константы 0, можно найти по формуле

$$\deg F = \max_{i \in \{0,\ldots,2^n-1\}\colon \delta_i \neq 0} \mathrm{wt}(i_{(2)}),$$

где $i_{(2)} \in \mathbb{F}_2^n$ — вектор двоичной записи i. Таким образом, аффинными являются функции следующего вида:

$$x \mapsto \alpha_0 x^{2^0} + \alpha_1 x^{2^1} + \cdots + \alpha_{n-1} x^{2^{n-1}} + \alpha_n, \quad \text{где } \alpha_0, \ldots, \alpha_n \in \mathbb{F}_{2^n}.$$

Булеву функцию можно представить как $\mathrm{tr}_1^n(F(x))$, где

$$\mathrm{tr}_1^n(x) = x^{2^0} + x^{2^1} + \cdots + x^{2^{n-1}}, \quad x \in \mathbb{F}_{2^n}.$$

Это линейная функция, значения которой лежат в $\mathbb{F}_2$. Будем пользоваться следующими связанными с ней свойствами:

$$\mathrm{tr}_1^n(x^2) \equiv \mathrm{tr}_1^n(x), \quad x^{k \cdot 2^i} \equiv x^{k \lll i}, \quad i \geqslant 0,\ k \in \{0, \ldots, 2^n - 1\}, \qquad (3)$$

где $k \lll i$ — число, двоичная запись которого является циклическим сдвигом двоичной записи $k_{(2)}$ на i позиций в сторону старших разрядов.

1.4. Класс Мэйорана — МакФарланда. Класс Мэйорана — МакФарланда $\mathcal{M}_{2n}$ от $2n$ переменных состоит из функций вида

$$f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y), \quad x,y \in \mathbb{F}_2^n,$$

где π — подстановка на $\mathbb{F}_2^n$ и $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Все они являются бент-функциями. Здесь используем $\langle\cdot,\cdot\rangle_n$, поскольку рассматриваем как «обычные» функции вида $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, для которых

$$\langle x,y\rangle_n = \langle x,y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n, \quad x,y \in \mathbb{F}_2^n,$$

так и функции над полем вида $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$, для которых

$$\langle x,y\rangle_n = \mathrm{tr}_1^n(xy), \quad x,y \in \mathbb{F}_{2^n},$$

т. е. в последнем случае рассматриваем $\mathbb{F}_2^n$ как $\mathbb{F}_{2^n}$. Все полученные в работе результаты справедливы, если в качестве $\langle\cdot,\cdot\rangle_n$ взять любую симметричную невырожденную билинейную форму над $\mathbb{F}_2^n$ ($\mathbb{F}_{2^n}$), которая линейна по обоим аргументам, её значение не меняется при перестановке аргументов и $\langle a,x\rangle_n \equiv 0$ только при $a = 0 \in \mathbb{F}_2^n$ [33].

Ортогональное пространство к линейному подпространству $L \subseteq \mathbb{F}_2^n$ определяется относительно используемой билинейной формы:

$$L^\perp = \{y \in \mathbb{F}_2^n \mid \langle x,y\rangle_n = 0 \text{ для всех } x \in L\} \subseteq \mathbb{F}_2^n.$$

Отметим, что $\dim L^\perp = n - \dim L$.

1.5. Бент-функции на расстоянии 2^n и $\mathcal{M}_{2n}$. Минимальное расстояние между двумя различными бент-функциями от $2n$ переменных равно 2^n [17]. Критерий такого расположения даёт

Утверждение 1 [17]. *Пусть $f \in \mathcal{F}_{2n}$ — бент-функция и $U \subset \mathbb{F}_2^{2n}$, $|U| = 2^n$. Тогда $f \oplus \mathrm{Ind}_U$ является бент-функцией, если и только если U — аффинное подпространство $\mathbb{F}_2^{2n}$ и $f|_U$ аффинная.*

Для любой бент-функции $f \in \mathcal{M}_{2n}$ существуют бент-функции на расстоянии 2^n от f, которые будем называть *ближайшими*. В настоящей работе большое внимание уделяется известной [28] нижней оценке числа таких бент-функций, которая уточнена в [29].

Утверждение 2 [28, 29]. *Число ближайших к $f \in \mathcal{M}_{2n}$ бент-функций не меньше $\ell_{2n} = 2^{2n+1} - 2^n$, при этом в точности ℓ_{2n} из них принадлежат классу $\mathcal{M}_{2n}$.*

Известно [30], что нижняя оценка ℓ_{2n} достижима при простых $n \geqslant 5$. Для произвольных функций $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, подобной используемым при построении класса $\mathcal{M}_{2n}$ подстановкам, и $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ положим:

- $\mathcal{L}_k(\pi) = \{U \in \mathcal{AS}_n^k \mid \pi(U) \in \mathcal{AS}_n^k\}$ и $\mathcal{L}(\pi) = \mathcal{L}_0(\pi) \cup \cdots \cup \mathcal{L}_n(\pi)$;
- $\mathcal{LA}_k(F) = \{U \in \mathcal{AS}_n^k \mid F|_U \text{ аффинна}\}$.

Например, построение всех ближайших к $f \in \mathcal{M}_{2n}$ бент-функций с помощью утверждения 1 эквивалентно нахождению множества $\mathcal{LA}_n(f)$, а число таких бент-функций равно $|\mathcal{LA}_n(f)|$. Далее также потребуется следующее известное свойство инверсии элементов конечного поля.

Утверждение 3 [34]. *Пусть* $\pi(x) = x^{2^n-2}$ *для* $x \in \mathbb{F}_{2^n}$ *и* $2 \leqslant k \leqslant n$. *Тогда если* $k \nmid n$, *то* $\mathcal{L}_k(\pi) = \varnothing$, *иначе* $\mathcal{L}_k(\pi) = \{s\mathbb{F}_{2^k} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}$, *где* $s\mathbb{F}_{2^k} = \{sx \mid x \in \mathbb{F}_{2^k}\}$.

Заметную роль [30] в достижимости оценки ℓ_{2n} играют APN-подстановки, каждую из которых эквивалентно можно определить как подстановку π на $\mathbb{F}_2^n$ такую, что $\mathcal{L}_2(\pi) = \varnothing$ (см. [14]).

2. Описание ближайших к $f \in \mathcal{M}_{2n}$ бент-функций и подсчёт их числа

Переформулируем критерий расположения ближайших к $f \in \mathcal{M}_{2n}$ бент-функций, предложенный в [30], используя другое представление элементов $\mathcal{LA}_n(f)$ (п. 2.1), а также определив специальный линейный оператор (п. 2.2), свойства которого позволяют найти $|\mathcal{LA}_n(f)|$. Для изучения этих свойств можно использовать некоторые упрощения (п. 2.3).

2.1. Представление аффинных подпространств $\mathbb{F}_2^k \times \mathbb{F}_2^m$. В работе [30] для представления подпространств использовались базисные GJB-матрицы (приведённые ступенчатые матрицы). Однако не всегда удобно работать с базисами, особенно если функции представлены в алгебраическом виде. Рассмотрим схожее представление подпространств $\mathbb{F}_2^k \times \mathbb{F}_2^m$ на языке множеств, задействующее меньшие подпространства $\mathbb{F}_2^k$ и $\mathbb{F}_2^m$ (пересечение и проекцию), а также аффинные функции:

$$\mathcal{S}(U, V, H) = \big\{(x \oplus H(y), y) \in \mathbb{F}_2^k \times \mathbb{F}_2^m \mid x \in V,\, y \in U\big\}, \tag{4}$$

где

- U — аффинное подпространство $\mathbb{F}_2^m$,
- V — линейное подпространство $\mathbb{F}_2^k$,
- $H \in \mathcal{A}_U^k$, т. е. функция $H\colon U \to \mathbb{F}_2^k$ аффинная.

Утверждение 4. *Множество* $\mathcal{S}(U, V, H)$ *образует аффинное подпространство в* $\mathbb{F}_2^k \times \mathbb{F}_2^m$ *размерности* $\dim U + \dim V$. *Более того,*

1) *любое аффинное подпространство* $S \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$ *представимо как* $S = \mathcal{S}(U, V, H)$ *с помощью проекции* U *и пересечения* V:

$$U = \big\{y \in \mathbb{F}_2^m \mid \text{существует } x \in \mathbb{F}_2^k \text{ такой, что } (x, y) \in S\big\},$$
$$V \times \{0\}^m = [S] \cap \big(\mathbb{F}_2^k \times \{0\}^m\big);$$

2) *представление* $S = \mathcal{S}(U, V, H)$ *единственно при* $H \in \mathcal{A}_U^k / \mathcal{A}_U^V$.

Доказательство. Нетрудно видеть, что $\mathcal{S}(U,V,H) \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$ — аффинное подпространство и $\mathcal{S}(U,V,H) = (H(a),a) \oplus [\mathcal{S}(U,V,H)]$ для произвольно выбранного $a \in U$. При этом для каждого значения второй части $y \in U$ есть ровно $|H(y) \oplus V|$ различных значений первой части. Итого $|\mathcal{S}(U,V,H)| = |U| \cdot |V|$, т. е. $\dim \mathcal{S}(U,V,H) = \dim U + \dim V$.

Представление. Если $S = \mathcal{S}(U,V,H)$ для некоторой $H \in \mathcal{A}_U^k$, то подпространства U и V определяются однозначно по приведённым в условии формулам в силу очевидных свойств конструкции. Рассмотрим произвольное аффинное подпространство $S \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$. Множества $U \subseteq \mathbb{F}_2^m$ и $V \subseteq \mathbb{F}_2^k$ однозначно задаются теми же формулами по S и являются аффинным и линейным подпространствами соответственно.

С целью подобрать подходящую аффинную функцию сначала найдём такую функцию $H\colon [U] \to \mathbb{F}_2^k$, что $[S] = \mathcal{S}([U],V,H)$. Пусть $C(y) = [S] \cap \big(\mathbb{F}_2^k \times \{y\}\big)$, $y \in [U]$. Очевидно, что $C(y)$ непусто и является смежным классом $V \times \{0\}^m = [S] \cap \big(\mathbb{F}_2^k \times \{0\}^m\big)$. Более того, $[S] = \bigcup\limits_{y \in [U]} C(y)$.

Пусть $y_1, \ldots, y_r \in \mathbb{F}_2^m$ образуют базис $[U]$, а $s_1, \ldots, s_r \in \mathbb{F}_2^k$ — любые векторы такие, что $(s_i, y_i) \in C(y_i)$ при $i \in \{1, \ldots, r\}$. Положим $H(y_i) = s_i$, $i \in \{1, \ldots, r\}$, а остальные значения H на $[U]$ определим из соотношения линейности. После этого произвольным образом продолжим функцию H до некоторой линейной функции $[H]\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ такой, что $H = [H]|_{[U]}$. Заметим, что $C(y) = (H(y),y) \oplus (V \times \{0\}^m)$. Действительно, если $y = y_{i_1} \oplus \cdots \oplus y_{i_t}$ для $0 \leqslant t \leqslant r$, то

$$(H(y),y) = (H(y_{i_1}),y_{i_1}) \oplus \cdots \oplus (H(y_{i_t}),y_{i_t}) \in [S],$$

поскольку $(H(y_{i_1}),y_{i_1}), \ldots, (H(y_{i_t}),y_{i_t})$ лежат в линейном $[S]$. Таким образом, $(H(y),y) \in C(y)$, т. е. $C(y) = (H(y),y) \oplus (V \times \{0\}^m)$. Это также означает, что $[S] = \mathcal{S}([U],V,H)$.

Далее, возьмём произвольно $(b,a) \in S$, т. е. $S = (b,a) \oplus [S]$. Получаем $S = \mathcal{S}(U,V,H')$ для $H'(x) = [H](x) \oplus [H](a) \oplus b$ при $x \in U = a \oplus [U]$.

Единственность. Если $S = \mathcal{S}(U,V,H) = \mathcal{S}(U',V',H')$, то по построению $U' = U$ и $V' = V$. Далее, подпространства $\mathcal{S}(U,V,H)$ и $\mathcal{S}(U,V,H')$ совпадают тогда и только тогда, когда для любого $y \in U$ смежные классы $H(y) \oplus V$ и $H'(y) \oplus V$ совпадают. Это эквивалентно тому, что $H(y) \oplus H'(y) \in V$, $y \in U$, т. е. $H \oplus H'$ — аффинная функция вида $U \to V$, откуда $H \overset{V}{=} H'$. Утверждение 4 доказано.

Замечание 1. Функции множества $\mathcal{A}_U^R$ являются представителями классов эквивалентности из $\mathcal{A}_U^k / \mathcal{A}_U^V$, где $R \subseteq \mathbb{F}_2^k$ — произвольное линейное подпространство размерности $k - \dim V$ такое, что $R \cap V = \{0\}$. Действительно, в этом случае $\mathbb{F}_2^k$ раскладывается в прямую сумму подпространств V и R, а равенство $R \cap V = \{0\}$ обеспечивает попарную

неэквивалентность представителей. Таким образом, любую аффинную функцию $H\colon U \to \mathbb{F}_2^k$ можно представить в виде суммы функций из множеств $\mathcal{A}_U^R$ и $\mathcal{A}_U^V$. Такое линейное подпространство R можно легко построить, например зная информационные координаты V [35].

Замечание 2. Линейное подпространство $\mathbb{F}_2^k \times \mathbb{F}_2^m$ также может быть представлено конструкцией $\mathcal{S}(U, V, H)$. Для этого достаточно применить линейные подпространство U и функцию H.

Далее в основном будем рассматривать пространство $\mathbb{F}_2^n \times \mathbb{F}_2^n$, т. е. $k = m = n$, поскольку именно на нём задаются бент-функции из класса Мэйорана —МакФарланда $\mathcal{M}_{2n}$.

2.2. Бент-функции, ближайшие к $f \in \mathcal{M}_{2n}$. Рассмотрим функцию $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и подпространство $U \in \mathcal{AS}_n^k$ такие, что $\pi(U) \in \mathcal{AS}_n^k$; положим $V = [\pi(U)]^\perp \in \mathcal{S}_n^{n-k}$. Линейный оператор $\mathcal{G}_\pi^U\colon \mathcal{A}_U^n/\mathcal{A}_U^V \to \widetilde{\mathcal{F}}_U$ определим следующим образом:

$$\mathcal{G}_\pi^U(H)\colon x \mapsto \langle H(x), \pi(x)\rangle_n, \quad x \in U. \tag{5}$$

Для удобства обозначим отношение $\overset{V}{=}$ на $\mathcal{A}_U^n/\mathcal{A}_U^V$ через $\overset{\pi}{=}$. Заметим, что при $U = \mathbb{F}_2^n$ не требуется использовать фактор-пространство входных аргументов, в этом случае будем обозначать $\mathcal{G}_\pi^{\mathbb{F}_2^n}$ через $\mathcal{G}_\pi\colon \mathcal{A}_n^n \to \widetilde{\mathcal{F}}_n$.

Утверждение 5. *Линейный оператор $\mathcal{G}_\pi^U$ определён корректно.*

Доказательство. Пусть $H, H'\colon U \to \mathbb{F}_2^n$ аффинные и $H \overset{\pi}{=} H'$, т. е. $H' = H \oplus \Delta$, где $\Delta\colon U \to [\pi(U)]^\perp$ аффинная. Тогда

$$\begin{aligned}\langle H'(x), \pi(x)\rangle_n &= \\ &= \langle H(x) \oplus \Delta(x), \pi(x)\rangle_n = \langle H(x), \pi(x)\rangle_n \oplus \langle \Delta(x), \pi(x)\rangle_n = \\ &= \langle H(x), \pi(x)\rangle_n \oplus \langle \Delta(x), \pi(a)\rangle_n \oplus \langle \Delta(x), \pi(a) \oplus \pi(x)\rangle_n,\end{aligned}$$

где $a \in U$. Тем самым $\pi(a) \oplus \pi(x) \in [\pi(U)]$, а в силу $\Delta(x) \in [\pi(U)]^\perp$ получаем

$$\langle \Delta(x), \pi(a) \oplus \pi(x)\rangle_n \equiv 0.$$

Поскольку $\pi(a)$ не зависит от x, а Δ аффинная, функция $\langle \Delta(x), \pi(a)\rangle_n$ также аффинная. Следовательно, $H \overset{\pi}{=} H'$ влечёт

$$\mathcal{G}_\pi^U(H) = \langle H(x), \pi(x)\rangle_n \simeq \langle H'(x), \pi(x)\rangle_n = \mathcal{G}_\pi^U(H').$$

Линейность оператора очевидна. Утверждение 5 доказано.

Используя ядро $\operatorname{Ker} \mathcal{G}_\pi^U = \{H \in \mathcal{A}_U^n/\mathcal{A}_U^V \mid \mathcal{G}_\pi^U(H) \simeq 0\}$ и образ $\operatorname{Im} \mathcal{G}_\pi^U = \mathcal{G}_\pi^U\left(\mathcal{A}_U^n/\mathcal{A}_U^V\right)$ оператора $\mathcal{G}_\pi^U$, переформулируем критерий из [30]. Заметим, что это можно сделать ещё одним схожим способом [35].

Теорема 1. *Пусть* $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$ *и* $L \subseteq \mathbb{F}_2^{2n}$. *Тогда* $f \oplus \mathrm{Ind}_L$ *— ближайшая бент-функция к* f, *если и только если*

$$L = \mathcal{S}(U, [\pi(U)]^\perp, H \oplus H_0),$$

где $U \in \mathcal{L}(\pi)$, $H \in \operatorname{Ker} \mathcal{G}_\pi^U$ *и* $\mathcal{G}_\pi^U(H_0) \simeq \varphi|_U$. *Произвольная пара* $U \in \mathcal{L}(\pi)$ *и* $H \oplus H_0 \in \mathcal{A}_U^n / \mathcal{A}_U^{[\pi(U)]^\perp}$ *однозначно определяет подходящее* L.

Доказательство. Заметим, что $\dim L = \dim U + \dim[\pi(U)]^\perp = n$, поскольку $U \subseteq \mathbb{F}_2^n$. В силу утверждения 1 достаточно проанализировать аффинность функции f на подпространстве $L \in \mathcal{AS}_{2n}^n$, которое в общем случае для подходящих подпространств V, U и функции H' имеет вид

$$L = \mathcal{S}(U, V, H') = \{(x \oplus H'(y), y) \mid x \in V,\ y \in U\}.$$

Для произвольных $x \in V$, $y \in U$ имеем

$$f|_L(x,y) = \langle x \oplus H'(y), \pi(y)\rangle_n \oplus \varphi(y) = \\ = \langle x, \pi(y)\rangle_n \oplus \langle H'(y), \pi(y)\rangle_n \oplus \varphi(y). \quad (6)$$

С одной стороны, если подпространство U и функции H, H_0 выбраны, как указано в условии теоремы, а $V = [\pi(U)]^\perp$ и $H' = H \oplus H_0$, то при помощи (6) нетрудно проверить, что f аффинна на L.

С другой стороны, если $f|_L$ аффинна, то из (6) при $a \in V$ следует, что

$$\mathcal{D}_{(a,0)} f|_L(x,y) = \langle a, \pi(y)\rangle \equiv \mathrm{const},$$

Зафиксируем произвольный $u \in U$ и рассмотрим $\pi'(y) = \pi(y) \oplus \pi(u)$. После подстановки получаем

$$\mathcal{D}_{(a,0)} f|_L(x,y) = \langle a, \pi'(y)\rangle \oplus \langle a, \pi(u)\rangle \equiv \mathrm{const},$$

откуда $\langle a, \pi'(y)\rangle \equiv \mathrm{const}$. При этом $\pi'(u) = 0$ и $\langle a, \pi'(u)\rangle = 0$, так что $\langle a, \pi'(y)\rangle \equiv 0$. Из произвольности $a \in V$ следует, что $\pi'(U) \subseteq V^\perp$. Однако по утверждению 4 выполняется $\dim U = n - \dim V = \dim V^\perp$, значит, $\pi'(U) = V^\perp$ и $\pi(U) = \pi(u) \oplus V^\perp$. Другими словами, имеем $U \in \mathcal{L}(\pi)$ и $V = [\pi(U)]^\perp$.

В этом случае согласно (6) аффинность $f|_L$ сводится к аффинности функции $\langle H'(y), \pi(y)\rangle_n \oplus \varphi(y)$. В свою очередь, это можно записать как $\mathcal{G}_\pi^U(H') \simeq \varphi|_U$, где $\varphi|_U$ рассматривается уже как функция из $\widetilde{\mathcal{F}}_U$. Так как оператор $\mathcal{G}_\pi^U$ линейный, последнее эквивалентно тому, что $H' = H \oplus H_0$, где $H \in \operatorname{Ker} \mathcal{G}_\pi^U$ и $\mathcal{G}_\pi^U(H_0) \simeq \varphi|_U$. Осталось заметить, что согласно утверждению 4 представление L единственно при выборе $H' \in \mathcal{A}_U^n / \mathcal{A}_U^V$. Теорема 1 доказана.

Из доказанного критерия и линейности $\mathcal{G}_\pi^U$ напрямую вытекает следствие о числе ближайших к $f \in \mathcal{M}_{2n}$ бент-функций, которое согласно утверждению 1 равно $|\mathcal{LA}_n(f)|$.

Следствие 1. *Если* $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$, *то*

$$|\mathcal{LA}_n(f)| = \sum_{L \in \mathcal{L}(\pi)} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\pi^L}(\varphi|_L) \cdot \left|\mathrm{Ker}\ \mathcal{G}_\pi^L\right|.$$

Далее докажем дополнительные свойства оператора $\mathcal{G}_\pi^U$, а в разд. 4–6 продемонстрируем удобство формулы из следствия 1, которую уточним в теореме 3. Заметим, что свойства чисел $|\mathcal{L}_2(\pi)|$ и $|\mathcal{L}(\pi)|$ исследовались в работах [36–38].

2.3. Свойства $\mathcal{G}_\pi^U$ и переход к $\mathcal{G}_{\pi'}$. Поиск ядра и образа $\mathcal{G}_\pi^U$ представляется непростой задачей из-за использования ограничений функций на $U \in \mathcal{AS}_n^k$. Например, нужно следить за однозначностью представления функций. Однако, мы покажем, что можно обойти ограничения функций, рассматривая свойства оператора $\mathcal{G}_{\pi'}$ для некоторой подстановки $\pi'\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$.

Теорема 2. *Пусть функция* $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *и подпространство* $U \in \mathcal{AS}_n^k$ *таковы, что* $\pi(U) \in \mathcal{AS}_n^k$, *а также*

- *функция* $\pi'\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ *определена равенством* $\pi' = B \circ \pi \circ A$, *где* $A\colon \mathbb{F}_2^k \to U$ *и* $B\colon \pi(U) \to \mathbb{F}_2^k$ *обратимы и аффинны;*
- $\mathcal{G}_\pi^U$ *и* $\mathcal{G}_{\pi'}$ *определены относительно* $\langle\cdot,\cdot\rangle_n$ *и* $\langle\cdot,\cdot\rangle_k$ *соответственно;*
- *функция* $[B]^*\colon \mathbb{F}_2^k \to \mathbb{F}_2^n$ *сопряжённая к* $[B]$, *т. е.*

$$\langle [B]^*(x), y\rangle_n = \langle x, [B](y)\rangle_k, \quad x \in \mathbb{F}_2^k,\ y \in \mathbb{F}_2^n.$$

Тогда

$$\mathrm{Ker}\ \mathcal{G}_\pi^U = [B]^* \circ \mathrm{Ker}\ \mathcal{G}_{\pi'} \circ A^{-1} = \{[B]^* \circ H \circ A^{-1} \mid H \in \mathrm{Ker}\ \mathcal{G}_{\pi'}\},$$
$$\mathrm{Im}\ \mathcal{G}_\pi^U = \mathrm{Im}\ \mathcal{G}_{\pi'} \circ A^{-1} = \{\varphi \circ A^{-1} \mid \varphi \in \mathrm{Im}\ \mathcal{G}_{\pi'}\},$$

при этом $\left|\mathrm{Ker}\ \mathcal{G}_\pi^U\right| = \left|\mathrm{Ker}\ \mathcal{G}_{\pi'}\right|$ *и* $\left|\mathrm{Im}\ \mathcal{G}_\pi^U\right| = \left|\mathrm{Im}\ \mathcal{G}_{\pi'}\right|$.

Доказательство. Пусть $V = [B]^*\big(\mathbb{F}_2^k\big)$ — линейное подпространство в $\mathbb{F}_2^n$, т. е. $[B]^*\colon \mathbb{F}_2^k \to V$. Докажем от противного, что $V \cap [\pi(U)]^\perp = \{0\}$. Пусть, напротив, $[B]^*(a) \in [\pi(U)]^\perp$ для некоторого $a \in \mathbb{F}_2^k \setminus \{0\}$. Выберем $u \in \pi(U)$; для любого $y \in [\pi(U)]$ имеем

$$\langle a, [B](u \oplus y)\rangle_k = \langle [B]^*(a), u \oplus y\rangle_n = \\ = \langle [B]^*(a), u\rangle_n \oplus \langle [B]^*(a), y\rangle_n = \langle [B]^*(a), u\rangle_n.$$

Заметим, что $[B]|_{\pi(U)} = B \oplus \mathrm{const}$. В силу обратимости B получаем $[B](\pi(U)) = B(\pi(U)) \oplus \mathrm{const} = \mathbb{F}_2^k \oplus \mathrm{const} = \mathbb{F}_2^k$. Таким образом, для любого $x \in \mathbb{F}_2^k$

$$\langle a, x\rangle_k = \langle [B]^*(a), u\rangle_n,$$

что противоречит невырожденности формы $\langle\cdot,\cdot\rangle_k$, поскольку $a \neq 0$.

Докажем, что $\dim V = k$, т. е. обратимость $[B]^*$. Действительно, если $[B]^*(x_1) = [B]^*(x_2)$ при $x_1, x_2 \in \mathbb{F}_2^k$ и $x_1 \neq x_2$, то из равенств

$$\langle [B]^*(x_1), y\rangle_n = \langle x_1, [B](y)\rangle_k, \quad \langle [B]^*(x_2), y\rangle_n = \langle x_2, [B](y)\rangle_k$$

вытекает, что для любого $y \in \mathbb{F}_2^n$

$$\langle x_1 \oplus x_2, [B](y)\rangle_k = 0.$$

Это противоречит невырожденности формы $\langle\cdot,\cdot\rangle_k$, поскольку $x_1 \oplus x_2 \neq 0$ и $[B](\pi(U)) = \mathbb{F}_2^k$. Тем самым функция $[B]^*\colon \mathbb{F}_2^k \to V$ обратима.

Обратимость A и $[B]^*$ позволяет любую функцию $H' \in \mathcal{A}_U^V$ представить в виде $H' = [B]^* \circ H \circ A^{-1}$ для некоторой $H \in \mathcal{A}_k^k$. В силу доказанных свойств V и замечания 1 именно такие функции можно рассматривать в качестве попарно неэквивалентных представителей фактор-пространства $\mathcal{A}_U^n / \mathcal{A}_U^{[\pi(U)]^\perp}$.

Осталось заметить, что для функции $\varphi = \mathcal{G}_{\pi'}(H)$ и любого $x \in \mathbb{F}_2^k$ по построению справедливы равенства

$$\begin{aligned}\varphi(x) &= \langle H(x), B(\pi(A(x)))\rangle_k \simeq \langle H(x), [B](\pi(A(x)))\rangle_k = \\ &= \langle [B]^*(H(x)), \pi(A(x))\rangle_n = \langle [B]^*(H(A^{-1}(y)))), \pi(y)\rangle_n = \varphi'(y),\end{aligned}$$

где $y = A(x) \in U$. Поскольку $A\big(\mathbb{F}_2^k\big) = U$, функция $\varphi'(y) = \varphi(A^{-1}(y))$ определена на всём U и $\varphi' = \mathcal{G}_\pi^U(H')$. При этом $\varphi' \overset{\pi}{=} 0$ тогда и только тогда, когда $\varphi \simeq 0$, что означает эквивалентность условий $H \in \operatorname{Ker} \mathcal{G}_{\pi'}$ и $H' \in \operatorname{Ker} \mathcal{G}_\pi^U$. Теорема 2 доказана.

Таким образом, теорема 2 позволяет использовать естественную билинейную форму, не ограничивая её область определения. Например, можно работать с $\mathrm{tr}_1^k(\cdot)$ над $\mathbb{F}_{2^k}$ вместо сужения $\mathrm{tr}_1^n(\cdot)$ на $U \in \mathcal{AS}_n^k$. Более того, можно переходить к другой билинейной форме, не меняя начального U. Полезными также являются следующие свойства.

Утверждение 6. *Пусть функции $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $B \in \mathcal{A}_n^n$ обратимы. Тогда $\operatorname{Im} \mathcal{G}_\pi^U = \operatorname{Im} \mathcal{G}_{B\circ\pi}^U$ для любого подпространства $U \in \mathcal{L}(\pi)$.*

Доказательство прямо следует из теоремы 2.

Утверждение 7. *Пусть $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ обратима, $\varphi \in \mathcal{F}_n$, $L, U \in \mathcal{L}(\pi)$ и $L \subseteq U$. Тогда если $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$, то $\varphi|_L \in \operatorname{Im} \mathcal{G}_\pi^L$.*

Доказательство. Условие $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$ означает, что существует функция $H \in \mathcal{A}_U^n$ такая, что $\mathcal{G}_\pi^U(H) \simeq \varphi|_U$, т. е. $\mathcal{G}_\pi^U(H) = \varphi|_U \oplus h$, где $h \in \mathcal{A}_U$. Рассмотрим сужение $H|_L$. Очевидно, что оно также будет аффинным, т. е. $H|_L \in \mathcal{A}_L^n$. Тогда для соответствующего фактор-пространства $\mathcal{G}_\pi^L(H|_L) = \varphi|_L \oplus h|_L$, но $h|_L$ также аффинна, т. е. $\mathcal{G}_\pi^L(H|_L) \simeq \varphi|_L$. Утверждение 7 доказано.

Замечание 3. Если для $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$ справедливо $\varphi \in \operatorname{Im} \mathcal{G}_\pi$, то $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$ для любого $U \in \mathcal{L}(\pi)$, что упрощает формулу из следствия 1. Вместе с тем, это означает EA-эквивалетность бент-функций f и $f'(x',y') = \langle x', \pi(y')\rangle_n$: достаточно сделать замену $x' = x \oplus H(y)$ и $y' = y$ для $\mathcal{G}_\pi(H) \simeq \varphi$, и получим f' с точностью до аффинной части.

3. Ядро и образ $\mathcal{G}_\pi$ для некоторых π

Найдём ядро (или мощность ядра) и образ оператора $\mathcal{G}_\pi$ для некоторых функций π. Остановимся на аффинных функциях и функциях от малого числа переменных в представлении над $\mathbb{F}_2^n$, а также функции инверсии элементов конечного поля, продемонстрировав алгебраический подход.

3.1. Аффинные подстановки и подстановки от 3 переменных. Свойства оператора $\mathcal{G}_\pi$ несложно определить для аффинных подстановок $\pi \in \mathcal{A}_n^n$. Заметим, что при $n \in \{1,2\}$ все подстановки на $\mathbb{F}_2^n$ аффинны. При $n = 1$ это очевидно, а при $n = 2$ достаточно вспомнить, что $\deg \pi < n$ для любой подстановки $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ (вообще говоря, при $n \geqslant 2$; см., например, [8]).

Рассматривая подстановки на $\mathbb{F}_2^n$, удобно пользоваться матричным представлением для функции $H \in \mathcal{A}_n^n$: $H(x) = xA \oplus a$, где A — невырожденная двоичная матрица порядка n и $a \in \mathbb{F}_2^n$, при этом

$$\mathcal{G}_\pi(H)\colon x \mapsto \langle xA \oplus a, \pi(x)\rangle, \quad |\operatorname{Ker} \mathcal{G}_\pi| \cdot |\operatorname{Im} \mathcal{G}_\pi| = 2^{n^2+n}. \tag{7}$$

Утверждение 8. *Пусть $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — взаимно однозначная аффинная функция. Тогда*

$$\operatorname{Im} \mathcal{G}_\pi = \{\varphi \in \widetilde{\mathcal{F}}_n \mid \deg \varphi \leqslant 2\}, \quad |\operatorname{Ker} \mathcal{G}_\pi| = 2^{\frac{n(n+3)}{2}}.$$

Доказательство. 1. В силу утверждения 6 можно считать без ограничения общности, что π — тождественное отображение, поэтому образ аффинной функции $H \in \mathcal{A}_n^n$ под действием оператора $\mathcal{G}_\pi$ представляет собой булеву функцию $\langle xA \oplus a, x\rangle \in \widetilde{\mathcal{F}}_n$, где A — невырожденная двоичная матрица порядка n и $a \in \mathbb{F}_2^n$. Ясно, что так можно получить любую квадратичную функцию, при этом степень получившейся функции не может быть больше 2.

2. Имеем $|\mathrm{Ker}\ \mathcal{G}_\pi| = 2^{n^2+n-\dim \mathrm{Im}\ \mathcal{G}_\pi} = 2^{n^2+n-n(n-1)/2} = 2^{\frac{n(n+3)}{2}}$ в силу (7). Утверждение 8 доказано.

Перейдём к произвольным подстановкам $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$.

Утверждение 9. *Пусть* $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ *— взаимно однозначная неаффинная функция. Тогда* $\mathrm{Im}\ \mathcal{G}_\pi = \widetilde{\mathcal{F}_3}$ *и* $|\mathrm{Ker}\ \mathcal{G}_\pi| = 256$.

Доказательство. 1. В силу того, что π взаимно однозначна и неаффинна, $\deg \pi = 2$. Таким образом, её полином Жегалкина можно представить в следующем виде:

$$\pi(x_1,x_2,x_3) = \begin{bmatrix} Q_1^1 \\ Q_2^1 \\ Q_3^1 \end{bmatrix}^\top x_2x_3 + \begin{bmatrix} Q_1^2 \\ Q_2^2 \\ Q_3^2 \end{bmatrix}^\top x_1x_3 + \begin{bmatrix} Q_1^3 \\ Q_2^3 \\ Q_3^3 \end{bmatrix}^\top x_1x_2 + xB + b,$$

где $Q_j^i \in \mathbb{F}_2$, $i,j \in \{1,2,3\}$, B — двоичная матрица порядка 3 и $b \in \mathbb{F}_2^3$. Поскольку $\deg \pi = 2$, существует вектор коэффициентов

$$q = (q_1,q_2,q_3) \in \left\{\left(Q_1^1,Q_1^2,Q_1^3\right),\ \left(Q_2^1,Q_2^2,Q_2^3\right),\ \left(Q_3^1,Q_3^2,Q_3^3\right)\right\},$$

с весом Хэмминга $\mathrm{wt}(q) \neq 0$, которому соответствует координатная функция f функции π, т. е.

$$f(x_1,x_2,x_3) = q_1x_2x_3 \oplus q_2x_1x_3 \oplus q_3x_1x_2 \oplus \langle a,x\rangle \oplus c,$$

где $a \in \mathbb{F}_2^3$ и $c \in \mathbb{F}_2$. Так как π обратима, все её компонентные функции уравновешенные, включая f [8]. Далее будем считать, что в $\langle xT \oplus s, \pi(x)\rangle$ функция $xT \oplus s \in \mathcal{A}_3^3$ имеет ненулевую координатную функцию только в координате, соответствующей f, т. е. $\langle xT \oplus s, \pi(x)\rangle = h(x)\cdot f(x)$, где $h \in \mathcal{A}_3$.

Случай 1: $\mathrm{wt}(q) = 1$. Без ограничения общности положим $q_3 = 1$. Заметим, что $x_1x_2 \oplus a_1x_1 \oplus a_2x_2 = (x_1 \oplus a_2)(x_2 \oplus a_1) \oplus a_1a_2$. Поскольку свободный член в полиноме Жегалкина f влияет только на аффинную часть $h(x)\cdot f(x)$, можно его не рассматривать. После замены

$$y_1 = x_1 \oplus a_2, \quad y_2 = x_2 \oplus a_1, \quad y_3 = x_3$$

функция f принимает вид

$$f(x_1,x_2,x_3) = y_1y_2 \oplus a_3y_3,$$

при этом f уравновешенна, так что $a_3 = 1$. Далее,

$$\begin{aligned} 1\cdot f(x) &= y_1y_2 \oplus y_3,\\ y_1\cdot f(x) &= y_1y_2 \oplus y_1y_3,\\ y_2\cdot f(x) &= y_1y_2 \oplus y_2y_3,\\ y_3\cdot f(x) &= y_1y_2y_3 \oplus y_3, \end{aligned}$$

т. е. $\{y_1y_2, y_1y_3, y_2y_3, y_1y_2y_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$. Отсюда получаем $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$, так как все функции из этого множества выражаются через функции y_1, y_2, y_3 и их суммы (с точностью до аффинной части). Тем самым $\operatorname{Im} \mathcal{G}_\pi = \widetilde{\mathcal{F}}_3$.

Случай 2: $\operatorname{wt}(q) = 2$. Без ограничения общности положим $q_1 = 0$. Сделав линейную замену

$$z_1 = x_1, \quad z_2 = x_2 \oplus x_3, \quad z_3 = x_3,$$

получим

$$f(x_1, x_2, x_3) = z_1z_2 \oplus a'_1z_1 \oplus a'_2z_2 \oplus a'_3z_3 \oplus c',$$

где $a' \in \mathbb{F}_2^3$ и $c' \in \mathbb{F}_2$. Далее действуя аналогично случаю 1 приходим к тому, что $\{z_1z_2, z_1z_3, z_2z_3, z_1z_2z_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$. Вместе с тем

$$z_1z_3 = x_1x_3, \quad z_1z_2 = x_1x_2 \oplus x_1x_3,$$
$$z_2z_3 = x_2x_3 \oplus x_3, \quad z_1z_2z_3 = x_1x_2x_3 \oplus x_1x_3.$$

Следовательно, $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$.

Случай 3: $\operatorname{wt}(q) = 3$, т. е. $q = (1, 1, 1)$. Здесь квадратичная часть f равна функции голосования $g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$, при этом $g(x_1 \oplus 1, x_2, x_3) = g(x_1, x_2, x_3) \oplus x_2 \oplus x_3$. Тем самым, сделав замену

$$y_1 = x_1 \oplus s_1, \quad y_2 = x_2 \oplus s_2, \quad y_3 = x_3 \oplus s_3$$

для подходящего $s \in \mathbb{F}_2^3$, получим $f(x) = g(y)$ либо $f(x) = g(y) \oplus y_3$ (с точностью до константы). Однако $\operatorname{wt}(g(y) \oplus y_3) = 2$, а сама g уравновешенная. Таким образом, $f(x) = g(y)$. Далее,

$$(y_1 \oplus y_2 \oplus y_3) \cdot f(x) = y_1y_2y_3,$$
$$(y_1 \oplus 1) \cdot f(x) = y_2y_3 \oplus y_1y_2y_3,$$
$$(y_2 \oplus 1) \cdot f(x) = y_1y_3 \oplus y_1y_2y_3,$$
$$(y_3 \oplus 1) \cdot f(x) = y_1y_2 \oplus y_1y_2y_3,$$

откуда вытекает, что $\{y_1y_2, y_1y_3, y_2y_3, y_1y_2y_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$ и, следовательно, $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$.

2. Имеем $|\operatorname{Ker} \mathcal{G}_\pi| = 2^{3^2+3-\dim \operatorname{Im} \mathcal{G}_\pi} = 2^{12-4} = 256$. Утверждение 9 доказано.

3.2. Инверсия элемента конечного поля. Применив теорему 6 из [30], можно найти образ оператора $\mathcal{G}_\sigma$ при простом $n \geqslant 5$, где σ — функция обращения элементов $\mathbb{F}_{2^n}$. При этом заметим, что $\operatorname{Im} \mathcal{G}_\sigma$ будет таким при любом n.

Утверждение 10. *Пусть* $\sigma(x) = x^{2^n-2}$ *для* $x \in \mathbb{F}_{2^n}$. *Тогда*

$$\operatorname{Ker} \mathcal{G}_\sigma = \left\{\alpha x + \beta x^2 + \gamma x^{2^{n-1}} + \gamma^2 \mid \alpha, \beta, \gamma \in \mathbb{F}_{2^n},\ \operatorname{tr}_1^n(\alpha) = 0\right\},$$

$$\operatorname{Im}\mathcal{G}_\sigma = \big\{\operatorname{tr}_1^n(c_2x^{2^2-1}+\cdots+c_{n-1}x^{2^{n-1}-1})+c_nx^{2^n-1} \mid c_2,\ldots,c_{n-1}\in\mathbb{F}_{2^n},\ c_n\in\mathbb{F}_2\big\},$$

при этом $|\operatorname{Ker}\mathcal{G}_\sigma| = 2^{3n-1}$ *и* $|\operatorname{Im}\mathcal{G}_\sigma| = 2^{(n-1)^2}$.

Доказательство. Любая аффинная функция $H\colon \mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ представима единственным образом в виде

$$H(x) = \alpha_0x^{2^0}+\alpha_1x^{2^1}+\cdots+\alpha_{n-1}x^{2^{n-1}}+\alpha_n,\quad \alpha_0,\ldots,\alpha_n\in\mathbb{F}_{2^n}.$$

Рассмотрим $\mathcal{G}_\sigma$:

$$\operatorname{tr}_1^n(x^{2^n-2}H(x)) = \operatorname{tr}_1^n(\alpha_0x^{2^n-1}+\alpha_1x^{2^1-1}+\cdots+\alpha_{n-1}x^{2^{n-1}-1}+\alpha_nx^{2^n-2}).$$

Согласно (3) имеем

$$\operatorname{tr}_1^n(\alpha_nx^{2^n-2}) = \operatorname{tr}_1^n\big(\big(\alpha_n^{2^{n-1}}x^{2^{n-1}-1}\big)^2\big) = \operatorname{tr}_1^n\big(\alpha_n^{2^{n-1}}x^{2^{n-1}-1}\big),$$
$$\operatorname{tr}_1^n(\alpha_0x^{2^n-1}) = \alpha_0^{2^0}x^{(2^n-1)\lll 0}+\cdots+\alpha_0^{2^{n-1}}x^{(2^n-1)\lll(n-1)} = \operatorname{tr}_1^n(\alpha_0)x^{2^n-1}.$$

Слагаемое $\operatorname{tr}_1^n(\alpha_1x^{2^1-1})$ линейно, поэтому элементами $\operatorname{Im}\mathcal{G}_\sigma$ являются функции вида

$$\operatorname{tr}_1^n(\alpha_2x^{2^2-1})+\cdots+\operatorname{tr}_1^n(\alpha_{n-2}x^{2^{n-2}-1})+ \\ +\operatorname{tr}_1^n\big(\big(\alpha_{n-1}+\alpha_n^{2^{n-1}}\big)x^{2^{n-1}-1}\big)+\operatorname{tr}_1^n(\alpha_0)x^{2^n-1}. \quad (8)$$

Для нахождения $\operatorname{Ker}\mathcal{G}_\sigma$ требуется определить все $\alpha_0,\ldots,\alpha_n$, для которых функция (8) аффинна. Раскрыв все tr_1^n с переменной и с помощью (3) записав общий полином, получим x в степенях $(2^j-1)\lll i$, где $j\in\{2,\ldots,n-1\}$ и $i\in\{0,\ldots,n-1\}$, причём

$$((2^j-1)\lll i)_{(2)} = (0,\ldots,0,\underbrace{1,\ldots,1}_{j})\lll i.$$

Это означает, что все эти степени попарно различны и не равны 2^n-1, причём их вес больше 1. Тогда единственный способ получить аффинную функцию в (8) — приравнять все коэффициенты нулю, т. е. положить $\alpha_2=\alpha_3=\cdots=\alpha_{n-2}=0$, $\alpha_{n-1}=\alpha_n^{2^{n-1}}$ (отсюда $\alpha_{n-1}^2=\alpha_n$) и $\operatorname{tr}_1^n(\alpha_0)=0$. Таким образом, коэффициенты α_1 и α_{n-1} можно выбрать из $\mathbb{F}_{2^n}$ произвольным образом, для α_0 подходит ровно половина элементов $\mathbb{F}_{2^n}$ в силу линейности tr_1^n, а $\alpha_n=\alpha_{n-1}^2$. Тем самым выражения для ядра $\operatorname{Ker}\mathcal{G}_\sigma$ и его мощности доказаны. Мощность образа, очевидно, находится по формуле $|\operatorname{Im}\mathcal{G}_\sigma| = 2^{n^2+n-(3n-1)} = 2^{(n-1)^2}$. Утверждение 10 доказано.

4. Достижимость нижней оценки ℓ_{2n} числа ближайших бент-функций

В этом разделе усилим результаты [30] о достижимости нижней оценки ℓ_{2n} (см. табл. 1 для $n \leqslant 10$), а также уточним формулу из следствия 1. Напомним, что при $|\mathcal{LA}_n(f)| = \ell_{2n}$ все ближайшие к $f \in \mathcal{M}_{2n}$ бент-функции также лежат в классе $\mathcal{M}_{2n}$.

Таблица 1

Достижимость нижней оценки ℓ_{2n} при $n \leqslant 10$

$2n$	Достижимость ℓ_{2n}	Комментарий
2	Достижима	$\ell_2 = \mathcal{U}_2 = 6$
4	Не достижима	См. [30] или теорему 3
6	Не достижима	Теорема 6
8	Не достижима	См. [30]
10	Достижима	См. [30]
12	Достижима	Эксп. данные для APN-подстановки из [39]
14	Достижима	См. [30]
16	Неизвестно	The big APN problem
18	Неизвестно	Выполнимо ли условие следствия 2?
20	Неизвестно	The big APN problem

4.1. Необходимое условие достижимости ℓ_{2n}. В [30] доказано, что для достижимости ℓ_{2n} необходимо в построении $f \in \mathcal{M}_{2n}$ использовать APN-подстановку, т. е. подстановку π, для которой $\mathcal{L}_2(\pi) = \varnothing$. Далее усилим это условие, уточнив формулу из следствия 1.

Теорема 3. *Пусть $f(x, y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$. Тогда*

$$|\mathcal{LA}_n(f)| = \sum_{k=0}^{n} S_k, \quad S_k = \sum_{L \in \mathcal{L}_k(\pi)} \operatorname{Ind}_{\operatorname{Im} \mathcal{G}_\pi^L}(\varphi|_L) \cdot \left|\operatorname{Ker} \mathcal{G}_\pi^L\right|, \quad 0 \leqslant k \leqslant n,$$

и, в частности,

$$S_0 + S_1 = \ell_{2n}, \quad S_2 = 2^5 \cdot |\mathcal{L}_2(\pi)|,$$
$$S_3 = 2^8 \cdot |\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| + 2^9 \cdot |\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}|.$$

Доказательство. По теореме 2 будем рассматривать подстановку $\pi' \colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ и функцию $\varphi' \in \widetilde{\mathcal{F}}_k$ вместо π и $\varphi|_L$, где $\operatorname{Im} \mathcal{G}_\pi^L = \operatorname{Im} \mathcal{G}_{\pi'} \circ A^{-1}$ для обратимой $A \in \mathcal{A}_k^L$.

При $k \in \{0, 1, 2\}$ подстановка π' аффинна на любом подпространстве $L \in \mathcal{L}_k(\pi)$. Согласно утверждению 8 имеем равенства $\operatorname{Im} \mathcal{G}_{\pi'} = \widetilde{\mathcal{F}}_k$

и $\left|\operatorname{Ker} \mathcal{G}_{\pi'}\right| = 2^{k(k+3)/2}$, т. е. $\operatorname{Im} \mathcal{G}_{\pi}^{L} = \widetilde{\mathcal{F}}_L$. Таким образом,

$$S_0 + S_1 = 2^n \cdot 2^0 + 2^n \cdot \frac{2^n - 1}{2} \cdot 2^2 = \ell_{2n},$$
$$S_2 = |\mathcal{L}_2(\pi)| \cdot 2^5.$$

Если $k = 3$ и π' не аффинна, то $\operatorname{Im} \mathcal{G}_{\pi'} = \widetilde{\mathcal{F}}_3$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^8$ в силу утверждения 9, а следовательно, соответствующая часть суммы S_3 равна $|\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| \cdot 2^8$.

Если $k = 3$ и подстановка π' аффинна, то $\operatorname{Im} \mathcal{G}_{\pi'} = \{g \in \widetilde{\mathcal{F}}_3 \mid \deg g \leqslant 2\}$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^9$ из утверждения 8. При этом $\operatorname{Im} \mathcal{G}_{\pi}^{L} = \operatorname{Im} \mathcal{G}_{\pi'} \circ A^{-1} = \{g \in \widetilde{\mathcal{F}}_L \mid \deg g \leqslant 2\}$, так как степень функции инвариантна относительно обратимого аффинного преобразования $A \in \mathcal{A}_3^L$. Тем самым оставшаяся часть суммы S_3 равна $|\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}| \cdot 2^9$, что в совокупности даёт искомое число. Теорема 3 доказана.

Сформулируем в виде следствия усиление необходимого условия.

Следствие 2. *Пусть* $f(x, y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$, *при этом* $\mathcal{L}_2(\pi) \cup \mathcal{L}_3(\pi) \neq \varnothing$. *Тогда* $|\mathcal{LA}_n(f)| > \ell_{2n}$.

Доказательство. Воспользуемся теоремой 3. Если $\mathcal{L}_2(\pi) \neq \varnothing$ или $\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi) \neq \varnothing$, то очевидно, что $|\mathcal{LA}_n(f)| > \ell_{2n}$. Вместе с тем, если найдётся $L \in \mathcal{LA}_3(\pi)$, то произвольное его аффинное подпространство $U \in \mathcal{AS}_n^2$ принадлежит $\mathcal{LA}_2(\pi) = \mathcal{L}_2(\pi)$, т. е. и в этом случае оценка не достигается. Следствие 2 доказано.

Заметим, что описание подпространств из множества $\mathcal{LA}_n(f)$, построенных при помощи $\mathcal{L}_2(\pi)$, можно найти в [35]. Там же доказано, что $|\mathcal{LA}_n(f)| \geqslant \ell_{2n} + 2^5 \cdot |\mathcal{L}_2(\pi)|$.

4.2. Достаточное условие достижимости ℓ_{2n}. Покажем, как можно построить $f \in \mathcal{M}_{2n}$ с $|\mathcal{LA}_n(f)| = \ell_{2n}$. Определим следующее множество функций из $\mathbb{F}_{2^m}$ в $\mathbb{F}_2$:

$$\mathcal{R}_m = \big\{c_0 + \operatorname{tr}_1^m(c_1 y^{2^1-1} + \cdots + c_{m-1} y^{2^{m-1}-1}) + c_m y^{2^m-1} \mid c_1, \ldots, c_{m-1} \in \mathbb{F}_{2^m},\ c_0, c_m \in \mathbb{F}_2\big\},$$

Нетрудно видеть, что это все функции, эквивалентные ($\simeq$) функциям из множества $\operatorname{Im} \mathcal{G}_\sigma$, приведённого в утверждении 10, поскольку мы добавили произвольную аффинную часть

$$c_0 + \operatorname{tr}_1^m(c_1 x^{2^1-1}) = c_0 + \operatorname{tr}_1^m(c_1 x).$$

Для $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, $m \mid n$ и $s \in \mathbb{F}_{2^n}$ определим функцию $\varphi_s^m\colon \mathbb{F}_{2^m} \to \mathbb{F}_2$ по правилу

$$\varphi_s^m\colon y \mapsto \varphi(sy), \quad y \in \mathbb{F}_{2^m},$$

т. е. φ_s^m построена по $\varphi|_{s\mathbb{F}_{2^m}}$.

Теорема 4. *Пусть $n = p^k$, где $p \geqslant 5$ простое и $k \geqslant 1$. Для функции $f_\varphi(x, y) = \operatorname{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$ равенство $|\mathcal{LA}_n(f_\varphi)| = \ell_{2n}$ имеет место тогда и только тогда, когда $\varphi_s^p \notin \mathcal{R}_p$ для всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$.*

Доказательство. Пусть $\sigma\colon y \mapsto y^{2^n-2}$, $y \in \mathbb{F}_2^n$. Согласно утверждению 3

$$\mathcal{L}_{p^i}(\sigma) = \{s\mathbb{F}_{2^{p^i}} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}, \quad i \in \{1, \dots, k\},$$

и $\mathcal{L}_m(\sigma) = \varnothing$ при всех $m \in \{2, \dots, p^k\} \setminus \{p^i\}_{i=1}^k$. Воспользуемся теоремой 3 для вычисления $\mathcal{LA}_n(f_\varphi)$. Определим функцию $A_s\colon \mathbb{F}_{2^{p^i}} \to s\mathbb{F}_{2^{p^i}}$ по правилу $A_s(x) = sx$ для $x \in \mathbb{F}_{2^{p^i}}$. Тогда

$$\varphi|_{s\mathbb{F}_{2^{p^i}}} = \varphi_s^{p^i} \circ A_s^{-1}, \tag{9}$$

а в силу теоремы 2 и утверждения 10 имеем

$$\left[\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}\right]_\simeq = \mathcal{R}_{p^i} \circ A_s^{-1}, \tag{10}$$

где $\left[\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}\right]_\simeq$ — множество функций $g\colon s\mathbb{F}_{2^{p^i}} \to \mathbb{F}_2$, эквивалентных ($\simeq$) функциям из $\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$.

Пусть $\varphi_s^p \in \mathcal{R}_p$ для некоторого $s \in \mathbb{F}_{2^n} \setminus \{0\}$. Тогда в силу (9) и (10) справедливо $\varphi|_{s\mathbb{F}_{2^{p^i}}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$. Так как $2^{p^i} > 1$, то $|\mathcal{LA}_n(f_\varphi)| > \ell_{2n}$ по теореме 3.

Пусть $\varphi_s^p \notin \mathcal{R}_p$ для всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$. По теореме 3 неравенство $|\mathcal{LA}_n(f_\varphi)| > \ell_{2n}$ возможно только в случае существования $s \in \mathbb{F}_{2^n} \setminus \{0\}$ и $i \in \{1, \dots, k\}$ таких, что $\varphi|_{s\mathbb{F}_{2^{p^i}}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$, но тогда и $\varphi|_{s\mathbb{F}_{2^p}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^p}}$ в силу утверждения 7, поскольку $s\mathbb{F}_{2^p} \subseteq s\mathbb{F}_{2^{p^i}}$ ($\mathbb{F}_{2^p}$ является подполем $\mathbb{F}_{2^{p^i}}$, так как $p \mid p^i$). Отсюда в силу (9) и (10) получаем $\varphi_s^p \in \mathcal{R}_p$; противоречие. Теорема 4 доказана.

Функции φ, о которых идёт речь в теореме 4, нетрудно перечислить конструктивно.

Следствие 3. *Если $m \mid n = p^k$, где $p \geqslant 5$ простое и $k \geqslant 1$, то существует ровно*

$$2\,(2^{2^m-1} - 2^{m^2-m+1})^{\frac{2^n-1}{2^m-1}}$$

функций $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, для которых $\varphi_s^m \notin \mathcal{R}_m$ при всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$.

Доказательство. Заметим, что

$$\mathbb{F}_{2^n} = s_1\mathbb{F}_{2^m} \cup \cdots \cup s_t\mathbb{F}_{2^m}$$

для подходящих $s_1, \ldots, s_t \in \mathbb{F}_{2^n}$ и $t = \frac{2^n-1}{2^m-1}$, причём различные $s_i\mathbb{F}_{2^m}$ пересекаются только по нулевому элементу. Следовательно, функцию φ можно «собрать» из функций $\varphi^m_{s_1}, \ldots, \varphi^m_{s_t}$, единственным общим значением которых является значение в нуле.

Значение $\varphi(0) \in \{0, 1\}$ зададим произвольно — для этого имеется два варианта. Таким образом фиксируем

$$\varphi^m_{s_1}(0) = \cdots = \varphi^m_{s_t}(0) = \varphi(0).$$

Остальные значения функции $\varphi^m_{s_1}, \ldots, \varphi^m_{s_t}$ принимают независимо. Заметим также, что $h \in \mathcal{R}_m$ равносильно $h + 1 \in \mathcal{R}_m$, или, что то же самое, $h \in \mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$ равносильно $h + 1 \in \mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$. Тем самым в зависимости от $\varphi(0)$ в качестве подходящей функции $\varphi^m_{s_i}$ можем выбрать одну из половины $\mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$, т. е. имеем

$$2^{2^m-1} - 2^{m^2-m+1}$$

вариантов, так как $|\mathcal{R}_m| = 2^{(m-1)^2} \cdot 2^{m+1}$ по утверждению 10. Поскольку функции из $\mathcal{R}_m$ имеют алгебраическое представление и ограничения касаются только представленных степеней, сделать это нетрудно. Осталось заметить, что нужно задать ровно t таких функций. Следствие 3 доказано.

Равенство $|\mathcal{LA}_n(f_\varphi)| = \ell_{2n}$ также может выполняться для некоторых других составных n и аналогично заданной функции $f_\varphi \in \mathcal{M}_{2n}$ (см. следствие 5 в п. 5.1).

5. Число ближайших бент-функций, близкое к его оценкам

Здесь продемонстрируем другое применение формулы из теоремы 3 (следствия 1). Сосредоточимся на подстановках, размерность ядра и образ которых найдены в разд. 3. Условно разделим их на две части: одни, для которых число ближайших к $f \in \mathcal{M}_{2n}$ бент-функций $|\mathcal{LA}_n(f)|$ близко к нижней оценке ℓ_{2n}, и другие, для которых это число близко к точной верхней оценке

$$\mathcal{U}_{2n} = 2^n(2^1 + 1)(2^2 + 1)\ldots(2^n + 1). \tag{11}$$

Напомним, что верхняя оценка достигается на квадратичных бент-функциях (в том числе из $\mathcal{M}_{2n}$) и только на них [29]. Минимальное значение $|\mathcal{LA}_n(f)|$ из полученных далее равно $\ell_{2n} + o(\ell_{2n})$ при $n \to \infty$, а максимальное — $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ при $n \to \infty$.

5.1. Число ближайших бент-функций, близкое к ℓ_{2n}. Бент-функцию $f \in \mathcal{M}_{2n}$ будем строить с помощью инверсии элементов конечного поля $\mathbb{F}_{2^n}$.

Следствие 4. *Пусть* $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2})$, *где* $x, y \in \mathbb{F}_{2^n}$. *Тогда*

$$|\mathcal{LA}_n(f)| = 2^{3n-1} + 2^{2n+1} - 2^n + \sum_{\substack{1<k<n:\\ k \mid n}} \frac{2^n-1}{2^k-1} \cdot 2^{3k-1}.$$

Доказательство. По теореме 3 для $k \in \{0,1\}$ имеем $2^{2n+1} - 2^n$ бент-функций. Для $2 \leqslant k \leqslant n$ по утверждению 3 нужно рассмотреть только $k \mid n$, причём $\mathcal{L}_k(\pi) = \{s\mathbb{F}_{2^k} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}$. Нетрудно видеть, что $|\mathcal{L}_k(\sigma)| = \frac{2^n-1}{2^k-1}$ для $\sigma\colon x \mapsto x^{2^n-2}$, $x \in \mathbb{F}_{2^n}$. С помощью теоремы 2 для каждого из этих подпространств перейдём к функции обращения в подполе $\mathbb{F}_{2^k}$: положим $\sigma_s = A \circ \pi \circ A\colon \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, где $A\colon x \mapsto sx$, т. е. $\sigma_s\colon x \mapsto x^{2^n-2} = x^{2^k-2}$. Поскольку $\varphi \equiv 0$, её ограничение всегда принадлежит $\mathrm{Im}\ \mathcal{G}_{\sigma_s}$. Наконец, $|\mathrm{Ker}\ \mathcal{G}_{\sigma_s}| = 2^{3k-1}$ по утверждению 10. Следствие 4 доказано.

Число из следствия 4 заметно больше нижней оценки. Однако для любого n существует бент-функция $f \in \mathcal{M}_{2n}$, для которой $|\mathcal{LA}_n(f)|$ имеет ту же асимптотику, что и ℓ_{2n}.

Теорема 5. *Существует функция* $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$, *для которой* $|\mathcal{LA}_n(f)| < 2^{2n+1} + 81 \cdot 2^n - 82$, *т. е.* $|\mathcal{LA}_n(f)| = \ell_{2n} + o(\ell_{2n})$ *при* $n \to \infty$.

Доказательство. Используя теорему 3, для функции $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ найдём число бент-функций, ближайших к $f(x,y) = \mathrm{tr}_1^n(x\sigma(y)) + \varphi(y)$, $\sigma(y) = y^{2^n-2}$, и не учтённых в оценке ℓ_{2n}. При этом усреднив его по множеству всех таких функций φ, получим

$$\begin{aligned}
M_n &= 2^{-2^n} \sum_{\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) \cdot \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| = \\
&= 2^{-2^n} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| \sum_{\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) = \\
&= 2^{-2^n} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| \cdot \left|\mathrm{Im}\ \mathcal{G}_\sigma^L\right| \cdot 2^{k+1} \cdot 2^{2^n-2^k} = \\
&= \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} 2^{k^2+k} \cdot 2^{k+1} \cdot 2^{-2^k} = \sum_{k=2}^{n} |\mathcal{L}_k(\sigma)| \cdot 2^{(k+1)^2-2^k}.
\end{aligned}$$

Здесь $\sum\limits_{\varphi} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) = \left|\mathrm{Im}\ \mathcal{G}_\sigma^L\right| \cdot 2^{k+1} \cdot 2^{2^n-2^k}$ в силу того, что в образ $\mathrm{Im}\ \mathcal{G}_\sigma^L$ включены функции с точностью до аффинной части, а вне подпространства L функцию φ можно задать произвольным образом.

Далее воспользуемся утверждением 3:

$$M_n = \sum_{k\geqslant 2:\ k\,|\,n} \frac{2^n-1}{2^k-1} 2^{(k+1)^2-2^k} = (2^n-1) \sum_{k\geqslant 2:\ k\,|\,n} \frac{2^{(k+1)^2-2^k}}{2^k-1}. \qquad (12)$$

Приведём значения $N_k = \frac{2^{(k+1)^2-2^k}}{2^k-1}$ для малых k:

$$N_2 = \frac{32}{3}, \quad N_3 = \frac{256}{7}, \quad N_4 = \frac{512}{15},$$
$$N_5 = \frac{16}{31}, \quad N_6 = \frac{1}{63\cdot 2^{15}}, \quad N_7 = \frac{1}{127\cdot 2^{64}}.$$

Оценим M_n сверху:

$$M_n < (2^n-1)\left(\sum_{k=2}^{5} N_k + \sum_{k=6}^{\infty} 2^{(k+1)^2-2^k-k+1}\right) < 82\,(2^n-1). \qquad (13)$$

Действительно, вторая часть суммы не превосходит $2N_6$, так как очевидно, что $N_{k+1} < \frac{1}{2}N_k$ при $k \geqslant 6$, при этом $N_2 + N_3 + N_4 + N_5 = 10 + \frac{2}{3} + 36 + \frac{4}{7} + 34 + \frac{2}{15} + \frac{16}{31} < 82 - 2N_6$.

Поскольку M_n — среднее значение по всем функциям φ, хотя бы для одной из них усредняемое число не превосходит M_n, в противном случае среднее значение было бы больше. Теорема 5 доказана.

Таким образом, при любом n можно найти бент-функцию $f \in \mathcal{M}_{2n}$, для которой среди её ближайших бент-функций не более $82\,(2^n-1)$ лежат вне $\mathcal{M}_{2n}$ (см. утверждение 2). В некоторых случаях теорема 5 влечёт достижимость ℓ_{2n}.

Следствие 5. *Пусть m — минимальный нетривиальный делитель n, $m \geqslant 6$ и $n \leqslant 2^m - m^2 - m - 3$. Тогда найдётся бент-функция $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$, для которой справедливо $|\mathcal{LA}_n(f)| = \ell_{2n}$.*

Доказательство. Поскольку $m \geqslant 6$, в силу (12) и (13) справедливо

$$M_n < (2^n-1)\sum_{k=m}^{\infty} 2^{(k+1)^2-2^k-k+1} < 2^n \cdot 2 \cdot 2^{(m+1)^2-2^m-m+1}.$$

Тем самым при $n \leqslant 2^m + m - (m+1)^2 - 2 = 2^m - m^2 - m - 3$ получаем $M_n < 1$. Однако M_n — среднее значение, поэтому усредняемое число хотя бы для одной из функции φ не превосходит M_n и, следовательно, равно 0. Следствие 5 доказано.

Условию на n из следствия 5 удовлетворяют числа $11 \cdot 13$, $11 \cdot 11 \cdot 13$, $11 \cdot 17$ и т. п., что дополняет результаты п. 4.2.

5.2. Число ближайших бент-функций, близкое к $\mathcal{U}_{2n}$. Для удобства в качестве подстановки π будем рассматривать тождественное отображение, т. е. речь пойдёт о функциях вида $f(x,y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$. Можно легко расширить этот подкласс без изменения $|\mathcal{LA}_n(f)|$.

Утверждение 11. *Пусть бент-функции $f, g \in \mathcal{M}_{2n}$ имеют вид*

$$f(x,y) = \langle x, y\rangle \oplus \varphi(y), \quad g(x,y) = \langle x, \pi(y)\rangle \oplus \psi(y),$$

подстановка π аффинна и $\deg(\varphi \oplus \psi) \leqslant 2$. Тогда f и g имеют одинаковое число ближайших к ним бент-функций.

Доказательство. По утверждению 8 в $\operatorname{Im} \mathcal{G}_\pi^L$ лежат все функции $h\colon L \to \mathbb{F}_2$ степени не выше 2, $\left|\operatorname{Ker} \mathcal{G}_\pi^L\right|$ зависит только от размерности L, а любое $L \in \mathcal{S}_n^k$ принадлежит $\mathcal{L}_k(\pi)$, поэтому по формуле из теоремы 3 получаем равенство $|\mathcal{LA}_n(f)| = |\mathcal{LA}_n(g)|$. Утверждение 11 доказано.

Мощность $\mathcal{LA}_n(f)$ можно вычислить через ограничения функции φ на подпространства $L \in \mathcal{AS}_n^k$, которые имеют степень не выше 2.

Следствие 6. *Пусть $f(x,y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$. Тогда*

$$|\mathcal{LA}_n(f)| = \sum_{k=0}^{n} \left|\left\{L \in \mathcal{AS}_n^k \mid \deg \varphi|_L \leqslant 2\right\}\right| \cdot 2^{\frac{k(k+3)}{2}}.$$

Доказательство. По условию $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — тождественное отображение. Воспользуемся теоремой 2. Для этого рассмотрим обратимую аффинную функцию $A\colon \mathbb{F}_2^k \to L$ и положим $B = A^{-1}$, так что получим $\varphi' = \varphi|_L \circ A$, а $\pi' = A^{-1} \circ \pi|_L \circ A\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ — также тождественное отображение. По утверждению 8 имеем $\operatorname{Im} \mathcal{G}_{\pi'} = \{\varphi' \in \widetilde{\mathcal{F}}_k \mid \deg \varphi' \leqslant 2\}$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^{\frac{k(k+3)}{2}}$, но степени $\varphi' = \varphi|_L \circ A$ и $\varphi|_L$ совпадают, так как A — невырожденное аффинное преобразование. Финальная формула получается из теоремы 3. Следствие 6 доказано.

Напрямую воспользоваться формулой из следствия 6 трудно, однако это можно сделать для следующего узкого класса бент-функций.

Следствие 7. *Пусть $f(x,y) = \langle x, y\rangle \oplus y_1 y_2 \dots y_m \in \mathcal{M}_{2n}$, $3 \leqslant m \leqslant n$. Тогда*

$$|\mathcal{LA}_n(f)| =$$
$$= \sum_{k=0}^{n} \left(2^{n-k} \cdot \left|\mathcal{S}_n^k\right| - \sum_{t=t_*(k)}^{t^*(k)} \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)} \right) \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \mathcal{U}_{2n} - \sum_{k=0}^{n} \sum_{t=t_*(k)}^{t^*(k)} \left|\mathcal{S}_{n-m}^{t}\right| \cdot \left|\mathcal{S}_{m}^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)} \cdot 2^{\frac{k(k+3)}{2}},$$

где $t_*(k) = \max\{0,\, k-m\}$, $t^*(k) = \min\{n-m,\, k-3\}$ *для* $k \in \{0, \ldots, n\}$.

Доказательство. Чтобы применить формулу из следствия 6, для каждого $k \in \{0, \ldots, n\}$ найдём число подпространств $L \in \mathcal{AS}_n^k$, для которых $\deg \varphi|_L \leqslant 2$ при $\varphi(y) = y_1 \ldots y_m$. Подсчитаем число L, для которых $\deg \varphi|_L \geqslant 3$, а затем вычтем его из $2^{n-k}\left|\mathcal{S}_n^k\right|$ — числа всех подпространств размерности k.

Без ограничения общности конъюнкцию $y_1 \ldots y_m$ заменим конъюнкцией $y_{n-m+1} \ldots y_n$, являющейся характеристической функцией подпространства $Z = \mathbb{F}_2^{n-m} \times \{1\}^m \in \mathcal{AS}_n^{n-m}$. Заметим, что $\varphi|_L(y) = 1$, если и только если $y \in L \cap Z = T$, причём это пересечение либо пусто, либо принадлежит $\mathcal{AS}_n^t$ для некоторого $t \in \{0, \ldots, n-m\}$. Таким образом, функция $\varphi|_L$ характеристическая для T, а её степень равна $k-t$. Значит, нам нужны подпространства T размерности $t \leqslant k-3$, точнее $t \leqslant \min\{k-3,\, n-m\}$.

Подсчитаем число $L \in \mathcal{AS}_n^k$ таких, что $\dim L \cap Z = t \leqslant k-3$. Нетрудно видеть, что оно равно числу подпространств $[L] \in \mathcal{S}_n^k$, пересекающихся с $[Z]$ по подпространству размерности t, умноженному на 2^{n-m-t} — именно столькими способами можно выбрать аффинное подпространство пространства L с фиксированной линейной частью.

Воспользуемся представлением линейных подпространств из п. 2.1: $L = \mathcal{S}(U, V, H) \subseteq \mathbb{F}_2^{n-m} \times \mathbb{F}_2^m$, где $U \in \mathcal{S}_m^{k-r}$, $V \in \mathcal{S}_{n-m}^r$ и $H \in \mathcal{A}_U^{n-m}/\mathcal{A}_U^V$ линейная (см. замечание 2). Согласно утверждению 4 имеем равенство $V \times \{0\}^m = [L] \cap [Z]$, т. е. $r = t$. Таких V ровно $\left|\mathcal{S}_{n-m}^t\right|$. Далее, $\left|\mathcal{S}_m^{k-t}\right|$ способами можем выбрать подпространство U и $2^{(k-t)(n-m-t)}$ способами — одну из попарно неэквивалентных функций H (см. замечание 1), так что в итоге получаем

$$\left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t)(n-m-t)}$$

вариантов выбора $[L]$. Отсюда находим число способов выбрать L:

$$2^{n-m-t} \cdot \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t)(n-m-t)} = \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)},$$

при этом $t \geqslant k-m$, поскольку $\dim U = \dim L - \dim V = k - t \leqslant m$ (см. утверждение 4). Полученное выражение суммируем по t от $\max\{0, k-m\}$ до $\min\{k-3,\, n-m\}$ и вычтем из $|\mathcal{AS}_n^k| = 2^{n-k}\left|\mathcal{S}_n^k\right|$. В результате приходим к первому равенству для $|\mathcal{LA}_n(f)|$ из условия теоремы.

Осталось заметить, что

$$\sum_{k=0}^{n} 2^{n-k} \cdot \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} = \mathcal{U}_{2n}. \tag{14}$$

Действительно, с одной стороны, по теореме 3 левая часть (14) равна $|\mathcal{LA}_n(g)|$ для квадратичной функции $g(x,y)=\langle x,y\rangle$ от $2n$ переменных. С другой стороны, $|\mathcal{LA}_n(g)|=\mathcal{U}_{2n}$ согласно [28]. Следствие 7 доказано.

Замечание 4. В условии следствия 7

1) вместо $y_1\dots y_m$ можно взять Ind_S для любого $S\in\mathcal{AS}_n^{n-m}$;

2) при $m=n$ и $m=n-1$ формулы справедливы для бент-функций $f(x,y)=\langle x,y\rangle\oplus\varphi(y)\in\mathcal{M}_{2n}$ таких, что $\mathrm{wt}(\varphi)=1$ и $\mathrm{wt}(\varphi)=2$ соответственно.

Формулы из следствия 7 весьма полезны, поскольку дают представление $|\mathcal{LA}_n(f)|$ через гауссовы коэффициенты

$$\left|\mathcal{S}_n^k\right|=\prod_{i=0}^{k-1}\frac{2^n-2^i}{2^k-2^i},\quad 0\leqslant k\leqslant n.$$

Для $m\in\{3,n\}$ можно получить ещё более простые выражения.

Следствие 8. *Пусть бент-функции $f_3,f_n\in\mathcal{M}_{2n}$, $n\geqslant 3$, имеют вид*

$$f_3(x,y)=\langle x,y\rangle\oplus y_1y_2y_3,\quad f_n(x,y)=\langle x,y\rangle\oplus y_1y_2\dots y_n.$$

Тогда

$$|\mathcal{LA}_n(f_3)|=\mathcal{U}_{2n}-2^{4n-3}(2^1+1)(2^2+1)\dots(2^{n-3}+1),$$

$$|\mathcal{LA}_n(f_n)|=(2^n-1)\prod_{k=2}^{n}(2^k+1)+\frac{32}{3}(2^{2n-1}+1)-3\cdot 2^{n+2}-3,$$

при этом $|\mathcal{LA}_n(f_3)|=o(\mathcal{U}_{2n})$, $|\mathcal{LA}_n(f_n)|=\frac{1}{3}\mathcal{U}_{2n}+o(\mathcal{U}_{2n})$ при $n\to\infty$.

Доказательство. Легко видеть, что при $3\leqslant k\leqslant n$

$$\sum_{t=t_*(k)}^{t^*(k)}\left|\mathcal{S}_{n-m}^t\right|\cdot\left|\mathcal{S}_m^{k-t}\right|\cdot 2^{(k-t+1)(n-m-t)}=\begin{cases}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)} & \text{для } m=3,\\ \left|\mathcal{S}_n^k\right| & \text{для } m=n,\end{cases}$$

а при $0\leqslant k\leqslant 2$ эта сумма равна нулю.

Случай 1: $m=3$. В силу следствия 7

$$|\mathcal{LA}_n(f_3)|=\mathcal{U}_{2n}-\sum_{k=3}^{n}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)}\cdot 2^{\frac{k(k+3)}{2}}.$$

Заменой индекса $k\to k+3$ сумма в правой части приводится к виду

$$\sum_{k=3}^{n}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)}\cdot 2^{\frac{k(k+3)}{2}}=\sum_{k=0}^{n-3}\left|\mathcal{S}_{n-3}^{k}\right|2^{4(n-k-3)}\cdot 2^{\frac{(k+3)(k+6)}{2}}=$$

$$= \sum_{k=0}^{n-3} \left|\mathcal{S}_{n-3}^k\right| \cdot 2^{4(n-3)-4k+3(k+3)} \cdot 2^{\frac{k(k+3)}{2}} = 2^{3n} \sum_{k=0}^{n-3} \left|\mathcal{S}_n^k\right| \cdot 2^{n-3-k} \cdot 2^{\frac{k(k+3)}{2}} \overset{(14)}{=}$$

$$\overset{(14)}{=} 2^{3n}\,\mathcal{U}_{2(n-3)} = 2^{3n} \cdot 2^{n-3}(2^1+1)(2^2+1)\dots(2^{n-3}+1),$$

откуда $|\mathcal{LA}_n(f_3)| = \mathcal{U}_{2n} - 2^{3n}\,\mathcal{U}_{2(n-3)} = o(\mathcal{U}_{2n})$ при $n \to \infty$.

Случай 2: $m = n$. В силу следствия 7 имеем

$$|\mathcal{LA}_n(f_n)| = 2^n(2^1+1)\dots(2^n+1) - \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} + \sum_{k=0}^{2} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}},$$

где последнее слагаемое равно

$$1 + (2^n-1)\cdot 2^2 + \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} \cdot 2^5 = \frac{32}{3}(2^{2n-1}+1) - 3\cdot 2^{n+2} - 3.$$

Упростим второе слагаемое

$$P(n) = \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}}.$$

Аналогично выводу равенства (14) в [28], применим очевидное свойство

$$\left|\mathcal{S}_n^k\right| = \left|\mathcal{S}_{n-1}^k\right| + 2^{n-k}\left|\mathcal{S}_{n-1}^{k-1}\right|, \quad 1 \leqslant k \leqslant n,$$

где по определению $\left|\mathcal{S}_{n-1}^n\right| = 0$. Поскольку $\left|\mathcal{S}_n^0\right| = \left|\mathcal{S}_{n-1}^0\right| = 1$, получаем

$$P(n) = \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k(k+3)}{2}} + \sum_{k=1}^{n} 2^{n-k} \cdot \left|\mathcal{S}_{n-1}^{k-1}\right| \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \{k \to k+1\} = P(n-1) + \sum_{k=0}^{n-1} 2^{n-1-k} \cdot \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{(k+1)(k+4)}{2}} =$$

$$= P(n-1) + 2^{n+1} \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k^2+5k+4-2k-4}{2}} =$$

$$= P(n-1) + 2^{n+1} \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k(k+3)}{2}} = (1+2^{n+1})P(n-1).$$

Таким образом, $P(n) = (2^{n+1}+1)P(n-1)$ и $P(0) = 1$, откуда

$$P(n) = (2^2+1)(2^3+1)\dots(2^{n+1}+1),$$

$$2^n(2^1+1)\dots(2^n+1) - P(n) = (2^2+1)\dots(2^n+1)(3\cdot 2^n - 2^{n+1} - 1).$$

Суммируя найденные слагаемые, приходим к требуемой формуле для $|\mathcal{LA}_n(f_n)|$, из которой нетрудно видеть, что $|\mathcal{LA}_n(f_n)| = \frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ при $n \to \infty$. Следствие 8 доказано.

Заметим, что $|\mathcal{LA}_n(f_n)| > |\mathcal{LA}_n(f_3)|$ при $n \geqslant 4$, хотя в этом случае $\deg f_3 = 3 < \deg f_n = n$, и вообще $|\mathcal{LA}_n(f_3)| = o(|\mathcal{LA}_n(f_n)|)$ при $n \to \infty$.

Интересно, что имеется ещё одна неквадратичная бент-функция, для которой ожидаемое число ближайших бент-функций велико, имеет их столько же, сколько и f_n.

Утверждение 12. *Пусть $f_\tau(x, y) = \langle x, \tau(y)\rangle \in \mathcal{M}_{2n}$, где τ — транспозиция на $\mathbb{F}_2^n$, переставляющая векторы $(1, \ldots, 1, 0)$ и $(1, \ldots, 1, 1)$ друг с другом. Тогда $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_n)|$.*

Доказательство. Нетрудно видеть, что

$$\tau(y) = y \oplus (0, \ldots, 0, y_1 \ldots y_{n-1}).$$

Действительно, если $(y_1, \ldots, y_{n-1}) \neq (1, \ldots, 1)$, то $\tau(y) = y$. Иначе получаем $\tau(1, \ldots, 1, 0) = (1, \ldots, 1, 0 \oplus 1)$ и $\tau(1, \ldots, 1, 1) = (1, \ldots, 1, 1 \oplus 1)$, что соответствует определению τ. Следовательно,

$$f_\tau(x, y) = \langle x, y\rangle \oplus x_n(y_1 \ldots y_{n-1}) = x_1y_1 \oplus \cdots \oplus x_ny_n \oplus y_1 \ldots y_{n-1}x_n.$$

Таким образом, переставив переменные x_n и y_n, получим в точности f_n и $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_n)|$. Утверждение 12 доказано.

Замечание 5. В условии утверждения 12 можно считать, что τ — произвольная транспозиция на $\mathbb{F}_2^n$, поскольку все f_τ EA-эквивалентны друг другу и, следовательно, имеют одинаковые $|\mathcal{LA}_n(f_\tau)|$. Для доказательства достаточно привести транспозицию τ к указанной в утверждении при помощи композиции $A \circ \tau \circ B$, где $A, B\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — некоторые обратимые аффинные преобразования. Также в условии утверждения 12 вместо транспозиции можно рассматривать саму приведённую композицию для произвольных транспозиции τ и обратимых аффинных A, B.

Согласно следствиям 1, 8 и утверждению 12 функции f_n и f_τ дают наиболее интуитивно очевидные способы построить бент-функции с максимально возможной $|\mathcal{LA}_n(f)|$ среди неквадратичных функций $f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$: либо выбираем тождественную (аффинную) подстановку π и минимально отличающуюся от тождественно нулевой функцию φ, либо, наоборот, выбираем тождественно нулевую φ и минимально отличающуюся от тождественной (аффинной) π. Эти рассуждения, а также принцип построения $\mathcal{M}_{2n}$, позволяют сделать предположение.

Гипотеза 1. *Пусть f — бент-функция от $2n$ переменных и $\deg f \geqslant 3$. Тогда $|\mathcal{LA}_n(f)| \leqslant |\mathcal{LA}_n(f_n)|$.*

6. Классификация бент-функций из $\mathcal{M}_6$

Теорема 3 (следствие 1) позволяет классифицировать $f \in \mathcal{M}_6$ на основе $|\mathcal{LA}_3(f)|$. Начнём с мощности $\mathcal{L}_2(\pi)$ для подстановок π на $\mathbb{F}_2^3$. Обратим также внимание, что возможные значения $|\mathcal{L}_{n-1}(\pi)|$ для подстановок π на $\mathbb{F}_2^n$ (без классификации π) были получены в работе [36].

Утверждение 13. *Пусть $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ взаимно однозначна. Тогда*

$$|\mathcal{L}_2(\pi)| = \begin{cases} 0, & \text{если } \delta(\pi) = 2, \\ 2, & \text{если } \delta(\pi) = 4, \\ 6, & \text{если } \delta(\pi) = 8 \text{ и } \pi \notin \mathcal{A}_3^3, \\ 14, & \text{если } \pi \in \mathcal{A}_3^3. \end{cases}$$

Других взаимно однозначных функций π нет.

Доказательство. 1. По одному из определений APN-подстановки π выполнено $\mathcal{L}_2(\pi) = \varnothing$.

2. Пусть $\delta(\pi) = 4$. Все $L \in \mathcal{L}_2(\pi)$ являются гиперплоскостями в $\mathbb{F}_2^3$, т. е. $L \in \mathcal{L}_2(\pi)$ тогда и только тогда, когда его сдвиг $\mathbb{F}_2^3 \setminus L \in \mathcal{L}_2(\pi)$.

Далее от противного: пусть есть различные $L, U \in \mathcal{L}_2(\pi)$, не являющиеся сдвигами друг друга. В этом случае $|V = L \cap U| = 2$. Обозначим $V = \{a,\, a \oplus v\}$, $a, v \in \mathbb{F}_2^3$ и $\pi(V) = \{\pi(a),\, \pi(a) \oplus v')\}$, $v' \in \mathbb{F}_2^3$. Тогда $L \setminus V = \{b,\, b \oplus v\}$ и $U \setminus V = \{c,\, c \oplus v\}$ для некоторых $b, c \in \mathbb{F}_2^3$, так как L и U — аффинные подпространства $\mathbb{F}_2^3$ и сумма всех их элементов должна быть равна 0. То же самое верно и для образов: $\pi(L) \setminus \pi(V) = \{b', b' \oplus v'\}$ и $\pi(U) \setminus \pi(V) = \{c', c' \oplus v'\}$, $b', c' \in \mathbb{F}_2^3$. В результате уравнение $\pi(x) \oplus \pi(x \oplus v) = v'$ имеет как минимум шесть решений a, $a \oplus v$, b, $b \oplus v$, c, $c \oplus v$, а это противоречит тому, что $\delta(\pi) = 4$. При этом $\delta(\pi) \neq 2$, откуда $|\mathcal{L}_2(\pi)| > 0$. Следовательно, $\mathcal{L}_2(\pi) = \{L,\, \mathbb{F}_2^3 \setminus L\}$ для некоторого L.

3. Пусть $\delta(\pi) = 8$ и π не аффинна, т. е. производная π по некоторому ненулевому направлению является константой, или, другими словами, подстановка π имеет непустую линейную структуру. Все такие функции можно аффинными преобразованиями привести к следующей (см., например, [8]):

$$\pi'(x) = qx_1x_2 + sx_3 + t = \pi(xB \oplus b), \quad x \in \mathbb{F}_2^3,$$

где $q, s, t \in \mathbb{F}_2^3$, $q \neq 0$, двоичная матрица B невырожденная и имеет порядок 3, $b \in \mathbb{F}_2^3$. Ясно, что $|\mathcal{L}_2(\pi)| = |\mathcal{L}_2(\pi')|$, поэтому далее вместо π будем рассматривать π'.

Очевидно, что $L \in \mathcal{L}_2(\pi)$ тогда и только тогда, когда $\pi|_L$ аффинна. Значит, в полиноме Жегалкина $\pi|_L$ нет квадратичного слагаемого x_1x_2. Тем самым $\mathcal{L}_2(\pi)$ состоит из всех таких $L \in \mathcal{AS}_3^2$, на которых функция $g(x) = x_1x_2$ аффинна.

Производное подпространство $L \in \mathcal{AS}_3^2$ можно задать уравнением $a_1x_1 \oplus a_2x_2 \oplus a_3x_3 = c$, причём различным парам $a \in \mathbb{F}_2^3$, $c \in \mathbb{F}_2$ соответствуют различные подпространства. Нам подходят L, заданные уравнениями $x_1 = c$, $x_2 = c$ и $x_1 \oplus x_2 = c$. Действительно, если $a_3 = 1$, то $L = \{(x_1, x_2, a_1x_1 \oplus a_2x_2 \oplus c) \in \mathbb{F}_2^3 \mid x_1, x_2 \in \mathbb{F}_2\}$ и $g|_L$ не аффинна. Таким образом, $\mathcal{L}_2(\pi)$ состоит из $3 \cdot 2 = 6$ элементов.

4. Очевидно, так как подстановка π аффинна на всех аффинных подпространствах размерности 2, которых в $\mathbb{F}_2^3$ имеется $7 \cdot 2 = 14$.

5. В силу взаимной однозначности функции π получаем $\deg \pi \leqslant 2$, поэтому её производные $\pi(x) \oplus \pi(x \oplus a)$ по всем направлениям $a \in \mathbb{F}_2^3$ аффинны. Тем самым число решений уравнений $\pi(x) \oplus \pi(x \oplus a) = b$ принадлежит множеству $\{0, 2, 4, 8\}$. Поскольку $\delta(\pi) \geqslant 2$, рассмотрены все возможные случаи. Утверждение 13 доказано.

Приведём классификацию функций $f \in \mathcal{M}_6$ относительно $|\mathcal{LA}_3(f)|$.

Теорема 6. *Пусть* $f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y) \in \mathcal{M}_6$. *Тогда*

$$|\mathcal{LA}_3(f)| = \begin{cases} 376, & \text{если } \delta(\pi) = 2, \\ 440, & \text{если } \delta(\pi) = 4, \\ 568, & \text{если } \delta(\pi) = 8 \text{ и } \pi \notin \mathcal{A}_3^3, \\ 568, & \text{если } \pi \in \mathcal{A}_3^3 \text{ и } \deg \varphi = 3, \\ 1080 = \mathcal{U}_6, & \text{если } \pi \in \mathcal{A}_3^3 \text{ и } \deg \varphi \leqslant 2. \end{cases}$$

Доказательство. По теореме 3

$$|\mathcal{LA}_3(f)| = \ell_6 + 2^5 \cdot |\mathcal{L}_2(\pi)| + 2^8 \cdot |\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| + \\ + 2^9 \cdot |\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}|. \quad (15)$$

Здесь $\ell_6 = 120$, а $|\mathcal{L}_2(\pi)|$ найдена в утверждении 13. Далее, $\mathcal{L}_3(\pi) = \{\mathbb{F}_2^3\}$, так как $n = 3$. Наконец, очевидно, что $\mathcal{LA}_3(\pi) = \mathcal{L}_3(\pi)$, если π аффинна, и $\mathcal{LA}_3(\pi) = \varnothing$ иначе. Подстановкой найденных чисел в формулу (15) получаем требуемое равенство. Теорема 6 доказана.

Теорема 6 даёт также классификацию функций из $\mathcal{M}_6$ относительно EA-эквивалентности (см., например, работу [40] о методах классификации булевых функций в общем случае). Действительно, число $|\mathcal{LA}_n(f)|$ бент-функций на расстоянии 2^n от f является инвариантом функции $f \in \mathcal{M}_{2n}$ относительно EA-эквивалентности. При этом в [1] доказано, что множество бент-функций от 6 переменных разбивается на 4 класса EA-эквивалентности. Таким образом, эти 4 класса представлены в теореме 6, и каждому из них соответствует своё значение $|\mathcal{LA}_3(f)|$.

Заключение

Предложенный в работе подход к перечислению бент-функций, ближайших к заданной функции из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$, обладает следующими достоинствами.

• Обеспечивает возможность подсчёта их точного числа для ряда функций с определёнными симметриями.

• Позволяет расширить известные необходимое и достаточное условия достижимости нижней оценки ℓ_{2n} для их числа.

• На основе свойств класса $\mathcal{M}_{2n}$ для функции степени 3 и выше выдвинута гипотеза, ограничивающая число ближайших к ней бент-функций величиной $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$.

Остаётся простор для дальнейших исследований, в ходе которых возможно установить другие примечательные свойства этого класса бент-функций (см., например, [35]).

Финансирование работы

Исследование выполнено при поддержке Математического центра в Академгородке (соглашение № 075–15–2025–349 с Министерством науки и высшего образования Российской Федерации). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Rothaus O.** On "bent" functions // J. Comb. Theory. Ser. A. 1976. V. 20, No. 3. P. 300–305. DOI: 10.1016/0097-3165(76)90024-8.
2. **Tokareva N. N.** Bent functions: Results and applications to cryptography. Amsterdam: Acad. Press, 2015. 220 p. DOI: 10.1016/c2014-0-02922-x.
3. **Токарева Н. Н.** Бент-функции: результаты и приложения. Обзор работ // Прикл. дискрет. математика. 2009. № 1. С. 15–37. DOI: 10.17223/20710410/3/2.
4. **Токарева Н. Н.** Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2010. Т. 17, № 1. С. 34–64.
5. **Helleseth T., Kholosha A.** Bent functions and their connections to combinatorics // Surveys in combinatorics 2013. Cambridge: Camb. Univ. Press, 2013. P. 91–126. (Lond. Math. Soc. Lect. Notes Ser.; V. 409). DOI: 10.1017/CBO9781139506748.004.
6. **Dobbertin H., Leander G.** A survey of some recent results on bent functions // Sequences and their applications — SETA 2004. Proc. Int. Conf. (Seoul, Korea, Oct. 24–28, 2005). Heidelberg: Springer, 2005. P. 1–29. (Lect. Notes Comput. Sci.; V. 3486). DOI: 10.1007/11423461_1.

7. **Mesnager S.** Bent functions: Fundamentals and results. Cham: Springer, 2018. 570 p. DOI: 10.1007/978-3-319-32595-8.
8. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
9. **Logachev O. A., Salnikov A. A., Yashchenko V. V.** Boolean functions in coding theory and cryptography. Providence, RI: AMS, 2012. 334 p.
10. **Агибалов Г. П.** Избранные теоремы начального курса криптографии. Томск: Изд. дом ТГУ, 2005. 112 с.
11. **Панкратова И. А.** Булевы функции в криптографии. Томск: Изд. дом ТГУ, 2014. 88 с.
12. **Токарева Н. Н.** Симметричная криптография: Краткий курс. Новосибирск: НГУ, 2012. 234 с.
13. **Cusick T. W., Stanica P.** Cryptographic Boolean functions and applications. Amsterdam: Acad. Press, 2017. 275 p. DOI: 10.1016/c2016-0-00852-5.
14. **Carlet C.** Boolean functions for cryptography and coding theory. Cambridge: Camb. Univ. Press, 2020. 562 p. DOI: 10.1017/9781108606806.
15. **McFarland R. L.** A family of difference sets in non-cyclic groups // J. Comb. Theory. Ser. A. 1973. V. 15, No. 1. P. 1–10. DOI: 10.1016/0097-3165(73)90031-9.
16. **Dillon J. F.** Elementary Hadamard difference sets: PhD thesis. College Park, 1974.
17. **Коломеец Н. А., Павлов А. В.** Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика. 2009. № 4. С. 5–20.
18. **Carlet C.** Two new classes of bent functions // Advances in cryptology — EUROCRYPT'93. Proc. Workshop on the Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 77–101. (Lect. Notes Comput. Sci.; V. 765). DOI: 10.1007/3-540-48285-7_8.
19. **Zhang F., Pasalic E., Cepak N., Wei Y.** Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class // Codes, cryptology and information security. Proc. 2nd Int. Conf. (Rabat, Morocco, Apr. 10–12, 2017). Cham: Springer, 2017. P. 298–313. (Lect. Notes Comput. Sci.; V. 10194). DOI: 10.1007/978-3-319-55589-8_20.
20. **Zhang F., Cepak N., Pasalic E., Wei Y.** Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$ // Discrete Appl. Math. 2020. V. 285. P. 458–472. DOI: 10.1016/j.dam.2020.06.012.
21. **Kudin S., Pasalic E.** A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ // Des. Codes Cryptogr. 2022. V. 90, No. 8. P. 1783–1796. DOI: 10.1007/s10623-022-01079-3.
22. **Kudin S., Pasalic E., Cepak N., Zhang F.** Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class // Cryptogr. Commun. 2022. V. 14, No. 1. P. 101–116. DOI: 10.1007/s12095-021-00523-w.

23. Bapić A, Pasalic E., Zhang F., Hodžić S. Constructing new superclasses of bent functions from known ones // Cryptogr. Commun. 2022. V. 14, No. 6. P. 1229–1256. DOI: 10.1007/s12095-022-00566-7.

24. Pasalic E., Bapić A., Zhang F., Wei Y. Explicit infinite families of bent functions outside the completed Maiorana–McFarland class // Des. Codes Cryptogr. 2023. V. 91, No. 7. P. 2365–2393. DOI: 10.1007/s10623-023-01204-w.

25. Pasalic E., Polujan A., Kudin S., Zhang F. Design and analysis of bent functions using $\mathcal{M}$-subspaces // IEEE Trans. Inf. Theory. 2024. V. 70, No. 6. P. 4464–4477. DOI: 10.1109/TIT.2024.3352824.

26. Kudin S., Pasalic E., Polujan A., Zhang F. The algebraic characterization of $\mathcal{M}$-subspaces of bent concatenations and its application // IEEE Trans. Inf. Theory. 2025. V. 71, No. 5. P. 3999–4011. DOI: 10.1109/TIT.2025.3547533.

27. Polujan A. A., Pott A. Cubic bent functions outside the completed Maiorana–McFarland class // Des. Codes Cryptogr. 2020. V. 88, No. 9. P. 1701–1722. DOI: 10.1007/s10623-019-00712-y.

28. Коломеец Н. А. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискрет. анализ и исслед. операций. 2012. Т. 19, № 1. С. 41–58.

29. Kolomeec N. The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. 2017. V. 85, No. 3. P. 395–410. DOI: 10.1007/s10623-016-0306-4.

30. Быков Д. А., Коломеец Н. А. О нижней оценке числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — Мак-Фарланда // Дискрет. анализ и исслед. операций. 2023. Т. 30, № 3. С. 57–80.

31. Nyberg K. Differentily uniform mappings for cryptography // Advances in cryptology — EUROCRYPT'93. Proc. Workshop Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 55–64. (Lect. Notes Comput. Sci.; V. 765). DOI: 10.1007/3-540-48285-7_6.

32. Carlet C. Open questions on nonlinearity and on APN functions // Arithmetic of finite fields. Rev. Sel. Pap. 5th Int. Workshop (Gebze, Turkey, Sept. 27–28, 2014). Cham: Springer, 2015. P. 83–107. (Lect. Notes Comput. Sci.; V. 9061). DOI: 10.1007/978-3-319-16277-5_5.

33. Jacobson N. Basic algebra. V. I. Mineola, NY: Dover Publ., 2009. 528 p.

34. Kolomeec N. A., Bykov D. A. On the image of an affine subspace under the inverse function within a finite field // Des. Codes Cryptogr. 2024. V. 92, No. 2. P. 467–476. DOI: 10.1007/s10623-023-01316-3.

35. Kolomeec N. A., Bykov D. A. On the Maiorana–McFarland class extensions. Ithaca, NY, 2025. 29 p. (e-Print Archive / Cornell Univ.; arXiv:2503.21440). DOI: 10.48550/arXiv.2503.21440.

36. Clark W. E., Hou X., Mihailovs A. The affinity of a permutation of a finite vector space // Finite Fields Appl. 2007. V. 13. P. 80–112. DOI: 10.1016/j.ffa.2005.07.004.

37. Li S., Meidl W., Polujan A., Pott A., Riera C., Stănică P. Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application // IEEE Trans. Inf. Theory. 2020. V. 66, No. 11. P. 7101–7112. DOI: 10.1109/TIT.2020.3002993.

38. Коломеец Н. А. О подстановках, разрушающих структуру подпространств определённых размерностей // Прикл. дискрет. математика. 2024. № 65. С. 5–20. DOI: 10.17223/20710410/65/1.

39. Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J. An APN permutation in dimension six // Finite fields: Theory and applications. Proc. 9th Int. Conf. (Dublin, Ireland, July 13–17, 2009). Providence, RI: AMS, 2010. P. 33–42. (Contemp. Math.; V. 518). DOI: 10.1090/conm/518/10194.

40. Черёмушкин А. В. Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. М.: Физматлит, 2001. С. 273–314.

Быков Денис Александрович
Коломеец Николай Александрович

Статья поступила
27 августа 2024 г.
После доработки —
26 марта 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 5–42

UDC 519.7 DOI: 10.33048/daio.2025.32.811

ON THE BENT FUNCTIONS CLOSEST TO A GIVEN MAIORANA–MCFARLAND BENT FUNCTION

D. A. Bykov[a] and *N. A. Kolomeec*[b]

Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia
E-mail: [a] den.bykov.2000i@gmail.com, [b] nkolomeec@gmail.com

Abstract. Bent functions of $2n$ variables closest to a given bent function in the Maiorana–McFarland class are considered. The known criterion for their construction is revised and the method of calculating their number is refined. We investigate functions such that the number of closest bent functions is approximate to its lower and sharp upper bounds. The existence of bent functions whose number of closest bent functions has the same asymptotics as the lower bound is proven. Examples of functions in the Maiorana–McFarland class are given for which the calculated number of closest bent functions is close to the upper bound. Attainability of the lower bound is considered, and known necessary and sufficient conditions are refined. We show that the lower bound is attained for n equaled to a power of a prime $p \geqslant 5$, as well as for some other n. A complete classification of functions of 6 variables in the Maiorana–McFarland class using the number of closest bent functions is obtained. Tab. 1, bibliogr. 40.

Keywords: bent function, Boolean function, affine subspace, minimum distance, Maiorana–McFarland class.

References

1. **O. Rothaus,** On "bent" functions, *J. Comb. Theory, Ser. A*, **20** (3), 300–305 (1976), DOI: 10.1016/0097-3165(76)90024-8.
2. **N. N. Tokareva,** *Bent Functions: Results and Applications to Cryptography* (Acad. Press, Amsterdam, 2015), DOI: 10.1016/c2014-0-02922-x.
3. **N. N. Tokareva,** Bent functions: Results and applications. A survey, *Prikl. Diskretn. Mat.*, No. 1, 15–37 (2009) [Russian], DOI: 10.17223/20710410/3/2.

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

4. **N. N. Tokareva,** Generalizations of bent functions. A survey, *Diskretn. Anal. Issled. Oper.* **17** (1), 34–64 (2010) [Russian] [*J. Appl. Ind. Math.* **5** (1), 110–129 (2011), DOI: 10.1134/S1990478911010133].
5. **T. Helleseth** and **A. Kholosha,** Bent functions and their connections to combinatorics, in *Surveys in Combinatorics 2013* (Camb. Univ. Press, Cambridge, 2013), pp. 91–126 (Lond. Math. Soc. Lect. Notes Ser., Vol. 409), DOI: 10.1017/CBO9781139506748.004.
6. **H. Dobbertin** and **G. Leander,** A survey of some recent results on bent functions, in *Sequences and Their Applications — SETA 2004*, Proc. Int. Conf. (Seoul, Korea, Oct. 24–28, 2005) (Springer, Heidelberg, 2005), pp. 1–29 (Lect. Notes Comput. Sci., Vol. 3486), DOI: 10.1007/11423461_1.
7. **S. Mesnager,** *Bent Functions: Fundamentals and Results* (Springer, Cham, 2018), DOI: 10.1007/978-3-319-32595-8.
8. **O. A. Logachev, A. A. Salnikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptography* (MTsNMO, Moscow, 2012) [Russian].
9. **O. A. Logachev, A. A. Salnikov,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptography* (AMS, Providence, RI, 2012).
10. **G. P. Agibalov,** *Selected Theorems of an Introductory Cryptography Course* (Izd. Dom TGU, Tomsk, 2005) [Russian].
11. **I. A. Pankratova,** *Boolean Functions in Cryptography* (Izd. Dom TGU, Tomsk, 2014) [Russian].
12. **N. N. Tokareva,** *Symmetric Cryptography: A Brief Course* (NGU, Novosibirsk, 2012) [Russian].
13. **T. W. Cusick** and **P. Stanica,** *Cryptographic Boolean Functions and Applications* (Acad. Press, Amsterdam, 2017), DOI: 10.1016/c2016-0-00852-5.
14. **C. Carlet,** *Boolean Functions for Cryptography and Coding Theory* (Camb. Univ. Press, Cambridge, 2020), DOI: 10.1017/9781108606806.
15. **R. L. McFarland,** A family of difference sets in non-cyclic groups, *J. Comb. Theory, Ser. A*, **15** (1), 1–10 (1973), DOI: 10.1016/0097-3165(73)90031-9.
16. **J. F. Dillon,** Elementary Hadamard difference sets, *PhD Thesis* (College Park, 1974).
17. **N. A. Kolomeec** and **A. V. Pavlov,** Properties of bent functions with minimal distance, *Prikl. Diskretn. Mat.*, No. 4, 5–20 (2009) [Russian].
18. **C. Carlet,** Two new classes of bent functions, in *Advances in Cryptology — EUROCRYPT'93*, Proc. Workshop on the Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 77–101 (Lect. Notes Comput. Sci., Vol. 765), DOI: 10.1007/3-540-48285-7_8.
19. **F. Zhang, E. Pasalic, N. Cepak,** and **Y. Wei,** Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class, in *Codes, Cryptology and Information Security*, Proc. 2nd Int. Conf. (Rabat, Morocco, Apr. 10–12, 2017) (Springer, Cham, 2017), pp. 298–313 (Lect. Notes Comput. Sci., Vol. 10194), DOI: 10.1007/978-3-319-55589-8_20.

20. **F. Zhang, N. Cepak, E. Pasalic,** and **Y. Wei,** Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$, *Discrete Appl. Math.* **285**, 458–472 (2020), DOI: 10.1016/j.dam.2020.06.012.

21. **S. Kudin** and **E. Pasalic,** A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, *Des. Codes Cryptogr.* **90** (8), 1783–1796 (2022), DOI: 10.1007/s10623-022-01079-3.

22. **S. Kudin, E. Pasalic, N. Cepak,** and **F. Zhang,** Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class, *Cryptogr. Commun.* **14** (1), 101–116 (2022), DOI: 10.1007/s12095-021-00523-w.

23. **A Bapić, E. Pasalic, F. Zhang, S. Hodžić** Constructing new superclasses of bent functions from known ones, *Cryptogr. Commun.* **14** (6), 1229–1256 (2022), DOI: 10.1007/s12095-022-00566-7.

24. **E. Pasalic** and **A. Bapić, F. Zhang, Y. Wei** Explicit infinite families of bent functions outside the completed Maiorana–McFarland class, *Des. Codes Cryptogr.* **91** (7), 2365–2393 (2023), DOI: 10.1007/s10623-023-01204-w.

25. **E. Pasalic, A. Polujan, S. Kudin,** and **F. Zhang,** Design and analysis of bent functions using $\mathcal{M}$-subspaces, *IEEE Trans. Inf. Theory* **70** (6), 4464–4477 (2024), DOI: 10.1109/TIT.2024.3352824.

26. **S. Kudin, E. Pasalic, A. Polujan,** and **F. Zhang,** The algebraic characterization of $\mathcal{M}$-subspaces of bent concatenations and its application, *IEEE Trans. Inf. Theory* **71** (5), 3999–4011 (2025), DOI: 10.1109/TIT.2025.3547533.

27. **A. A. Polujan** and **A. Pott,** Cubic bent functions outside the completed Maiorana–McFarland class, *Des. Codes Cryptogr.* **88** (9), 1701–1722 (2020), DOI: 10.1007/s10623-019-00712-y.

28. **N. A. Kolomeec,** Enumeration of the bent functions of least deviation from a quadratic bent function, *Diskretn. Anal. Issled. Oper.* **19** (1), 41–58 (2012) [Russian] [*J. Appl. Ind. Math.* **6** (3), 306–317 (2012), DOI: 10.1134/S1990478912030052].

29. **N. Kolomeec,** The graph of minimal distances of bent functions and its properties, *Des. Codes Cryptogr.* **85** (3), 395–410 (2017), DOI: 10.1007/s10623-016-0306-4.

30. **D. A. Bykov** and **N. A. Kolomeec,** On a lower bound for the number of bent functions at the minimum distance from a bent function in the Maiorana–McFarland class, *Diskretn. Anal. Issled. Oper.* **30** (3), 57–80 (2023) [Russian] [*J. Appl. Ind. Math.* **17** (3) 507–520 (2023)].

31. **K. Nyberg,** Differentily uniform mappings for cryptography, in *Advances in Cryptology — EUROCRYPT'93*, Proc. Workshop Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 55–64 (Lect. Notes Comput. Sci., Vol. 765), DOI: 10.1007/3-540-48285-7_6.

32. **C. Carlet,** Open questions on nonlinearity and on APN functions, in *Arithmetic of Finite Fields*, Rev. Sel. Pap. 5th Int. Workshop (Gebze, Turkey, Sept. 27–28, 2014) (Springer, Cham, 2015), pp. 83–107 (Lect. Notes Comput. Sci., Vol. 9061), DOI: 10.1007/978-3-319-16277-5_5.

33. N. Jacobson, *Basic Algebra*, V. I (Dover Publ., Mineola, NY, 2009).
34. N. A. Kolomeec and **D. A. Bykov,** On the image of an affine subspace under the inverse function within a finite field, *Des. Codes Cryptogr.* **92** (2), 467–476 (2024), DOI: 10.1007/s10623-023-01316-3.
35. N. A. Kolomeec and **D. A. Bykov,** On the Maiorana–McFarland class extensions (Ithaca, NY, 2025) (e-Print Archive / Cornell Univ., arXiv:2503.21440), DOI: 10.48550/arXiv.2503.21440.
36. W. E. Clark, X. Hou, and **A. Mihailovs,** The affinity of a permutation of a finite vector space, *Finite Fields Appl.* **13**, 80–112 (2007), DOI: 10.1016/j.ffa.2005.07.004.
37. S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and **P. Stănică,** Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application, *IEEE Trans. Inf. Theory* **66** (11), 7101–7112 (2020), DOI: 10.1109/TIT.2020.3002993.
38. N. A. Kolomeec, On permutations that break subspaces of specified dimensions, *Prikl. Diskretn. Mat.*, No. 65, 5–20 (2024) [Russian], DOI: 10.17223/20710410/65/1.
39. K. A. Browning, J. F. Dillon, M. T. McQuistan, and **A. J. Wolfe,** An APN permutation in dimension six, in *Finite Fields: Theory and Applications*, Proc. 9th Int. Conf. (Dublin, Ireland, July 13–17, 2009) (AMS, Providence, RI, 2010), pp. 33–42 (Contemp. Math., Vol. 518), DOI: 10.1090/conm/518/10194.
40. A. V. Cheryomushkin, Methods for affine and linear classification of Boolean functions, in *Transactions on Discrete Mathematics*, Vol. 4 (Fizmatlit, Moscow, 2001) [Russian], pp. 273–314.

Denis A. Bykov
Nikolay A. Kolomeec

Received August 27, 2024
Revised March 26, 2025
Accepted June 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 43–70

УДК 519.8 DOI: 10.33048/daio.2025.32.821

МАКСИМИЗАЦИЯ РАДИУСА ПОРОГОВОЙ УСТОЙЧИВОСТИ В МОДЕЛИ РАЗМЕЩЕНИЯ ПРОИЗВОДСТВА И ФАБРИЧНОГО ЦЕНООБРАЗОВАНИЯ

М. Е. Водян[a], *А. А. Панин*[b], *А. В. Плясунов*[c]

Институт математики им. С. Л. Соболева СО РАН,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия

E-mail: [a]m.vodyan@g.nsu.ru,
[b]aapanin1988@gmail.com, [c]apljas@math.nsc.ru

Аннотация. Исследуется пороговая устойчивость задачи с медианным размещением предприятий и фабричным ценообразованием. Задача пороговой устойчивости имеет следующие отличия от исходной двухуровневой постановки: в задаче верхнего уровня максимизируется отклонение бюджетов потребителей от ожидаемых значений при условии, что доход производителя не меньше заданного порога. Главное отличие исследуемой постановки от задач, чья пороговая устойчивость изучалась ранее, заключается в том, что при фиксированном размещении предприятий задача фабричного ценообразования NP-трудна в сильном смысле.

Для решения задачи пороговой устойчивости предлагается алгоритм на основе спуска с чередующимися окрестностями (VND). Численное исследование алгоритма проводится на известных примерах и случайно сгенерированных данных. Эксперимент показал, что идея итеративного вычитания радиуса пороговой устойчивости из бюджетов потребителей, впервые реализованная в данной работе, сильно снижает время работы алгоритма. На примерах, для которых был найден оптимум, алгоритм ошибся в среднем на 0,63%. На всех примерах алгоритм находит решение в среднем на 2,97% лучше, чем решатель Gurobi. Табл. 4, ил. 2, библиогр. 33.

Ключевые слова: двухуровневая задача, пороговая устойчивость, радиус пороговой устойчивости, размещение производства, фабричное ценообразование, спуск с чередующимися окрестностями.

Введение

В настоящей работе продолжаются исследования пороговой устойчивости двухуровневых задач размещения и ценообразования [1–4]. Неформально устойчивость — это свойство оптимизационной задачи, которое выражает в том или ином смысле меру её нечувствительности к неопределённости в исходных данных. Любой изученный тип устойчивости связан с определённым типом неопределённости в исходных данных. В зависимости от типа доступной информации такие проблемы исследуются в рамках следующих направлений: стохастического программирования, оптимизации на основе нечёткого представления данных, робастной оптимизации, постоптимального анализа чувствительности и устойчивости решений задач линейного и целочисленного программирования [5–10].

С каждым из классических подходов к анализу надёжности решений при различных возмущениях исходных данных связаны определённые проблемы. В основе моделей стохастического программирования лежит информация о вероятностном распределении случайных параметров, которая на практике зачастую недоступна. Ряд исследований демонстрирует очень высокую сложность многоэтапных задач стохастического программирования, которые оказываются PSPACE-трудными [5]. Разработка моделей на основе нечёткого представления данных существенно более сложное занятие, чем классическое математическое моделирование. Качество получаемых моделей существенно зависит от качества используемых экспертных оценок.

Узкое место робастной оптимизации заключается в том, что её применение ориентируется на учёт худших сценариев [7]. С вычислительной точки зрения это приводит к решению значительно более сложных оптимизационных задач, чем исходная постановка. Некоторые полиномиально разрешимые задачи становятся NP-трудными в робастной постановке [11–15].

Подход к исследованию неопределённости на основе постоптимального анализа чувствительности и устойчивости решений попросту игнорирует влияние неопределённости данных в своих моделях. Сам по себе анализ чувствительности — только лишь инструмент для анализа устойчивости решения, и он не может быть использован для поиска решений, устойчивых к вариации данных. Таким образом, помимо проблем с получением информации, которая требуется в том или ином подходе при анализе устойчивости задачи, возникают и существенные вычислительные трудности.

Относительно недавно в обсуждаемой области возникло новое направление исследований, названное пороговой устойчивостью. При исследовании устойчивости задачи Вебера авторы [16] предложили применить

пороговую модель вместо робастной оптимизации. В качестве неопределённых данных применён вектор спроса, а для того чтобы не допустить слишком большого роста транспортных затрат, введён порог, ограничивающий значение целевой функции сверху.

В задаче пороговой устойчивости для заданного набора входных данных задачи Вебера вместо минимизации транспортных расходов ищется размещение предприятий с максимальным радиусом устойчивости и транспортными затратами, не превосходящими заданного бюджетного порога. В [17] эта идея реализована для задачи о p-медиане и для простейшей задачи размещения предприятий.

Далее в работе используется близкое по смыслу определение радиуса пороговой устойчивости, в котором с каждым размещением предприятий связывается величина, равная максимальному отклонению спроса от ожидаемых значений при условии, что выполняется пороговое ограничение. Такое определение восходит к впервые введённому в [18] понятию радиуса устойчивости, на основе которого в [1] предложен радиус пороговой устойчивости для двухуровневых задач. Небольшой, но информативный обзор работ, связанных с понятием радиуса устойчивости, и развитых на его основе подходов к исследованию устойчивости оптимизационных задач можно найти в [1, 2, 19–25].

Идея конструкции такова, что с каждой оптимизационной задачей можно связать задачу пороговой устойчивости, в которой ищется максимальное значение параметра (радиус устойчивости), ограничивающего нормы вариаций исходных данных исследуемой задачи, и подходящее допустимое решение базовой постановки, удовлетворяющее пороговому ограничению. В [1] этот подход обобщён и применён к исследованию пороговой устойчивости многоуровневых задач размещения и ценообразования.

Первые результаты в области пороговой устойчивости двухуровневых задач получены в работах [1–4]. Задачи такого типа образуют новый класс двухуровневых задач, для которых не известны ни точные, ни приближённые методы решения. Исследование новых классов двухуровневых задач несомненно является важной теоретической проблемой, поскольку при этом разрабатываются новые точные и приближённые методы для их решения. Современное состояние дел в области двухуровневой оптимизации можно найти в обзорах [26, 27].

В [1] впервые исследована пороговая устойчивость задачи ценообразования с различными ценовыми политиками и задачи конкурентного ценообразования. Обзор по проблемам размещения производства и ценообразования и пороговой устойчивости можно найти в [2]. В [3, 4] изучаются задачи с медианным ограничением на открытие предприятий и двумя стратегиями ценообразования: равномерной и дискриминационной.

В текущей работе впервые исследуется пороговая устойчивость NP-трудной в сильном смысле задачи медианного размещения производства и фабричного ценообразования [30, 31]. Производитель определяет, в каких местах он должен открыть заданное количество предприятий, и решает, какие цены на однородную продукцию нужно установить на каждом из них (фабричное ценообразование), чтобы максимизировать прибыль от обслуживания потребителей. Каждый потребитель имеет ограниченный бюджет, который он готов потратить на покупку и транспортировку продукта в единичном экземпляре. Потребители действуют рационально, т. е. минимизируют свои затраты. Будем полагать, что транспортные затраты известны и неизменны, а информация о бюджетах неточная, но предполагается, что известны ожидаемые значения. В таком случае множество сценариев (неопределённость) задаётся как множество отклонений бюджетов от прогнозируемых значений.

В разд. 1 приводятся постановка и математическая модель исследуемой проблемы. В разд. 2 содержатся результаты о вычислительной сложности задачи пороговой устойчивости. Приближённые алгоритмы для её решения предлагаются в разд. 3, а в разд. 4 описывается численный эксперимент для сравнения разработанных алгоритмов с решателем Gurobi. В заключении обсуждаются полученные результаты и направления дальнейших исследований.

1. Постановка задачи пороговой устойчивости

Прежде чем сформулировать постановку задачи пороговой устойчивости, заметим, что робастная оптимизация и пороговая устойчивость исследуют один тип неопределённости. Однако, в робастной оптимизации предполагается, что вектор данных задачи не известен, но принадлежит некоторому множеству, которое описывает неопределённость и называется множеством сценариев. Оптимальное решение в такой задаче строится с учётом всех сценариев и фактически сводится к решению минимаксной задачи, ограничения которой удовлетворяют всем сценариям [7]. В задаче пороговой устойчивости предполагается, что вектор данных известен и необходимо найти такое множество возмущений, для которого найдётся допустимое решение, удовлетворяющее пороговому ограничению. Искомая область возмущений определяется радиусом пороговой устойчивости.

В [1] содержится формальное определение радиуса пороговой устойчивости и постановка задачи пороговой устойчивости для оптимизационных задач. Основная идея этого подхода заключается в следующем. *Пороговое значение* в таких задачах — это величина дохода, которую рациональный лидер считает достаточной. Далее, *радиус устойчивости*

допустимого решения задачи — это такое число, для которого любое одновременное возмущение бюджетов клиентов на величину, не превышающую этого числа, не нарушает допустимости этого решения, а значение целевой функции на этом решении не превышает значения выбранного порога.

Пусть V — некоторый порог. В задаче пороговой устойчивости необходимо найти допустимое решение, которое удовлетворяет пороговому ограничению и имеет максимальный радиус устойчивости.

Там же приводится модификация этого подхода для двухуровневых задач и реализация для задач ценообразования. Разделим переменные двухуровневой задачи на две группы (x, y), где x — переменные верхнего уровня, y — переменные нижнего уровня. В определении радиуса устойчивости заменяем требование допустимости решения при возмущении бюджетов условием существования y такого, что (x, y) является допустимым решением двухуровневой задачи.

При анализе пороговой устойчивости двухуровневой задачи необходимо найти вектор значений переменных верхнего уровня x с наибольшим радиусом возможного варьирования входных данных, при котором целевая функция продолжает удовлетворять пороговому ограничению.

В рассматриваемой постановке варьируются не все входные данные, а только бюджеты потребителей, возмущение которых происходит в сторону их уменьшения. При увеличении бюджетов задача пороговой устойчивости становится тривиальной, а радиус пороговой устойчивости стремится к бесконечности. Таким образом, в задаче ниже фиксируем доход производителя и ищем решение, которое предоставляет доход не менее зафиксированного.

Приведём содержательную постановку базовой задачи размещения производства и ценообразования, пороговая устойчивость которой исследуется ниже. Сформулируем её в виде игры Штакельберга «лидер — последователи». В качестве лидера выступает производитель, который размещает r предприятий и формирует цены на каждом из них. В качестве последователей — потребители, выбирающие предприятия так, чтобы минимизировать суммарные затраты на покупку и транспортировку товаров. При этом потребитель совершает покупку только в том случае, если эти затраты не превышают его бюджета. Требуется выбрать такое размещение предприятий и такие цены, при которых доход производителя максимален.

Далее рассматривается оптимистическая постановка двухуровневой задачи, для чего необходимо ввести следующее соглашение. Если у потребителя есть несколько предприятий с одинаковой минимальной суммой платежей, то он выберет предприятие с минимальными транспортными затратами.

Обычно в подобных постановках рассматриваются три следующие стратегии ценообразования [32]:

• равномерное (uniform pricing) — на всех предприятиях устанавливается одна цена;

• фабричное (mill pricing) — на каждом предприятии устанавливается своя цена;

• дискриминационное (discriminatory pricing) — на каждом предприятии для каждого потребителя устанавливается своя цена.

В настоящей статье рассматривается фабричное ценообразование.

Отличие задачи пороговой устойчивости от базовой постановки — в заранее заданном доходе производителя, который определяет пороговое ограничение, и в наличии неопределённости в бюджетах потребителей, для которой необходимо предусмотреть максимально возможное отклонение от ожидаемых (определённых заранее) бюджетов.

Для того чтобы сформулировать математическую модель задачи пороговой устойчивости, введём следующие обозначения и переменные.

Обозначения:

• $I = \{1, \ldots, n\}$ — множество возможных мест для открытия предприятий;

• $J = \{1, \ldots, m\}$ — множество потребителей;

• $r \in Z$ — число размещаемых предприятий;

• $b_j \in \mathbb{Z}$ — бюджет потребителя j;

• $c_{ij} \in \mathbb{Z}$ — транспортные затраты потребителя j при обслуживании на предприятии i;

• $V \in \mathbb{Z}$ — доход производителя.

Переменные:

• $\rho \in \mathbb{Q}_+$ — радиус пороговой устойчивости;

• $p_i \in \mathbb{Q}_+$ — цена товара на предприятии i;

• $x_{ij} = \begin{cases} 1, & \text{если потребитель } j \text{ обслуживается на предприятии } i, \\ 0 & \text{иначе.} \end{cases}$

• $y_i = \begin{cases} 1, & \text{если предприятие } i \text{ открыто,} \\ 0 & \text{иначе.} \end{cases}$

Двухуровневая смешанно целочисленная квадратичная математическая модель задачи пороговой устойчивости имеет следующий вид:

$$\rho \to \max_{p,y,x,\rho}, \tag{1}$$

$$\sum_{i \in I} \sum_{j \in J} p_i x_{ij} \geqslant V, \tag{2}$$

$$\sum_{i \in I} y_i = r, \tag{3}$$

$$y_i \in \{0,1\},\ p_i, \rho \in \mathbb{Q}_+,\ x \in \mathcal{F}^*(p,y,\rho), \quad i \in I,\ j \in J, \tag{4}$$

где $\mathcal{F}^*(p,y,\rho)$ — множество оптимальных решений задачи нижнего уровня:

$$\sum_{i\in I}\sum_{j\in J}(b_j - c_{ij} - \rho - p_i)x_{ij} \to \max_x, \tag{5}$$

$$\sum_{i\in I} x_{ij} \leqslant 1, \quad j \in J, \tag{6}$$

$$x_{ij} \leqslant y_i, \quad i \in I,\ j \in J, \tag{7}$$

$$x_{ij} \in \{0,1\}, \quad i \in I,\ j \in J. \tag{8}$$

Максимизируя целевую функцию (1) на верхнем уровне, получим максимально возможное отклонение от ожидаемых (данных) размеров бюджетов. Неравенство (2) устанавливает пороговое ограничение, гарантирующее, что доход производителя не меньше заданного, а равенство (3) требует, чтобы было открыто ровно r предприятий. Условия (4) определяют область значений переменных верхнего уровня и фиксируют фундаментальное свойство двухуровневых задач: переменные нижнего уровня x принимают свои значения из множества оптимальных решений задачи нижнего уровня. Таким образом, в работе исследуется оптимистический вариант постановки. Целевая функция нижнего уровня (5) представляет собой сумму неизрасходованных потребителями средств, а ограничения (6)–(8) гарантируют, что каждый потребитель обслуживается не более чем одним предприятием производителя, которое должно быть открыто.

2. Вычислительная сложность задачи пороговой устойчивости

Используемые далее понятия и обозначения классов сложности, связанные с полиномиальной и аппроксимационной иерархиями, можно найти в [2, 4, 33]. Будем предполагать, что переменные ρ и p целочисленные. Обозначим через D_ρ и D стандартные задачи распознавания для задачи (1)–(8) и базовой задачи соответственно. Приведём доказательство следующей теоремы в варианте, который демонстрирует тесную связь между этими задачами распознавания.

Теорема 1. *Задача D_ρ* NP*-полна в сильном смысле.*

Доказательство. Будем следовать идее, использованной при обосновании аналогичного результата в [4], при этом необходимо учесть особенности новой постановки. Покажем, что задача D_ρ полиномиально сводится к некоторому модифицированному варианту задачи D. Для этого рассмотрим произвольный пример с ответом «да» задачи D_ρ с некоторой целой константой $\widehat{\rho}$.

Из определения задачи D_ρ следует, что существует такое допустимое решение (ρ, y, p, x), что $\rho \geqslant \widehat{\rho}$. Можно считать, что $\rho = \widehat{\rho}$. Действительно, если $\rho > \widehat{\rho}$, то при уменьшении ρ до $\widehat{\rho}$ при фиксированных (y, p) будет изменяться только оптимальное решение x задачи нижнего уровня, так как могут появиться клиенты, бюджеты которых увеличатся, и они будут обслужены на открытых предприятиях. Доход лидера при этом только возрастёт, т. е. пороговое ограничение не будет нарушено.

Тем самым существование для некоторого целого $\widehat{\rho}$ такого допустимого решения (ρ, y, p, x), что $\rho \geqslant \widehat{\rho}$, эквивалентно существованию такого размещения предприятий y и такого набора цен, при которых в базовой задаче с бюджетами $b_j - \widehat{\rho}$, $j \in J$, множеством открытых предприятий $\{i \mid y_i = 1\}$ и множеством цен p доход лидера больше заданного порога V.

Таким образом, для заданного целого $\widehat{\rho}$ требуемые в базовой задаче размещение y и набор фабричных цен p могут быть найдены за недетерминированное полиномиальное время, если в задаче D_ρ ответ «да». Отсюда следует, что задача D_ρ принадлежит классу NP.

Полнота задачи D_ρ в классе NP следует из полиномиальной сводимости задачи D к задаче D_ρ. Действительно, в D для заданного порога V надо найти допустимое решение (y, p, x), которое приносит лидеру доход не меньше порога. В качестве исходных данных задачи D_ρ возьмём $\widehat{\rho} = 0$ и исходные данные задачи D. Из результатов, полученных в [2], следует, что задача D NP-полна в сильном смысле. Теорема 1 доказана.

Теорема 2. *Для задачи* (1)–(8) *не существует детерминированных полиномиальных приближённых алгоритмов с абсолютной или относительной оценкой уклонения от оптимального решения, если* $\mathrm{P} \neq \mathrm{NP}$.

Доказательство. Предположим, что существует детерминированный полиномиальный приближённый алгоритм для задачи (1)–(8). Покажем, что тогда задача D полиномиально разрешима. Рассмотрим произвольный вход данной задачи с порогом V. Применим приближённый алгоритм к входу задачи (1)–(8), который получается из входа задачи D так же, как в доказательстве теоремы 1. Если в задаче D для порога V ответ «да», то алгоритм выдаст некоторое приближённое допустимое решение (ρ, y, p, x) задачи (1)–(8). Если $\rho > 0$, то, рассуждая как в доказательстве теоремы 1, получим её допустимое решение $(0, y, p, \widehat{x})$, которое подтверждает, что в задаче D для текущего входа ответ «да». Таким образом получаем полиномиальный алгоритм для задачи D, что противоречит условию $\mathrm{P} \neq \mathrm{NP}$. Теорема 2 доказана.

Сформулируем ещё одно утверждение, которое следует из доказанных теорем и позволяет уточнить возможности полиномиальных алгоритмов относительно исследуемой задачи.

Следствие 1. *Для задачи* (1)–(8) *можно разработать точный полиномиальный алгоритм только в классе детерминированных алгоритмов с оракулами из класса* NP, *если* $\mathrm{P} \neq \mathrm{NP}$.

Доказательство. Из теорем 1 и 2 следует, что задача (1)–(8) принадлежит классу NPO, причём лежит выше класса Exp-APX. В силу предположения классы NPO и PO не совпадают, следовательно, для задачи (1)–(8) не существует полиномиального детерминированного алгоритма. Из включения $\mathrm{NPO} \subseteq \Delta_2^{\mathrm{P}}\mathrm{O}$, где $\Delta_2^{\mathrm{P}}\mathrm{O}$ — класс оптимизационных задач, разрешимых детерминированными полиномиальными алгоритмами с оракулами из класса NP, следует требуемый результат. Следствие 1 доказано.

Полученные результаты о неаппроксимируемости утверждают, что невозможно разработать детерминированные полиномиальные точные и приближённые алгоритмы с оценками относительного уклонения. Это означает, что исследуемая задача пороговой устойчивости либо NPO-полна относительно подходящей сводимости, сохраняющей аппроксимируемость, либо лежит в промежуточном классе задач выше класса Exp-APX.

3. Алгоритмы

При разработке алгоритмов для решения задачи (1)–(8) использована VND-эвристика, идея которой содержится в [28]. Позднее эта эвристика применена в [29–31] для разработки эффективных алгоритмов решения задачи размещения и фабричного ценообразования. В настоящей работе для решения задачи пороговой устойчивости разработана модификация этой эвристики — двухэтапная VND-эвристика. Для определения и выбора лучшего размещения необходимы критерии их сравнения.

Введём некоторые вспомогательные величины и опишем алгоритм определения радиуса пороговой устойчивости на основе поиска цены. Если для поиска цены применить точный алгоритм, то алгоритм определения радиуса пороговой устойчивости будет точным. Для поиска цены при фиксированном размещении используем VND-эвристику, основываясь на идеях [30, 31].

Пусть $d(y,p) = V - \sum\limits_{i\in I}\sum\limits_{j\in J} x_{ij}p_i$ — сверхприбыль производителя относительно порога V при фиксированном размещении; $c(y,p) = \sum\limits_{i\in I}\sum\limits_{j\in J} x_{ij}$ — число обслуживаемых клиентов при фиксированном размещении; $B = (b_1,\ldots,b_m)$ — вектор бюджетов потребителей; $\mathrm{PC}(y,B)$ — алгоритм поиска цены при фиксированном размещении [30, 31]. Для поиска радиуса пороговой устойчивости использовался следующий алгоритм $\mathrm{RC}(y,B)$.

Алгоритм 1. Алгорим $\mathrm{RC}(y, B)$

Вход: y, B.
Выход: ρ — радиус пороговой устойчивости.

1: $\rho \leftarrow 0$; $p \leftarrow \mathrm{PC}(y, B)$;
2: **if** $d(y, p) < 0$ **then stop**;
3: **else** $\Delta\rho \leftarrow d(y, p)/c(y, p)$; $\rho \leftarrow \rho + \Delta\rho$;
4: **if** $\Delta\rho < \min\limits_{i \in I} p_i$ **then stop**;
5: **else** $B \leftarrow B - (\Delta\rho, \ldots, \Delta\rho)$; $p \leftarrow \mathrm{PC}(y, B)$;
6: **goto** 2;

Предлагаемая ниже реализация алгоритма для поиска цены основана на VND-эвристике, поэтому в функции PC и RC добавим аргумент flip, ограничивающий число просматриваемых окрестностей. Этот аргумент используется для остановки алгоритма, а именно для процедуры улучшения, описанной в [4].

Если алгоритм остановился после шага 1, то считаем размещение y недопустимым. На шаге 2 выполняется проверка возможности увеличить радиус пороговой устойчивости, и если сверхприбыль положительная, то увеличиваем радиус. На шаге 4 происходит проверка необходимости поиска цены, и если есть необходимость, то на шаге 5 ищем цены относительно новых бюджетов. Тем самым на каждой итерации алгоритма имеем бюджеты потребителей, содержащие радиус пороговой устойчивости, размещение и цены для него такие, что доход производителя больше порога V, т. е. получаем допустимое решение задачи пороговой устойчивости.

Пусть y_1 и y_2 — различные размещения, для сравнения которых выпишем два критерия. Первый критерий выбирает размещение, при котором доход производителя больше, а второй — то, для которого больше радиус пороговой устойчивости.

Критерий 1. Полагаем $p_1 = \mathrm{PC}(y_1, B, \mathrm{flip})$, $p_2 = \mathrm{PC}(y_2, B, \mathrm{flip})$, и если $\sum\limits_{i \in I} \sum\limits_{j \in J} p_{1i} x_{ij} > \sum\limits_{i \in I} \sum\limits_{j \in J} p_{2i} x_{ij}$, то считаем размещение y_1 лучше y_2.

Критерий 2. Полагаем $\rho_1 = \mathrm{RC}(y_1, B, \mathrm{flip})$, $\rho_2 = \mathrm{RC}(y_2, B, \mathrm{flip})$, и если $\rho_1 > \rho_2$, то считаем размещение y_1 лучше чем y_2.

С целью построения основного алгоритма для размещения y определим окрестность $\overline{k}$-$\mathrm{Swap}(y)$ и процедуру улучшения k-$\mathrm{Improve}(y)$, как это сделано в [3]. Здесь $k, \overline{k} \in \mathbb{N}$ — некоторые параметры. Для сравнения размещений в окрестности используем критерии 1 и 2. Основной алгоритм

Алгоритм 2. Алгорим VND_1

Вход: $I_{\max}$, B, k, flip.
Выход: размещение y и радиус пороговой устойчивости ρ.

1: $I \leftarrow 0$; $y \leftarrow \mathrm{rand}\{y' \in \{0,1\}^n \mid \sum\limits_i y'_i = r\}$ — случайный булев вектор; $\rho \leftarrow \mathrm{RC}(y, B, \mathrm{flip})$; $B \leftarrow B - (\rho, \ldots, \rho)$;
2: применить локальный поиск для 1-Swap(y) и найти локальный оптимум y^*;
3: $\rho^* \leftarrow \mathrm{RC}(y^*, B, \mathrm{flip})$; $B \leftarrow B - (\rho^*, \ldots, \rho^*)$; $\rho \leftarrow \rho + \rho^*$;
4: $I \leftarrow I + 1$; $(\widehat{y}, \widehat{\rho}) \leftarrow k$-Improve($y^*$);
5: **if** $\widehat{y} = y^*$ **or** $I > I_{\max}$ **then stop**;
6: **else** $\widehat{\rho} \leftarrow \mathrm{RC}(\widehat{y}, B, \mathrm{flip})$; $B \leftarrow B - (\widehat{\rho}, \ldots, \widehat{\rho})$; $\rho \leftarrow \rho + \widehat{\rho}$; $y \leftarrow \widehat{y}$;
7: **goto** 2;

представим в виде вложенной VND-эвристики с двумя этапами. На первом этапе выбираем размещение, фиксируем его и строим относительно него окрестность. На втором этапе просматриваем элементы окрестности и для каждого размещения считаем доход производителя или радиус пороговой устойчивости — в зависимости от применяемого критерия.

В алгоритме VND_1 для выбора наилучшего размещения используем критерий 1. Для каждого размещения y из окрестности 1-Swap(y) при помощи алгоритма PC с параметром $\mathrm{flip} = 1$ находим доход производителя и выбираем то размещение, на котором доход производителя наибольший. Далее вычисляем радиус пороговой устойчивости при помощи

Алгоритм 3. Алгорим VND_2

Вход: $I_{\max}$, B, k, flip.
Выход: размещение y и радиус пороговой устойчивости ρ.

1: $I \leftarrow 0$; $y \leftarrow \mathrm{rand}\{y' \in \{0,1\}^n \mid \sum\limits_i y'_i = r\}$ — случайный булев вектор; $\rho \leftarrow \mathrm{RC}(y, B, \mathrm{flip})$; $B \leftarrow B - (\rho, \ldots, \rho)$;
2: применить локальный поиск для 1-Swap(y) и найти локальный оптимум y^* с радиусом пороговой устойчивости $\rho^* = \mathrm{RC}(y^*, B, 1)$;
3: $B \leftarrow B - (\rho^*, \ldots, \rho^*)$; $\rho \leftarrow \rho + \rho^*$;
4: **if** $\mathrm{flip} > 1$ **then**
5: $\quad \rho^{**} \leftarrow \mathrm{RC}(y^*, B, \mathrm{flip})$; $B \leftarrow B - (\rho^{**}, \ldots, \rho^{**})$; $\rho \leftarrow \rho + \rho^{**}$;
6: $I \leftarrow I + 1$; $(\widehat{y}, \widehat{\rho}) \leftarrow k$-Improve($y^*$);
7: **if** $\widehat{y} = y^*$ **or** $I > I_{\max}$ **then stop**;
8: **else** $B \leftarrow B - (\widehat{\rho}, \ldots, \widehat{\rho})$; $\rho \leftarrow \rho + \widehat{\rho}$; $y \leftarrow \widehat{y}$;
9: **goto** 2;

алгоритма RC. Отметим, что алгоритме VND_1 просмотр окрестности занимает меньшее время, чем в VND_2, так как здесь цены для размещения вычисляются один раз.

В алгоритме VND_2 на шаге 2 применяется локальный поиск в окрестности 1-Swap(y). Для каждого размещения из окрестности вычисляем радиус пороговой устойчивости при помощи алгоритма RC с параметром flip $= 1$ и при помощи критерия 2 выбираем локальный оптимум. Если использовать параметр flip, переданный на вход, то поиск локального оптимума сильно замедлится. Для выбранного на шаге 2 локального оптимума пытаемся улучшить результат на шаге 4, используя алгоритм RC и параметр flip, полученный на входе алгоритма.

Таблица 1

Результаты численного эксперимента $n = 100$, $m = 40$, $r = 5$

Пример		Gurobi		VND_1		VND_2		VND'_2	
№	%	gap	Время	gap	Время	gap	Время	gap	Время
FLPr01	10	0	$1{,}1_{+2}$	$6{,}5_{-3}$	$1{,}5_{+0}$	0	$7{,}3_{-1}$	$5{,}6_{-3}$	$1{,}1_{+2}$
	30	0	$4{,}2_{+3}$	0	$1{,}8_{+1}$	0	$8{,}0_{+0}$	$3{,}6_{-2}$	$1{,}3_{+2}$
	50	$9{,}5_{-3}$	$4{,}3_{+4}$	$4{,}7_{-3}$	$2{,}7_{+1}$	$1{,}4_{-2}$	$8{,}3_{+0}$	$1{,}4_{-2}$	$1{,}5_{+2}$
	70	$1{,}3_{-2}$	$4{,}3_{+4}$	$3{,}5_{-3}$	$2{,}0_{+1}$	$4{,}6_{-2}$	$2{,}2_{+1}$	$3{,}2_{-4}$	$1{,}5_{+2}$
	90	$7{,}1_{-2}$	$4{,}3_{+4}$	$-3{,}2_{-2}$	$5{,}6_{+1}$	$-6{,}7_{-2}$	$2{,}8_{+1}$	$-6{,}7_{-2}$	$2{,}1_{+2}$
FLPr02	10	0	$1{,}1_{+2}$	$1{,}3_{-9}$	$4{,}8_{+0}$	$1{,}3_{-9}$	$1{,}4_{+0}$	$1{,}2_{-2}$	$2{,}6_{+2}$
	30	0	$4{,}8_{+3}$	$1{,}6_{-2}$	$1{,}3_{+1}$	0	$3{,}9_{+0}$	$7{,}1_{-2}$	$1{,}6_{+2}$
	50	$5{,}0_{-3}$	$4{,}3_{+4}$	$4{,}7_{-3}$	$2{,}3_{+1}$	$-1{,}8_{-4}$	$8{,}9_{+0}$	$3{,}4_{-2}$	$1{,}6_{+2}$
	70	$1{,}1_{-2}$	$4{,}3_{+4}$	$9{,}1_{-2}$	$1{,}0_{+2}$	$7{,}0_{-2}$	$1{,}8_{+1}$	$2{,}1_{-4}$	$1{,}4_{+2}$
	90	$6{,}4_{-2}$	$4{,}3_{+4}$	$2{,}9_{-1}$	$1{,}4_{+2}$	$2{,}8_{-2}$	$2{,}7_{+1}$	$2{,}8_{-2}$	$1{,}8_{+2}$
FLPr03	10	0	$8{,}3_{+1}$	0	$1{,}1_{+0}$	0	$6{,}4_{-1}$	$7{,}5_{-3}$	$1{,}3_{+2}$
	30	0	$2{,}9_{+3}$	$6{,}9_{-4}$	$9{,}7_{+0}$	$2{,}3_{-3}$	$4{,}3_{+0}$	$5{,}3_{-2}$	$8{,}0_{+1}$
	50	$4{,}2_{-3}$	$4{,}3_{+4}$	$-5{,}4_{-5}$	$3{,}2_{+1}$	$1{,}7_{-2}$	$6{,}8_{+0}$	$9{,}8_{-3}$	$1{,}5_{+2}$
	70	$1{,}8_{-2}$	$4{,}3_{+4}$	$1{,}9_{-4}$	$5{,}2_{+1}$	$1{,}9_{-4}$	$1{,}2_{+1}$	$1{,}9_{-4}$	$9{,}4_{+1}$
	90	$6{,}8_{-2}$	$4{,}3_{+4}$	$2{,}8_{-1}$	$6{,}8_{+1}$	$7{,}7_{-4}$	$1{,}7_{+1}$	$7{,}7_{-4}$	$1{,}0_{+2}$
FLPr04	10	0	$5{,}6_{+1}$	$3{,}6_{-3}$	$2{,}3_{+0}$	$3{,}6_{-3}$	$3{,}8_{-1}$	$6{,}0_{-3}$	$5{,}4_{+1}$
	30	0	$2{,}3_{+2}$	$2{,}9_{-4}$	$4{,}3_{+0}$	$6{,}9_{-3}$	$1{,}7_{+0}$	$7{,}9_{-3}$	$1{,}1_{+2}$
	50	0	$1{,}6_{+3}$	0	$2{,}3_{+1}$	0	$4{,}0_{+0}$	$3{,}0_{-2}$	$7{,}3_{+1}$
	70	0	$8{,}0_{+3}$	0	$3{,}9_{+1}$	$7{,}4_{-2}$	$7{,}0_{+0}$	$2{,}2_{-2}$	$8{,}8_{+1}$
	90	$3{,}7_{-2}$	$4{,}3_{+4}$	$2{,}7_{-1}$	$6{,}8_{+1}$	$5{,}9_{-3}$	$1{,}6_{+1}$	$9{,}1_{-2}$	$1{,}4_{+2}$
FLPr05	10	0	$1{,}1_{+2}$	$7{,}6_{-3}$	$9{,}7_{-1}$	$4{,}0_{-3}$	$9{,}3_{-1}$	$1{,}2_{-2}$	$2{,}3_{+2}$
	30	0	$2{,}4_{+3}$	$8{,}5_{-3}$	$2{,}1_{+1}$	$1{,}0_{-2}$	$3{,}3_{+0}$	$4{,}2_{-2}$	$2{,}1_{+2}$
	50	0	$1{,}3_{+4}$	$7{,}4_{-3}$	$9{,}3_{+1}$	$1{,}5_{-2}$	$9{,}2_{+0}$	0	$4{,}4_{+2}$
	70	$7{,}9_{-3}$	$4{,}3_{+4}$	$7{,}1_{-5}$	$1{,}4_{+2}$	$1{,}5_{-2}$	$3{,}0_{+1}$	$1{,}2_{-1}$	$2{,}5_{+2}$
	90	$5{,}4_{-2}$	$4{,}3_{+4}$	$-1{,}2_{-1}$	$1{,}2_{+2}$	$-2{,}0_{-1}$	$4{,}7_{+1}$	$-9{,}1_{-2}$	$3{,}1_{+2}$

Таблица 1 (окончание)

Пример		Gurobi		VND_1		VND_2		VND_2'	
№	%	gap	Время	gap	Время	gap	Время	gap	Время
FLPr06	10	0	$6{,}3_{+1}$	0	$1{,}7_{+0}$	0	$7{,}3_{-1}$	$2{,}3_{-2}$	$9{,}6_{+1}$
	30	0	$3{,}1_{+3}$	$9{,}0_{-3}$	$1{,}7_{+1}$	0	$3{,}1_{+0}$	$4{,}8_{-2}$	$8{,}1_{+1}$
	50	0	$1{,}0_{+4}$	$9{,}1_{-3}$	$1{,}6_{+1}$	$1{,}1_{-2}$	$6{,}3_{+0}$	$6{,}2_{-2}$	$1{,}1_{+2}$
	70	$9{,}7_{-3}$	$4{,}3_{+4}$	$1{,}2_{-1}$	$6{,}6_{+1}$	$1{,}3_{-4}$	$2{,}7_{+1}$	$9{,}7_{-2}$	$8{,}2_{+1}$
	90	$5{,}2_{-2}$	$4{,}3_{+4}$	$2{,}6_{-1}$	$7{,}9_{+1}$	$6{,}1_{-2}$	$4{,}5_{+1}$	$-1{,}4_{-2}$	$1{,}6_{+2}$
FLPr07	10	0	$8{,}9_{+1}$	$1{,}0_{-4}$	$1{,}6_{+0}$	$6{,}5_{-9}$	$7{,}2_{-1}$	$4{,}3_{-3}$	$2{,}5_{+2}$
	30	0	$2{,}7_{+3}$	$8{,}7_{-3}$	$1{,}5_{+1}$	$6{,}6_{-3}$	$8{,}5_{+0}$	$5{,}1_{-2}$	$2{,}6_{+2}$
	50	0	$1{,}5_{+4}$	$1{,}3_{-2}$	$1{,}7_{+1}$	0	$8{,}4_{+0}$	$4{,}9_{-2}$	$1{,}2_{+2}$
	70	$7{,}4_{-3}$	$4{,}3_{+4}$	$-9{,}0_{-3}$	$5{,}3_{+1}$	$-1{,}7_{-2}$	$2{,}5_{+1}$	$-1{,}3_{-2}$	$2{,}7_{+2}$
	90	$3{,}6_{-2}$	$4{,}3_{+4}$	$1{,}4_{-1}$	$6{,}8_{+1}$	$9{,}3_{-3}$	$2{,}6_{+1}$	$9{,}3_{-3}$	$1{,}4_{+2}$
FLPr08	10	0	$5{,}6_{+1}$	0	$1{,}6_{+0}$	0	$6{,}1_{-1}$	$4{,}9_{-3}$	$2{,}7_{+2}$
	30	0	$3{,}9_{+3}$	0	$1{,}2_{+1}$	0	$7{,}4_{+0}$	$2{,}9_{-1}$	$1{,}3_{+2}$
	50	$2{,}1_{-3}$	$4{,}3_{+4}$	$1{,}6_{-4}$	$5{,}4_{+1}$	$9{,}2_{-3}$	$9{,}1_{+0}$	$3{,}5_{-2}$	$2{,}1_{+2}$
	70	$8{,}6_{-3}$	$4{,}3_{+4}$	$3{,}3_{-3}$	$7{,}1_{+1}$	$3{,}3_{-3}$	$2{,}8_{+1}$	$3{,}2_{-2}$	$2{,}0_{+2}$
	90	$7{,}2_{-2}$	$4{,}3_{+4}$	$1{,}5_{-1}$	$1{,}6_{+2}$	$-8{,}6_{-2}$	$3{,}1_{+1}$	$-7{,}6_{-2}$	$1{,}3_{+2}$
FLPr09	10	0	$7{,}3_{+1}$	1.4e-14	$1{,}0_{+0}$	1.4e-14	$6{,}0_{-1}$	$3{,}1_{-1}$	$1{,}9_{+0}$
	30	0	$1{,}9_{+3}$	$8{,}8_{-3}$	$1{,}5_{+1}$	$2{,}6_{-3}$	$2{,}6_{+0}$	$4{,}6_{-2}$	$1{,}2_{+2}$
	50	0	$6{,}3_{+3}$	0	$3{,}1_{+1}$	$6{,}9_{-3}$	$6{,}0_{+0}$	$1{,}0_{-3}$	$1{,}1_{+2}$
	70	$2{,}7_{-3}$	$4{,}3_{+4}$	$2{,}4_{-2}$	$3{,}9_{+1}$	$2{,}1_{-4}$	$1{,}0_{+1}$	$2{,}1_{-4}$	$2{,}1_{+2}$
	90	$3{,}2_{-2}$	$4{,}3_{+4}$	$1{,}9_{-1}$	$6{,}5_{+1}$	$5{,}1_{-4}$	$1{,}7_{+1}$	$2{,}1_{-2}$	$9{,}6_{+1}$
FLPr10	10	0	$5{,}5_{+1}$	$8{,}9_{-9}$	$3{,}2_{+0}$	$1{,}0_{-3}$	$1{,}3_{+0}$	$5{,}6_{-3}$	$2{,}3_{+2}$
	30	0	$3{,}2_{+3}$	$2{,}2_{-3}$	$1{,}4_{+1}$	$4{,}8_{-3}$	$3{,}9_{+0}$	$4{,}7_{-3}$	$1{,}5_{+2}$
	50	$8{,}0_{-4}$	$4{,}3_{+4}$	$5{,}2_{-3}$	$6{,}6_{+1}$	$1{,}8_{-4}$	$8{,}7_{+0}$	$1{,}7_{-3}$	$9{,}5_{+1}$
	70	$5{,}7_{-3}$	$4{,}3_{+4}$	$2{,}8_{-4}$	$5{,}2_{+1}$	$2{,}8_{-4}$	$1{,}6_{+1}$	$2{,}8_{-4}$	$9{,}8_{+1}$
	90	$6{,}0_{-2}$	$4{,}3_{+4}$	$2{,}1_{-1}$	$7{,}8_{+1}$	$-9{,}1_{-4}$	$2{,}5_{+1}$	$-9{,}1_{-4}$	$1{,}1_{+2}$

В обоих алгоритмах найденный радиус пороговой устойчивости сразу вычитается из бюджетов потребителей. При вызове алгоритма RC внутри VND вектор бюджетов меняется локально внутри RC. Вычитание радиуса из бюджетов не влияет на результат алгоритма VND (пройденный им путь), но сильно снижает время работы. В численном эксперименте сравним алгоритм VND_2 с его версией, реализованной без вычитания радиуса пороговой устойчивости из бюджетов потребителей.

Предложенный алгоритм допускает использование мультистарта: запуск на разных стартовых решениях и выбор лучшего из найденных решений. Результаты такого подхода показаны далее.

4. Численный эксперимент

Для численного эксперимента использованы входные данные, взятые из библиотеки «Дискретные задачи размещения», и данные, сгенерированные случайным образом. Сначала готовим входные данные для исходной задачи, решаем её и в результате определяем максимально возможный доход производителя V. Далее фиксируем вход исходной задачи, берём некоторую часть от V в качестве порогового ограничения и получаем вход для задачи пороговой устойчивости. Варьируя пороговое ограничение таким образом, для одного входа исходной задачи можно сгенерировать несколько входов задачи пороговой устойчивости. Более подробно эта процедура описана в [3].

Таблица 2

Результаты численного эксперимента $n = 100$, $m = 100$, $r = 5$

Пример		Gurobi		VND_1		VND_2		VND'_2	
№	%	gap	Время	gap	Время	gap	Время	gap	Время
FLPr01	10	0	$5{,}4_{+2}$	$3{,}3_{-9}$	$2{,}3_{+1}$	$3{,}3_{-9}$	$4{,}2_{+0}$	$1{,}1_{-2}$	$1{,}3_{+3}$
	30	0	$1{,}3_{+4}$	$8{,}0_{-4}$	$6{,}6_{+1}$	0	$2{,}4_{+1}$	$8{,}0_{-4}$	$1{,}2_{+3}$
	50	$1{,}1_{-2}$	$4{,}3_{+4}$	$4{,}1_{-3}$	$2{,}1_{+2}$	$4{,}1_{-3}$	$5{,}8_{+1}$	$-4{,}2_{-5}$	$1{,}1_{+3}$
	70	$1{,}6_{-2}$	$4{,}3_{+4}$	$-4{,}5_{-3}$	$3{,}9_{+2}$	$2{,}2_{-4}$	$1{,}4_{+2}$	$-6{,}6_{-3}$	$8{,}5_{+2}$
	90	$1{,}2_{-1}$	$4{,}3_{+4}$	$1{,}8_{-1}$	$6{,}2_{+2}$	$-3{,}7_{-2}$	$3{,}0_{+2}$	$-1{,}8_{-2}$	$1{,}1_{+3}$
FLPr02	10	0	$6{,}2_{+2}$	0	$2{,}5_{+1}$	0	$1{,}1_{+1}$	$9{,}2_{-3}$	$2{,}1_{+3}$
	30	$7{,}1_{-3}$	$4{,}3_{+4}$	$5{,}3_{-3}$	$1{,}5_{+2}$	$5{,}5_{-3}$	$5{,}7_{+1}$	$4{,}8_{-2}$	$1{,}3_{+3}$
	50	$1{,}7_{-2}$	$4{,}3_{+4}$	$-2{,}9_{-2}$	$4{,}1_{+2}$	$-3{,}4_{-2}$	$1{,}3_{+2}$	$-3{,}4_{-2}$	$3{,}8_{+3}$
	70	$2{,}4_{-2}$	$4{,}3_{+4}$	$-4{,}5_{-2}$	$4{,}0_{+2}$	$-4{,}8_{-2}$	$1{,}2_{+2}$	$-4{,}5_{-2}$	$2{,}2_{+3}$
	90	$1{,}0_{-1}$	$4{,}3_{+4}$	$2{,}5_{-1}$	$7{,}1_{+2}$	$1{,}7_{-1}$	$3{,}6_{+2}$	$-4{,}1_{-2}$	$1{,}1_{+3}$
FLPr03	10	0	$4{,}0_{+2}$	$1{,}7_{-3}$	$1{,}4_{+1}$	0	$4{,}7_{+0}$	$1{,}0_{-2}$	$9{,}2_{+2}$
	30	0	$9{,}2_{+3}$	0	$1{,}0_{+2}$	0	$2{,}0_{+1}$	$2{,}0_{-2}$	$2{,}0_{+3}$
	50	$1{,}3_{-2}$	$4{,}3_{+4}$	$3{,}9_{-3}$	$3{,}0_{+2}$	$6{,}9_{-4}$	$5{,}7_{+1}$	$6{,}1_{-5}$	$1{,}7_{+3}$
	70	$2{,}3_{-2}$	$4{,}3_{+4}$	$-5{,}2_{-2}$	$4{,}2_{+2}$	$-4{,}6_{-2}$	$9{,}1_{+1}$	$9{,}1_{-3}$	$1{,}2_{+3}$
	90	$8{,}6_{-2}$	$4{,}3_{+4}$	$2{,}9_{-1}$	$5{,}0_{+2}$	$1{,}5_{-1}$	$1{,}5_{+2}$	$1{,}0_{-1}$	$1{,}9_{+3}$
FLPr04	10	0	$4{,}2_{+2}$	$2{,}0_{-4}$	$1{,}4_{+1}$	$2{,}2_{-3}$	$6{,}5_{+0}$	$1{,}2_{-2}$	$1{,}0_{+3}$
	30	0	$1{,}2_{+4}$	0	$1{,}8_{+2}$	0	$3{,}6_{+1}$	$4{,}7_{-2}$	$2{,}3_{+3}$
	50	$1{,}6_{-2}$	$4{,}3_{+4}$	$-9{,}2_{-5}$	$4{,}1_{+2}$	$-9{,}2_{-5}$	$6{,}8_{+1}$	$1{,}0_{-2}$	$1{,}0_{+3}$
	70	$3{,}6_{-2}$	$4{,}3_{+4}$	$-1{,}5_{-2}$	$3{,}3_{+2}$	$6{,}8_{-3}$	$1{,}5_{+2}$	$-1{,}5_{-2}$	$1{,}6_{+3}$
	90	$1{,}1_{-1}$	$4{,}3_{+4}$	$1{,}4_{-1}$	$9{,}6_{+2}$	$-1{,}3_{-1}$	$3{,}1_{+2}$	$-1{,}3_{-1}$	$2{,}1_{+3}$
FLPr05	10	0	$5{,}2_{+2}$	$1{,}5_{-8}$	$9{,}0_{+0}$	$1{,}5_{-8}$	$8{,}2_{+0}$	$3{,}7_{-3}$	$1{,}4_{+3}$
	30	0	$1{,}1_{+4}$	0	$9{,}2_{+1}$	0	$3{,}2_{+1}$	$1{,}6_{-2}$	$9{,}6_{+2}$
	50	$1{,}1_{-2}$	$4{,}3_{+4}$	$5{,}3_{-3}$	$1{,}8_{+2}$	$8{,}5_{-3}$	$5{,}1_{+1}$	$1{,}2_{-2}$	$1{,}4_{+3}$
	70	$1{,}5_{-2}$	$4{,}3_{+4}$	$6{,}7_{-3}$	$2{,}5_{+2}$	$1{,}5_{-2}$	$1{,}6_{+2}$	$6{,}7_{-5}$	$9{,}6_{+2}$
	90	$7{,}8_{-2}$	$4{,}3_{+4}$	$1{,}9_{-1}$	$3{,}9_{+2}$	0	$2{,}2_{+2}$	0	$1{,}2_{+3}$

Таблица 2 (окончание)

Пример		Gurobi		VND_1		VND_2		VND'_2	
№	%	gap	Время	gap	Время	gap	Время	gap	Время
FLPr06	10	0	$6{,}1_{+2}$	$1{,}8_{-3}$	$1{,}3_{+1}$	$7{,}0_{-10}$	$5{,}2_{+0}$	$4{,}6_{-3}$	$1{,}7_{+3}$
	30	0	$1{,}0_{+4}$	0	$1{,}3_{+2}$	0	$2{,}4_{+1}$	$6{,}4_{-3}$	$1{,}5_{+3}$
	50	$4{,}6_{-3}$	$4{,}3_{+4}$	$-1{,}5_{-2}$	$3{,}4_{+2}$	$-1{,}5_{-2}$	$8{,}0_{+1}$	$-1{,}3_{-2}$	$1{,}0_{+3}$
	70	$1{,}4_{-2}$	$4{,}3_{+4}$	$2{,}2_{-2}$	$4{,}4_{+2}$	$-4{,}4_{-2}$	$1{,}2_{+2}$	$-3{,}4_{-2}$	$1{,}6_{+3}$
	90	$1{,}0_{+7}$	$4{,}3_{+4}$	$-1{,}0_{+0}$	$9{,}1_{+2}$	$-1{,}0_{+0}$	$1{,}9_{+2}$	$-1{,}0_{+0}$	$1{,}0_{+3}$
FLPr07	10	0	$4{,}8_{+2}$	$7{,}6_{-4}$	$2{,}2_{+1}$	$7{,}6_{-4}$	$4{,}0_{+0}$	$3{,}6_{-3}$	$1{,}7_{+3}$
	30	0	$9{,}1_{+3}$	0	$8{,}4_{+1}$	0	$2{,}4_{+1}$	$1{,}5_{-2}$	$8{,}4_{+2}$
	50	$5{,}0_{-3}$	$4{,}3_{+4}$	$8{,}3_{-3}$	$2{,}6_{+2}$	$8{,}0_{-3}$	$5{,}8_{+1}$	$-1{,}6_{-4}$	$1{,}3_{+3}$
	70	$2{,}9_{-2}$	$4{,}3_{+4}$	$-1{,}9_{-3}$	$4{,}0_{+2}$	$1{,}2_{-2}$	$1{,}4_{+2}$	$2{,}7_{-2}$	$8{,}3_{+2}$
	90	$4{,}5_{-2}$	$4{,}3_{+4}$	$2{,}5_{-1}$	$5{,}0_{+2}$	$2{,}1_{-2}$	$1{,}8_{+2}$	$-9{,}1_{-2}$	$1{,}3_{+3}$
FLPr08	10	0	$4{,}6_{+2}$	3.5e-14	$1{,}8_{+1}$	3.7e-14	$4{,}0_{+0}$	$1{,}6_{-2}$	$8{,}2_{+2}$
	30	0	$1{,}2_{+4}$	0	$5{,}6_{+1}$	0	$4{,}3_{+1}$	$4{,}4_{-3}$	$8{,}4_{+2}$
	50	$1{,}4_{-2}$	$4{,}3_{+4}$	$9{,}5_{-5}$	$1{,}8_{+2}$	$2{,}8_{-2}$	$5{,}2_{+1}$	$1{,}3_{-2}$	$1{,}7_{+3}$
	70	$2{,}9_{-2}$	$4{,}3_{+4}$	$-1{,}2_{-2}$	$2{,}5_{+2}$	$4{,}4_{-3}$	$9{,}7_{+1}$	$-2{,}1_{-2}$	$8{,}7_{+2}$
	90	$1{,}3_{-1}$	$4{,}3_{+4}$	$8{,}1_{-2}$	$8{,}2_{+2}$	$-1{,}6_{-1}$	$2{,}5_{+2}$	$-1{,}6_{-1}$	$9{,}5_{+2}$
FLPr09	10	0	$7{,}4_{+2}$	$1{,}5_{-3}$	$2{,}5_{+1}$	0	$4{,}3_{+0}$	$2{,}1_{-3}$	$9{,}0_{+2}$
	30	0	$1{,}1_{+4}$	0	$9{,}7_{+1}$	0	$2{,}4_{+1}$	$5{,}1_{-2}$	$7{,}2_{+2}$
	50	$1{,}9_{-2}$	$4{,}3_{+4}$	$-3{,}3_{-2}$	$3{,}7_{+2}$	$-4{,}0_{-2}$	$1{,}0_{+2}$	$1{,}1_{-1}$	$5{,}4_{+2}$
	70	$3{,}9_{-2}$	$4{,}3_{+4}$	$-5{,}4_{-2}$	$3{,}8_{+2}$	$-5{,}0_{-2}$	$9{,}8_{+1}$	$-6{,}1_{-2}$	$6{,}1_{+2}$
	90	$1{,}4_{-1}$	$4{,}3_{+4}$	$2{,}1_{-1}$	$5{,}0_{+2}$	$-5{,}1_{-2}$	$2{,}7_{+2}$	$-5{,}1_{-2}$	$5{,}7_{+2}$
FLPr10	10	0	$6{,}8_{+2}$	$3{,}0_{-4}$	$1{,}6_{+1}$	$2{,}8_{-9}$	$8{,}3_{+0}$	$3{,}0_{-4}$	$1{,}4_{+3}$
	30	$2{,}1_{-3}$	$4{,}3_{+4}$	$-3{,}3_{-3}$	$1{,}3_{+2}$	$-8{,}1_{-5}$	$5{,}0_{+1}$	$1{,}4_{-2}$	$1{,}3_{+3}$
	50	$1{,}3_{-2}$	$4{,}3_{+4}$	$3{,}1_{-3}$	$2{,}0_{+2}$	$1{,}2_{-4}$	$1{,}6_{+2}$	$1{,}2_{-4}$	$1{,}4_{+3}$
	70	$1{,}7_{-2}$	$4{,}3_{+4}$	$-1{,}0_{-2}$	$6{,}6_{+2}$	$4{,}9_{-3}$	$1{,}2_{+2}$	$-2{,}6_{-2}$	$1{,}1_{+3}$
	90	$9{,}4_{-2}$	$4{,}3_{+4}$	$4{,}3_{-1}$	$4{,}7_{+2}$	$-3{,}0_{-3}$	$2{,}0_{+2}$	$5{,}4_{-2}$	$2{,}0_{+3}$

Сначала рассмотрим примеры задач из библиотеки. Для поиска точного решения применяем решатель Gurobi версии 10. Тестирование производится на сервере с двумя процессорами AMD EPYC 7502 32-Core и 512 ГБ оперативной памяти. При этом решатель Gurobi может использовать свободные ядра, и каждую задачу решаем параллельно на 7 ядрах. Время работы решателя для каждой задачи ограничено 12 ч. Основной алгоритм выполняем одним потоком, т. е. на одном ядре.

Эмпирически подобраны наилучшие параметры $k = 2$ и $\mathrm{flip} = 2$, которые применены в дальнейших экспериментах. Результаты, отражённые в табл. 1 и 2, получены на входных данных из библиотеки «Дискретные задачи размещения», а в табл. 3 и 4 — на входных данных, сгенерированных случайным образом. Полученные значения представлены в экспоненциальной записи, при этом порядок числа приводится в нижнем

индексе мантиссы для экономии места. В колонке % указана доля максимального дохода производителя, взятая в качестве порога V. Красным отмечено оптимальное значение gap, а синим — значение gap в случае, если решение предложенного алгоритма лучше в сравнении с решением Gurobi.

Размерность каждого входа в табл. 1 фиксирована числами $n = 100$, $m = 40$, $r = 5$. VND_2' — это версия алгоритма VND_2 без вычитания радиуса пороговой устойчивости из бюджетов потребителей. Время работы VND_2' больше, чем VND_2, на всех примерах в среднем в 13 раз. Ускорение происходит в силу того, что при вычитании радиуса пороговой устойчивости из бюджетов потребителей алгоритм чаще останавливается на шаге 4 алгоритма RC, тем самым экономя время на поиске цен. В 24 из 50 случаев решатель не смог найти оптимального решения. Алгоритм VND_2 с критерием 2 находит в среднем более качественное решение.

Размерность каждого входа в табл. 2 фиксирована числами $n = 100$, $m = 100$, $r = 5$. Как в предыдущем случае, время работы алгоритма

Таблица 3

Результаты эксперимента на средней и большой размерностях

Пример						Gurobi		VND_1		VND_2		VND_2'	
№	n	m	r	V	%	gap	Время	gap	Время	gap	Время	gap	Время
1	100	100	10	621	10	$3{,}2_{-3}$	$4{,}3_{+4}$	$-7{,}5_{-3}$	$6{,}4_{+4}$	$-8{,}7_{-5}$	$4{,}8_{+3}$	$2{,}0_{-1}$	$2{,}1_{+4}$
				1863	30	$9{,}2_{-3}$	$4{,}3_{+4}$	$-3{,}3_{-2}$	$1{,}4_{+5}$	$-2{,}9_{-2}$	$1{,}4_{+4}$	$-6{,}4_{-3}$	$1{,}1_{+4}$
				3105	50	$1{,}8_{-2}$	$4{,}3_{+4}$	$-2{,}5_{-2}$	$1{,}5_{+5}$	$-1{,}3_{-2}$	$1{,}5_{+4}$	$-1{,}4_{-2}$	$2{,}6_{+4}$
				4347	70	$2{,}2_{-2}$	$4{,}3_{+4}$	$-5{,}9_{-2}$	$1{,}6_{+5}$	$-6{,}0_{-2}$	$1{,}9_{+4}$	$-5{,}1_{-2}$	$1{,}3_{+4}$
				5589	90	$1{,}0_{+7}$	$4{,}3_{+4}$	$-1{,}0_{+0}$	$1{,}1_{+5}$	$-1{,}0_{+0}$	$1{,}8_{+4}$	$-1{,}0_{+0}$	$6{,}2_{+4}$
2	20	20	10	101	10	0	$9{,}7_{+0}$	$1{,}5_{-2}$	$4{,}6_{-1}$	$1{,}3_{-8}$	$3{,}1_{-1}$	$5{,}8_{-3}$	$1{,}2_{+1}$
				303	30	0	$2{,}3_{+1}$	$2{,}4_{-1}$	$3{,}1_{+0}$	$2{,}1_{-1}$	$7{,}7_{-1}$	$2{,}4_{-1}$	$5{,}7_{+0}$
				505	50	0	$2{,}5_{+2}$	$7{,}9_{-2}$	$1{,}4_{+1}$	$7{,}5_{-2}$	$1{,}6_{+0}$	$7{,}0_{-2}$	$1{,}6_{+1}$
				707	70	0	$4{,}6_{+2}$	$1{,}2_{-1}$	$2{,}8_{+0}$	$5{,}0_{-2}$	$2{,}2_{+0}$	$3{,}7_{-2}$	$3{,}7_{+0}$
				909	90	0	$5{,}1_{+2}$	$8{,}8_{-2}$	$1{,}1_{+1}$	$1{,}5_{-1}$	$2{,}5_{+0}$	$5{,}0_{-2}$	$4{,}1_{+1}$
3	20	20	15	128	10	0	$2{,}6_{+1}$	$2{,}3_{-2}$	$1{,}1_{+1}$	$1{,}5_{-1}$	$4{,}1_{-1}$	$1{,}7_{-1}$	$4{,}1_{+1}$
				384	30	0	$9{,}9_{+1}$	$2{,}0_{-2}$	$4{,}9_{+0}$	$1{,}5_{-2}$	$3{,}4_{+0}$	$1{,}3_{-1}$	$7{,}0_{+0}$
				641	50	0	$8{,}4_{+1}$	$1{,}1_{-1}$	$2{,}2_{+1}$	$1{,}1_{-1}$	$3{,}5_{+0}$	$9{,}9_{-2}$	$8{,}3_{+0}$
				898	70	0	$1{,}5_{+2}$	$1{,}5_{-1}$	$4{,}1_{+0}$	$8{,}5_{-2}$	$5{,}6_{+0}$	$8{,}5_{-2}$	$3{,}7_{+1}$
				1154	90	0	$1{,}3_{+2}$	$3{,}6_{-1}$	$2{,}8_{+1}$	$2{,}1_{-1}$	$3{,}2_{+0}$	$1{,}9_{-1}$	$3{,}4_{+1}$
4	40	40	10	288	10	$2{,}0_{-4}$	$4{,}3_{+4}$	$5{,}9_{-3}$	$1{,}6_{+2}$	$4{,}8_{-3}$	$2{,}6_{+1}$	$7{,}7_{-2}$	$1{,}1_{+3}$
				866	30	$1{,}3_{-3}$	$4{,}3_{+4}$	$1{,}6_{-3}$	$5{,}8_{+2}$	$1{,}2_{-2}$	$2{,}2_{+2}$	$1{,}6_{-2}$	$1{,}8_{+3}$
				1443	50	$2{,}6_{-3}$	$4{,}3_{+4}$	$-2{,}2_{-3}$	$1{,}0_{+3}$	$3{,}5_{-3}$	$1{,}2_{+2}$	$1{,}1_{-2}$	$8{,}6_{+2}$
				2020	70	$4{,}0_{-3}$	$4{,}3_{+4}$	$3{,}7_{-3}$	$1{,}1_{+3}$	$-6{,}7_{-3}$	$1{,}3_{+2}$	$1{,}4_{-3}$	$1{,}2_{+3}$
				2598	90	$5{,}9_{-3}$	$4{,}3_{+4}$	$1{,}5_{-2}$	$1{,}1_{+3}$	$7{,}0_{-4}$	$2{,}5_{+2}$	$8{,}8_{-2}$	$5{,}8_{+2}$

Таблица 3 (окончание)

Пример						Gurobi		VND_1		VND_2		VND'_2	
№	n	m	r	V	%	gap	Время	gap	Время	gap	Время	gap	Время
5	40	40	15	225	10	0	$2{,}3_{+2}$	$1{,}5_{-2}$	$2{,}3_{+2}$	$1{,}5_{-2}$	$2{,}1_{+1}$	$9{,}1_{-3}$	$2{,}9_{+3}$
				677	30	$1{,}2_{-3}$	$4{,}3_{+4}$	$-7{,}4_{-4}$	$1{,}0_{+3}$	$7{,}4_{-4}$	$1{,}9_{+2}$	$4{,}0_{-2}$	$2{,}7_{+3}$
				1129	50	$3{,}0_{-3}$	$4{,}3_{+4}$	$8{,}3_{-4}$	$2{,}5_{+3}$	$1{,}2_{-2}$	$2{,}1_{+2}$	$2{,}8_{-3}$	$5{,}4_{+2}$
				1581	70	$4{,}7_{-3}$	$4{,}3_{+4}$	$1{,}7_{-2}$	$1{,}4_{+3}$	$-1{,}7_{-2}$	$5{,}4_{+2}$	$1{,}4_{-2}$	$1{,}2_{+3}$
				2033	90	$5{,}9_{-3}$	$4{,}3_{+4}$	$1{,}6_{-1}$	$1{,}7_{+3}$	$1{,}5_{-1}$	$4{,}8_{+2}$	$-3{,}6_{-3}$	$8{,}5_{+2}$
6	60	60	10	411	10	$1{,}0_{-3}$	$4{,}3_{+4}$	$5{,}4_{-3}$	$4{,}8_{+3}$	$3{,}6_{-3}$	$2{,}1_{+2}$	$1{,}5_{-1}$	$1{,}2_{+4}$
				1234	30	$4{,}6_{-3}$	$4{,}3_{+4}$	$-1{,}9_{-2}$	$6{,}6_{+3}$	$-1{,}6_{-2}$	$7{,}6_{+2}$	$-9{,}6_{-3}$	$5{,}5_{+3}$
				2058	50	$8{,}9_{-3}$	$4{,}3_{+4}$	$-7{,}4_{-3}$	$5{,}4_{+3}$	$-1{,}5_{-2}$	$1{,}4_{+3}$	$5{,}2_{-3}$	$4{,}0_{+3}$
				2881	70	$1{,}0_{-2}$	$4{,}3_{+4}$	$1{,}8_{-2}$	$1{,}2_{+4}$	$3{,}0_{-2}$	$4{,}0_{+3}$	$4{,}6_{-2}$	$4{,}9_{+3}$
				3704	90	$5{,}0_{-2}$	$4{,}3_{+4}$	$-1{,}8_{-1}$	$1{,}8_{+4}$	$-1{,}3_{-1}$	$2{,}8_{+3}$	$-1{,}4_{-1}$	$3{,}6_{+3}$
7	60	60	15	381	10	$1{,}5_{-3}$	$4{,}3_{+4}$	$8{,}9_{-3}$	$2{,}0_{+3}$	$3{,}2_{-3}$	$2{,}0_{+2}$	$6{,}5_{-3}$	$2{,}0_{+4}$
				1143	30	$3{,}5_{-3}$	$4{,}3_{+4}$	$-1{,}2_{-2}$	$3{,}6_{+4}$	$-1{,}0_{-2}$	$4{,}1_{+3}$	$-5{,}5_{-3}$	$1{,}3_{+4}$
				1906	50	$7{,}4_{-3}$	$4{,}3_{+4}$	$8{,}4_{-2}$	$2{,}0_{+4}$	$7{,}3_{-2}$	$3{,}7_{+3}$	$8{,}0_{-2}$	$1{,}4_{+4}$
				2669	70	$1{,}8_{-2}$	$4{,}3_{+4}$	$-5{,}3_{-2}$	$3{,}6_{+4}$	$-4{,}5_{-2}$	$5{,}1_{+3}$	$-7{,}6_{-3}$	$8{,}1_{+3}$
				3431	90	$5{,}0_{-2}$	$4{,}3_{+4}$	$-8{,}9_{-2}$	$9{,}8_{+3}$	$6{,}3_{-3}$	$4{,}0_{+3}$	$-3{,}1_{-2}$	$1{,}2_{+4}$
8	90	90	10	583	10	$1{,}5_{-3}$	$4{,}3_{+4}$	$1{,}4_{-3}$	$4{,}9_{+3}$	$1{,}8_{-3}$	$5{,}7_{+2}$	$7{,}8_{-2}$	$1{,}6_{+4}$
				1749	30	$6{,}6_{-3}$	$4{,}3_{+4}$	$-7{,}1_{-3}$	$7{,}5_{+3}$	$-1{,}0_{-2}$	$3{,}4_{+3}$	$-1{,}7_{-2}$	$3{,}2_{+4}$
				2915	50	$4{,}6_{-3}$	$4{,}3_{+4}$	$-3{,}1_{-2}$	$1{,}7_{+4}$	$-4{,}7_{-2}$	$1{,}1_{+4}$	$-4{,}0_{-2}$	$1{,}3_{+4}$
				4081	70	$8{,}2_{-3}$	$4{,}3_{+4}$	$-5{,}0_{-2}$	$3{,}4_{+4}$	$-5{,}1_{-2}$	$1{,}5_{+4}$	$-1{,}8_{-2}$	$3{,}2_{+4}$
				5247	90	$5{,}1_{-2}$	$4{,}3_{+4}$	$-1{,}4_{-1}$	$3{,}7_{+4}$	$-1{,}6_{-1}$	$1{,}2_{+4}$	$-5{,}8_{-2}$	$1{,}9_{+4}$

VND'_2 в сравнении с VND_2 больше на всех примерах в среднем в 13 раз. В 32 случаях из 50 решателю не удалось найти оптимального решения, а в одном случае — хотя бы допустимого. Алгоритм VND_2 с критерием 2 в среднем находит решение лучше. Это происходит, скорее всего, в силу того, что критерий 2 нацелен на поиск максимального радиуса, а не дохода производителя. Время работы решателя значительно превышает время работы алгоритмов VND.

Согласно табл. 3 на примерах средней или большой размерности алгоритм VND работает продолжительное время. Здесь отчётливо видно различие во времени работы алгоритмов VND_2 и VND'_2. Количество найденных оптимумов — 11 из 40. Так же есть пример, в котором решатель Gurobi не смог найти допустимого решения за отведённое время работы. Критерий 2 на этих примерах наиболее предпочтителен.

Результаты в табл. 4 получены на входных данных малой размерности. Решатель Gurobi нашёл 29 оптимальных решений на 50 примерах. Алгоритм VND_2 находит решение в среднем немного хуже, чем решатель, но время работы в тысячи раз меньше.

На рис. 1 отображены средние показатели алгоритмов с разными параметрами. По горизонтали отмечен алгоритм VND(k, flip) с параметрами k и flip. Запись VND$(k, \text{flip})(x)$ означает, что использована идея мультистарта и этот алгоритм запускался x раз. Приведены значение gap и время работы алгоритмов, масштабированные по максимальному значению, а максимальное указано в легенде. Из рис. 1 видно, что идея мультистарта позволяет найти решение лучше, при этом время работы увеличивается пропорционально количеству запусков.

Если ограничиться примерами, для которых найден оптимум, то для алгоритма VND наилучшими параметрами будут $k = 2$ и flip $= 2$. При увеличении одного из параметров время счёта сильно возрастает, а значение целевой функции улучшается незначительно.

Таблица 4

Результаты численного эксперимента на малой размерности

Пример						Gurobi		VND_1		VND_2		VND'_2	
№	n	m	r	V	%	gap	Время	gap	Время	gap	Время	gap	Время
1	30	30	5	177	10	$4{,}0_{-4}$	$4{,}3_{+4}$	$1{,}9_{-3}$	$6{,}4_{+0}$	$3{,}8_{-5}$	$1{,}5_{+0}$	$4{,}9_{-2}$	$8{,}5_{+1}$
				531	30	$2{,}1_{-3}$	$4{,}3_{+4}$	$1{,}5_{-1}$	$9{,}2_{+0}$	$1{,}4_{-1}$	$5{,}0_{+0}$	$1{,}7_{-2}$	$1{,}4_{+2}$
				885	50	$5{,}5_{-3}$	$4{,}3_{+4}$	$8{,}1_{-2}$	$1{,}5_{+1}$	$7{,}8_{-2}$	$5{,}1_{+0}$	$8{,}3_{-2}$	$3{,}9_{+1}$
				1239	70	$1{,}1_{-2}$	$4{,}3_{+4}$	$3{,}0_{-2}$	$9{,}3_{+0}$	$1{,}1_{-2}$	$6{,}7_{+0}$	$-1{,}9_{-4}$	$3{,}9_{+1}$
				1593	90	$3{,}0_{-2}$	$4{,}3_{+4}$	$2{,}8_{-2}$	$1{,}2_{+1}$	$5{,}6_{-2}$	$6{,}2_{+0}$	$5{,}1_{-3}$	$3{,}6_{+1}$
2	35	35	5	167	10	0	$1{,}6_{+2}$	$2{,}2_{-3}$	$1{,}8_{+0}$	$2{,}2_{-3}$	$5{,}8_{-1}$	$6{,}8_{-3}$	$7{,}6_{+1}$
				503	30	$2{,}5_{-3}$	$4{,}3_{+4}$	$2{,}8_{-2}$	$2{,}4_{+1}$	$2{,}0_{-2}$	$3{,}6_{+0}$	$9{,}3_{-2}$	$2{,}3_{+2}$
				839	50	$7{,}8_{-3}$	$4{,}3_{+4}$	$5{,}5_{-3}$	$4{,}0_{+1}$	$-3{,}4_{-3}$	$9{,}4_{+0}$	$8{,}6_{-3}$	$1{,}6_{+2}$
				1175	70	$1{,}2_{-2}$	$4{,}3_{+4}$	$7{,}4_{-3}$	$1{,}9_{+1}$	$-2{,}4_{-2}$	$2{,}0_{+1}$	$-2{,}3_{-2}$	$7{,}3_{+1}$
				1511	90	$2{,}2_{-2}$	$4{,}3_{+4}$	$-8{,}6_{-3}$	$1{,}6_{+1}$	$-8{,}6_{-3}$	$1{,}5_{+1}$	$-8{,}6_{-3}$	$6{,}6_{+1}$
3	35	35	5	170	10	0	$1{,}3_{+2}$	$2{,}3_{-3}$	$1{,}8_{+0}$	$1{,}3_{-8}$	$7{,}5_{-1}$	$2{,}3_{-2}$	$9{,}6_{+1}$
				512	30	$2{,}3_{-3}$	$4{,}3_{+4}$	$9{,}8_{-3}$	$2{,}0_{+1}$	$1{,}0_{-2}$	$4{,}9_{+0}$	$9{,}3_{-2}$	$1{,}4_{+2}$
				854	50	$9{,}3_{-3}$	$4{,}3_{+4}$	$-4{,}2_{-2}$	$5{,}6_{+1}$	$-3{,}4_{-2}$	$8{,}4_{+0}$	$-3{,}3_{-2}$	$1{,}2_{+2}$
				1196	70	$1{,}3_{-2}$	$4{,}3_{+4}$	$3{,}1_{-2}$	$4{,}3_{+1}$	$-1{,}8_{-3}$	$1{,}0_{+1}$	$2{,}5_{-2}$	$6{,}2_{+1}$
				1538	90	$2{,}1_{-2}$	$4{,}3_{+4}$	$5{,}4_{-2}$	$4{,}5_{+1}$	$6{,}4_{-2}$	$1{,}8_{+1}$	$-3{,}4_{-2}$	$6{,}4_{+1}$
4	35	35	5	169	10	0	$1{,}0_{+2}$	$1{,}1_{-3}$	$3{,}2_{+0}$	$2{,}3_{-3}$	$9{,}5_{-1}$	$1{,}3_{-2}$	$2{,}5_{+2}$
				507	30	$3{,}2_{-3}$	$4{,}3_{+4}$	$3{,}6_{-2}$	$3{,}6_{+1}$	$3{,}7_{-2}$	$6{,}0_{+0}$	$1{,}7_{-1}$	$1{,}3_{+2}$
				845	50	$8{,}2_{-3}$	$4{,}3_{+4}$	$-3{,}4_{-2}$	$3{,}1_{+1}$	$-4{,}0_{-2}$	$9{,}1_{+0}$	$4{,}3_{-3}$	$7{,}0_{+1}$
				1183	70	$1{,}2_{-2}$	$4{,}3_{+4}$	$6{,}2_{-4}$	$3{,}6_{+1}$	$6{,}2_{-4}$	$2{,}4_{+1}$	$2{,}4_{-2}$	$6{,}1_{+1}$
				1521	90	$2{,}7_{-2}$	$4{,}3_{+4}$	$7{,}6_{-2}$	$3{,}0_{+1}$	$-7{,}6_{-2}$	$1{,}8_{+1}$	$9{,}0_{-2}$	$5{,}6_{+1}$
5	35	35	5	174	10	0	$1{,}2_{+2}$	$3{,}4_{-3}$	$4{,}5_{+0}$	$2{,}3_{-3}$	$7{,}2_{-1}$	$1{,}4_{-2}$	$1{,}3_{+2}$
				524	30	$2{,}7_{-3}$	$4{,}3_{+4}$	$1{,}7_{-2}$	$2{,}2_{+1}$	$5{,}9_{-3}$	$3{,}2_{+0}$	$5{,}8_{-2}$	$2{,}3_{+2}$
				874	50	$7{,}2_{-3}$	$4{,}3_{+4}$	$-1{,}6_{-3}$	$2{,}0_{+1}$	$-4{,}2_{-3}$	$1{,}5_{+1}$	$1{,}9_{-2}$	$6{,}4_{+1}$
				1224	70	$1{,}2_{-2}$	$4{,}3_{+4}$	$-1{,}9_{-3}$	$2{,}8_{+1}$	$-1{,}9_{-3}$	$1{,}4_{+1}$	$2{,}3_{-2}$	$5{,}6_{+1}$
				1574	90	$3{,}4_{-2}$	$4{,}3_{+4}$	$-6{,}8_{-2}$	$2{,}1_{+1}$	$-6{,}8_{-2}$	$1{,}3_{+1}$	$-6{,}8_{-2}$	$5{,}9_{+1}$

Таблица 4 (окончание)

Пример						Gurobi		VND_1		VND_2		VND'_2	
№	n	m	r	V	%	gap	Время	gap	Время	gap	Время	gap	Время
6	20	20	5	108	10	0	$9{,}6_{+0}$	$7{,}2_{-3}$	$1{,}7_{-1}$	$1{,}2_{-3}$	$5{,}5_{-2}$	$5{,}0_{-2}$	$7{,}6_{+0}$
				324	30	0	$1{,}2_{+2}$	$2{,}0_{-2}$	$1{,}4_{+0}$	$3{,}0_{-2}$	$2{,}7_{-1}$	$4{,}1_{-2}$	$9{,}4_{+0}$
				541	50	0	$1{,}1_{+2}$	$3{,}3_{-2}$	$7{,}2_{-1}$	$1{,}6_{-2}$	$5{,}8_{-1}$	$3{,}0_{-2}$	$5{,}1_{+0}$
				757	70	0	$1{,}2_{+2}$	$3{,}9_{-3}$	$1{,}9_{+0}$	$4{,}1_{-3}$	$1{,}2_{+0}$	$5{,}5_{-2}$	$3{,}4_{+0}$
				973	90	0	$1{,}4_{+2}$	$1{,}6_{-2}$	$2{,}6_{+0}$	$1{,}2_{-2}$	$7{,}0_{-1}$	$1{,}5_{-3}$	$4{,}6_{+0}$
7	25	25	5	151	10	0	$1{,}5_{+2}$	$7{,}6_{-3}$	$1{,}5_{+0}$	$3{,}9_{-3}$	$2{,}5_{-1}$	$7{,}0_{-2}$	$3{,}1_{+1}$
				454	30	0	$4{,}3_{+3}$	$5{,}5_{-3}$	$6{,}9_{+0}$	$1{,}1_{-2}$	$1{,}2_{+0}$	$1{,}1_{-2}$	$2{,}6_{+1}$
				757	50	0	$4{,}8_{+3}$	$1{,}5_{-2}$	$8{,}1_{+0}$	$5{,}6_{-3}$	$2{,}2_{+0}$	$5{,}6_{-3}$	$1{,}6_{+1}$
				1060	70	0	$4{,}5_{+3}$	$2{,}2_{-2}$	$1{,}1_{+1}$	$2{,}2_{-2}$	$3{,}6_{+0}$	$2{,}2_{-2}$	$2{,}7_{+1}$
				1363	90	0	$1{,}7_{+3}$	$3{,}4_{-2}$	$1{,}1_{+1}$	$2{,}9_{-1}$	$2{,}4_{+0}$	$2{,}3_{-2}$	$1{,}4_{+1}$
8	20	20	5	126	10	0	$1{,}3_{+1}$	$2{,}3_{-3}$	$9{,}5_{-2}$	$2{,}3_{-3}$	$1{,}2_{-1}$	$1{,}8_{-2}$	$1{,}2_{+1}$
				378	30	0	$1{,}4_{+2}$	0	$8{,}6_{-1}$	$2{,}2_{-2}$	$3{,}1_{-1}$	$3{,}7_{-2}$	$4{,}5_{+0}$
				631	50	0	$1{,}8_{+2}$	$1{,}2_{-2}$	$1{,}5_{+0}$	$1{,}1_{-2}$	$5{,}7_{-1}$	$1{,}1_{-2}$	$4{,}5_{+0}$
				884	70	0	$1{,}4_{+2}$	$2{,}8_{-2}$	$2{,}9_{+0}$	$1{,}8_{-2}$	$6{,}4_{-1}$	$1{,}6_{-2}$	$7{,}2_{+0}$
				1136	90	0	$1{,}9_{+2}$	$6{,}4_{-2}$	$4{,}6_{+0}$	$3{,}2_{-2}$	$7{,}7_{-1}$	$3{,}2_{-2}$	$4{,}8_{+0}$
9	15	15	5	98	10	0	$2{,}0_{+1}$	$7{,}4_{-4}$	$7{,}3_{-2}$	$5{,}8_{-3}$	$4{,}3_{-2}$	$1{,}4_{-2}$	$2{,}7_{+0}$
				294	30	0	$3{,}6_{+1}$	$1{,}4_{-3}$	$2{,}2_{-1}$	$2{,}8_{-9}$	$2{,}4_{-1}$	$2{,}8_{-9}$	$1{,}4_{+0}$
				491	50	0	$3{,}1_{+1}$	$2{,}0_{-3}$	$2{,}9_{-1}$	$2{,}4_{-9}$	$2{,}9_{-1}$	$2{,}4_{-2}$	$8{,}0_{-1}$
				688	70	0	$4{,}1_{+1}$	$3{,}3_{-3}$	$2{,}6_{-1}$	$8{,}8_{-9}$	$3{,}0_{-1}$	$8{,}8_{-9}$	$1{,}2_{+0}$
				884	90	0	$4{,}1_{+1}$	$5{,}5_{-9}$	$8{,}7_{-1}$	$5{,}5_{-9}$	$2{,}9_{-1}$	$5{,}5_{-9}$	$1{,}4_{+0}$
10	15	15	10	87	10	0	$8{,}8_{+0}$	$7{,}0_{-2}$	$3{,}2_{-1}$	$8{,}1_{-2}$	$1{,}3_{-1}$	$1{,}2_{-1}$	$1{,}2_{+1}$
				263	30	0	$7{,}7_{+1}$	$6{,}7_{-2}$	$1{,}2_{+0}$	$1{,}0_{-2}$	$5{,}0_{-1}$	$2{,}3_{-2}$	$7{,}1_{+0}$
				438	50	0	$5{,}8_{+1}$	$6{,}0_{-2}$	$8{,}8_{-1}$	$4{,}9_{-2}$	$6{,}7_{-1}$	$3{,}8_{-2}$	$1{,}2_{+0}$
				613	70	0	$3{,}8_{+1}$	$3{,}7_{-2}$	$5{,}9_{-1}$	$1{,}5_{-2}$	$2{,}9_{-1}$	$1{,}8_{-2}$	$7{,}8_{-1}$
				789	90	0	$6{,}6_{+1}$	$2{,}2_{-2}$	$1{,}1_{+0}$	$4{,}8_{-9}$	$3{,}2_{-1}$	$4{,}8_{-9}$	$3{,}1_{+0}$

Из рис. 2 видно, что наименьший gap, отмеченный по вертикали, имеет реализация алгоритма с параметрами $k = 2$, flip $= 2$ при запуске 10 раз. Алгоритм с параметрами $k = 2$, flip $= 3$ и запуском 10 раз справился в среднем хуже: так происходит из-за того, что стартовое решение выбирается случайным образом. Эксперименты показывают, что для идеи мультистарта наилучшее число запусков алгоритма равно 10.

Заключение

Исследование пороговой устойчивости двух- и трёхуровневых задач размещения и ценообразования начато в работах [1, 2]. На их основе рассмотрена пороговая устойчивость двухуровневых задач размещения и ценообразования с медианным типом размещения предприятий [3, 4].

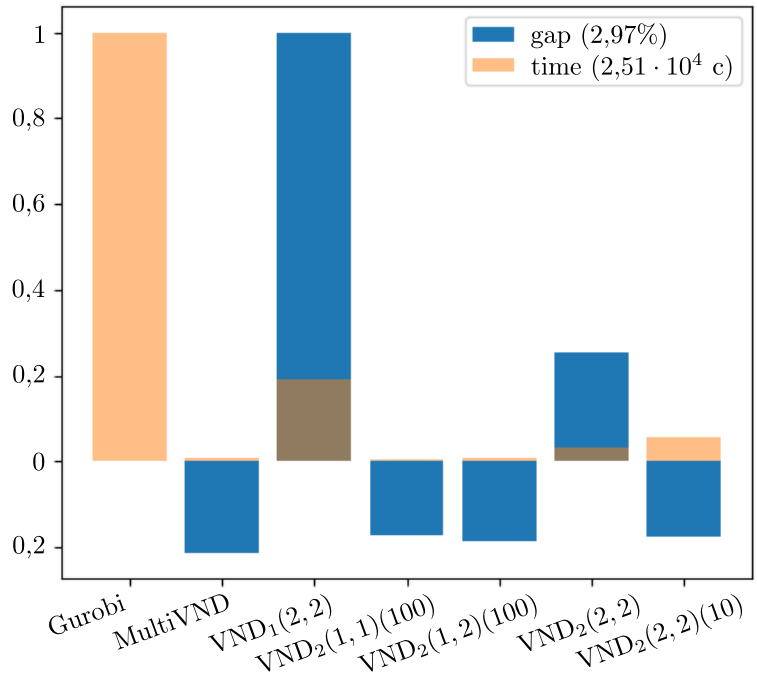


Рис. 1. Средние значения gap и времени по всем примерам

В указанных работах развит оригинальный подход к разработке алгоритмов решения соответствующих задач, основанный на использовании методов решения исходной задачи и её подзадач. Численный эксперимент показал весьма высокую эффективность разработанных алгоритмов как по качеству приближённых решений, так и по трудоёмкости алгоритмов [3, 4]. Однако базовые задачи, для которых исследована пороговая устойчивость, объединяет общее свойство — при фиксированном размещении предприятий соответствующие задачи ценообразования полиномиально разрешимы. Стало быть, для объективной оценки подхода, развитого в указанных работах, желательно исследовать пороговую устойчивость, например, задачи размещения и фабричного ценообразования, поскольку при фиксированном размещении предприятий задача фабричного ценообразования NP-трудна в сильном смысле.

В настоящей работе показано, что развитый в [3, 4] подход к разработке эффективных приближённых алгоритмов для определения пороговой устойчивости двухуровневой задачи размещения производства и ценообразования оказывается продуктивным и в случае базовой задачи с фабричным ценообразованием. Для решения задачи пороговой устойчивости предлагается алгоритм, основанный на спуске с чередующимися окрестностями (VND).

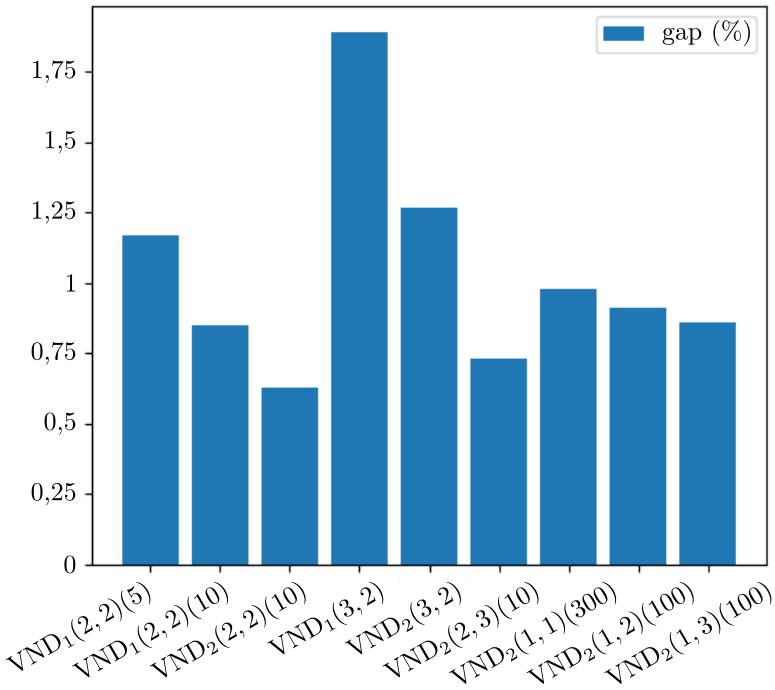


Рис. 2. Среднее значение gap для примеров с известным оптимумом

Численное исследование алгоритма проводится на известных примерах и случайно сгенерированных данных. Эксперименты показывают, что итеративное вычитание радиуса пороговой устойчивости из бюджетов потребителей значительно снижает время работы алгоритма. На примерах с найденным оптимумом алгоритм ошибается в среднем на 0,63% относительно оптимального значения целевой функции. На всех примерах алгоритм находит решение со значением целевой функции в среднем на 2,97% лучше в сравнении с решением Gurobi.

Теоремы 1 и 2 приводят также к следующей гипотезе: задачи пороговой устойчивости, исследованные в этой работе, полны в классе NPO относительно подходящей сводимости, сохраняющей аппроксимируемость.

Вторая гипотеза вытекает из следствия 1, анализа доказательств теорем 1, 2 и представленных алгоритмов решения. Точный детерминированный полиномиальный алгоритм с оракулом из класса NP, о котором говорится в следствии 1, легко получить, взяв в качестве оракула стандартную задачу распознавания. В силу этого высокая эффективность разработанных алгоритмов связана, возможно, с тем, что использованный в работе подход позволяет хорошо аппроксимировать оракул, доставляющий информацию для детерминированного полиномиального

точного алгоритма из класса Δ_2^{P}. С учётом того, что оракул представляет собой NP-полную задачу, в алгоритме используется итеративная процедура поиска (ρ, y, p) в обход фазы недетерминированного угадывания этих величин, которые и образуют сертификат.

Финансирование работы

Исследование выполнено при финансовой поддержке Российского научного фонда (проект № 23–21–00424). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Panin A. A., Plyasunov A. V.** Stability analysis for pricing // Mathematical optimization theory and operations research. Rev. Sel. Pap. 19th Int. Conf. MOTOR 2020 (Novosibirsk, Russia, July 6–10, 2020). Cham: Springer, 2020. P. 57–69. (Commun. Comput. Inf. Sci.; V. 1275).
2. **Panin A. A., Plyasunov A. V.** The multilevel facility location and pricing problems: The computational complexity and the stability analysis // Optim. Lett. 2023. V. 17, No. 6. P. 1295–1315. DOI: 10.1007/s11590-022-01924-3.
3. **Vodyan M. E., Panin A. A., Plyasunov A. V.** Metaheuristics for finding the stability radius in the bilevel facility location and uniform pricing problem // Proc. 19th Int. Asian School-Seminar Optimization Problems of Complex Systems (Novosibirsk, Russia, Aug. 14–22, 2023). Piscataway: IEEE, 2023. P. 130–135. DOI: 10.1109/OPCS59592.2023.10275325.
4. **Водян М. Е., Панин А. А., Плясунов А. В.** Исследование пороговой устойчивости двухуровневой задачи размещения производства и дискриминационного ценообразования // Дискрет. анализ и исслед. операций. 2024. Т. 31, № 3. С. 79–104.
5. **Dyer M., Stougie L.** Computational complexity of stochastic programming problems // Math. Program. Ser. A. 2006. V. 106, No. 3. P. 423–432. DOI: 10.1007/s10107-005-0597-0.
6. **Кибзун А. И., Кан Ю. С.** Задачи стохастического программирования с вероятностными критериями. М.: Физматлит, 2009. 372 с.
7. **Ben-Tal A., Nemirovski A.** Robust optimization — Methodology and applications // Math. Program. Ser. B. 2002. V. 92, No. 3. P. 453–480. DOI: 10.1007/s101070100286.
8. **Snyder L. V.** Facility location under uncertainty: A review // IIE Trans. 2006. V. 38. P. 537–554. DOI: 10.1080/07408170500216480.
9. **Greenberg H. J.** An annotated bibliography for post-solution analysis in mixed integer programming and combinatorial optimization // Advances in computational and stochastic optimization, logic programming, and heuristic search. New York: Springer, 1998. P. 97–147.

10. **Correia I., da Gama F. S.** Facility location under uncertainty // Location science. Cham: Springer, 2015. P. 177–203.
11. **Ben-Tal A., Nemirovski A.** Robust solutions of uncertain linear programs // Oper. Res. Lett. 1999. V. 25, No. 1. P. 1–13.
12. **Yu G., Yang J.** On the shortest path problem // Comput. Oper. Res. 1988. V. 25, No. 6. P. 457–68.
13. **Kouvelis P., Yu G.** Robust discrete optimization and its applications. Dordrecht: Kluwer Acad. Publ., 1997. 358 p.
14. **Averbakh I., Lebedev V.** Interval data minmax regret network optimization problems // Discrete Appl. Math. 2004. V. 138. P. 289–301.
15. **Aissi H., Bazgan C., Vanderpooten D.** Complexity of the min-max and min-max regret assignment problems // Oper. Res. Lett. 2005. V. 33, No. 6. P. 634–640.
16. **Carrizosa E., Nickel S.** Robust facility location // Math. Methods Oper. Res. 2003. V. 58, No. 2. P. 331–349.
17. **Carrizosa E., Ushakov A., Vasilyev I.** Threshold robustness in discrete facility location problems: A bi-objective approach // Optim. Lett. 2015. V. 9, No. 7. P. 1297–1314.
18. **Леонтьев В. К.** Устойчивость задачи коммивояжера // Журн. вычисл. математики и мат. физики. 1975. Т. 15, № 5. С. 1298–1309.
19. **Rossi A., Gurevsky E., Battaia O., Dolgui A.** Maximizing the robustness for simple assembly lines with fixed cycle time and limited number of workstations // Discrete Appl. Math. 2016. V. 208. P. 123–136.
20. **Gurevsky E., Rasamimanana A., Pirogov A., Dolgui A., Rossi A.** Stability factor for robust balancing of simple assembly lines under uncertainty // Discrete Appl. Math. 2022. V. 318. P. 113–132.
21. **Pirogov A., Gurevsky E., Rossi A., Dolgui A.** Robust balancing of transfer lines with blocks of uncertain parallel tasks under fixed cycle time and space restrictions // Eur. J. Oper. Res. 2021. V. 290. P. 946–955.
22. **Sotskov Yu. N.** Assembly and production line designing, balancing and scheduling with inaccurate data: A survey and perspectives // Algorithms. 2023. V. 16, No. 2. Article ID 100. 43 p.
23. **Леонтьев В. К., Гордеев Э. Н.** Качественное исследование траекторных задач // Кибернетика. 1986. № 5. С. 82–89.
24. **Sotskov Yu. N., Leontiev V. K., Gordeev E. N.** Some concepts of stability analysis in combinatorial optimization // Discrete Appl. Math. 1995. V. 58, No. 2. P. 169–190.
25. **Кузьмин К. Г.** Единый подход к нахождению радиусов устойчивости в многокритериальной задаче о максимальном разрезе графа // Дискрет. анализ и исслед. операций. 2015. Т. 22, № 5. С. 30–51.
26. **Dempe S., Zemkoho A.** Bilevel optimization. Advances and next challenges. Cham: Springer, 2020. 672 p. (Springer Optim. Its Appl.; V. 161). DOI: 10.1007/978-3-030-52119-6.
27. **Talbi E.-G.** Metaheuristics: From design to implementation. Berlin: Wiley, 2009. 624 p.

28. Mladenovic N., Hansen P. Variable neighbourhood search // Comput. Oper. Res. 1997. V. 24. P. 1097–1100.

29. Кочетов Ю. А., Младенович Н., Хансен П. Локальный поиск с чередующимися окрестностями // Дискрет. анализ и исслед. операций. 2003. Т. 10, № 1. С. 11–43.

30. Diakova Z. S., Kochetov Yu. A. A double VNS heuristic for the facility location and pricing problem // Electron. Notes Discrete Math. 2012. V. 39. P. 29–34. DOI: 10.1016/j.endm.2012.10.005.

31. Кочетов Ю. А., Панин А. А., Плясунов А. В. Сравнение метаэвристик для решения двухуровневой задачи размещения предприятий и фабричного ценообразования // Дискрет. анализ и исслед. операций. 2015. Т. 22, № 3. С. 36–54.

32. Hanjoul P., Hansen P., Peeters D., Thisse J.-F. Uncapacitated plant location under alternative spatial price policies // Manage. Sci. 1990. V. 36, No. 1. P. 41–57. DOI: 10.1287/mnsc.36.1.41.

33. Панин А. А., Пащенко М. Г., Плясунов А. В. Двухуровневые модели конкурентного размещения производства и ценообразования // Автоматика и телемеханика. 2014. № 4. С. 153–169.

Водян Максим Евгеньевич
Панин Артём Александрович
Плясунов Александр Владимирович

Статья поступила
29 ноября 2024 г.
После доработки —
2 февраля 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 43–70

UDC 519.8 DOI: 10.33048/daio.2025.32.821

MAXIMIZING THE THRESHOLD STABILITY IN THE MODEL OF FACILITY LOCATION AND THE MILL PRICING

M. E. Vodyan[a], *A. A. Panin*[b], and *A. V. Plyasunov*[c]

Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue, 630090 Novosibirsk, Russia
E-mail: [a]m.vodyan@g.nsu.ru,
[b]aapanin1988@gmail.com, [c]apljas@math.nsc.ru

Abstract. We study the threshold stability of the problem with the median location of facilities and mill pricing. The problem of threshold stability has the following differences from the original two-level formulation: in the top-level problem, the deviation of consumer budgets from expected values is maximized provided that the producer's income is not less than a given threshold. The problem statement considered in this paper differs from those previously studied in that the pricing problem is NP-hard in the strong sense when the location of facilities is fixed.

A variable neighborhoods descent based algorithm (VND) to solve the threshold stability problem is proposed. Numerical investigation of the algorithm is carried out on known examples and randomly generated data. The experiment shows that iteratively subtracting the threshold stability radius from the consumer budgets, which is first implemented in this paper, strongly reduces the running time of the algorithm. On the examples with the optimum known, the algorithm was wrong on average by 0.63%. In all the examples, the algorithm finds a solution on average 2.97% better than the Gurobi solver. Tab. 4, illustr. 2, bibliogr. 33.

Keywords: bilevel problem, threshold stability, radius of threshold stability, facility location, mill pricing, variable neighborhood descent.

References

1. **A. A. Panin** and **A. V. Plyasunov,** Stability analysis for pricing, in *Mathematical Optimization Theory and Operations Research*, Rev. Sel. Pap. 19th Int. Conf. MOTOR 2020 (Novosibirsk, Russia, July 6–10, 2020) (Springer, Cham, 2020), pp. 57–69 (Commun. Comput. Inf. Sci., Vol. 1275).

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

2. **A. A. Panin** and **A. V. Plyasunov,** The multilevel facility location and pricing problems: The computational complexity and the stability analysis, *Optim. Lett.* **17** (6), 1295–1315 (2023), DOI: 10.1007/s11590-022-01924-3.
3. **M. E. Vodyan, A. A. Panin,** and **A. V. Plyasunov,** Metaheuristics for finding the stability radius in the bilevel facility location and uniform pricing problem, in *Proc. 19th Int. Asian School-Seminar Optimization Problems of Complex Systems* (Novosibirsk, Russia, Aug. 14–22, 2023) (IEEE, Piscataway, 2023), pp. 130–135, DOI: 10.1109/OPCS59592.2023.10275325.
4. **M. E. Vodyan, A. A. Panin,** and **A. V. Plyasunov,** A study of the threshold stability of the bilevel problem of facility location and discriminatory pricing, *Diskretn. Anal. Issled. Oper.* **31** (3), 79–104 (2024) [Russian] [*J. Appl. Ind. Math.* **18** (3) 558–574 (2024), DOI: 10.1134/S1990478924030165].
5. **M. Dyer** and **L. Stougie,** Computational complexity of stochastic programming problems, *Math. Program, Ser. A*, **106** (3), 423–432 (2006), DOI: 10.1007/s10107-005-0597-0.
6. **A. I. Kibzun** and **Yu. S. Kan,** *Stochastic Programming Problems with Probability Criteria* (Fizmatlit, Moscow, 2009) [Russian].
7. **A. Ben-Tal** and **A. Nemirovski,** Robust optimization — Methodology and applications, *Math. Program, Ser. B*, **92** (3), 453–480 (2002), DOI: 10.1007/s101070100286.
8. **L. V. Snyder,** Facility location under uncertainty: A review, *IIE Trans.* **38**, 537–554 (2006), DOI: 10.1080/07408170500216480.
9. **H. J. Greenberg,** An annotated bibliography for post-solution analysis in mixed integer programming and combinatorial optimization, in *Advances in Computational and Stochastic Optimization, Logic Programming, and Heuristic Search* (Springer, New York, 1998), pp. 97–147, DOI: 10.1007/978-1-4757-2807-1_4.
10. **I. Correia, F. S. da Gama,** Facility location under uncertainty, in *Location Science* (Springer, Cham, 2015), pp. 177–203.
11. **A. Ben-Tal** and **A. Nemirovski,** Robust solutions of uncertain linear programs, *Oper. Res. Lett.* **25** (1), 1–13 (1999).
12. **G. Yu** and **J. Yang,** On the shortest path problem, *Comput. Oper. Res.* **25** (6), 457–68 (1988).
13. **P. Kouvelis** and **G. Yu,** *Robust Discrete Optimization and Its Applications* (Kluwer Acad. Publ., Dordrecht, 1997).
14. **I. Averbakh** and **V. Lebedev,** Interval data minmax regret network optimization problems, *Discrete Appl. Math.* **138**, 289–301 (2004).
15. **H. Aissi, C. Bazgan,** and **D. Vanderpooten,** Complexity of the min-max and min-max regret assignment problems, *Oper. Res. Lett.* **33** (6), 634–640 (2005).
16. **E. Carrizosa** and **S. Nickel,** Robust facility location, *Math. Methods Oper. Res.* **58** (2), 331–349 (2003).
17. **E. Carrizosa, A. Ushakov,** and **I. Vasilyev,** Threshold robustness in discrete facility location problems: A bi-objective approach, *Optim. Lett.* **9** (7), 1297–1314 (2015).

18. **V. K. Leontiev,** Stability of the travelling salesman problem, *Zh. Vychisl. Mat. Mat. Fiz.* **15** (5), 1298–1309 (1975) [Russian] [*USSR Comput. Math. Math. Phys.* **15** (5), 199–213 (1975), 10.1016/0041-5553(75)90116-0].
19. **A. Rossi, E. Gurevsky, O. Battaia,** and **A. Dolgui,** Maximizing the robustness for simple assembly lines with fixed cycle time and limited number of workstations, *Discrete Appl. Math.* **208**, 123–136 (2016).
20. **E. Gurevsky, A. Rasamimanana, A. Pirogov, A. Dolgui,** and **A. Rossi,** Stability factor for robust balancing of simple assembly lines under uncertainty, *Discrete Appl. Math.* **318**, 113–132 (2022).
21. **A. Pirogov, E. Gurevsky, A. Rossi,** and **A. Dolgui,** Robust balancing of transfer lines with blocks of uncertain parallel tasks under fixed cycle time and space restrictions, *Eur. J. Oper. Res.* **290**, 946–955 (2021).
22. **Yu. N. Sotskov,** Assembly and production line designing, balancing and scheduling with inaccurate data: A survey and perspectives, *Algorithms* **16** (2), ID 100 (2023).
23. **V. K. Leontiev** and **È. N. Gordeev,** Qualitative investigation of path problems, *Kibernetika*, No. 5, 82–89 (1986) [Russian] [**22** (5) 636–646 (1986), DOI: 10.1007/BF01068361].
24. **Yu. N. Sotskov, V. K. Leontiev,** and **É. N. Gordeev,** Some concepts of stability analysis in combinatorial optimization, *Discrete Appl. Math.* **58** (2), 169–190 (1995).
25. **K. G. Kuzmin,** A general approach to the calculation of stability radii for the max-cut problem with multiple criteria, *Diskretn. Anal. Issled. Oper.* **22** (5), 30–51 (2015) [Russian] [*J. Appl. Ind. Math.* **9** (4) 527–539 (2015), DOI: 10.1134/S1990478915040092].
26. **S. Dempe** and **A. Zemkoho,** *Bilevel Optimization: Advances and Next Challenges* (Springer, Cham, 2020) (Springer Optim. Its Appl., Vol. 161), DOI: 10.1007/978-3-030-52119-6.
27. **E.-G. Talbi,** *Metaheuristics: From Design to Implementation* (Wiley, Berlin, 2009).
28. **N. Mladenović** and **P. Hansen,** Variable neighbourhood search, *Comput. Oper. Res.* **24**, 1097–1100 (1997).
29. **Yu. A. Kochetov, N. Mladenović,** and **P. Hansen,** Local variable neighbourhood search, *Diskretn. Anal. Issled. Oper., Ser. 2*, **10** (1), 11–43 (2003) [Russian].
30. **Z. S. Diakova** and **Yu. A. Kochetov,** A double VNS heuristic for the facility location and pricing problem, *Electron. Notes Discrete Math.* **39**, 29–34 (2012), DOI: 10.1016/j.endm.2012.10.005.
31. **Yu. A. Kochetov, A. A. Panin,** and **A. V. Plyasunov,** Comparison of metaheuristics for the bilevel facility location and mill pricing problem, *Diskretn. Anal. Issled. Oper.* **22** (3), 36–54 (2015) [Russian] [*J. Appl. Ind. Math.* **9** (3) 392–401 (2015), DOI: 10.1134/S1990478915030102].
32. **P. Hanjoul, P. Hansen, D. Peeters,** and **J.-F. Thisse,** Uncapacitated plant location under alternative spatial price policies, *Manag. Sci.* **36** (1), 41–57 (1990), DOI: 10.1287/mnsc.36.1.41.

33. A. A. Panin, M. G. Pashchenko, and **A. V. Plyasunov,** Bilevel competitive facility location and pricing problems, *Avtom. Telemekh.*, No. 4, 153–169 (2014) [Russian] [*Autom. Remote Control* **75** (4), 715–727 (2014), DOI: 10.1134/S0005117914040110].

Maksim E. Vodyan
Artyom A. Panin
Aleksandr V. Plyasunov

Received November 29, 2024
Revised February 2, 2025
Accepted June 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 71–83

УДК 519.8 DOI: 10.33048/daio.2025.32.829

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ЗАДАЧИ СИНТЕЗА АНТЕННОЙ РЕШЁТКИ

А. В. Еремеев

Институт математики им. С. Л. Соболева,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия

E-mail: eremeev@ofim.oscsbras.ru

Аннотация. Рассматривается задача синтеза фазированной антенной решётки, которая заключается в выборе фаз и амплитуд для всех излучающих элементов, когда требуется, чтобы получаемая диаграмма направленности по каждому рассматриваемому направлению принадлежала заданному множеству. Установлено, что поиск допустимого решения является NP-трудной в сильном смысле задачей в случае, когда по каждому рассматриваемому направлению допускается одно или два значения мощности излучения. Кроме того, доказана NP-трудность поиска допустимого решения в задаче синтеза частично заполненной антенной решётки, когда требуется, чтобы получаемая диаграмма направленности по каждому рассматриваемому направлению принадлежала заданному интервалу и амплитуды всех излучателей были одинаковы. Библиогр. 19.

Ключевые слова: вычислительная сложность, антенная решётка, сводимость, NP-полнота.

Введение

Фазированная антенная решётка (ФАР) представляет собой совокупность излучателей, подключённых к устройствам, обеспечивающим требуемое распределение фаз и амплитуд на этих излучателях. ФАР широко используются в диапазоне сверхвысоких частот для получения излучения с заданной диаграммой направленности (см., например, [1]). В диапазоне высоких частот, который соответствует коротким волнам, такие системы позволяют получить увеличение энергии канала связи или сокращение занимаемого пространства [2, 3].

Задача синтеза ФАР заключается в выборе фаз и амплитуд для всех излучающих элементов, когда требуется, чтобы получаемая диаграмма

направленности по каждому из рассматриваемых направлений принадлежала заданному множеству. В некоторых формулировках задачу синтеза ФАР удаётся решить с использованием методов выпуклого программирования [4, 5] или методов линейной алгебры [6, 7]. В частности, в [8] показано, что задачей выпуклого программирования является отыскание возбуждений заданного набора произвольно расположенных источников таким образом, чтобы создать интенсивность дальнего поля, которая максимальна в заданном направлении и подчиняется произвольным верхним границам в других направлениях. Однако, многие авторы вынуждены использовать более трудоёмкие методы, разработанные для решения многоэкстремальных задач, такие как мультистарт градиентной оптимизации [9, 10], метаэвристики [11, 12], методы, основанные на полуопределённой релаксации [13] и т. д.

В настоящей работе для двух вариантов задачи синтеза ФАР доказывается NP-трудность в сильном смысле. Первый вариант соответствует постановке из [13], но имеет специфические требования к диаграмме направленности. Второй вариант предполагает синтез фаз в излучателях частично заполненной решётки с более реалистичными требованиями относительно диаграммы направленности. NP-трудность вытекает из полученных в теоремах 1 и 2 свойств NP-полноты соответствующих задач распознавания, сформулированных в разд. 1 и 2.

1. Задача синтеза фазированной антенной решётки

Рассмотрим ФАР, состоящую из N излучающих элементов, размещённых в точках $\mathbf{r}_1, \ldots, \mathbf{r}_N \in \mathbb{R}^3$. Для упрощения обозначений задача описана в случае, когда диаграмма направленности параметризована только значениями полярного угла θ в фиксированной азимутальной плоскости, которая опущена в обозначениях. Обобщение на случай, когда диаграмма направленности задаётся как по азимутальному, так и по полярному угловому направлению, существенно не усложнит задачу.

Пусть каждый элемент k создаёт парциальное поле $g_k(\theta)$ в направлении θ, т. е. $g_k(\theta)$ — напряжённость электромагнитного поля, создаваемого в направлении θ на большом расстоянии (т. е. когда размеры ФАР пренебрежимо малы по сравнению с расстоянием до приёмника) при протекании единичного тока через излучающий элемент k. Тогда на большом расстоянии напряжённость поля $f(\theta)$, излучаемого всей ФАР в направлении θ, имеет вид (см., например, [13] или подробнее в [14, § 1.13])

$$f(\theta) = \mathbf{a}(\theta)^{\mathsf{H}}\mathbf{w}, \tag{1}$$

$$\mathbf{a}(\theta) = (g_1(\theta)e^{2\pi j\langle \mathbf{r}_1, \mathbf{r}(\theta)\rangle/\lambda}, \ldots, g_N(\theta)e^{2\pi j\langle \mathbf{r}_N, \mathbf{r}(\theta)\rangle/\lambda}), \tag{2}$$

где λ — длина волны, j — мнимая единица, $\langle\cdot,\cdot\rangle$ — скалярное произведение, $\mathbf{w}$ — комплексный вектор возбуждения, определяющий как амплитуду тока $|w_k|$, так и его фазу $\operatorname{Arg} w_k$ в каждом излучателе k. Наконец, $\mathbf{r}(\theta)$ — единичный вектор в направлении θ, а верхний индекс $^{\mathsf{H}}$ обозначает эрмитову транспозицию вектора. Введём обозначения

$$\mathbf{a}_i = \mathbf{a}(\theta_i), \quad f_i = f(\theta_i) = \mathbf{a}_i^{\mathsf{H}}\mathbf{w}, \quad \mathbf{x} = (\operatorname{Re}\mathbf{w}, \operatorname{Im}\mathbf{w})^\top \in \mathbb{R}^{2N\times 1},$$

$$\mathbf{A}_i = \begin{pmatrix} \operatorname{Re}\mathbf{a}_i^\top & -\operatorname{Im}\mathbf{a}_i^\top \\ \operatorname{Im}\mathbf{a}_i^\top & \operatorname{Re}\mathbf{a}_i^\top \end{pmatrix} = \begin{pmatrix} a_i^{(11)} & \dots & a_i^{(1,2N)} \\ a_i^{(21)} & \dots & a_i^{(2,2N)} \end{pmatrix} \in \mathbb{R}^{2\times 2N}.$$

Вещественнозначная версия (1), (2) для напряжённости поля в направлении θ_i тогда примет вид (подробнее см., например, [9, п. 2.1])

$$(\operatorname{Re} f_i, \operatorname{Im} f_i)^\top = \mathbf{A}_i\mathbf{x}. \tag{3}$$

Мощность, излучаемая ФАР в направлении θ_i, равна

$$|f_i|^2 = \mathbf{x}^\top\mathbf{Q}_i\mathbf{x}, \quad \mathbf{Q}_i = \mathbf{A}_i^\top\mathbf{A}_i. \tag{4}$$

Задача синтеза ФАР (см., например, [13]) сводится к поиску вектора возбуждений $\mathbf{x}$ такого, что для всех направлений $i = 1,\dots,I$ мощность $|f_i|^2$, излучаемая решёткой в направлении i, принадлежит заданному подмножеству $\mathcal{C}_i \subset \mathbb{R}$.

Эта задача полагалась NP-трудной в [13] без строгого доказательства. Очевидно, что она не проще, чем следующая задача распознавания, которую назовём распознавательным вариантом дискретной задачи синтеза ФАР.

Задача 1 (дискретная задача синтеза ФАР). *Дано $I \in \mathbb{N}$ целочисленных $(2\times 2N)$-матриц $\mathbf{A}_i$, $i = 1,\dots,I$, и $2I$ целочисленных значений $\alpha_i \leqslant \beta_i$, $i = 1,\dots,I$. Существует ли вектор $\mathbf{x} \in \mathbb{R}^{2N}$ такой, что*

$$\mathbf{x}^\top\mathbf{A}_i^\top\mathbf{A}_i\mathbf{x} \in \{\alpha_i, \beta_i\}, \quad i = 1,\dots,I? \tag{5}$$

Теорема 1. *Распознавательный вариант дискретной задачи синтеза* ФАР *является* NP*-полной в сильном смысле задачей.*

Перед доказательством теоремы получим следующую техническую лемму, которая предполагает определённую координацию (синхронизацию) возбуждений в элементах $k = 1,\dots,N-1$ с элементом N.

Лемма 1. *Если $N \geqslant 3$ и система ограничений содержит условия*

$$\mathbf{x}^\top\mathbf{Q}_k\mathbf{x} = x_k^2 + x_{N+k}^2 \in \{0,1\}, \quad k < N, \tag{6}$$

$$\mathbf{x}^\top\mathbf{Q}_N\mathbf{x} = x_N^2 + x_{2N}^2 = 1, \tag{7}$$

$$\mathbf{x}^\top\mathbf{Q}_{N+k}\mathbf{x} = 4x_k^2 + 4x_{N+k}^2 + x_N^2 + x_{2N}^2 + 4x_kx_N + 4x_{N+k}x_{2N} = 1, \quad k < N, \tag{8}$$

то для любых $k, \ell < N$ перекрёстные произведения удовлетворяют равенству

$$x_k x_\ell + x_{N+k} x_{N+\ell} = \begin{cases} 1, & \text{если } x_k^2 + x_{N+k}^2 = x_\ell^2 + x_{N+\ell}^2 = 1, \\ 0 & \text{в противном случае.} \end{cases} \tag{9}$$

Доказательство. Очевидно, что если имеет место $x_k^2 + x_{N+k}^2 = 0$ или $x_\ell^2 + x_{N+\ell}^2 = 0$, то немедленно получаем $x_k x_\ell + x_{N+k} x_{N+\ell} = 0$, что удовлетворяет (9).

Рассмотрим случай $x_k^2 + x_{N+k}^2 = x_\ell^2 + x_{N+\ell}^2 = 1$. Тогда условие (8) означает, что

$$x_k x_N + x_{N+k} x_{2N} = -1. \tag{10}$$

Легко видеть, что при условии $x_k^2 + x_{N+k}^2 = x_N^2 + x_{2N}^2 = 1$ минимум выражения $x_k x_N + x_{N+k} x_{2N}$ равен -1, и он достигается тогда и только тогда, когда $x_k = -x_N$, $x_{N+k} = -x_{2N}$. Как раз этого и требует условие (10) для всех $k < N$, поэтому в рассматриваемом случае $x_k x_\ell + x_{N+k} x_{N+\ell} = x_N^2 + x_{2N}^2 = 1$, где последнее равенство следует из условия (7). Лемма 1 доказана.

Как видно из леммы 1, ограничения (8) обеспечивают согласование фаз во всех излучающих элементах $k < N$ с фазой в элементе N, которая может быть произвольной.

Доказательство теоремы 1. Прежде всего отметим, что распознавательный вариант дискретной задачи синтеза ФАР принадлежит классу NP. Далее к рассматриваемой задаче распознавания сведём NP-полную в сильном смысле задачу Независимое множество (см., например, [15]).

Задача 2 (Независимое множество). *Даны граф $G = (V, E)$ и целое число $K > 0$. Содержит ли граф G подмножество попарно несмежных вершин S мощности K (т. е. независимое множество S, $|S| = K$)?*

Пусть $n = |V|$, $m = |E|$, $V = \{v_1, \ldots, v_n\}$, а ребро с номером $r = 1, \ldots, m$ имеет вид $e_r = v_{k(r)} v_{\ell(r)}$.

Для заданного графа G, т. е. примера задачи Независимое множество, построим пример распознавательной дискретной задачи синтеза ФАР следующим образом. Пусть $N = n + 1$ и все N векторов $\mathbf{a}_1, \ldots, \mathbf{a}_N$ вещественнозначны:

$$\mathbf{a}_1 = (1, 0, 0 \ldots, 0)^\top, \quad \mathbf{a}_2 = (0, 1, 0 \ldots, 0)^\top, \quad \ldots, \quad \mathbf{a}_N = (0, 0, \ldots, 0, 1)^\top.$$

Тогда для любого $k = 1, \ldots, N$ все элементы матрицы $\mathbf{A}_k$ нулевые, за исключением $a_k^{(1,k)} = a_k^{(2,N+k)} = 1$.

Подмножества $\mathcal{C}_k$, $k = 1, \ldots, n$, задаются двумя допустимыми значениями излучаемой мощности $\alpha_k = 0$, $\beta_k = 1$. Тем самым $\mathbf{Q}_k = \mathbf{A}_k^\top \mathbf{A}_k$, где все элементы равны нулю, за исключением $q_k^{(kk)} = q_k^{(N+k,N+k)} = 1$ при $k = 1, \ldots, n$, т. е. первые n ограничений в системе (5) имеют вид

$$x_k^2 + x_{N+k}^2 \in \{0, 1\}, \quad k = 1, \ldots, n. \tag{11}$$

Ограничения (11) задают альтернативу (0 или 1) для амплитуды возбуждения в излучающих элементах $1, \ldots, n$, что соответствует альтернативе в задаче Независимое множество: либо включить вершину v_k в набор S (когда $x_k^2 + x_{N+k}^2 = 1$), либо пропустить эту вершину (когда $x_k^2 + x_{N+k}^2 = 0$).

Для последнего элемента ФАР фиксируем единичную амплитуду:

$$x_N^2 + x_{2N}^2 = 1, \tag{12}$$

поэтому $\mathcal{C}_N = \{1\}$. Этот элемент ФАР используем для координации фаз во всех других излучающих элементах в том же смысле, в каком элемент с номером N используется в лемме 1. С этой целью в каждом векторе $\mathbf{a}_{N+k}$, $k = 1, \ldots, n$, положим действительную часть k-го компонента равной 2, а действительную часть компонента N положим равной 1. Остальные действительные и все мнимые части комплексного вектора $\mathbf{a}_{N+k}$ полагаются равными 0. Тогда для любого $k = 1, \ldots, n$ все элементы матрицы $\mathbf{A}_{N+k}$ нулевые, за исключением $a_{N+k}^{(1k)} = a_{N+k}^{(2,N+k)} = 2$ и $a_{N+k}^{(1N)} = a_{N+k}^{(2,N)} = 1$.

Подмножества $\mathcal{C}_{N+k}$, $k = 1, \ldots, n$, состоят из одного элемента, равного 1: $\alpha_k = 1$, $\beta_k = 1$ для $k = N+1, \ldots, N+n$. Тогда для любого $k = 1, \ldots, n$ справедливо $\mathbf{Q}_{N+k} = \mathbf{A}_{N+k}^\top \mathbf{A}_{N+k}$, где все элементы равны нулю, за исключением четырёх элементов, соответствующих действительным частям: $q_{N+k}^{(kk)} = 4$, $q_{N+k}^{(N,N)} = 1$, $q_{N+k}^{(kN)} = 2$, $q_{N+k}^{(Nk)} = 2$, и четырёх элементов, соответствующих мнимым частям:

$$q_{N+k}^{(N+k,N+k)} = 4, \quad q_{N+k}^{(2N,2N)} = 1, \quad q_{N+k}^{(N+k,2N)} = 2, \quad q_{N+k}^{(2N,N+k)} = 2.$$

Следовательно, матрицы $\mathbf{Q}_{N+k}, k = 1, \ldots, n$, определяют ограничения

$$4x_k^2 + 4x_{N+k}^2 + x_N^2 + x_{2N}^2 + 4x_k x_N + 4x_{N+k} x_{2N} = 1, \tag{13}$$

где $k = 1. \ldots, n$. Заметим, что ввиду леммы 1 ограничения (13) вместе с (12) дают

$$x_k x_\ell + x_{N+k} x_{N+\ell} \in \{0, 1\}, \quad k = 1, \ldots, n, \; \ell = 1, \ldots, n. \tag{14}$$

Чтобы представить граф в терминах дискретной задачи синтеза ФАР, для каждого ребра e_r, $r = 1, \ldots, m$, положим равными 1 действительные части двух компонент с индексами $k(r)$ и $\ell(r)$ в векторе $\mathbf{a}_{N+n+r}$, остальные действительные части $\operatorname{Re} \mathbf{a}_{N+n+r}$ полагаем равными нулю, как

и все мнимые части, т. е. $\operatorname{Im}\mathbf{a}_{N+n+r} = (0,0,\ldots,0)^\top$. Тогда для любого $r = 1,\ldots,m$ матрица $\mathbf{A}_{N+n+r}$ состоит из нулевых элементов, за исключением

$$a_{N+n+r}^{(1,k(r))} = a_{N+n+r}^{(1,\ell(r))} = a_{N+n+r}^{(2,N+k(r))} = a_{N+n+r}^{(2,N+\ell(r))} = 1.$$

Подмножества $\mathcal{C}_{N+n+r}$ снова состоят из двух элементов, нуля и единицы: $\alpha_i = 0$, $\beta_i = 1$ для $i = N+n+1,\ldots,N+n+m$. Тогда для любого $r = 1,\ldots,m$ имеем $\mathbf{Q}_{N+n+r} = \mathbf{A}_{N+n+r}^\top \mathbf{A}_{N+n+r}$, где все элементы равны нулю, за исключением четырёх элементов, соответствующих действительным частям:

$$q_{N+n+r}^{(k(r),k(r))} = q_{N+n+r}^{(\ell(r),\ell(r))} = q_{N+n+r}^{(k(r),\ell(r))} = q_{N+n+r}^{(\ell(r),k(r))} = 1,$$

и четырёх элементов, соответствующих мнимым частям:

$$q_{N+n+r}^{(N+k(r),N+k(r))} = q_{N+n+r}^{(N+\ell(r),N+\ell(r))} = q_{N+n+r}^{(N+k(r),N+\ell(r))} = q_{N+n+r}^{(N+\ell(r),N+k(r))} = 1.$$

Следовательно, матрицы $\mathbf{Q}_{N+n+r}$, $r = 1,\ldots,m$, определяют ограничения

$$x_{k(r)}^2 + x_{N+k(r)}^2 + x_{\ell(r)}^2 + x_{N+\ell(r)}^2 + \\ + 2x_{k(r)}x_{\ell(r)} + 2x_{N+k(r)}x_{N+\ell(r)} \in \{0,1\}, \quad r = 1,\ldots,m, \quad (15)$$

которые вместе с (14) показывают, что должно выполняться хотя бы одно из равенств $x_{k(r)}^2 + x_{N+k(r)}^2 = 0$, $x_{\ell(r)}^2 + x_{N+\ell(r)}^2 = 0$. Это соответствует требованию, чтобы оба конца ребра e_r не принадлежали одновременно множеству S.

Для подсчёта числа излучающих элементов с единичной амплитудой возбуждения определим вектор $\mathbf{a}_I$, $I = N+n+m+1$, равенствами

$$\operatorname{Re}\mathbf{a}_I = (1,1,\ldots,1,0)^\top, \quad \operatorname{Im}\mathbf{a}_I = (0,0,\ldots,0,0)^\top,$$

т. е.

$$\mathbf{A}_I = \begin{pmatrix} 1,\ldots,1,0 & 0,\ldots,0,0 \\ 0,\ldots,0,0 & 1,\ldots,1,0 \end{pmatrix},$$

и в $\mathbf{Q}_I = \mathbf{A}_I^\top \mathbf{A}_I$ имеем $q_I^{(k\ell)} = q_I^{(N+k,N+\ell)} = 1$ для всех $k,\ell = 1,\ldots,n$, остальные элементы в $\mathbf{Q}_I$ равны нулю.

Пусть $M = \bigl\{k \in \{1,\ldots,n\} \mid x_k^2 + x_{N+k}^2 = 1\bigr\}$. Тогда

$$\mathbf{x}^\top \mathbf{Q}_I \mathbf{x} = \sum_{k,\ell \in M} (x_k x_\ell + x_{N+k} x_{N+\ell}) = |M|^2 \quad (16)$$

в силу леммы 1 и определения множества M.

Наконец, положим $\alpha_I = \beta_I = K^2$, т. е. последнее ограничение в задаче синтеза ФАР имеет вид

$$\mathbf{x}^\top \mathbf{Q}_I \mathbf{x} = |K|^2. \quad (17)$$

С одной стороны, если этот экземпляр распознавательной задачи синтеза ФАР имеет допустимое решение, то из (16) следует, что $|M| = K$,

а множество вершин $S = \{v_i \mid i \in M\}$ является независимым в графе G и имеет размер K. С другой стороны, если $|S| = K$ в задаче Независимое множество, то можно положить $x_k = 1$ для всех $k \leqslant n$ таких, что $v_k \in S$, и для $k = n + 1$, а остальные компоненты вектора $\mathbf{x}$ установить равными нулю. Легко проверить, что все ограничения соответствующего экземпляра распознавательной задачи синтеза ФАР выполнены.

Следовательно, индивидуальная задача Независимое множество имеет положительный ответ тогда и только тогда, когда построенный нами пример имеет положительный ответ, и это построение выполнимо за полиномиальное время. Таким образом, распознавательный вариант дискретной задачи синтеза ФАР — NP-полная задача. Более того, эта задача NP-полна в сильном смысле, поскольку числовые параметры построенного примера полиномиально ограничены от размера графа в исходной задаче Независимое множество. Теорема 1 доказана.

2. Интервальная задача синтеза фаз в частично заполненной антенной решётке

Как правило, излучатели ФАР располагаются некоторым регулярным образом с фиксированным шагом, например, на линии, в узлах прямоугольной решётки, в вершинах правильного многоугольника и т. п. Однако в некоторых случаях могут использоваться и *прореженные* ФАР, в которых часть регулярных позиций не заполнена. Пусть $\mathbf{r}_1, \ldots, \mathbf{r}_N \in \mathbb{R}^3$ далее описывают расположение регулярных позиций. Прореженные ФАР, таким образом, имеют менее N излучателей, что выгодно снижает стоимость и взаимное влияние между элементами, но также невыгодно повышает излучаемую мощность в нежелательных направлениях (см., например, [14, 16, § 1.17]). Прореженные ФАР, в которых все элементы имеют одинаковую мощность возбуждения, могут быть основаны на случайном расположении элементов (см., например, [17, 18, гл. 7]) или специально выбранном подмножестве регулярных положений излучателей, например, с использованием разностных множеств [16, 19].

Некоторое снижение излучаемой мощности в нежелаемых направлениях может быть получено путём подачи неравных по амплитуде возбуждений на элементы антенны. Как отмечено в [16], недостаток этого подхода заключается в том, что усиление ФАР будет меньше, чем у решётки, в которой полная мощность прикладывается ко всем элементам, что также согласуется с результатами вычислительных экспериментов в [9, § 3.2]. В связи с этим в этом разделе рассмотрим задачу синтеза ФАР, где амплитуды возбуждения не подлежат оптимизации.

Задача заключается в выборе подмножества излучателей из заданной ФАР, состоящей из N элементов, и в назначении фаз возбуждения

выбранным элементам так, чтобы для всех направлений $i = 1, \ldots, I$ мощность, излучаемая решёткой в направлении i, принадлежала соответствующему интервальному подмножеству $\mathcal{C}_i = [L_i, U_i] \subset \mathbb{R}$. Без потери общности можно предположить, что амплитуда в каждом элементе равна 1. Очевидно, что такая задача синтеза ФАР не будет проще следующей задачи распознавания, которую назовём распознавательным вариантом задачи синтеза частично заполненной ФАР.

Задача 3 (синтез частично заполненной ФАР). *Даны $I \in \mathbb{N}$ целочисленных $(2 \times 2N)$-матриц $\mathbf{A}_i$, $i = 1, \ldots, I$, и $2I$ целочисленных значений $L_i \leqslant U_i$, $i = 1, \ldots, I$. Существует ли вектор $\mathbf{x} \in \mathbb{R}^{2N}$ такой, что*

$$x_k^2 + x_{N+k}^2 \in \{0, 1\}, \quad k = 1, \ldots, N, \tag{18}$$

$$\mathbf{x}^\top \mathbf{A}_i^\top \mathbf{A}_i \mathbf{x} \in [L_i, U_i], \quad i = 1, \ldots, I? \tag{19}$$

Условие (18) здесь подразумевает, что излучающий элемент создаётся на позиции k тогда и только тогда, когда $x_k^2 + x_{N+k}^2 \in \{0, 1\}$.

Заметим, что в отличие от распознавательного варианта дискретной задачи синтеза ФАР, сформулированная здесь задача требует, чтобы излучаемая мощность в каждом направлении $i = 1, \ldots, I$ принадлежала непрерывному интервалу $[L_i, U_i]$, а не дискретному множеству $\{\alpha_i, \beta_i\}$. В этом смысле распознавательный вариант задачи синтеза частично заполненной ФАР имеет более реалистичную постановку.

Теорема 2. *Распознавательный вариант задачи синтеза частично заполненной* ФАР *является* NP*-полной в сильном смысле задачей.*

Доказательство аналогично доказательству теоремы 1 с тем отличием, что здесь при построении сводимости не требуются ограничения (11), так как они следуют из условия (18), содержащегося в формулировке задачи. Аналоги всех прочих ограничений — (12), (13), (15) и (17) — отличаются тем, что в правой части содержат интервалы $[L_i, U_i]$, где $L_i = \alpha_i$, $U_i = \beta_i$. Теорема 2 доказана.

Заключение

С использованием эффективной сводимости известной NP-полной задачи Независимое множество показано, что поиск допустимого возбуждения ФАР является NP-трудной в сильном смысле задачей в случае, когда по каждому направлению допускается одно или два значения мощности излучения (теорема 1). Формально эта задача является частным случаем рассмотренной в [13] задачи синтеза ФАР. Однако более реалистичной постановкой является другой частный случай, когда по каждому направлению задан непрерывный интервал для мощности излучения

(интервальная постановка). Частный случай этой задачи, когда допустимые интервалы на излучаемую мощность представляют собой верхние границы, эффективно разрешим [8]. Предполагается, что дальнейшие исследования позволят уточнить границу, разделяющую труднорешаемые варианты задачи синтеза ФАР от эффективно разрешимых случаев.

В работе также рассмотрена модификация интервальной постановки задачи, когда в каждой известной позиции можно установить или не устанавливать излучающий элемент, амплитуды всех излучателей одинаковы, а фазы излучателей требуется найти. NP-трудность поиска допустимого решения для этой задачи следует из теоремы 2.

Автор благодарен А. С. Юркову за полезные замечания и М. Н. Макурину за указание на известные результаты по прореженным ФАР.

Финансирование работы

Исследование выполнено в рамках государственного задания Института математики им. С. Л. Соболева (проект № FWNF–2022–0020). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Автор заявляет, что у него нет конфликта интересов.

Литература

1. **Hansen R. C.** Phased array antennas. Hoboken, NJ: John Wiley & Sons, 1979. 580 p.
2. **Kudzin V. P., Lozovsky V. N., Shlyk N. I.** The compact linear antenna array system of the short-wave band consisting of “butterfly” radiators // Proc. 9th Int. Conf. Antenna Theory and Techniques (Odessa, Ukraine, Sept. 16–20, 2013). Piscataway: IEEE, 2013. P. 252–253.
3. **Wilensky R.** High-power, broad-bandwidth HF dipole curtain array with extensive vertical and azimuthal beam control // IEEE Trans. Broadcast. 1988. V. 34, No. 2. P. 201–209. DOI: 10.1109/11.1437.
4. **Echeveste J. I., González de Aza M. A., Zapata J.** Shaped beam synthesis of real antenna arrays via finite-element method, floquet modal analysis, and convex programming // IEEE Trans. Antennas Propag. 2016. V. 64, No. 4. P. 1279–1286. DOI: 10.1109/TAP.2016.2526038.
5. **Bucci O., Caccavale L., Isernia T.** Optimal far-field focusing of uniformly spaced arrays subject to arbitrary upper bounds in non-target directions // IEEE Trans. Antennas Propag. 2002. V. 50, No. 11. P. 1539–1554. DOI: 10.1109/TAP.2002.803959.
6. **Юрков А. С.** Оптимизация возбуждения передающих фазированных антенных решёток декаметрового диапазона длин волн. Омск: ОНИИП, 2014. 65 с.

7. **Юрков А. С.** Максимизация направленности фазированных антенных решёток коротковолнового диапазона // Техника радиосвязи. 2016. № 2. С. 46–53.
8. **Isernia T., Di Iorio P., Soldovieri F.** An effective approach for the optimal focusing of array fields subject to arbitrary upper bounds // IEEE Trans. Antennas Propag. 2000. V. 48, No. 12. P. 1837–1847. DOI: 10.1109/8.901272.
9. **Тюнин Н. Н.** Задачи невыпуклого квадратичного программирования, связанные с оптимизацией фазированных антенных решёток // Дискрет. анализ и исслед. операций. 2021. Т. 28, № 3. С. 65–89.
10. **Indenbom M., Izhutkin V., Sharapov A., Zonov A.** Synthesis of conical phased antenna arrays optimization of amplitude distribution parameters // Proc. 9th Int. Conf. Optimization and Applications (Petrovac, Montenegro, Oct. 1–5, 2018). Lancaster, PA: DEStech Publ., 2018. P. 273–285.
11. **Akdagli A., Guney K.** Shaped-beam pattern synthesis of equally and unequally spaced linear antenna arrays using a modified tabu search algorithm algorithm // Microw. Opt. Technol. Lett. 2003. V. 36, No. 1. P. 16–20. DOI: 10.1002/mop.10657.
12. **Villegas F. J.** Parallel genetic-algorithm optimization of shaped beam coverage areas using planar 2-D phased arrays // IEEE Trans. Antennas Propag. 2007. V. 55, No. 6. P. 1745–1753. DOI: 10.1109/TAP.2007.898601.
13. **Fuchs B.** Application of convex relaxation to array synthesis problems // IEEE Trans. Antennas Propag. 2014. V. 62, No. 2. P. 634–640.
14. **Щелкунов С. А., Фриис Г. Т.** Антенны: Теория и практика. М.: Советское радио, 1955. 604 с.
15. **Garey M. R., Johnson D. S.** Computers and intractability: A guide to the theory of NP-completeness. San Francisco: Freeman, 1979. 338 p.
16. **Leeper D. G.** Thinned aperiodic antenna arrays with improved peak sidelobe level control. US Patent 4,071,848 (Jan 31, 1978). Murray Hill, NJ: Bell Teleph. Lab., 1976. URL: patentimages.storage.googleapis.com/30/73/fa/25b9b72c3d3e8a/US4071848.pdf (accessed: 20.09.2025).
17. **Steinberg B. D.** The peak sidelobe of the phased array having randomly located elements // IEEE Trans. Antennas Propag. 1972. V. 20, No. 2. P. 129–136. DOI: 10.1109/TAP.1972.1140162.
18. **Steinberg B. D.** Principles of aperture and array system design. New York: John Wiley & Sons, 1976. 356 p.
19. **Копилович Л. Е., Содин Л. Г.** Линейные не-эквидистантные антенны-решётки на базе разностных множеств // Радиотехника и электроника. 1989. Т. 34, № 10. С. 2059–2066.

Еремеев Антон Валентинович

Статья поступила
17 февраля 2025 г.
После доработки —
5 мая 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 71–83

UDC 519.8 DOI: 10.33048/daio.2025.32.829

ON COMPUTATIONAL COMPLEXITY OF PHASED ANTENNA ARRAY SYNTHESIS

A. V. Eremeev

Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue, 630090 Novosibirsk, Russia

E-mail: eremeev@ofim.oscsbras.ru

Abstract. We consider the problem of phased antenna array synthesis, which consists of choosing phases and amplitudes for all radiating elements when it is required that the resulting radiation pattern in each direction considered belongs to a given set. It is established that the search for an admissible solution is a strongly NP-hard problem in the case when, for each direction considered, one or two radiation power values are allowed. In addition, the NP-hardness of finding an admissible solution in the problem of synthesis of a thinned antenna array is proven in the case when, for each direction considered, radiation power belongs to a given interval and excitation amplitudes in all elements are identical. Bibliogr. 19.

Keywords: computational complexity, antenna array, reduction, NP-completeness.

References

1. **R. C. Hansen,** *Phased Array Antennas* (John Wiley & Sons, Hoboken, NJ, 1979).
2. **V. P. Kudzin, V. N. Lozovsky,** and **N. I. Shlyk,** The compact linear antenna array system of the short-wave band consisting of "butterfly" radiators, in *Proc. 9th Int. Conf. Antenna Theory and Techniques* (Odessa, Ukraine, Sept. 16–20, 2013) (IEEE, Piscataway, 2013), pp. 252–253.
3. **R. Wilensky,** High-power, broad-bandwidth HF dipole curtain array with extensive vertical and azimuthal beam control, *IEEE Trans. Broadcast.* **34** (2), 201–209 (1988), DOI: 10.1109/11.1437.

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

4. **J. I. Echeveste, M. A. González de Aza,** and **J. Zapata,** Shaped beam synthesis of real antenna arrays via finite-element method, floquet modal analysis, and convex programming, *IEEE Trans. Antennas Propag.* **64** (4), 1279–1286 (2016), DOI: 10.1109/TAP.2016.2526038.
5. **O. Bucci, L. Caccavale,** and **T. Isernia,** Optimal far-field focusing of uniformly spaced arrays subject to arbitrary upper bounds in non-target directions, *IEEE Trans. Antennas Propag.* **50** (11), 1539–1554 (2002), DOI: 10.1109/TAP.2002.803959.
6. **A. S. Yurkov,** *Optimizing Excitation of Transmitting Phased Antenna Arrays in the Decameter Wavelength Range* (ONIIP, Omsk, 2014) [Russian].
7. **A. S. Yurkov,** Maximizing the directivity of short-range phased antenna arras, *Tekh. Radiosvyazi*, No. 2, 46–53 (2016) [Russian].
8. **T. Isernia, P. Di Iorio,** and **F. Soldovieri,** An effective approach for the optimal focusing of array fields subject to arbitrary upper bounds, *IEEE Trans. Antennas Propag.* **48** (12), 1837–1847 (2000). DOI: 10.1109/8.901272.
9. **N. N. Tyunin,** The problems of non-convex quadratic programming related to phased antenna arrays optimization, *Diskretn. Anal. Issled. Oper.* **28** (3), 65–89 (2021) [Russian] [*J. Appl. Ind. Math.* **15** (3), 543-557 (2021), DOI:10.1134/S1990478921030157].
10. **M. Indenbom, V. Izhutkin, A. Sharapov,** and **A. Zonov,** Synthesis of conical phased antenna arrays optimization of amplitude distribution parameters, in *Proc. 9th Int. Conf. Optimization and Applications* (Petrovac, Montenegro, Oct. 1–5, 2018) (DEStech Publ., Lancaster, PA, 2018), pp. 273–285.
11. **A. Akdagli** and **K. Guney,** Shaped-beam pattern synthesis of equally and unequally spaced linear antenna arrays using a modified tabu search algorithm algorithm, *Microw. Opt. Technol. Lett.* **36** (1), 16–20 (2003), DOI: 10.1002/mop.10657.
12. **F. J. Villegas,** Parallel genetic-algorithm optimization of shaped beam coverage areas using planar 2-D phased arrays, *IEEE Trans. Antennas Propag.* **55** (6), 1745–1753 (2007), DOI: 10.1109/TAP.2007.898601.
13. **B. Fuchs,** Application of convex relaxation to array synthesis problems, *IEEE Trans. Antennas Propag.* **62** (2), 634–640 (2014). DOI: 10.1109/TAP.2013.2290797.
14. **S. A. Schelkunoff** and **H. T. Friis,** *Antennas: Theory and Practice* (John Wiley & Sons, New York, 1952; Sov. Radio, Moscow, 1955 [Russian]).
15. **M. R. Garey** and **D. S. Johnson,** *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979).
16. **D. G. Leeper,** Thinned aperiodic antenna arrays with improved peak sidelobe level control, *US Patent 4,071,848* (Jan 31, 1978) (Bell Teleph. Lab., Murray Hill, NJ, 1976), URL: patentimages.storage.googleapis.com/30/73/fa/25b9b72c3d3e8a/US4071848.pdf (accessed: 20.09.2025).
17. **B. D. Steinberg,** The peak sidelobe of the phased array having randomly located elements, *IEEE Trans. Antennas Propag.* **20** (2), 129–136 (1972), DOI: 10.1109/TAP.1972.1140162.

18. B. D. Steinberg, *Principles of Aperture and Array System Design* (John Wiley & Sons, New York, 1976).

19. L. E. Kopilovich and **L. G. Sodin,** Linear non-equidistant antenna arrays based on difference sets, *Radiotekh. Elektron.* **34** (10), 2059–2066 (1989).

Anton V. Eremeev

Received February 17, 2025
Revised May 5, 2025
Accepted June 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 84–97

УДК 512.534.1 DOI: 10.33048/daio.2025.32.824

ОБОБЩЁННЫЕ ЦЕНТРАЛИЗАТОРЫ БИНАРНОГО ОТНОШЕНИЯ

М. В. Лежнин[a], *Д. А. Хвощевский*[b]

НИУ «Московский институт электронной техники»,
пл. Шокина, 1, 124498 Москва, Россия
E-mail: [a]max.lezhnin@gmail.com, [b]dima1667@gmail.com

Аннотация. Рассматриваются обобщённые централизаторы бинарного отношения σ, представляющие собой полугруппы отношений (многозначных отображений), сохраняющих отношение σ в определённом смысле. Определяется восемь неэквивалентных условий того, что может значить термин «сохранять отношение». Рассмотрены все возможные комбинации этих условий, приводящие к различным полугруппам обобщённых централизаторов бинарного отношения, в зависимости от мощности множества, на котором это отношение задано. В частности, доказано восемь теорем, устанавливающих связь между этими условиями: первые четыре теоремы выполняются только для конечных множеств, а последние — для произвольных. Также установлена полнота этого списка теорем для множеств мощности не меньше 4. Для каждой мощности дан исчерпывающий ответ на вопрос о числе обобщённых централизаторов. Табл. 2, библиогр. 5.

Ключевые слова: обобщённый централизатор, полугруппа бинарных отношений.

Введение

Для непустого множества X определим следующие множества:

- $S(X)$ — множество всех биективных отображений $\alpha\colon X \to X$;
- $T(X)$ — множество всех отображений $\alpha\colon X \to X$;
- $P(X)$ — множество всех частичных отображений $\alpha\colon X_1 \to X$, где $X_1 \subseteq X$ — произвольное подмножество;
- $B(X)$ — множество всех многозначных отображений $\alpha\colon X \to X$, т. е. бинарных отношений $\alpha \subseteq X \times X$.

Элементы из $S(X)$, $T(X)$, $P(X)$ можно также рассматривать как бинарные отношения, т. е. отождествлять отображение α с отношением $\{(x, x\alpha) \in X \times X \mid \text{образ } x\alpha \text{ определён}\}$.

На этих множествах можно ввести умножение следующим образом:

$$\alpha\beta = \{(x, y) \in X \times X \mid \exists\, z\colon (x, z) \in \alpha,\ (z, y) \in \beta\}.$$

Относительно этой бинарной операции вышеописанные множества образуют полугруппы, а $S(X)$ — группу.

Замечание 1. Справедливы включения $S(X) \subseteq T(X) \subseteq P(X) \subseteq B(X)$, и при $|X| \geqslant 2$ все включения строгие. Каждая предыдущая полугруппа — подполугруппа следующей, а $S(X)$ — подгруппа $T(X)$.

Например, при $X = \{1, 2, 3, 4\}$ имеем

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 3 & 1 & 4 \end{pmatrix} \in T(X) \setminus S(X), \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & 3 & 3 & 1 \end{pmatrix} \in P(X) \setminus T(X),$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \{1,3\} & - & 2 & \{2,3,4\} \end{pmatrix} \in B(X) \setminus P(X).$$

Замечание 2. Бинарные отношения можно понимать и в более широком смысле как $\alpha \subseteq A \times B$. Тогда можно будет умножать $\alpha \subseteq A \times B$ на $\beta \subseteq B \times C$, получая $\alpha\beta \subseteq A \times C$ (см. [1]).

Для $\alpha \in B(X)$ определяется отношение

$$\alpha^{-1} = \{(y, x) \in X \times X \mid (x, y) \in \alpha\}.$$

Вообще, для $\alpha \subseteq X \times Y$ аналогично определяется $\alpha^{-1} \subseteq Y \times X$.

Пусть $x, y \in X$ и $\alpha \in T(X)$. Определим действие полугруппы отображений на множестве X следующим образом:

$$x\alpha = y \Leftrightarrow (x, y) \in \alpha.$$

Что означает фраза «преобразование α сохраняет отношение σ»? Для $\alpha \in P(X)$ можно определять сохранение σ разными неэквивалентными способами, как описано в [2]. Бинарное отношение σ можно рассматривать как граф с множеством вершин X, тогда фраза «отображение $\alpha\colon X \to X$ сохраняет σ» может означать, что α является эндоморфизмом графа. Различные подходы к понятию эндоморфизма графа описаны в [3]. Сохранение n-арного отношения рассматривалось в [4].

В качестве определения понятия «отображение $\alpha\colon X \to X$ сохраняет отношение $\sigma \in B(X)$» возьмём следующее:

$$\forall\, x, y \in X \quad (x, y) \in \sigma \to (x\alpha, y\alpha) \in \sigma.$$

Легко доказать, что это условие равносильно каждому из включений $\sigma \subseteq \alpha\sigma\alpha^{-1}$, $\alpha^{-1}\sigma\alpha \subseteq \sigma$, $\sigma\alpha \subseteq \alpha\sigma$, $\alpha^{-1}\sigma \subseteq \sigma\alpha^{-1}$. При рассмотрении произвольного отношения вместо отображения α эти условия оказываются, вообще говоря, неэквивалентными. Например, полугруппы отношений с условиями $\sigma \subseteq \alpha\sigma\alpha^{-1}$ и $\alpha^{-1}\sigma\alpha \subseteq \sigma$, рассмотренные в [5], различны.

Отметим также, что в случае, когда α представляет собой отношение, а не отображение, α и α^{-1} равноправны. По этой причине кроме приведённых выше четырёх включений имеет смысл рассматривать также четыре двойственных к ним, которые получаются заменой α на α^{-1}, поэтому в настоящей работе рассматриваются следующие 8 соотношений:

$$\begin{array}{ll} (1)\ \alpha\sigma\alpha^{-1} \subseteq \sigma, & (2)\ \sigma \subseteq \alpha\sigma\alpha^{-1}, \\ (3)\ \alpha^{-1}\sigma\alpha \subseteq \sigma, & (4)\ \sigma \subseteq \alpha^{-1}\sigma\alpha, \\ (5)\ \sigma\alpha \subseteq \alpha\sigma, & (6)\ \alpha\sigma \subseteq \sigma\alpha, \\ (7)\ \sigma\alpha^{-1} \subseteq \alpha^{-1}\sigma, & (8)\ \alpha^{-1}\sigma \subseteq \sigma\alpha^{-1}. \end{array}$$

Пусть $I = \{1, \ldots, 8\}$ — множество номеров рассматриваемых условий. Каждой паре отношений (σ, α) поставим в соответствие набор $K(\sigma, \alpha) = (k_1, \ldots, k_8) \in \{0, 1\}^8$, в котором $k_i = 0$, если соотношение (i) не выполняется, и $k_i = 1$, если соотношение (i) выполняется, где $i \in I$. Всего есть $2^{|I|} = 2^8 = 256$ наборов, однако многие из них невозможны, так как из некоторых соотношений можно вывести другие. Например, как будет показано далее, $(2) \wedge (3) \to (5)$, а значит, все наборы вида $*11*0***$ невозможны. Далее для всех мощностей множества X будет определено, какие наборы возможны, а какие невозможны.

Для $\sigma \in B(X)$ и $i \in I$ положим

$$B^i_\sigma(X) = \{\alpha \in B(X) \mid \alpha \text{ удовлетворяет условию } (i)\}.$$

Нетрудно проверить, что множество $B^i_\sigma(X)$ — подполугруппа полугруппы $B(X)$. Следовательно, если $\{i_1, i_2, \ldots, i_k\} \subseteq I$, то множество

$$B^{i_1,i_2,\ldots,i_k}_\sigma(X) = B^{i_1}_\sigma(X) \cap B^{i_2}_\sigma(X) \cap \cdots \cap B^{i_k}_\sigma(X)$$

также представляет собой подполугруппу полугруппы $B(X)$. Полугруппу $B^{i_1,i_2,\ldots,i_k}_\sigma(X)$ можно условно считать полугруппой отображений (возможно, многозначных), сохраняющих σ. Наряду с $B^i_\sigma(X)$ можно рассматривать полугруппы $P^i_\sigma(X) = P(X) \cap B^i_\sigma(X)$ и $T^i_\sigma(X) = T(X) \cap B^i_\sigma(X)$, а также их пересечения.

Множество $B^{i_1,i_2,\ldots,i_k}_\sigma(X)$ будем называть *обобщённым централизатором бинарного отношения* $\sigma \in B(X)$, а функцию $B^{i_1,i_2,\ldots,i_k}_\bullet(X)\colon \sigma \mapsto B^{i_1,i_2,\ldots,i_k}_\sigma(X)$ — *обобщённым централизатором*. Сразу видно, что для любого множества X имеется не больше чем $2^{|I|} = 2^8 = 256$ обобщённых централизаторов. Оказывается, что их всегда будет значительно меньше чем 256, так как из некоторых соотношений можно вывести другие, а значит, многие обобщённые централизаторы будут совпадать друг с другом. Например, как будет показано далее, $(2) \wedge (3) \to (5)$, а значит, $B^{2,3}_\bullet(X)$ и $B^{2,3,5}_\bullet(X)$ совпадают. Цель этой работы — для всех мощностей X определить, какие обобщённые централизаторы совпадают, а какие нет.

Утверждение 1. *Для произвольного множества X возможных наборов не больше, чем обобщённых централизаторов.*

Доказательство. Пусть $P = (p_1, \ldots, p_8)$ и $Q = (q_1, \ldots, q_8)$ — произвольные наборы. Введём отношение частичного порядка на наборах следующим образом:

$$P \preccurlyeq Q \Leftrightarrow \forall\, i \in I\ p_i \leqslant q_i.$$

Будем называть набор $P = (p_1, \ldots, p_8)$ *допустимым* для обобщённого централизатора $B^S_\bullet(X)$ в том и только том случае, когда выполняется импликация $i \in S \to p_i = 1$. Например, для обобщённого централизатора $B^{1,4,5}_\bullet(X)$ допустимыми будут наборы вида 1**11*** и только они.

Произвольному возможному набору $P = (p_1, \ldots, p_8)$ поставим в соответствие обобщённый централизатор $f(P) = B^S_\bullet(X)$ для множества $S = \{i \in I \mid p_i = 1\}$. Покажем, что отображение f из множества возможных наборов в множество обобщённых централизаторов инъективно. Пусть $f(P) = f(Q)$, покажем, что $P = Q$. Рассмотрим множество $\{K(\sigma, \alpha) \mid \alpha \in f(P)(\sigma)\}$ возможных допустимых наборов для обобщённого централизатора $f(P)$. У него есть наименьший относительно порядка $\preccurlyeq$ элемент P. Аналогично у множества $\{K(\sigma, \alpha) \mid \alpha \in f(Q)(\sigma)\}$ есть наименьший элемент Q. Так как $f(P) = f(Q)$, эти множества равны, а поскольку у любого частично упорядоченного множества не больше одного наименьшего элемента, получаем $P = Q$. Следовательно, отображение f инъективное, т. е. возможных наборов не больше, чем обобщённых централизаторов. Утверждение 1 доказано.

Замечание 3. Отметим, что число возможных наборов и число обобщённых централизаторов не всегда совпадают, так как существуют обобщённые централизаторы, для которых множество возможных наборов не имеет наименьшего элемента. Например, для множеств мощности 2 выполняется (4) $\to$ (1) $\vee$ (2), при этом (4) $\nrightarrow$ (1) и (4) $\nrightarrow$ (2), а значит, у $B^4_\bullet(X)$ нет наименьшего возможного набора. Здесь и далее при записи утверждений вывода будем подразумевать, что импликация имеет наименьший приоритет перед операциями в левой и правой частях.

Утверждение 2. *Пусть $|X| \leqslant |Y|$ для множеств X и Y.*

1. *Если набор возможен для X, то он возможен для Y. В частности, число возможных наборов для X не больше, чем для Y.*

2. *Если два обобщённых централизатора различны для X, то они различны для Y. В частности, число обобщённых централизаторов для X не больше, чем для Y.*

Доказательство. Так как $|X| \leqslant |Y|$, существует инъективное отображение $f\colon X \to Y$.

1. Если набор P возможен на множестве X, то существует пара (σ, α) отношений на множестве X таких, что $K(\sigma, \alpha) = P$. Тогда имеем следующую пару $(\widetilde{\sigma}, \widetilde{\alpha})$ отношений на множестве Y таких, что $K(\widetilde{\sigma}, \widetilde{\alpha}) = P$:

$$\widetilde{\sigma} = \{(f(a), f(b)) \mid (a, b) \in \sigma\}, \quad \widetilde{\alpha} = \{(f(a), f(b)) \mid (a, b) \in \alpha\}.$$

2. Если $B^S_\bullet(X)$ и $B^T_\bullet(X)$ различны на множестве X, то существует пара (σ, α) отношений на множестве X таких, что $\alpha \in B^S_\sigma(X)$ и $\alpha \notin B^T_\sigma(X)$, или таких, что $\alpha \notin B^S_\sigma(X)$ и $\alpha \in B^T_\sigma(X)$. Без ограничения общности будем считать, что выполняется первый случай, т. е. $\alpha \in B^S_\sigma(X)$ и $\alpha \notin B^T_\sigma(X)$. Тогда имеем следующую пару $(\widetilde{\sigma}, \widetilde{\alpha})$ отношений на множестве Y таких, что $\widetilde{\alpha} \in B^S_{\widetilde{\sigma}}(X)$ и $\widetilde{\alpha} \notin B^T_{\widetilde{\sigma}}(X)$:

$$\widetilde{\sigma} = \{(f(a), f(b)) \mid (a, b) \in \sigma\}, \quad \widetilde{\alpha} = \{(f(a), f(b)) \mid (a, b) \in \alpha\}.$$

Утверждение 2 доказано.

1. Результаты для конечных множеств

С помощью полного компьютерного перебора пар (σ, α) бинарных отношений на множестве X мощности $|X| \leqslant 4$ найдены все возможные наборы и все обобщённые централизаторы, их количества приведены в табл. 1. Так как для некоторых мощностей их достаточно много, вместо возможных наборов и обобщённых централизаторов для каждой мощности приведём системы утверждений, по которым их можно восстановить.

Все представленные ниже системы утверждений обладают тремя полезными свойствами:

1) *корректность,* т. е. для каждого возможного набора выполняются все утверждения системы;

2) *полнота,* т. е. каждый набор, для которого выполняются все утверждения системы, возможный;

3) *независимость,* т. е. если исключить какое-нибудь утверждение из системы, то появятся новые наборы, для которых выполняются все утверждения системы.

Таблица 1

Результаты компьютерного перебора

|X|	Число возможных наборов	Число обобщённых централизаторов
0	1	1
1	2	2
2	38	127
3	143	151
4	151	151

Система утверждений для $|X| = 0$:

$$(1), \quad (2), \quad (3), \quad (4), \quad (5), \quad (6), \quad (7), \quad (8).$$

Система утверждений для $|X| = 1$:

$$(1), \quad (2) \to (4), \quad (3), \quad (4) \to (2), \quad (5), \quad (6), \quad (7), \quad (8).$$

Система утверждений для $|X| = 2$:

$$\begin{gathered}
(3) \wedge (4) \wedge (6) \wedge (7) \to (1), \quad (3) \wedge (6) \wedge (7) \wedge (8) \to (5), \\
(3) \wedge (4) \wedge (5) \wedge (8) \to (2), \quad (1) \wedge (5) \wedge (7) \wedge (8) \to (6), \\
(1) \wedge (2) \wedge (5) \wedge (8) \to (3), \quad (1) \wedge (5) \wedge (6) \wedge (8) \to (7), \\
(1) \wedge (2) \wedge (6) \wedge (7) \to (4), \quad (3) \wedge (5) \wedge (6) \wedge (7) \to (8), \\
(2) \wedge (3) \to (5), \quad (6) \wedge (7) \to (1) \vee (5), \quad (6) \to (1) \vee (5) \vee (8), \\
(1) \wedge (4) \to (6), \quad (6) \wedge (7) \to (1) \vee (8), \quad (7) \to (1) \vee (5) \vee (8), \\
(1) \wedge (4) \to (7), \quad (5) \wedge (8) \to (3) \vee (6), \quad (5) \to (3) \vee (6) \vee (7), \\
(2) \wedge (3) \to (8), \quad (5) \wedge (8) \to (3) \vee (7), \quad (8) \to (3) \vee (6) \vee (7), \\
(1) \wedge (5) \to (2) \vee (6) \vee (7), \quad (1) \wedge (8) \to (2) \vee (6) \vee (7), \\
(3) \wedge (6) \to (4) \vee (5) \vee (8), \quad (3) \wedge (7) \to (4) \vee (5) \vee (8), \\
(4) \to (1) \vee (2), \quad (6) \to (1) \vee (2), \quad (7) \to (1) \vee (2), \\
(2) \to (3) \vee (4), \quad (5) \to (3) \vee (4), \quad (8) \to (3) \vee (4).
\end{gathered}$$

Система утверждений для $|X| = 3$:

$$\begin{gathered}
(1) \wedge (2) \wedge (7) \to (5) \vee (6), \quad (3) \wedge (4) \wedge (8) \to (5) \vee (6), \\
(1) \wedge (2) \wedge (6) \to (7) \vee (8), \quad (3) \wedge (4) \wedge (5) \to (7) \vee (8), \\
(3) \wedge (4) \wedge (6) \wedge (7) \to (1), \quad (2) \wedge (3) \to (5), \\
(3) \wedge (4) \wedge (5) \wedge (8) \to (2), \quad (1) \wedge (4) \to (6), \\
(1) \wedge (2) \wedge (5) \wedge (8) \to (3), \quad (1) \wedge (4) \to (7), \\
(1) \wedge (2) \wedge (6) \wedge (7) \to (4), \quad (2) \wedge (3) \to (8).
\end{gathered}$$

Система утверждений для $|X| = 4$:

$$\begin{gathered}
(3) \wedge (4) \wedge (6) \wedge (7) \to (1), \quad (2) \wedge (3) \to (5), \\
(3) \wedge (4) \wedge (5) \wedge (8) \to (2), \quad (1) \wedge (4) \to (6), \\
(1) \wedge (2) \wedge (5) \wedge (8) \to (3), \quad (1) \wedge (4) \to (7), \\
(1) \wedge (2) \wedge (6) \wedge (7) \to (4), \quad (2) \wedge (3) \to (8).
\end{gathered}$$

Отметим, что корректность, полнота и независимость приведённых выше систем несложно проверяются с помощью компьютера.

Оказывается, что для конечного множества X мощности $|X| \geqslant 4$ система утверждений будет выглядеть так же, как и для множества мощности 4, что докажем далее. Независимость системы несложно проверяется с помощью компьютера. Полнота системы следует из её полноты для $|X| = 4$ и утверждения 2. Корректность системы показывают следующие восемь теорем.

Теорема 1. *Пусть σ и α — отношения на конечном множестве X и выполняются соотношения*

(3) $\alpha^{-1}\sigma\alpha \subseteq \sigma$, (4) $\sigma \subseteq \alpha^{-1}\sigma\alpha$, (6) $\alpha\sigma \subseteq \sigma\alpha$, (7) $\sigma\alpha^{-1} \subseteq \alpha^{-1}\sigma$.

Тогда выполняется соотношение (1) $\alpha\sigma\alpha^{-1} \subseteq \sigma$.

Доказательство. Поскольку множество X конечно, степени α начнут периодически повторяться начиная с некоторого числа:

$$\exists\, n \in \mathbb{Z}_{\geqslant 0}\ \exists\, t \in \mathbb{Z}_{\geqslant 0} \colon \alpha^{n+t+1} = \alpha^n.$$

Здесь $n \geqslant 0$ — целое, с которого начинаются повторения, а $t + 1 \geqslant 1$ — период. В этом случае из цепочки соотношений

$$\alpha\sigma\alpha^{-1} \overset{(7)}{\subseteq} \alpha\alpha^{-1}\sigma \overset{(4)}{\subseteq} \alpha(\alpha^{-1})^{n+t+1}\sigma\alpha^{n+t} = \alpha(\alpha^{-1})^n\sigma\alpha^{n+t} \overset{(3)}{\subseteq}$$
$$\overset{(3)}{\subseteq} \alpha\sigma\alpha^t \overset{(6)}{\subseteq} \sigma\alpha^{t+1} \overset{(4)}{\subseteq} (\alpha^{-1})^n\sigma\alpha^{n+t+1} = (\alpha^{-1})^n\sigma\alpha^n \overset{(3)}{\subseteq} \sigma$$

получаем (1) $\alpha\sigma\alpha^{-1} \subseteq \sigma$. Теорема 1 доказана.

Теорема 2. *Пусть σ и α — отношения на конечном множестве X и выполняются соотношения*

(3) $\alpha^{-1}\sigma\alpha \subseteq \sigma$, (4) $\sigma \subseteq \alpha^{-1}\sigma\alpha$, (5) $\sigma\alpha \subseteq \alpha\sigma$, (8) $\alpha^{-1}\sigma \subseteq \sigma\alpha^{-1}$.

Тогда выполняется соотношение (2) $\sigma \subseteq \alpha\sigma\alpha^{-1}$.

Доказательство. Используя конечность множества X, делаем вывод, что начиная с какого-то номера, степени α начнут периодически повторяться:

$$\exists\, n \in \mathbb{Z}_{\geqslant 0}\ \exists\, t \in \mathbb{Z}_{\geqslant 0} \colon \alpha^{n+t+1} = \alpha^n.$$

Здесь n — номер, с которого начинаются повторения, а $t+1$ — период, который обязательно не меньше 1. В этом случае из цепочки соотношений

$$\sigma \overset{(4)}{\subseteq} (\alpha^{-1})^{n+t+1}\sigma\alpha^{n+t+1} = (\alpha^{-1})^n\sigma\alpha^{n+t+1} \overset{(3)}{\subseteq} \sigma\alpha^{t+1} \overset{(5)}{\subseteq} \alpha\sigma\alpha^t \overset{(4)}{\subseteq}$$
$$\overset{(4)}{\subseteq} \alpha(\alpha^{-1})^{n+1}\sigma\alpha^{n+t+1} = \alpha(\alpha^{-1})^{n+1}\sigma\alpha^n \overset{(3)}{\subseteq} \alpha\alpha^{-1}\sigma \overset{(8)}{\subseteq} \alpha\sigma\alpha^{-1}$$

получаем (2) $\sigma \subseteq \alpha\sigma\alpha^{-1}$. Теорема 2 доказана.

Теорема 3. *Пусть σ и α — отношения на конечном множестве X и выполняются соотношения*

$$(1)\ \alpha\sigma\alpha^{-1} \subseteq \sigma, \quad (2)\ \sigma \subseteq \alpha\sigma\alpha^{-1}, \quad (5)\ \sigma\alpha \subseteq \alpha\sigma, \quad (8)\ \alpha^{-1}\sigma \subseteq \sigma\alpha^{-1}.$$

Тогда выполняется соотношение $(3)\ \alpha^{-1}\sigma\alpha \subseteq \sigma$.

Доказательство. С помощью замены α на α^{-1} можно увидеть, что эта теорема равносильна теореме 1. Теорема 3 доказана.

Теорема 4. *Пусть σ и α — отношения на конечном множестве X и выполняются соотношения*

$$(1)\ \alpha\sigma\alpha^{-1} \subseteq \sigma, \quad (2)\ \sigma \subseteq \alpha\sigma\alpha^{-1}, \quad (6)\ \alpha\sigma \subseteq \sigma\alpha, \quad (7)\ \sigma\alpha^{-1} \subseteq \alpha^{-1}\sigma.$$

Тогда выполняется соотношение $(4)\ \sigma \subseteq \alpha^{-1}\sigma\alpha$.

Доказательство. С помощью замены α на α^{-1} можно увидеть, что эта теорема равносильна теореме 2. Теорема 4 доказана.

Оставшиеся четыре теоремы сформулируем и докажем в обобщённом виде. Вместо одного множества X рассмотрим два множества X и Y, а вместо одного отношения σ — два отношения ρ и σ. При этом в частном случае, когда $X = Y$ и $\rho = \sigma$, получим интересующие нас утверждения. Отметим, что первые четыре теоремы не допускают аналогичного обобщения, что несложно проверить с помощью компьютера. Также для четырёх теорем ниже не будем требовать конечности множеств X и Y.

Теорема 5. *Пусть $\rho \in B(X)$, $\sigma \in B(Y)$, α — отношение между множествами X и Y, т. е. $\alpha \subseteq X \times Y$, и выполняются обобщённые соотношения*

$$(2)\ \rho \subseteq \alpha\sigma\alpha^{-1}, \quad (3)\ \alpha^{-1}\rho\alpha \subseteq \sigma.$$

Тогда выполняется обобщённое соотношение $(5)\ \rho\alpha \subseteq \alpha\sigma$.

Доказательство. В этом случае из цепочки соотношений

$$(x,y) \in \rho\alpha \overset{(2)}{\Leftrightarrow} (x,y) \in \rho\alpha \wedge (x,y) \in \alpha\sigma\alpha^{-1}\alpha \Leftrightarrow$$

$$\Leftrightarrow \exists\, y' \in Y\ (x,y) \in \rho\alpha \wedge (x,y') \in \alpha \Rightarrow (x,y) \in \alpha\alpha^{-1}\rho\alpha \overset{(3)}{\Rightarrow} (x,y) \in \alpha\sigma$$

получаем утверждение $\forall\, x \in X\ \forall\, y \in Y\ (x,y) \in \rho\alpha \to (x,y) \in \alpha\sigma$, равносильное соотношению $(5)\ \rho\alpha \subseteq \alpha\sigma$. Теорема 5 доказана.

Теорема 6. *Пусть $\rho \in B(X)$, $\sigma \in B(Y)$, α — отношение между множествами X и Y, т. е. $\alpha \subseteq X \times Y$, и выполняются обобщённые соотношения*

$$(1)\ \alpha\sigma\alpha^{-1} \subseteq \rho, \quad (4)\ \sigma \subseteq \alpha^{-1}\rho\alpha.$$

Тогда выполняется обобщённое соотношение $(6)\ \alpha\sigma \subseteq \rho\alpha$.

Доказательство. В этом случае из цепочки соотношений

$$(x,y) \in \alpha\sigma \overset{(4)}{\Leftrightarrow} (x,y) \in \alpha\sigma \wedge (x,y) \in \alpha\alpha^{-1}\rho\alpha \Leftrightarrow$$

$$\Leftrightarrow \exists\, x' \in X\ (x,y) \in \alpha\sigma \wedge (x',y) \in \alpha \Rightarrow (x,y) \in \alpha\sigma\alpha^{-1}\alpha \overset{(1)}{\Rightarrow} (x,y) \in \rho\alpha$$

получаем утверждение $\forall\, x \in X\ \forall\, y \in Y\ (x,y) \in \alpha\sigma \to (x,y) \in \rho\alpha$, равносильное утверждению (6) $\alpha\sigma \subseteq \rho\alpha$. Теорема 6 доказана.

Теорема 7. *Пусть $\rho \in B(X)$, $\sigma \in B(Y)$, α — отношение между множествами X и Y, т. е. $\alpha \subseteq X \times Y$, и выполняются обобщённые соотношения*

$$(1)\ \alpha\sigma\alpha^{-1} \subseteq \rho, \quad (4)\ \sigma \subseteq \alpha^{-1}\rho\alpha.$$

Тогда выполняется обобщённое соотношение (7) $\sigma\alpha^{-1} \subseteq \alpha^{-1}\rho$.

Доказательство. С помощью замен

$$X \leftrightarrow Y, \quad \rho \leftrightarrow \sigma, \quad \alpha \leftrightarrow \alpha^{-1}$$

можно увидеть, что эта теорема равносильна теореме 5. Теорема 7 доказана.

Теорема 8. *Пусть $\rho \in B(X)$, $\sigma \in B(Y)$, α — отношение между множествами X и Y, т. е. $\alpha \subseteq X \times Y$, и выполняются обобщённые соотношения*

$$(2)\ \rho \subseteq \alpha\sigma\alpha^{-1}, \quad (3)\ \alpha^{-1}\rho\alpha \subseteq \sigma.$$

Тогда выполняется обобщённое соотношение (8) $\alpha^{-1}\rho \subseteq \sigma\alpha^{-1}$.

Доказательство. С помощью замен

$$X \leftrightarrow Y, \quad \rho \leftrightarrow \sigma, \quad \alpha \leftrightarrow \alpha^{-1}$$

можно увидеть, что эта теорема равносильна теореме 6. Теорема 8 доказана.

2. Результаты для бесконечных множеств

Первые четыре теоремы доказаны в предположении, что множество X конечно. Оказывается, что они не выполняются для бесконечных множеств. При этом никаких более слабых утверждений не добавляется, т. е. система утверждений для бесконечных множеств имеет вид

$$(2) \wedge (3) \to (5), \quad (1) \wedge (4) \to (6), \quad (1) \wedge (4) \to (7), \quad (2) \wedge (3) \to (8).$$

Независимость системы несложно проверяется с помощью компьютера. Теоремы 5–8 показывают корректность системы. Для того чтобы показать полноту, нужно доказать, что все наборы, удовлетворяющие системе, возможны, т. е. достаточно предъявить пару (σ, α) для каждого такого набора. Оказывается, что таких наборов 169, при этом для 151 из них несложно с помощью компьютера найти пары (σ, α) отношений

на множестве мощности 4, а потом преобразовать их в пары отношений на бесконечном множестве с использованием утверждения 2. Значит, остаётся привести 18 пар отношений на множестве мощности $\aleph_0$. При этом достаточно привести 9 пар отношений, а остальные 9 получаются из них заменой α на α^{-1}. Далее в виде примеров приведены эти 9 пар отношений на множестве $\mathbb{Z}_{\geqslant 0}$. Подробно опишем один из примеров, остальные проверяются аналогично.

Пример 1. Для наборов $K(\sigma,\alpha) = 10111111$ и $K(\sigma,\alpha^{-1}) = 11101111$ возьмём отношения

$$\sigma = \{(i,i) \mid i \in \mathbb{Z}_{\geqslant 0}\}, \quad \alpha = \{(i+1,i) \mid i \in \mathbb{Z}_{\geqslant 0}\}.$$

Заметим, что

$$\sigma\alpha = \alpha\sigma = \alpha, \quad \sigma\alpha^{-1} = \alpha^{-1}\sigma = \alpha^{-1},$$
$$\alpha^{-1}\sigma\alpha = \alpha^{-1}\alpha, \quad \alpha\sigma\alpha^{-1} = \alpha\alpha^{-1}.$$

Из равенств в первой строке очевидно, что выполняются соотношения (5)–(8). Далее по определению α получаем

$$\alpha\alpha^{-1} = \{(i+1,i+1) \mid i \in \mathbb{Z}_{\geqslant 0}\} \subset \sigma, \quad \alpha^{-1}\alpha = \{(i,i) \mid i \in \mathbb{Z}_{\geqslant 0}\} = \sigma,$$

откуда непосредственно следует, что $K(\sigma,\alpha) = 10111111$. Такой набор невозможен для конечных множеств в силу теоремы 2.

Пример 2. Для наборов $K(\sigma,\alpha) = 00111001$ и $K(\sigma,\alpha^{-1}) = 11000110$

$$\sigma = \{(i+1,i+1) \mid i \in \mathbb{Z}_{\geqslant 0}\}, \quad \alpha = \{(i+2,i+1) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,1)\}.$$

Пример 3. Для наборов $K(\sigma,\alpha) = 00111011$ и $K(\sigma,\alpha^{-1}) = 11001110$

$$\sigma = \{(i+1,i+1) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(1,0)\},$$
$$\alpha = \{(i+3,i+2) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,0),(0,1),(1,1)\}.$$

Пример 4. Для наборов $K(\sigma,\alpha) = 00111101$ и $K(\sigma,\alpha^{-1}) = 11000111$

$$\sigma = \{(i+1,i+1) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,1)\},$$
$$\alpha = \{(i+3,i+2) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,0),(0,1),(1,1)\}.$$

Пример 5. Для наборов $K(\sigma,\alpha) = 01111111$ и $K(\sigma,\alpha^{-1}) = 11011111$

$$\sigma = \{(i,i) \mid i \in \mathbb{Z}_{\geqslant 0}\}, \quad \alpha = \{(i+1,i) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,0)\}.$$

Пример 6. Для наборов $K(\sigma,\alpha) = 00110110$ и $K(\sigma,\alpha^{-1}) = 11001001$

$$\sigma = \{(i,i) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(0,1),(1,0)\},$$
$$\alpha = \{(i+3,i+2) \mid i \in \mathbb{Z}_{\geqslant 0}\} \cup \{(1,0),(1,1),(2,2)\}.$$

Пример 7. Для наборов $K(\sigma,\alpha)=00110111$ и $K(\sigma,\alpha^{-1})=11001101$

$$\sigma=\{(i+3,i+3)\mid i\in\mathbb{Z}_{\geqslant 0}\}\cup\{(1,0),(2,0)\},$$
$$\alpha=\{(i+4,i+3)\mid i\in\mathbb{Z}_{\geqslant 0}\}\cup\{(0,0),(2,1),(2,2),(3,3)\}.$$

Пример 8. Для наборов $K(\sigma,\alpha)=00111110$ и $K(\sigma,\alpha^{-1})=11001011$

$$\sigma=\{(i+3,i+3)\mid i\in\mathbb{Z}_{\geqslant 0}\}\cup\{(2,0),(2,1)\},$$
$$\alpha=\{(i+4,i+3)\mid i\in\mathbb{Z}_{\geqslant 0}\}\cup\{(1,0),(1,1),(2,2),(3,3)\}.$$

Пример 9. Для наборов $K(\sigma,\alpha)=00111111$ и $K(\sigma,\alpha^{-1})=11001111$

$$\sigma=\{(i,i)\mid i\in\mathbb{Z}_{\geqslant 0}\},\quad \alpha=\{(i+2,i)\mid i\in\mathbb{Z}_{\geqslant 0}\}\cup\{(0,0)\}.$$

В заключение приведём табл. 2 — дополненную версию табл. 1. Отметим, что при любом σ все обобщённые централизаторы непусты, так как $K(\sigma,\varepsilon)=11111111$, а значит, ε принадлежит каждому обобщённому централизатору. Вместе с тем, $B^{\varnothing}_{\sigma}(X)=B(X)$ при любом отношении σ, поэтому интересных обобщённых централизаторов на один меньше, чем числа, приведённые в табл. 2. Наконец, значения в табл. 1 и 2 соответствуют утверждениям 1 и 2, поскольку не убывают при движении по таблицам слева направо или сверху вниз.

Таблица 2

Результаты перебора для всех мощностей

|X|	Число возможных наборов	Число обобщённых централизаторов
0	1	1
1	2	2
2	38	127
3	143	151
$4\leqslant\lvert X\rvert<\aleph_0$	151	151
$\lvert X\rvert\geqslant\aleph_0$	169	169

Авторы выражают благодарность научному руководителю И. Б. Кожухову за полезные советы по подготовке и оформлению статьи.

Финансирование работы

Исследование выполнено за счёт бюджета НИУ «Московский институт электронной техники». Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Вагнер В. В.** Теория отношений и алгебра частичных отображений // Теория полугрупп и её приложения. Саратов: Изд-во Саратов. ун-та, 1965. С. 3–178.
2. **Ярошевич В. А.** Полугруппы частичных и многозначных изотонных отображений: Дис. ... канд. физ.-мат. наук: 01.01.06. Москва, 2009. 91 с.
3. **Böttcher M., Knauer U.** Endomorphism spectra of graphs // Discrete Math. 1992. V. 109. P. 45–57.
4. **Клюшин А. А, Кожухов И. Б., Манилов Д. Ю., Решетников А. В.** Определяемость отношений полугруппами изотонных преобразований // Дискрет. анализ и исслед. операций. 2024. Т. 31, № 1. С. 19–34.
5. **Кожухов И. Б., Ярошевич В. А.** Полугруппы отображений, сохраняющих бинарное отношение // Фундамент. и прикл. математика. 2008. Т. 14, № 7. С. 129–135.

Лежнин Максим Витальевич
Хвощевский Дмитрий Алексеевич

Статья поступила
9 января 2025 г.
После доработки —
2 июня 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 84–97

UDC 512.534.1 DOI: 10.33048/daio.2025.32.824

GENERALIZED CENTRALIZERS OF A BINARY RELATION

M. V. Lezhnin[a] and *D. A. Khvoshchevskiy*[b]

National Research University of Electronic Technology,
1 Shokin Square, 124498 Moscow, Russia
E-mail: [a]max.lezhnin@gmail.com, [b]dima1667@gmail.com

Abstract. We consider generalized centralizers of a binary relation σ, which are semi-groups of relations (multi-valued mappings) that preserve the relation σ in a certain sense. Eight nonequivalent conditions are defined to specify what the term "to preserve a relation" can mean. All possible combinations of these conditions are considered, resulting in different semi-groups of generalized centralizers of a binary relation, depending on the cardinality of the set on which the relation is defined. Specifically, eight theorems are proven, establishing the connection between these conditions: the first four theorems hold only for finite sets, while the last four are valid for arbitrary sets. Furthermore, the completeness of this list of theorems is demonstrated for sets of cardinality no less than 4. For each cardinality, an exhaustive answer is provided regarding the number of distinct generalized centralizers. Tab. 2, bibliogr. 5.

Keywords: generalised centralizer, semi-group of binary relations.

References

1. **V. V. Vagner,** Relation theory and algebra of partial mappings, in *Semigroup Theory and Its Applications* (Izd. Saratov. Univ., Saratov, 1965), pp. 3–178.
2. **V. A. Yaroshevich,** Semigroups of partial and multivalued isotone mappings, *Candidate Sci. Diss.* (Moscow, 2009).
3. **M. Böttcher** and **U. Knauer,** Endomorphism spectra of graphs, *Discrete Math.* **109**, 45–57 (1992).
4. **A. A Klyushin, I. B. Kozhukhov, D. Yu. Manilov,** and **A. V. Reshetnikov,** Definability of relations by semigroups of isotone transformations, *Diskretn. Anal. Issled. Oper.* **31** (1), 19–34 (2024) [Russian], DOI: 10.33048/daio.2024.31.783 [*J. Appl. Ind. Math.* **18** (1) 60–69 (2024), DOI: 10.1134/S199047892401006X].

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

5. I. B. Kozhukhov and **V. A. Yaroshevich,** Transformation semigroups preserving a binary relation, *Fundam. Prikl. Mat.* **14** (7), 129–135 (2008) [Russian] [*J. Math. Sci.* **164** (2) 240–244 (2010), DOI: 10.1007/s10958-009-9723-5].

Maksim V. Lezhnin
Dmitry A. Khvoshchevskiy

Received January 9, 2025
Revised June 2, 2025
Accepted June 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 98–116

УДК 519.176+519.8+519.7 DOI: 10.33048/daio.2025.32.820

ПОИСК И ИССЛЕДОВАНИЕ ИДЕАЛЬНЫХ ДВУМЕРНЫХ ЦИРКУЛЯНТНЫХ СЕТЕЙ НА ОСНОВЕ ГРАФОВЫХ БАЗ ДАННЫХ

Э. А. Монахова [a], *О. Г. Монахов* [b]

Институт вычислительной математики и математической геофизики,
пр. Акад. Лаврентьева, 6, 630090 Новосибирск, Россия
E-mail: [a] emilia@rav.sscc.ru, [b] monakhov@rav.sscc.ru

Аннотация. На основе анализа больших массивов экспериментальных данных производится поиск идеальных двумерных кольцевых циркулянтных сетей, оптимальных по двум параметрам — диаметру и среднему расстоянию. Ранее авторами был получен большой датасет (база данных) оптимальных по диаметру двумерных кольцевых циркулянтных сетей. В настоящей работе получен новый датасет рассматриваемых сетей, оптимальных по среднему расстоянию. Исследование графов указанных датасетов позволило вывести новые свойства соотношений диаметра и среднего расстояния в оптимальных циркулянтах и получить семейства наилучших по двум параметрам оптимальных циркулянтных сетей, для которых применим настраиваемый по числу узлов эффективный алгоритм маршрутизации константной сложности. Идеальные двумерные кольцевые циркулянты представляют интерес как эффективные и надёжные топологии для межузловых связей в сетях на кристалле и информационно-коммуникационных системах. Ил. 6, библиогр. 27.

Ключевые слова: кольцевая циркулянтная сеть, диаметр, среднее расстояние, датасет оптимальных циркулянтов, алгоритм маршрутизации.

Введение

Циркулянтные графы степени четыре изучаются в теории и различных прикладных областях, включая использование в качестве топологий сетей связи суперкомпьютеров и сетей на кристалле [1–9]. Дадим общее определение исследуемого класса сетей. *Циркулянтная сеть* (circulant network) степени четыре представляет собой неориентированный граф $C(N; s_1, s_2)$, где $1 \leqslant s_1 < s_2 < N/2$, с множеством вершин $V = \mathbb{Z}_N =$

$\{0, 1, \ldots, N-1\}$, в котором каждая вершина $i \in V$ смежна с вершинами $(i \pm s_1) \bmod N$ и $(i \pm s_2) \bmod N$. Числа s_1, s_2 — образующие, N — порядок графа. Граф $C(N; s_1, s_2)$ связен, если НОД$(N, s_1, s_2) = 1$. Если $s_1 = 1$, то граф $C(N; 1, s)$ называется *двумерным кольцевым циркулянтным графом* (двумерный — по числу образующих $k = 2$). В англоязычной литературе для этого графа применяются также названия undirected double-loop network, chordal ring of fourth degree. На рис. 1 изображена циркулянтная сеть $C(10; 1, 4)$.

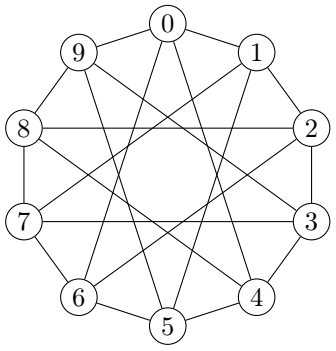


Рис. 1. Циркулянтная сеть $C(10; 1, 4)$

Диаметром графа называется длина $d = d(N; s_1, s_2)$ максимального кратчайшего пути на множестве всевозможных пар вершин. *Среднее расстояние* (mean path length, average distance) определяется как

$$\overline{d} = \overline{d}(N; s_1, s_2) = \frac{1}{N-1} \sum_{i=1}^{d} i n_i,$$

где n_i — число вершин графа, находящихся на расстоянии i от нулевой вершины. В ряде работ показано, что минимизация диаметра (среднего расстояния) при заданных порядке и степени графа оптимизирует структурные задержки при передаче данных, пропускную способность и другие характеристики топологии сети связи и напрямую влияет на повышение производительности вычислительного кластера [1, 10].

Основной объект исследования в данной работе — класс циркулянтных графов вида $C(N; 1, s)$, где $N \geqslant 5$, $2 \leqslant s < N/2$. Пусть

$$d(N) = \min_s d(N; 1, s), \quad \overline{d}(N) = \min_s \overline{d}(N; 1, s).$$

Назовём *оптимальным по диаметру* граф $C(N; 1, s)$ с минимально возможным для данного N диаметром $d = d(N)$, *оптимальным по среднему расстоянию* — граф $C(N; 1, s)$ с минимально возможным для данного N

средним расстоянием $\overline{d} = \overline{d}(N)$. Граф $C(10; 1, 4)$ — пример графа, оптимального по диаметру и среднему расстоянию, при этом $d = d(10) = 2$, $\overline{d} = \overline{d}(10) = 1{,}4$. Например, для графов $C(10; 1, 2)$ и $C(10; 1, 3)$ имеем $d = 3$, $\overline{d} = 1{,}5$.

В настоящей работе для класса двумерных кольцевых сетей $C(N; 1, s)$ рассматривается решение оптимизационной проблемы поиска семейств оптимальных по двум параметрам сетей (с минимально возможными одновременно диаметром и средним расстоянием) и получения применимого для таких сетей эффективного алгоритма маршрутизации.

Для класса сетей $C(N; 1, s)$ авторами были ранее представлены в открытом доступе датасет (база данных) оптимальных по диаметру графов до $N \leqslant 50\,000$ вершин [11], а также полученные на его основе аналитически описываемые семейства оптимальных графов [12]. В настоящей работе путём полного перебора образующих для каждого испытуемого $N \leqslant 4100$ получен новый датасет оптимальных по среднему расстоянию графов класса $C(N; 1, s)$. На основе анализа и сравнения этих двух датасетов, а также рассмотрения свойств соотношений диаметра и среднего расстояния, построена база данных идеальных графов — циркулянтных сетей класса $C(N; 1, s)$ с минимально возможными одновременно диаметром и средним расстоянием. Найдены аналитически задаваемые семейства идеальных сетей, для которых применим масштабируемый по числу узлов алгоритм маршрутизации сложности $O(1)$.

1. Теоретические основы исследования

Известна [9] точная нижняя граница диаметра двумерных циркулянтов $C(N; s_1, s_2)$ для любого $N \geqslant 5$:

$$d(N) \geqslant D(N) = \lceil(-1 + \sqrt{2N - 1})/2\rceil.$$

Гипотеза Цвиели [13] предполагает, что для любого N имеет место верхняя оценка

$$d(N) \leqslant D(N) + 1,$$

которая подтверждена при $N \leqslant 6 \cdot 10^6$. Графы с $d(N) = D(N) + 1$ называются *субоптимальными*. Большая часть работ в литературе посвящена изучению диаметра циркулянтных графов, и известно немного работ по исследованиям среднего расстояния циркулянтов и его соотношения с диаметром.

В [14] показано, что нижняя граница среднего расстояния графов $C(N; s_1, s_2)$ асимптотически стремится к $\sqrt{2N}/3$. В [15] получена нижняя граница среднего расстояния двумерных циркулянтов:

$$\overline{d}(N) = (N - 1)\sqrt{2N - 1}/3N.$$

В [16] приведены некоторые соотношения между диаметром и средним расстоянием в оптимальных графах $C(N;1,s)$. Дан пример, когда оптимальный по диаметру граф хуже по среднему расстоянию графа с большим на единицу диаметром. Аналогичное свойство отмечено для циркулянтных графов большей размерности $k=3,4,5$.

Очевидно, что среднее расстояние, как показатель топологии сети связи, зависит от числа вершин графа, находящихся на определённых расстояниях (уровнях одинакового расстояния) от выделенной вершины. В силу вершинной симметрии циркулянтов в качестве выделенной рассматривается вершина с номером 0. Пусть n_i обозначает число вершин, находящихся на расстоянии i от 0, $i \in \overline{1,d}$, d — диаметр графа. Для двумерных циркулянтов максимально возможное число вершин на i-м уровне равно $4i$ [17, 18]. Циркулянт с полностью заполненными уровнями, включая диаметр, называется *экстремальным*. Семейство экстремальных двумерных кольцевых циркулянтов существует при любом диаметре [9] и имеет вид $\{C(N_d;1,2d+1) \mid d \geqslant 1\}$, где $N_d = 2d^2+2d+1$. При этом среднее расстояние для графов экстремального семейства равно $\overline{d} = (2d+1)/3$ [15]. Исследованию распределения вершин графов по уровням для семейств экстремальных (и наибольших известных) циркулянтов размерностей $k=2,3,4,5$ посвящена работа [19].

Введём понятие *идеального* оптимального графа $C(N;1,s)$, следуя [5]. В идеальном оптимальном графе распределение вершин по уровням расстояния относительно вершины 0 задаётся формулой

$$N = 1 + \sum_{i=1}^{d-1} n_i + (N - N_{d-1}), \quad n_i = 4i,\ i \in \overline{1,d-1}. \tag{1}$$

Другими словами, для идеального циркулянта распределение числа вершин по уровням расстояний от 0 до d можно представить в виде $(d+1)$-мерного вектора $(1,4,\ 8,\ldots,4(d-1),N-N_{d-1})$. Следует отметить, что впервые формула для среднего расстояния идеальных графов появилась в работе [17]. Из принадлежности графа к множеству идеальных следует равенство его диаметра точной нижней границе $D(N)$. Идеальные графы достигают минимумов структурных задержек и максимума связности [17, 20].

В работе [5] в диапазоне $5 \leqslant N \leqslant 1000$ найден 361 идеальный граф и проведён анализ полученного множества идеальных графов. Получено несколько семейств идеальных графов, описываемых полиномами от диаметра:

$$N \in \{2d^2; 2d^2 \pm 1; 2d^2+2d-1\}, \quad s = 2d-1, \quad d > 1;$$
$$N = 2d^2 - 2d + 5, \quad d > 5, \tag{2}$$

$$s = \begin{cases} (2d^2 - 4d)/3 + 2 & \text{при } d = 3i,\ i \geqslant 2, \\ (2d^2 + 4)/3 & \text{при } d = 3i + 1,\ i \geqslant 2. \end{cases} \tag{3}$$

Формулу (3) для образующей s последнего семейства авторы [5] найти не смогли, при этом указали формулу (2) для N и для всех семейств вычислили среднее расстояние в виде функции от диаметра. Исправляя неточность в [5], приводим выражение среднего расстояния для семейства (2), (3):

$$\overline{d}(N; 1, s) = d(2d^2 - 3d + 7)/(3(d^2 - d + 2)), \quad d > 5.$$

Для других идеальных графов авторы [5] отмечают, что не нашли общего способа их построения.

В разд. 2 дано решение этого вопроса, а также построены новые базы данных — оптимальных по среднему расстоянию циркулянтов и идеальных графов. В разд. 3 приведены результаты получения большого количества семейств идеальных оптимальных графов $C(N; 1, s)$ с порядками и образующими, описанными в виде полиномов от диаметра, а также дана общая формула для среднего расстояния в графах идеальных семейств. В разд. 4 среди семейств идеальных графов найдены масштабируемые семейства, для которых применим оптимальный алгоритм маршрутизации, использующий параметры укладки циркулянтов на плоскости.

2. Новые датасеты оптимальных циркулянтов

В Интернете можно найти датасет оптимальных циркулянтов размерностей $k = 2, 3, 4, 5$ порядков $10 \leqslant N \leqslant 500$ [21], в котором для каждого N приведён один набор образующих при $s_1 = 1$. Полученный авторами и представленный в открытом доступе [11] датасет оптимальных по диаметру циркулянтов $C(N; 1, s)$ размерности $k = 2$ порядков $10 \leqslant N \leqslant 50\,000$ включает уже весь набор образующих оптимальных графов, что позволяет находить семейства оптимальных по диаметру циркулянтных графов, описанных полиномами от диаметра [12]. В настоящей работе продолжен поиск и исследование наилучших возможных графов класса $C(N; 1, s)$.

Найдено аналитическое выражение для среднего расстояния идеального графа $C(N; 1, s)$, используемое далее при получении множеств (семейств) идеальных графов. Эта же формула является нижней границей среднего расстояния в графах $C(N; 1, s)$ при $N_{d-1} < N \leqslant N_d$. Из определения идеального графа $C(N; 1, s)$ с числом вершин N, где $d(N) = D(N)$, следует равенство

$$\overline{D}(N) = \overline{d}(N) = d(3N - 2d^2 - 1)/(3(N - 1)), \tag{4}$$

которое является необходимым и достаточным условием того, что двумерный кольцевой циркулянт с числом вершин N и диаметром $d = D(N)$ является идеальным графом. Тем самым обобщён результат из [5] и найдена в общем виде формула среднего расстояния идеального графа, поэтому при проверке на принадлежность графа к множеству идеальных достаточно проверять выполнение (4). Формулу (4) можно использовать также для аналитического определения среднего расстояния в графах семейств идеальных графов в случае, если порядок N графов идеального семейства описан как функция от диаметра d.

Результатом представленной работы являются два новых датасета оптимальных графов $C(N; 1, s)$:

1) MPLset — параметры оптимальных по среднему расстоянию графов;

2) IDset — параметры идеальных графов.

Для вычислений используется система Wolfram Mathematica. Отметим, что также можно использовать систему Wolfram Engine — свободно распространяемую альтернативу Wolfram Mathematica с урезанным графическим интерфейсом.

Алгоритм построения датасета MPLset сводится к полному перебору образующих $2 \leqslant s < N/2$ для каждого испытуемого порядка $N \leqslant 4100$ и формированию описаний всех графов с минимально возможным для

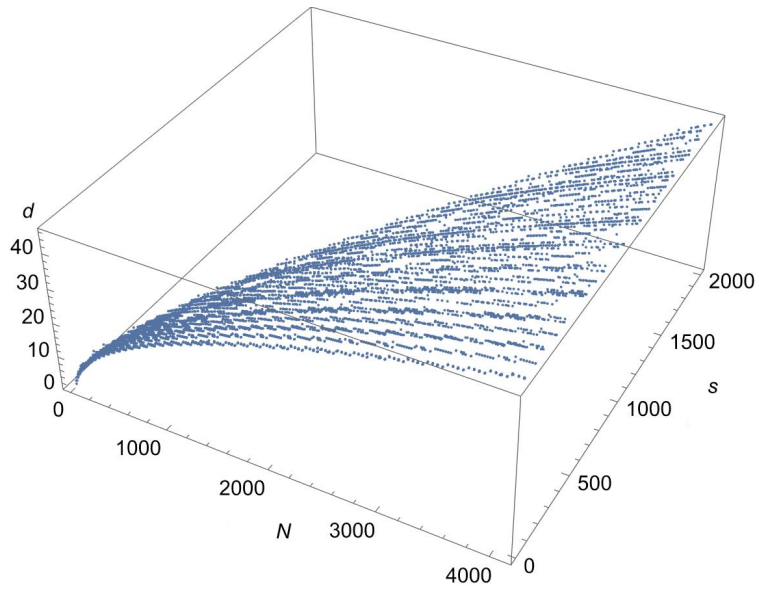


Рис. 2. Параметры графов $C(N; 1, s)$ из датасета MPLset

данного N средним расстоянием:

$$\mathrm{MPLset} = \big\{(N,s) \in \mathbb{N} \mid \overline{d}(N) = \min_{2 \leqslant s < N/2} \overline{d}(N;1,s),\ N \leqslant 4100\big\}.$$

Для повышения скорости вычислений проведено их распараллеливание по наборам образующих.

Датасет IDset идеальных графов строится перебором и поиском графов из множества MPLset, удовлетворяющих условию идеальности (1). Для найденных графов также проведена проверка равенства среднего расстояния нижней границе (4).

На рис. 2 и 3 представлены трёхмерные графики полученных датасетов точек $(N, s, d, \overline{d})$ при $10 \leqslant N \leqslant 4100$, отражающие параметры оптимальных по среднему расстоянию и идеальных графов. Для каждого значения N на графиках показаны все образующие $s < N/2$, определяющие оптимальный граф. Датасеты найденных оптимальных графов с числом вершин $N \leqslant 4100$ доступны по ссылке [11].

На рис. 4 изображены графики зависимостей диаметра d и среднего расстояния $\overline{d}$ от порядка N для графов из датасета MPLset — циркулянтов $C(N;1,s)$ с минимально возможным средним расстоянием.

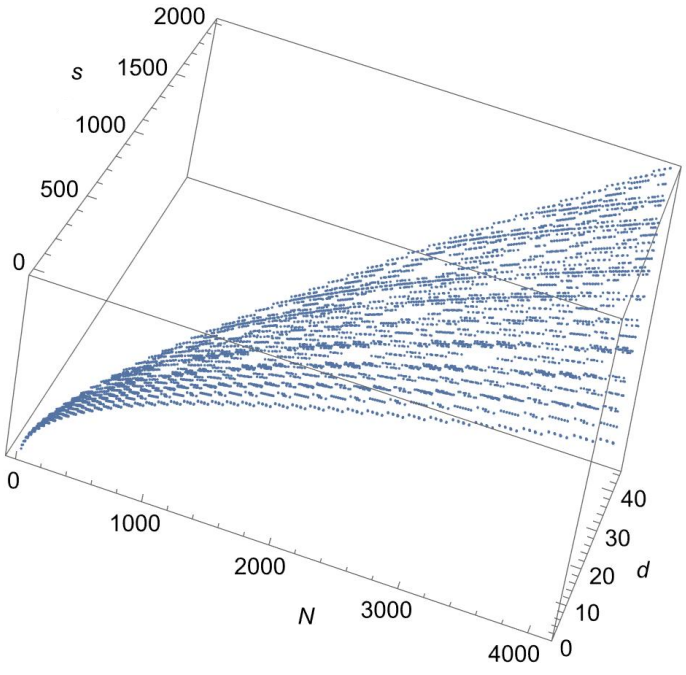


Рис. 3. Параметры идеальных графов $C(N;1,s)$ из датасета IDset

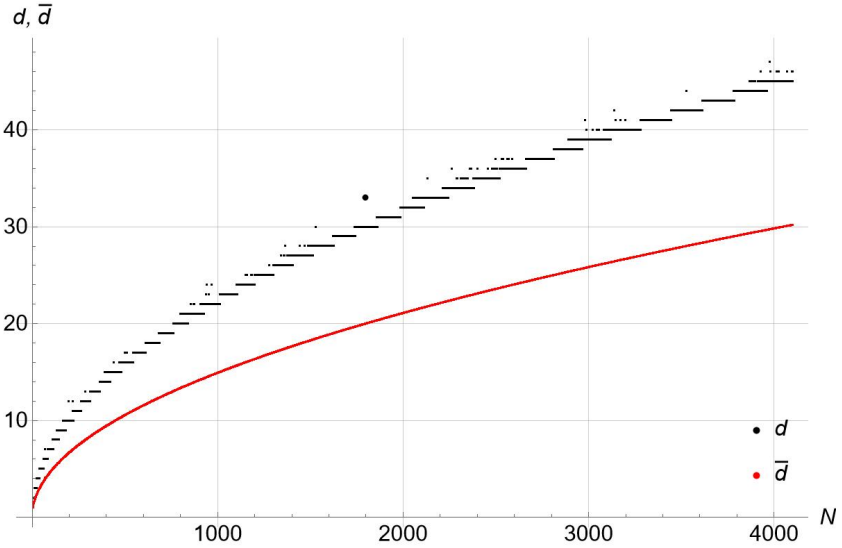


Рис. 4. Зависимости диаметра и среднего расстояния от порядка графа для датасета MPLset

На основе анализа найденных графов можно отметить следующие соотношения свойств оптимальных графов трёх видов.

1. Не для всех N достигаются нижние границы диаметра и среднего расстояния в классе циркулянтов $C(N;1,s)$.

2. Существуют субоптимальные и оптимальные по диаметру графы с одинаковым средним расстоянием. Например, $d(30;1,8) = D(30) = 4$, $d(30;1,6) = 5$. Векторы распределения вершин по уровням: $(1,4,8,9,8)$ для $s = 8$ и $(1,4,8,10,6,1)$ для $s = 6$, при этом для обоих графов имеем $\overline{d} = 2{,}6333$.

3. При одинаковом $d = D(N) + 1$ различные распределения вершин по уровням могут давать одинаковое среднее расстояние. Например, неизоморфные субоптимальные графы $C(30;1,4)$ и $C(30;1,7)$ имеют одинаковые диаметр $d = 5$ и среднее расстояние $\overline{d} = 2{,}7$, а векторы распределения по уровням равны $(1,4,8,8,8,1)$ и $(1,4,8,9,6,2)$ соответственно.

4. Диаметр графа с минимальным средним расстоянием может превышать нижнюю границу для диаметра на 3 (на рис. 4 этот случай отмечен крупной точкой). Так, оптимальный по среднему расстоянию граф $C(1798;1,762)$ имеет $d = 33$ и $\overline{d} = \overline{d}(1798) = 20{,}01$ в отличие от оптимального по диаметру графа $C(1798;1,544)$, у которого $d = d(1798) = D(1798) = 30$ и $\overline{d} = 20{,}02$.

5. Только идеальные циркулянты достигают одновременно нижних границ диаметра $D(N)$ и среднего расстояния $\overline{D}(N)$.

Среди 8499 графов датасета MPLset с $5 \leqslant N \leqslant 4100$ идеальными оказались 7955 (более 93%). Отметим, что для $5 \leqslant N \leqslant 1000$ число идеальных графов равно 911, что существенно больше, чем 361 идеальный граф, найденный ранее в [5].

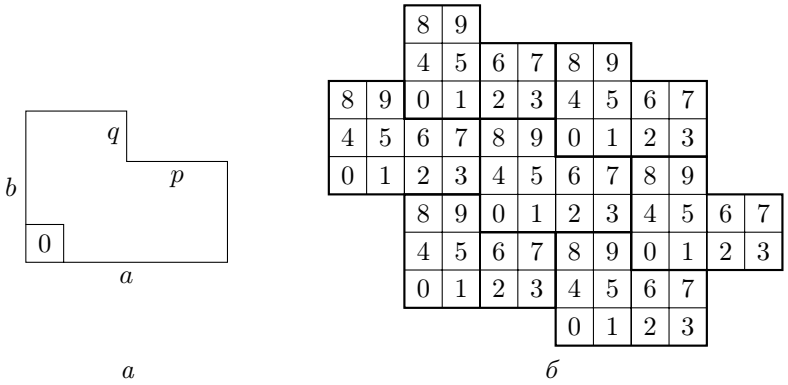
3. Экспериментальные результаты поиска семейств идеальных сетей

Дадим сначала общую формулировку понятия семейства оптимальных графов в классе $C(N;1,s)$. Под семейством оптимальных (идеальных) сетей будем понимать подмножество оптимальных (идеальных) графов класса $C(N;1,s)$ с общим аналитическим описанием $N = N(d)$ и $s = s(d)$ и диаметром, растущим по правилу $d = d_m + kP$, где $k \geqslant 0$, d_m — минимальный диаметр, при котором граф семейства является оптимальным (идеальным), $P = \text{const} \in \mathbb{N}$ — период повторяемости, равный разности диаметров «соседних» графов семейства.

На первом этапе поиска семейств идеальных сетей к графам датасета MPLset, оптимальных по среднему расстоянию, применены алгоритмы автоматизированного поиска аналитически описываемых семейств [12]. Порядки найденных семейств графов представляют собой квадратичные полиномы, а их образующие — квадратичные или линейные полиномы от диаметра d. Полученные семейства графов существуют в соответствующих диапазонах изменения диаметра d. Затем проверено существование найденных семейств при диаметрах больших, чем диаметры графов датасета MPLset (при $4100 < N \leqslant 50\,000$). Для этого этапа использована программа анализа структурных характеристик циркулянтных графов, которая дополнительно находит векторы распределения вершин по уровням. На заключительном этапе графы оставшихся семейств проверены на выполнение равенства (4). В результате осталось 1756 семейств идеальных сетей, список которых также помещён в [11].

4. Идеальные циркулянтные сети и оптимальный алгоритм маршрутизации

В [22] на основе датасета оптимальных по диаметру графов $C(N;1,s)$ получено множество семейств оптимальных графов, для которых дополнительно разработан эффективный оптимальный алгоритм маршрутизации [22] сложности $O(1)$, не требующий таблиц маршрутизации и использующий параметры плотной укладки циркулянтов на плоскости в виде L-образных шаблонов (L-shapes) [18, 23, 24]. Параметры a, b, p, q L-образных шаблонов для циркулянтов $C(N;1,s)$ показаны на рис. 5а. На рис. 5б изображена плотная укладка на плоскости L-образного шаблона для графа $C(10;1,4)$ с параметрами $a = 4$, $b = 3$, $p = 2$, $q = 1$.



а *б*

Рис. 5. а) Параметры L-образного шаблона; б) плотная укладка L-образного шаблона на плоскости для графа $C(10; 1, 4)$

В [23] доказано, что L-образный шаблон циркулянтов $C(N; s_1, s_2)$ всегда образует плотную укладку на плоскости, и получена следующая базовая система сравнений для расположения нулей (вершин с номером 0) на плоскости:

$$\begin{aligned} as_1 - qs_2 &\equiv 0 \pmod N, \\ -ps_1 + bs_2 &\equiv 0 \pmod N. \end{aligned} \tag{5}$$

В [22] введено понятие L-масштабируемости аналитически описанных семейств оптимальных графов, которое будем использовать далее при анализе множества полученных семейств идеальных сетей. Семейство $C(N(d); 1, s(d))$ *L-масштабируемо*, если существуют функции $a(d)$, $b(d)$, $p(d)$, $q(d)$, описывающие параметры L-образных шаблонов плотной укладки графов семейства на плоскости, для которых выполняется система сравнений (5). L-масштабируемость семейств графов позволяет определить параметры a, b, p, q укладки графов семейств в виде линейных полиномов от диаметра, тем самым сокращая сложность алгоритмов их определения с $O(N)$ [18] (или $O(\log N)$ [24]) до $O(1)$.

С использованием системы Wolfram Mathematica авторами проведена проверка выполнения сравнений (5) для идеальных семейств, взятых из датасета IDset с параметрами N, s, a, b, p, q, описанными в виде полиномов от диаметра. После проверки, проведённой на всём множестве идеальных семейств, найдено 869 описаний L-масштабируемых идеальных семейств, список которых дан в соответствующем разделе датасета [11]. Для этих семейств применим алгоритм маршрутизации из [22] с аналитическим определением параметров L-образных шаблонов. Ниже приведён фрагмент описаний семейств, существующих для каждого диаметра $d \geqslant d_m$. Список включает для представленных семейств значения d_m, период повторяемости P, полиномы для N и s, коэффициенты

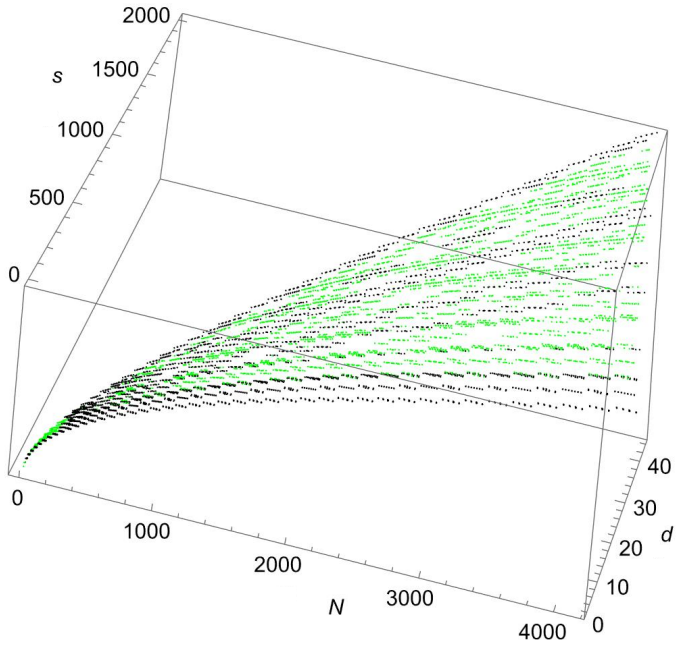


Рис. 6. Точки датасета L-масштабируемых идеальных семейств (чёрные) и датасета IDset идеальных циркулянтных графов (зелёные точки)

при степенях d для параметров a, b, p, q. На рис. 6 показан трёхмерный график датасета точек (N, s, d), $10 \leqslant N \leqslant 4100$, полученных по описаниям L-масштабируемых идеальных семейств (чёрные точки) на фоне датасета всех идеальных графов (зелёные точки). Здесь N — число вершин графа, s — образующая, d — диаметр, $\overline{d}$ — среднее расстояние графа $C(N; 1, s)$.

Фрагмент датасета семейств идеальных графов с аналитическим описанием и масштабируемыми параметрами L-образных шаблонов в формате $\{d_m, P = 1, \{N, s\}, \{\{a_1, a_0\}, \{b_1, b_0\}, \{p_1, p_0\}, \{q_1, q_0\}\}\}$:

$$\{2, 1, \{1 + 2d + 2d^2, 1 + 2d\}, \{\{2, 1\}, \{1, 1\}, \{1, 0\}, \{0, 1\}\}\},$$
$$\{3, 1, \{2d^2, -1 + 2d\}, \{\{2, -1\}, \{1, 1\}, \{1, -1\}, \{0, 1\}\}\},$$
$$\{3, 1, \{2d^2, 1 + 2d\}, \{\{1, 0\}, \{3, -1\}, \{1, -1\}, \{1, 0\}\}\},$$
$$\{3, 1, \{-1 + 2d^2, -1 + 2d\}, \{\{2, -1\}, \{1, 1\}, \{1, 0\}, \{0, 1\}\}\},$$
$$\{3, 1, \{-1 + 2d^2, 1 + 2d\}, \{\{1, 1\}, \{2, -1\}, \{0, 1\}, \{1, 0\}\}\},$$
$$\{3, 1, \{1 + 2d^2, -1 + 2d\}, \{\{2, -1\}, \{1, 1\}, \{1, -2\}, \{0, 1\}\}\},$$
$$\{3, 1, \{1 + 2d^2, 1 + 2d\}, \{\{2, 1\}, \{1, 0\}, \{1, -1\}, \{0, 1\}\}\},$$

$$\{2,1,\{d+2d^2,2d\},\{\{2,0\},\{1,1\},\{1,0\},\{0,1\}\}\},$$
$$\{3,1,\{-1-d+2d^2,-2+2d\},\{\{2,-2\},\{1,1\},\{1,-1\},\{0,1\}\}\},$$
$$\{3,1,\{-d+2d^2,2d\},\{\{1,0\},\{2,-1\},\{0,0\},\{1,0\}\}\},$$
$$\{3,1,\{-d+2d^2,-2+2d\},\{\{2,-2\},\{1,1\},\{1,-2\},\{0,1\}\}\},$$
$$\{3,1,\{1-d+2d^2,2d\},\{\{2,0\},\{1,0\},\{1,-1\},\{0,1\}\}\},$$
$$\{3,1,\{-3+d+2d^2,-2+2d\},\{\{2,-2\},\{1,2\},\{1,-1\},\{0,1\}\}\},$$
$$\{3,1,\{-2+d+2d^2,-2+2d\},\{\{2,-2\},\{1,2\},\{1,-2\},\{0,1\}\}\}.$$

Интересно отметить, что оптимальный граф $C(10;1,4)$, изображённый на рис. 1, идеальный и принадлежит семейству $\{C(2d^2+d;1,2d) \mid d \geqslant 2\}$. Более того, это семейство L-масштабируемо, что покажем далее.

Лемма 1. *Параметры L-образных шаблонов для семейства оптимальных циркулянтов $C(2d^2+d;1,2d)$, где $d \geqslant 2$, равны $a=2d$, $b=d+1$, $p=d$, $q=1$.*

Доказательство. Достаточно показать, что базовая система сравнений (5) для расположения нулевых вершин на плоскости выполняется для указанных параметров при любом $d \geqslant 2$. Имеем

$$2d-2d=0\equiv 0 \pmod N,$$
$$-d+(d+1)2d=2d^2+d=N\equiv 0 \pmod N.$$

Лемма 1 доказана.

Покажем, что семейство идеальных графов (2), (3) также L-масштабируемо.

Лемма 2. *Параметры L-образных шаблонов для семейства оптимальных циркулянтов $C(2d^2-2d+5;1,s)$ с образующей*

$$s=\begin{cases}(2d^2-4d)/3+2 & \text{при } d=3i,\\ (2d^2+4)/3 & \text{при } d=3i+1,\end{cases}$$

где $d>5$, равны

$$\begin{cases}a=d+1,\ b=2d-1,\ p=3,\ q=d-2 & \text{при } d=3i,\\ a=2d-1,\ b=d+1,\ p=d-2,\ q=3 & \text{при } d=3i+1.\end{cases}$$

Доказательство. Покажем, что базовая система сравнений (5) выполняется для указанных параметров при $d>5$.

Если $d=3i$, $i\geqslant 2$, имеем

$$(d+1)-(d-2)((2d^2-4d)/3+2)=(1-d/3)N\equiv 0 \pmod N,$$
$$-3+(2d-1)((2d^2-4d)/3+2)=(2d/3-1)N\equiv 0 \pmod N.$$

Аналогично, если $d = 3i + 1$, $i \geqslant 2$, имеем

$$(2d-1) - 3(2d^2+4)/3 = -N \equiv 0 \pmod{N},$$
$$-(d-2) + (d+1)(2d^2+4)/3 = ((d+2)/3)N \equiv 0 \pmod{N}.$$

Лемма 2 доказана.

Таким образом, ко всем графам семейств из лемм 1 и 2, а также всех найденных идеальных L-масштабируемых семейств может быть применён оптимальный алгоритм маршрутизации из [22]. В отличие от ряда других алгоритмов поиска кратчайших путей, использующих плотную укладку графов на плоскости [25, 26], указанный алгоритм использует минимальное число (пять) соседних нулей, при этом затрачивает меньшее число операций при расчёте кратчайшего пути по сравнению с алгоритмом из [27]. Продемонстрируем работу алгоритма маршрутизации на примере графов идеального семейства из леммы 2. Ниже запись вида $a_1[+1] + b_1[+s]$ означает, что путь из 0 в вершину i содержит a_1 шагов по образующей $s_1 = 1$ и b_1 шагов по образующей s. Знаки a_1 и b_1 определяют направление движения: в направлении образующей $(+)$ или против образующей $(-)$.

Пример 1. В качестве топологии рассмотрим граф $C(65; 1, 18)$ семейства (2), (3) диаметра $d = 6$. Пусть требуется вычислить кратчайший путь из 0 в вершину $i = 50$. Имеем $a = 7$, $b = 11$, $p = 3$, $q = 4$, $u = a - p = 4$, $v = b - q = 7$.

Шаг 1. $a_0 = 7$, $b_0 = 4$.

Шаг 2. $(a_1, b_1) = (50, 0) - \mathrm{round}\big(\frac{1}{65}(50, 0)\left(\begin{smallmatrix} 4 & -7 \\ 7 & 4 \end{smallmatrix}\right)\big)\left(\begin{smallmatrix} 4 & 7 \\ -7 & 4 \end{smallmatrix}\right) = (3, -1)$.

Шаг 3. $P_1 = (3)[+1] + (-1)[+18]$; $P_2 = (-1)[+1] + (-8)[+18]$; $P_3 = (10)[+1] + (-5)[+18]$; $P_4 = (7)[+1] + (6)[+18]$; $P_5 = (-4)[+1] + (3)[+18]$. Кратчайший из пяти путей в вершину $i = 50$ есть $P' = P_1$.

Пример 2. Рассмотрим граф $C(89; 1, 34)$ семейства (2), (3) диаметра $d = 7$. Требуется вычислить кратчайший путь из 0 в вершину $i = 6$. Имеем $a = 13$, $b = 8$, $p = 5$, $q = 3$, $u = a - p = 8$, $v = b - q = 5$.

Шаг 1. $a_0 = 5$, $b_0 = 8$.

Шаг 2. $(a_1, b_1) = (6, 0) - \mathrm{round}\big(\frac{1}{89}(6, 0)\left(\begin{smallmatrix} 8 & -5 \\ 5 & 8 \end{smallmatrix}\right)\big)\left(\begin{smallmatrix} 8 & 5 \\ -5 & 8 \end{smallmatrix}\right) = (-2, -5)$.

Шаг 3. $P_1 = (-2)[+1] + (-5)[+34]$; $P_2 = (-10)[+1] + (-10)[+34]$; $P_3 = (3)[+1] + (-13)[+34]$; $P_4 = (6)[+1] + (0)[+34]$; $P_5 = (-7)[+1] + (3)[+34]$. Кратчайший из пяти путей в вершину $i = 6$ есть $P' = P_4$.

Таким образом, графы из найденных в настоящей работе семейств идеальных циркулянтных сетей обладают не только минимально возможными структурными задержками при межузловых обменах, но и эффективной организацией маршрутизации. Вопросы полноты множества

семейств идеальных графов $C(N;1,s)$ на основе полученных датасетов являются темой для будущих исследований.

Заключение

В данной работе продолжены исследования, начатые в цикле статей по генерации датасетов оптимальных кольцевых циркулянтных сетей степени четыре. Проектирование оптимальных сетевых топологий, обладающих симметрией связей и минимальными структурными задержками при межузловых обменах, является одним из основных критериев при разработке сетей на кристалле. На основе анализа больших массивов экспериментальных данных нами исследовано решение проблемы поиска двумерных кольцевых циркулянтных сетей, оптимальных по двум параметрам — диаметру и среднему расстоянию. Получены и представлены в открытом доступе новые датасеты рассматриваемых сетей - оптимальных по среднему расстоянию и наилучших возможных по двум параметрам так называемых идеальных сетей. Существенно расширено исследование свойств идеальных циркулянтных сетей, что позволило открыть множество аналитически задаваемых семейств идеальных циркулянтных сетей. Для таких семейств идеальных сетей применим эффективный, масштабируемый по числу узлов алгоритм маршрутизации сложности $O(1)$. Нахождение аналитическими вычислениями оптимальных топологий с симметричной структурой построения подсистемы связей и минимальными задержками гарантирует простоту инженерных решений и повышение эффективности функционирования сетей на кристалле при обменах.

Финансирование работы

Исследование выполнено за счёт бюджетного проекта Института вычислительной математики и математической геофизики СО РАН (проект № FWNM–2025–0005). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Huang X., Ramos A. F., Deng Y.** Optimal circulant graphs as low-latency network topologies // J. Supercomputing. 2022. V. 78, No. 11. P. 13491–13510. DOI: 10.1007/s11227-022-04396-5.
2. **Liu H., Li X., Wang S.** Construction of dual optimal bidirectional double-loop networks for optimal routing // Mathematics. 2022. V. 10. Article ID 4016. 17 p. DOI: 10.3390/math10214016.

3. **Hoffmann R., Deserable D., Seredynski F.** Cellular automata rules solving the wireless sensor network coverage problem // Nat. Comput. 2022. V. 21. P. 417–447.
4. **Fei J., Lu C.** Adaptive sliding mode control of dynamic systems using double loop recurrent neural network structure // IEEE Trans. Neural Netw. Learn. Syst. 2018. V. 29. P. 1275–1286.
5. **Ledziński D., Bujnowski S., Marciniak T., Pedersen J. M., Gutierrez Lopez J. M.** Networks structures constructed on basis of chordal rings 4th degree // Image processing and communications challenges 5. Proc. 5th Int. Conf. (Bydgoszcz, Poland, Sept. 11–13, 2013). Cham: Springer, 2014. P. 281–299. (Adv. Intell. Syst. Comput.; V. 233). DOI: 10.1007/978-3-319-01622-1_33.
6. **Martínez C., Vallejo E., Beivide R., Izu C., Moretó M.** Dense Gaussian networks: Suitable topologies for on-chip multiprocessors // Int. J. Parallel Program. 2006. V. 34, No. 3. P. 193–211. DOI: 10.1007/s10766-006-0014-1.
7. **Bermond J.-C., Comellas F., Hsu D. F.** Distributed loop computer networks: A survey // J. Parallel Distrib. Comput. 1995. V. 24, No. 1. P. 2–10. DOI: 10.1006/jpdc.1995.1002.
8. **Hwang F. K.** A survey on multi-loop networks // Theor. Comput. Sci. 2003. V. 299, No. 1–3. P. 107–121.
9. **Monakhova E. A.** A survey on undirected circulant graphs // Discrete Math. Algorithms Appl. 2012. V. 4, No. 1. Article ID 1250002. 30 p.
10. **Deng Y., Guo M., Ramos A. F., Huang X., Xu Z., Liu W.** Optimal low-latency network topologies for cluster performance enhancement // J. Supercomputing. 2020. V. 76, No. 12. P. 9558–9584.
11. **Monakhova E. A., Monakhov O. G.** Double-loop-networks. Datasets of optimal double loop networks or optimal circulant graphs $(N; 1, s)$. 2024. github.com/mila0411/Double-loop-networks (accessed: 29.08.2025).
12. **Монахова Э. А., Монахов О. Г.** Анализ базы данных оптимальных двухконтурных кольцевых сетей // Прикл. дискрет. математика. 2024. № 64. С. 56–71.
13. **Tzvieli D.** Minimal diameter double-loop networks. I. Large infinite optimal families // Networks. 1991. V. 21, No. 4. P. 387–415.
14. **Bermond J.-C., Illiades G., Peyrat C.** An optimization problem in distributed loop computer networks // Ann. New York Acad. Sci. 1989. V. 555, No. 1. P. 45–55.
15. **Browne R. F., Hodgson R. M.** Symmetric degree-four chordal ring networks // IEE Proc. Ser. E. 1990. V. 137, No. 4. P. 310–318.
16. **Bian Q.-F., Hang T., Liu H., Fang M.** Research on the diameter and average diameter of undirected double-loop networks // Proc. 9th Int. Conf. Grid and Cloud Computing (Nanjing, China, Nov. 1–5, 2010). Los Alamitos: IEEE Comput. Soc., 2010. P. 461–466.
17. **Корнеев В. В.** О макроструктуре однородных вычислительных систем // Вычислительные системы. Вып. 60. Вопросы теории и построения вычислительных систем. Новосибирск: ИМ СО АН СССР, 1974. С. 17–34.

18. Wong C. K., Coppersmith D. A combinatorial problem related to multimodule memory organizations // J. ACM. 1974. V. 21, No. 3. P. 392–402.
19. Lewis R. R. Distance partitions of extremal and largest known circulant graphs of degree 2 to 9. Ithaca, NY, 2014. 22 p. (e-Print Archive / Cornell Univ.; arXiv:1408.0988).
20. Boesch F., Wang J.-F. Reliable circulant networks with minimum transmission delay // IEEE Trans. Circuits Syst. 1985. V. 32, No. 12. P. 1286–1291.
21. Romanov A. Yu. The dataset for optimal circulant topologies // Big Data Cogn. Comput. 2023. V. 7, No. 2. Article ID 80. 14 p.
22. Монахов О. Г., Монахова Э. А. Масштабируемый подход к кодизайну топологий и алгоритмов маршрутизации для семейств оптимальных циркулянтных сетей степени четыре // Дискрет. анализ и исслед. операций. 2025. Т. 32, № 2. С. 88–106.
23. Fiol M. À., Yebra J. L. A., Alegre I., Valero M. A discrete optimization problem in local networks and data alignment // IEEE Trans. Comput. 1987. V. C-36, No. 6. P. 702–713.
24. Hwang F. K. A complementary survey on double-loop networks // Theor. Comput. Sci. 2001. V. 263, No. 1–2. P. 211–229.
25. Jha P. K. Dimension-order routing algorithms for a family of minimal-diameter circulants // J. Interconnect. Netw. 2013. V. 14, No. 1. Article ID 1350002. 24 p.
26. Camarero C., Martinez C., Beivide R. L-networks: A topological model for regular two-dimensional interconnection networks // IEEE Trans. Comput. 2013. V. 62, No. 7. P. 1362–1375.
27. Chen B.-X., Meng J.-X., Xiao W.-J. A constant time optimal routing algorithm for undirected double-loop networks // Mobile ad-hoc and sensor networks. Proc. 1st Int. Conf. (Wuhan, China, Dec. 13–15, 2005). Heidelberg: Springer, 2005. P. 308–316. (Lect. Notes Comput. Sci.; V. 3794).

Монахова Эмилия Анатольевна
Монахов Олег Геннадьевич

Статья поступила
29 ноября 2024 г.
После доработки —
21 декабря 2024 г.
Принята к публикации
22 марта 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 98–116

UDC 519.176+519.8+519.7 DOI: 10.33048/daio.2025.32.820

SEARCH AND RESEARCH OF IDEAL TWO-DIMENSIONAL CIRCULANT NETWORKS BASED ON GRAPH DATABASES

E. A. Monakhova[a] and *O. G. Monakhov*[b]

Institute of Computational Mathematics and Mathematical Geophysics,
6 Acad. Lavrentiev, 630090 Novosibirsk, Russia
E-mail: [a] emilia@rav.sscc.ru, [b] monakhov@rav.sscc.ru

Abstract. Based on analysis of large arrays of experimental data, the problem of finding ideal two-dimensional ring circulant networks optimal with respect to two parameters, diameter and average distance, is investigated. Previously, the authors obtained a large dataset (database) of two-dimensional ring circulant networks that are optimal with respect to diameter. In this paper, a new dataset of the considered networks that are optimal with respect to average distance is obtained. The study of the graphs of these datasets allowed us to derive new properties of the ratios of diameter and average distance in optimal circulants and to obtain families of the best optimal circulant networks with respect to two parameters, for which an efficient routing algorithm of constant complexity, adjustable by the number of nodes, is applicable. Ideal two-dimensional ring circulants are of interest as efficient and reliable topologies for inter-node connections in networks on a chip and information and communication systems. Illustr. 6, bibliogr. 27.

Keywords: undirected double loop network, diameter, mean distance, dataset of optimal circulant networks, routing algorithm.

References

1. **X. Huang, A. F. Ramos,** and **Y. Deng,** Optimal circulant graphs as low-latency network topologies, *J. Supercomputing* **78** (11), 13491–13510 (2022), DOI: 10.1007/s11227-022-04396-5.
2. **H. Liu, X. Li,** and **S. Wang,** Construction of dual optimal bidirectional double-loop networks for optimal routing, *Mathematics* **10**, ID 4016 (2022), DOI: 10.3390/math10214016.

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

3. **R. Hoffmann, D. Deserable,** and **F. Seredynski,** Cellular automata rules solving the wireless sensor network coverage problem, *Nat. Comput.* **21**, 417–447 (2022).
4. **J. Fei** and **C. Lu,** Adaptive sliding mode control of dynamic systems using double loop recurrent neural network structure, *IEEE Trans. Neural Netw. Learn. Syst.* **29**, 1275–1286 (2018).
5. **D. Ledziński, S. Bujnowski, T. Marciniak, J. M. Pedersen,** and **J. M. Gutierrez Lopez,** Networks structures constructed on basis of chordal rings 4th degree, in *Image Processing and Communications Challenges 5*, Proc. 5th Int. Conf. (Bydgoszcz, Poland, Sept. 11–13, 2013) (Springer, Cham, 2014), pp. 281–299 (Adv. Intell. Syst. Comput., Vol. 233), DOI: `10.1007/978-3-319-01622-1_33`.
6. **C. Martínez, E. Vallejo, R. Beivide, C. Izu,** and **M. Moretó,** Dense Gaussian networks: Suitable topologies for on-chip multiprocessors, *Int. J. Parallel Program.* **34** (3), 193–211 (2006), DOI: `10.1007/s10766-006-0014-1`.
7. **J.-C. Bermond, F. Comellas,** and **D. F. Hsu,** Distributed loop computer networks: A survey, *J. Parallel Distrib. Comput.* **24** (1), 2–10 (1995), DOI: `10.1006/jpdc.1995.1002`.
8. **F. K. Hwang,** A survey on multi-loop networks, *Theor. Comput. Sci.* **299** (1–3), 107–121 (2003).
9. **E. A. Monakhova,** A survey on undirected circulant graphs, *Discrete Math. Algorithms Appl.* **4** (1), ID 1250002 (2012).
10. **Y. Deng, M. Guo, A. F. Ramos, X. Huang, Z. Xu,** and **W. Liu,** Optimal low-latency network topologies for cluster performance enhancement, *J. Supercomputing* **76** (12), 9558–9584 (2020).
11. **E. A. Monakhova** and **O. G. Monakhov,** Double-loop-networks. Datasets of optimal double loop networks or optimal circulant graphs $(N; 1, s)$ (2024), `github.com/mila0411/Double-loop-networks` (accessed: 29.08.2025).
12. **E. A. Monakhova** and **O. G. Monakhov,** Database analysis of optimal double-loop networks, *Prikl. Diskretn. Mat.*, No. 64, 56–71 (2024) [Russian].
13. **D. Tzvieli,** Minimal diameter double-loop networks. I. Large infinite optimal families, *Networks* **21** (4), 387–415 (1991).
14. **J.-C. Bermond, G. Illiades,** and **C. Peyrat,** An optimization problem in distributed loop computer networks, *Ann. New York Acad. Sci.* **555** (1), 45–55 (1989).
15. **R. F. Browne** and **R. M. Hodgson,** Symmetric degree-four chordal ring networks, *IEE Proc, Ser. E*, **137** (4), 310–318 (1990).
16. **Q.-F. Bian, T. Hang, H. Liu,** and **M. Fang,** Research on the diameter and average diameter of undirected double-loop networks, in *Proc. 9th Int. Conf. Grid and Cloud Computing* (Nanjing, China, Nov. 1–5, 2010) (IEEE Comput. Soc., Los Alamitos, 2010), pp. 461–466.
17. **V. V. Korneev,** On macrostructure of homogeneous computing systems, in *Computing Systems*, Vol. 60. Problems of Theory and Construction of Computing Systems (IM SO AN SSSR, Novosibirsk, 1974) [Russian], pp. 17–34.

18. C. K. Wong and **D. Coppersmith,** A combinatorial problem related to multimodule memory organizations, *J. ACM* **21** (3), 392–402 (1974).
19. R. R. Lewis, Distance partitions of extremal and largest known circulant graphs of degree 2 to 9 (Ithaca, NY, 2014) (e-Print Archive / Cornell Univ., arXiv:1408.0988).
20. F. Boesch and **J.-F. Wang,** Reliable circulant networks with minimum transmission delay, *IEEE Trans. Circuits Syst.* **32** (12), 1286–1291 (1985).
21. A. Yu. Romanov, The dataset for optimal circulant topologies, *Big Data Cogn. Comput.* **7** (2), ID 80 (2023).
22. O. G. Monakhov and **E. A. Monakhova,** A scalable approach to co-design of topologies and routing algorithms for families of optimal degree-four circulant networks, *Diskretn. Anal. Issled. Oper.* **32** (2), 88–106 (2025) [Russian] [*J. Appl. Ind. Math.* **19** (2) (2025)].
23. M. À. Fiol, J. L. A. Yebra, I. Alegre, and **M. Valero,** A discrete optimization problem in local networks and data alignment, *IEEE Trans. Comput.* **C-36** (6), 702–713 (1987).
24. F. K. Hwang, A complementary survey on double-loop networks, *Theor. Comput. Sci.* **263** (1–2), 211–229 (2001).
25. P. K. Jha, Dimension-order routing algorithms for a family of minimal-diameter circulants, *J. Interconnect. Netw.* **14** (1), ID 1350002 (2013).
26. C. Camarero, C. Martinez, and **R. Beivide,** L-networks: A topological model for regular two-dimensional interconnection networks, *IEEE Trans. Comput.* **62** (7), 1362–1375 (2013).
27. B.-X. Chen, J.-X. Meng, and **W.-J. Xiao,** A constant time optimal routing algorithm for undirected double-loop networks, in *Mobile Ad-Hoc and Sensor Networks*, Proc. 1st Int. Conf. (Wuhan, China, Dec. 13–15, 2005) (Springer, Heidelberg, 2005), pp. 308–316 (Lect. Notes Comput. Sci., Vol. 3794).

Emilia A. Monakhova
Oleg G. Monakhov

Received November 29, 2024
Revised December 21, 2024
Accepted March 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 117–144

УДК 519.8 DOI: 10.33048/daio.2025.32.827

ГИБРИДНЫЙ АЛГОРИТМ ДЛЯ ДВУХКРИТЕРИАЛЬНОЙ ЗАДАЧИ ОПТИМИЗАЦИИ ТРАФИКА В СЕТИ

А. Д. Юськов[1, a], *И. Н. Кулаченко*[2, b],
А. А. Мельников[2, c], *Ю. А. Кочетов*[2, d]

[1] Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
[2] Институт математики им. С. Л. Соболева,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия
E-mail: [a] a.yuskov@g.nsu.ru, [b] ink@math.nsc.ru,
[c] melnikov@math.nsc.ru, [d] jkochet@math.nsc.ru

Аннотация. Рассматривается задача оптимизации трафика в сети передачи данных. Для моделирования трафика используется имитационная модель. Пути передачи задаются неявно весами дуг. Если поток по дуге превышает её пропускную способность, то дуга считается перегруженной. Задача состоит в минимизации двух целевых функций: числа перегруженных дуг и расстояния от исходного вектора весов при соблюдении ограничений на суммарный поток в сети и появление новых перегруженных дуг. Предложена двухстадийная эволюционная схема, включающая алгоритм локального поиска по окрестностям большой мощности для получения стартового приближения границы Парето. Лучшее соседнее решение ищется при помощи оригинальной модели целочисленного линейного программирования. Проведено сравнение предложенного подхода с лучшими эволюционными алгоритмами на примерах с 628 каналами и 1324 запросами, и показано, что новая схема демонстрирует результаты, статистически лучшие на 15–49% по многим показателям качества (9 из 10). Табл. 3, ил. 6, библиогр. 42.

Ключевые слова: оптимизация «чёрного ящика», матэвристика, поиск с чередующимися окрестностями, OSPF, эволюционный алгоритм.

Введение

В связи с постоянно растущим объёмом интернет-трафика важно эффективно управлять сетевыми ресурсами, что может быть достигнуто

путём грамотной маршрутизации трафика по каналам. Для выбора путей маршрутизации трафика существуют различные протоколы. Методы управления трафиком включают в себя настройку весов каналов (например, в протоколах Open shortest path first (OSPF) и Intermediate system to intermediate system (IS-IS) [1]), использование многопротокольной коммутации по меткам (multiprotocol label switching, MPLS) [2], использование централизованных контроллеров таких, как программно определяемая сеть (software-defined networking, SDN) [3] и сегментная маршрутизация [4].

Такие протоколы, как MPLS, позволяют явно задавать пути для запросов. Это позволяет производить тонкую настройку сети и добиваться большой эффективности. Например, в работах [5, 6] обсуждаются различные точные методы и эвристики для построения маршрутов в сети. Однако такой подход требует больших вычислительных ресурсов для нахождения пути для каждого запроса и из-за этого плохо масштабируется на большие сети. Также в случае отказа соединения или узла придётся заново пересчитать маршруты для всех запросов, которые должны были пройти по этим каналам.

В данной работе рассматриваются протоколы, которые настраиваются путём задания весов сетевых соединений. Часто эти протоколы используют стратегию маршрутизации по кратчайшему пути [1]. Однако в работе не используются какие-либо предположения о структуре протокола. Это связано с тем, что протоколы, используемые на практике, может быть трудно явно записать математически, но потоки трафика, создаваемые протоколом, часто могут быть смоделированы с помощью компьютерной программы. Такие задачи, в которых мы не можем явно оценить целевую функцию и ограничения, называются задачами оптимизации «чёрного ящика» [7–9]. Способ маршрутизации, основанный на кратчайших путях, может быть не таким гибким, как например MPLS, так как не позволяет задавать различные маршруты для отдельных пакетов. Однако он более прост в настройке и эксплуатации, так как требует только настройки весов соединений, а также лучше масштабируется и более устойчив к отказам оборудования.

В протоколе OSPF основной задачей является настройка весов каналов. Это можно сделать, следуя некоторым простым правилам, например установив веса обратно пропорционально пропускной способности канала [10]. Однако такое решение может быть не оптимальным, поэтому существуют также метаэвристические подходы к решению данной задачи. Например, в статье [11] авторы разработали эвристику локального поиска, используя специальную нелинейную функцию стоимости. Следует заметить, что предложенная целевая функция обрела большую популярность в литературе и используется во многих источниках, приведённых

далее. В этой же работе авторы приводят некоторые оценки того, насколько маршрутизация, основанная на весах, может отличаться от оптимальной. В [12] представлен генетический алгоритм для этой задачи поиска весов. Авторы [13] разработали алгоритм реагирования на изменяющиеся условия в сети. Предложенный алгоритм пытается исправить неудовлетворительное состояние сети, возникшее из-за отказа каналов или изменения спроса, путём небольших изменений весов. В последние годы растущий интерес к машинному обучению побудил исследователей применить эти методы и к решению задач маршрутизации трафика [14].

Компании могут преследовать различные цели при построении и изменении сети. В большинстве случаев целью задач маршрутизации трафика является минимизация максимальной нагрузки на канал связи [15], уменьшение задержек в сети [16], улучшение балансировки нагрузки [17] или энергоэффективности [18]. Также популярна целевая функция в виде упомянутой ранее специальной нелинейной функции стоимости [11].

Из-за многокритериального характера задач маршрутизации существует множество статей, посвящённых оптимизации нескольких целевых функций, а наиболее популярным методом решения таких задач являются генетические алгоритмы, так как они естественным образом используют популяцию различных решений. Например, в [19] авторы применяют генетический алгоритм NSGA-II для оптимизации затрат и балансировки нагрузки. Авторы используют точный метод, чтобы получить решения для небольших примеров, и сравнивают эффективность эвристики с решениями на истинной границе Парето. В [20] обсуждается использование эволюционных алгоритмов SPEA2 и NSGA-II для минимизации перегрузки и задержки в сети. Авторы предлагают схему оптимизации, которая должна помочь сетевым администраторам выбрать подходящую конфигурацию для удовлетворения требований. В [18] оптимизируются балансировка нагрузки и энергоэффективность. Авторы предлагают эвристическую схему и сравнивают её с оптимальной производительностью сети. Сравнение алгоритмов SPEA2 и NSGA-II для задачи определения весов с возможными сбоями соединения представлено в [21]. Авторы обнаружили, что алгоритм NSGA-II демонстрирует лучшие общие результаты для больших задач. Более подробный обзор литературы о задаче маршрутизации трафика можно найти в [22].

Также можно отметить, что существует важная задача, являющаяся расширением данной: задача планирования сети, в которой требуется определить, какие соединения будут существовать между узлами и их пропускную способность. В этой задаче обычно учитывается как физическая топология сети, на которой находятся проложенные кабели, так и логическая топология, состоящая из сконфигурированных IP-каналов [23]. Обычно целью оптимизации является нахождение баланса

между стоимостью решения и его устойчивостью к отказам оборудования [24], хотя дополнительно существует большое количество различных критериев, которым должна удовлетворять сеть [25]. Для решения этой задачи также существуют различные методы: запись в виде ЦЛП-модели [26], генетические алгоритмы [27] и подходы с использованием машинного обучения [28]. Данная задача может представлять интерес для будущего исследования. Обзор различных направлений и задач можно найти в [29].

В данной работе рассматривается задача оптимизации, целью которой является минимизация общего числа перегруженных каналов в сети путём корректировки весов каналов. Канал называется перегруженным, если поток по нему превышает его пропускную способность. Потоки вычисляются во время моделирования сетевого протокола, который назначает пути для запросов на основе взвешенных длин путей. В задаче также предпочтительно не изменять веса значительно, поскольку это может привести к неожиданному поведению при практической реализации. Стало быть, вторая целевая функция задачи — минимизировать расстояние до исходного вектора весов. После оптимизации существующей сети качество обслуживания клиентов должно быть не хуже, чем оно было до оптимизации. Тем самым если канал не был перегружен до оптимизации, то в полученном после оптимизации решении он должен оставаться таковым. Кроме того, суммарная нагрузка на сетевые каналы не должна увеличиваться. Эти два условия являются строгими ограничениями в задаче. Такие целевые функции и ограничения зависят от значений потока трафика, полученных с помощью имитационной модели.

Основным результатом работы является следующее. Для данной задачи маршрутизации трафика в сети передачи данных предложена двухстадийная эволюционная схема. Она включает в себя алгоритм локального поиска по окрестностям большой мощности для получения стартового приближения границы Парето. Лучшее соседнее решение ищется при помощи оригинальной модели целочисленного линейного программирования. Проведено сравнение предложенного подхода с лучшими эволюционными алгоритмами, и показано, что новая схема демонстрирует результаты, которые статистически лучше на 15–49% по многим показателям качества (9 из 10). Данная статья является расширенным вариантом работы, представленной на конференции OPTIMA 2023 [30].

В разд. 1 приведена математическая модель задачи. В разд. 2 представлен подход, основанный на модели линейного программирования. Вычислительные эксперименты обсуждаются в разд. 3. Они включают в себя описание различных показателей качества в п. 3.1, описание способа запуска эволюционных алгоритмов в п. 3.2, проверку правильности выбора соотношения бюджетов в двухэтапной схеме в п. 3.4, сравнение

приведённых подходов в п. 3.5 и, наконец, оценку дисперсии качества получаемых решений в п. 3.6. Краткие выводы, приведённые в заключении, завершают статью.

1. Постановка задачи

В работе используются следующие обозначения:

- A — это множество дуг в графе, соответствующих каналам связи в сети;
- $\boldsymbol{w}^0 = \left(w_a^0\right)_{a \in A}$ — начальный вектор весов каналов;
- c_a — пропускная способность канала $a \in A$.

Оптимизируемые переменные записаны в виде вектора $\boldsymbol{w} = (w_a)_{a \in A}$, содержащего веса каналов. После задания этих весов можно смоделировать поведение сети и вычислить следующие её характеристики:

- $l_a(\boldsymbol{w})$ — суммарная нагрузка дуги a;
- $o_a(\boldsymbol{w}) = \begin{cases} 1, & \text{если дуга } a \in A \text{ перегружена,} \\ 0 & \text{иначе;} \end{cases}$
- $no_a(\boldsymbol{w}) = \begin{cases} 1, & \text{если } o_a(\boldsymbol{w}) = 1 \text{ и } o_a(\boldsymbol{w}^0) = 0, \\ 0 & \text{иначе.} \end{cases}$

По величинам потока в сети вычисляются следующие характеристики решения:

- общее число перегруженных каналов $O(\boldsymbol{w}) = \sum\limits_{a \in A} o_a(\boldsymbol{w})$;
- расстояние $D(\boldsymbol{w}) = ||\boldsymbol{w} - \boldsymbol{w}^0||_{\ell_1}$ между начальным и текущим векторами весов дуг;
- суммарная загрузка сети $L(\boldsymbol{w}) = \sum\limits_{a \in A} l_a(\boldsymbol{w})$;
- число новых перегруженных каналов $NO(\boldsymbol{w}) = \sum\limits_{a \in A} no_a(\boldsymbol{w})$.

Используя эти обозначения, задачу можно сформулировать как двухкритериальную задачу целочисленного программирования с использованием «чёрного ящика»:

$$O(\boldsymbol{w}) \to \min, \tag{1}$$

$$D(\boldsymbol{w}) \to \min, \tag{2}$$

$$L(\boldsymbol{w}) \leqslant L(\boldsymbol{w}^0), \tag{3}$$

$$NO(\boldsymbol{w}) = 0, \tag{4}$$

$$\boldsymbol{w} \in W. \tag{5}$$

Формулы (1)–(5) показывают, что цель состоит в том, чтобы найти векторы весов каналов, которые минимизируют число перегруженных каналов и имеют наименьшее расстояние от исходного вектора $\boldsymbol{w}^0$, при

условии, что решения должны обеспечивать общую нагрузку на каналы, не превышающую первоначальной, и не должны вызывать новых перегрузок каналов.

Вектор весов $\boldsymbol{w} \in W$ называется *допустимым*, если он удовлетворяет условиям (3) и (4). Для двух допустимых весовых векторов $\boldsymbol{w}^1, \boldsymbol{w}^2 \in W$ говорим, что $\boldsymbol{w}^1$ *доминирует* $\boldsymbol{w}^2$, если $O(\boldsymbol{w}^1) \leqslant O(\boldsymbol{w}^2)$, $D(\boldsymbol{w}^1) \leqslant D(\boldsymbol{w}^2)$ и по крайней мере одно из этих неравенств строгое. Задача состоит в том, чтобы найти Парето-множество решений, т. е. множество всех возможных решений без доминирования в рамках модели (1)–(5). Набор допустимых решений $S \subseteq W$ называется *приближением к множеству Парето* или *аппроксимирующим множеством*, если в S нет доминируемых решений. Далее в разд. 3.1 будут представлены показатели эффективности, которые характеризуют качество аппроксимирующего множества с разных точек зрения.

2. Эвристика, основанная на модели ЦЛП

Эвристический подход, который представлен в этом разделе, основан на модели целочисленного линейного программирования. Установлено, что классический локальный поиск, изменяющий вес одной дуги за раз, быстро останавливается в локальном оптимуме. Одновременное изменение нескольких весов помогает решить эту проблему, но размер такой окрестности экспоненциально увеличивается с ростом количества изменяемых весов, и её просмотр становится невозможным в рамках выделенного вычислительного бюджета. Для того чтобы обойти этот недостаток, предложено предсказывать изменения потока в сети, вызванные изменением нескольких весов, по изменениям, вызванным изменениями веса одной дуги. Представленная далее математическая модель целочисленного линейного программирования способна предсказать такие изменения и выбрать лучшее решение в окрестности. Она использует значения изменений потока трафика в зависимости от изменений веса какого-либо канала и пытается подобрать комбинацию изменений нескольких весов одновременно так, чтобы минимизировать число перегруженных дуг. Так как изменения весов влияют друг на друга, решения, предсказанные моделью, могут отличаться по качеству от настоящих, однако эксперименты показывают, что предложенный подход позволяет находить хорошие решения.

2.1. Модель минимизации перегрузки. Путём изменения отдельного веса в векторе $\boldsymbol{w}$ можно вычислить, как изменение веса одной дуги $e \in E \subseteq A$ влияет на нагрузку каждой дуги. Далее рассматриваем только подмножество всех весов, поскольку моделирование требует больших

вычислительных затрат, при этом желательно свести к минимуму число вызовов имитационной модели. Структура множества E будет представлена ниже в разд. 2.2. Пусть h обозначает размер шага, а $\boldsymbol{w}^{e+}$ — весовой вектор, полученный из $\boldsymbol{w}$ путём увеличения его e-й компоненты по формуле $w_e^{e+} = \min\{w_e^{\max}, w_e + h\}$. Аналогично e-я компонента вектора уменьшенного веса $\boldsymbol{w}^{e-}$ равна $w_e^{e-} = \max\{w_e^{\min}, w_e - h\}$. Изменение нагрузки для каждой дуги $a \in A$ может быть вычислено в рамках одного запуска имитационной модели следующим образом:

$$l_a^{e+} = l_a(\boldsymbol{w}^{e+}) - l_a(\boldsymbol{w}), \quad l_a^{e-} = l_a(\boldsymbol{w}^{e-}) - l_a(\boldsymbol{w}).$$

Чтобы сформулировать модель ЦЛП для минимизации перегрузки, введём булевы переменные $(x_a)_{a\in A}$, указывающие, перегружена соответствующая дуга или нет, и булевы переменные (λ_e^+), (λ_e^-), указывающие, увеличивается или уменьшается вес соответствующего канала.

С этими обозначениями модель минимизации перегрузки записывается следующим образом:

$$\sum_{a\in A} x_a \to \min, \tag{6}$$

$$\sum_{e\in E} (\lambda_e^+ + \lambda_e^-) \leqslant k, \tag{7}$$

$$\lambda_e^+ + \lambda_e^- \leqslant 1, \quad e \in E, \tag{8}$$

$$l_a(\boldsymbol{w}) + \sum_{e\in E} l_a^{e+}\lambda_e^+ + \sum_{e\in E} l_a^{e-}\lambda_e^- \leqslant c_a + o_a(\boldsymbol{w}^0)Mx_a, \quad a \in A, \tag{9}$$

$$\sum_{a\in A}\left(l_a(\boldsymbol{w}) + \sum_{e\in E} l_a^{e+}\lambda_e^+ + \sum_{e\in E} l_a^{e-}\lambda_e^-\right) \leqslant L(\boldsymbol{w}^0), \tag{10}$$

$$\lambda_e^+, \lambda_e^-, x_a \in \{0,1\}, \quad a \in A,\ e \in E. \tag{11}$$

Целевая функция (6) минимизирует число перегруженных каналов. Условия (7) ограничивают количество модификаций текущего весового вектора $\boldsymbol{w}$. Это необходимо, поскольку изменения компонентов вектора веса влияют друг на друга, и одновременное изменение нескольких компонентов приводит к непредсказуемым изменениям нагрузки. Поскольку изменения нагрузки, вызванные увеличением и уменьшением веса соединения, не противоположны друг другу, в оптимальное решение модели теоретически могут входить обе модификации одной дуги. Чтобы это предотвратить, ограничения (8) запрещают такое поведение. Ограничения (9) указывают, что соединения, которые не были перегружены изначально, не должны стать перегруженными после изменения веса. Эти ограничения, включающие достаточно большую константу M, гарантируют, что переменной x_a будет присвоено значение, равное единице, если

пропускная способность соответствующего канала a будет превышена. Наконец, неравенство (10) гарантирует, что общая нагрузка после изменения весов не превысит начального значения общей нагрузки $L(\boldsymbol{w}^0)$.

2.2. Поиск с чередующимися окрестностями. Здесь описан алгоритм, который использует модель, представленную в п. 2.1. Он напоминает схему спуска с чередующимися окрестностями с изменяемым шагом [31]. При такой аналогии окрестность решения $\boldsymbol{w}$ включает решения, которые могут быть достигнуты путём изменения не более чем k элементов вектора $\boldsymbol{w}$ на величину h. Лучшее решение из этой окрестности в предположении, что модификации различных дуг не влияют друг на друга, можно найти, взяв оптимальное решение для модели (6)–(11). Различные значения k и h задают различные окрестности. Введём множества K и H для возможных значений k и h. Пусть множество K зависит от двух параметров: $k_{\max} \in \mathbb{N}$ и категориального параметра $\texttt{RT} \in \{\texttt{fixed}, \texttt{decremental}, \texttt{exp}\}$, обозначающего тип диапазона:

$$K(\texttt{RT}) = \begin{cases} \{k_{\max}\}, & \text{если } \texttt{RT} = \texttt{fixed}, \\ \{k_{\max}, k_{\max} - 1, \ldots, 1\}, & \text{если } \texttt{RT} = \texttt{decremental}, \\ \{k_{\max}, \lfloor k_{\max}/2^1 \rfloor, \lfloor k_{\max}/2^2 \rfloor, \ldots, 1\}, & \text{если } \texttt{RT} = \texttt{exp}. \end{cases}$$

Пусть множество H зависит от параметров $h_{\min}$ и $h_{\max}$ следующим образом:

$$H(h_{\min}, h_{\max}) = \{2^i h_{\min} \mid i \in 0, 1, \ldots, \lfloor \log_2 (h_{\max}/h_{\min}) \rfloor\}.$$

Для определения размера шага h алгоритм делит все дуги на группы в зависимости от начальных весов:

$$E_g = \left\{ i \in A \mid 10^g \leqslant w_i^0 < 10^{g+1} \right\}, \quad G = \left\{ E_g \mid g = 0, \ldots, \left\lfloor \log_{10} \max_{i \in A} w_i^0 \right\rfloor \right\}.$$

В каждой группе используются границы $h_{\min,g} = \left\lceil \min \left\{ w_i^0 \mid i \in E_g \right\} / 4 \right\rceil$ и $h_{\max,g} = 64 h_{\min,g}$ для шага h. В экспериментах также рассматривается вариант без разделения на группы и $|G| = 1$. В этом случае устанавливаются параметры $h_{\min} = 1$ и $h_{\max} = 0{,}5 \max\limits_{i \in A} w_i^0$. Схема поиска с чередующимися окрестностями на основе модели VNMS представлена алгоритмом 1.

Процедура локального улучшения $\texttt{solveModel}(\boldsymbol{w}, h, E, k)$ заключается в решении модели (6)–(11) с соответствующими значениями $\boldsymbol{w}$, h, E и k. Алгоритм начинает с $g = 1$, $h = h_{\min,1}$, $k = k_{\max}$. Если новое решение, полученное после решения модели, не лучше старого, то параметры обновляются следующим образом. Сначала уменьшается значение k. Если оно становится меньше $k_{\min}$, то k сбрасывается до $k_{\max}$, а значение h удваивается. Если h оказывается больше, чем $h_{\max}$, то его значение устанавливается равным $h_{\min}$, и алгоритм переходит к следующей группе.

Алгоритм 1. Поиск с чередующимися окрестностями на основе модели

```
1: function VNMS(G, H, K)
2:     for g = 1, ..., |G| do
3:         H ← H(h_min,g, h_max,g);
4:         for all h ∈ H do
5:             i ← 0;
6:             while i ⩽ |K| do
7:                 w′ ← solveModel(w, h, E_g,p, K[i]);
8:                 if w′ недопустимое then greedyFix(w′);
9:                 if w′ лучше, чем w then w ← w′;
10:                else i ← i + 1;
11:    return w;
```

После завершения работы с последней группой алгоритм останавливается. Однако в ходе экспериментов он перезапускался с начала, пока бюджет вычислений оставался неисчерпанным.

Дополнительно в схеме реализован механизм быстрой починки решения, который задействуется, если решение на выходе модели ЦЛП недопустимо из-за перегрузки новых дуг. Указанный механизм жадно увеличивает веса вновь перегруженных дуг, при этом выполняется не более 200 итераций увеличения; эта процедура названа `greedyFix`. Также, чтобы ускорить поиск и внести разнообразие в алгоритм, оценивается только случайное подмножество соседей $E_{g,p}$, в которое каждое изменение попадает с вероятностью $p \in (0, 1]$.

Хотя такой эвристический подход может применяться сам по себе, большой интерес представляет гибридизация этой схемы с хорошо известными многокритериальными эволюционными алгоритмами (multi-objective evolutionary algorithm, MOEA). Оба метода имеют свои преимущества и недостатки. Эволюционные алгоритмы доказали свою способность находить решения, которые очень близки к множеству Парето. Однако им может быть трудно удовлетворить ограничения, в то время как подход на основе представленной модели, учитывает эти ограничения явным образом. Эвристический подход позволяет получить допустимые точки, далёкие от начального решения, однако он возвращает лишь небольшое число решений, причём часть из них могут находиться значительном расстоянии от истинной границы Парето. Следовательно, двухэтапная схема, в которой эволюционные алгоритмы используются для последующей оптимизации аппроксимации множества Парето, найденного с помощью подхода, основанного на модели, должна обеспечить хорошие результаты.

3. Вычислительные эксперименты

Все эксперименты, описанные в этом разделе, проводились на компьютере, оснащённом процессором Intel Core i7-8700 3,20 ГГц и 32 ГБ оперативной памяти, под управлением операционной системы Microsoft Windows 10 Pro. Для реализации модели, описанной в разд. 2, применены библиотека PuLP [1)] на языке Python и пакет CBC [32]. CBC был запущен в одном потоке, в то время как все остальные операции выполнялись параллельно с использованием всех доступных ядер.

Для оценки качества работы алгоритма было сгенерировано 13 тестовых примеров из предоставленного нам реального. Исходный пример содержит $|A| = 628$ каналов и 1324 запроса (пары источник-назначение). Сгенерированные примеры имеют ту же структуру графа и матрицу источник — назначение, что и исходный пример. Отличие заключается в векторе начальных весов $\boldsymbol{w}^0$. В работе использованы различные схемы выбора начальных весов: выбор согласно рекомендации Cisco [10], нормализация весов исходного примера, перемешивание исходных весов и случайное равномерное распределение весов. В итоге максимальный вес в примерах варьируется от 10 до 10 000. Подробнее механизм генерации примеров описан в [30].

3.1. Показатели качества. Для численного анализа эффективности алгоритмов применяются показатели эффективности, разработанные специально для задач многокритериальной оптимизации [33] для сравнении приближений множеств Парето. Для описания показателей потребуются обозначения S или S_k, $k \in \mathbb{N}$, для приближений границы Парето, полученных с помощью исследуемых алгоритмов. В некоторых определениях показателей используется специальное множество решений R, называемое *эталонным множеством*, которое является точной Парето-границей или же заведомо достаточно хорошим приближением к ней. Вектор целевых функций для удобства можно обозначить через $F = (f_i)_{i \in I}$. В нашем случае $I = \{1, 2\}$, $f_1 = O$ и $f_2 = D$. Рассматриваются следующие показатели.

• *Гиперобъём* (hypervolume) определяется как объём в пространстве целевых функций, который доминируется приближением к границе Парето и ограничен сверху некоторой точкой. В качестве такой точки используем $\big(O(\boldsymbol{w}^0), \max\limits_{\boldsymbol{w} \in R} D(\boldsymbol{w})\big)$.

• *Вклад* (contribution) — доля точек из эталонного множества R, которые присутствуют в S.

[1)] `https://github.com/coin-or/pulp`

• *Расстояние до эталона* (generational distance, GD) — это расстояние от S до R:

$$\mathrm{GD}(S,R)=\frac{1}{|S|}\Big(\sum_{\boldsymbol{w}^s\in S}\min_{\boldsymbol{w}^r\in R}\|F(\boldsymbol{w}^s)-F(\boldsymbol{w}^r)\|^p\Big)^{\frac{1}{p}}.$$

• *Расстояние от эталона* (inverted generational distance, IGD) — расстояние от R до S: $\mathrm{IGD}(S,R)=\mathrm{GD}(R,S)$. Для GD и IGD используем $p=2$.

• *ε-Индикатор* — это значение, необходимое для того, чтобы S аддитивно ε-доминировало R. Говорим, что вектор $\boldsymbol{w}^1$ *аддитивно ε-доминирует* $\boldsymbol{w}^2$, если $f_i(\boldsymbol{w}^1)\leqslant\varepsilon+f_i(\boldsymbol{w}^2)$ для любого $i\in I$.

• *Максимальная ошибка* (maximum Pareto front error, MPFE) — максимальное расстояние точки из S до R:

$$\mathrm{MPFE}(S,R)=\max_{\boldsymbol{w}^s\in S}\min_{\boldsymbol{w}^r\in R}\|F(\boldsymbol{w}^s)-F(\boldsymbol{w}^r)\|.$$

• *Показатели R_1 и R_2*. Пусть S_1 и S_2 — две аппроксимации множества Парето, U — набор функций полезности $u\colon\mathbb{R}^m\to\mathbb{R}$. Для каждого $u\in U$ и $s=1,2$ пусть задано $u^\star(S_s)=\min\limits_{\boldsymbol{w}\in S_s}u(F(\boldsymbol{w}))$. Эти два показателя измеряют, в какой степени S_1 лучше, чем S_2, по набору функций полезности U:

$$C(S_1,S_2,u)=\begin{cases}1, & \text{если } u^\star(S_1)<u^\star(S_2),\\ 1/2, & \text{если } u^\star(S_1)=u^\star(S_2),\\ 0, & \text{если } u^\star(S_1)>u^\star(S_2);\end{cases}$$

$$R_1(S_1,S_2,U)=\frac{1}{|U|}\sum_{u\in U}C(S_1,S_2,u);$$

$$R_2(S_1,S_2,U)=\frac{1}{|U|}\sum_{u\in U}(u^\star(S_1)-u^\star(S_2)).$$

Если $R_1(S_1,S_2,U)>0.5$, то считается, что S_1 лучше, чем S_2. Аналогично $R_2(S_1,S_2,U)<0$ соответствует тому, что S_1 показывает результаты лучше, чем S_2.

• *Расстояние между решениями* (spacing) рассчитывается как

$$\mathrm{SP}(S)=\sqrt{\frac{1}{|S|-1}\sum_{i=1}^{|S|}(\bar{d}-d_i)^2},$$

где $d_i=\min\limits_{\boldsymbol{w}^j\in S\setminus\boldsymbol{w}^i}\|F(\boldsymbol{w}^i)-F(\boldsymbol{w}^j)\|_{\ell_1}$ — расстояние между точкой $\boldsymbol{w}^i\in S$ и ближайшей точкой аппроксимации множества Парето, полученной с помощью того же алгоритма, а $\bar{d}$ — среднее значение d_i.

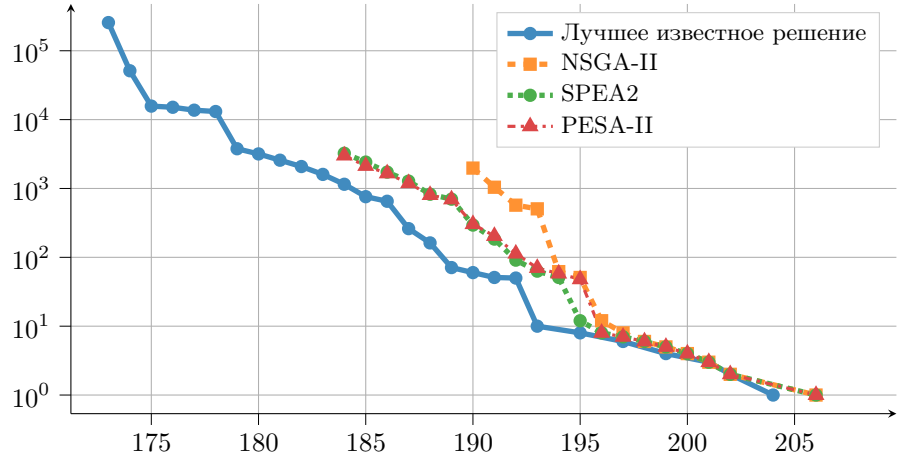


Рис. 1. Качество полученной границы Парето: без начального решения $\boldsymbol{w}^1$

- *Минимальное число перегруженных дуг* равно $O_{\min}(S) = \min\limits_{\boldsymbol{w} \in S} O(\boldsymbol{w})$.
- *Число решений* (cardinality) равно $|S|$.

3.2. Многокритериальные популяционные алгоритмы. В литературе одними из самых популярных для многокритериальной оптимизации являются алгоритмы, основанные на популяции решений [34], поэтому в этой работе также рассмотрены несколько наиболее широко

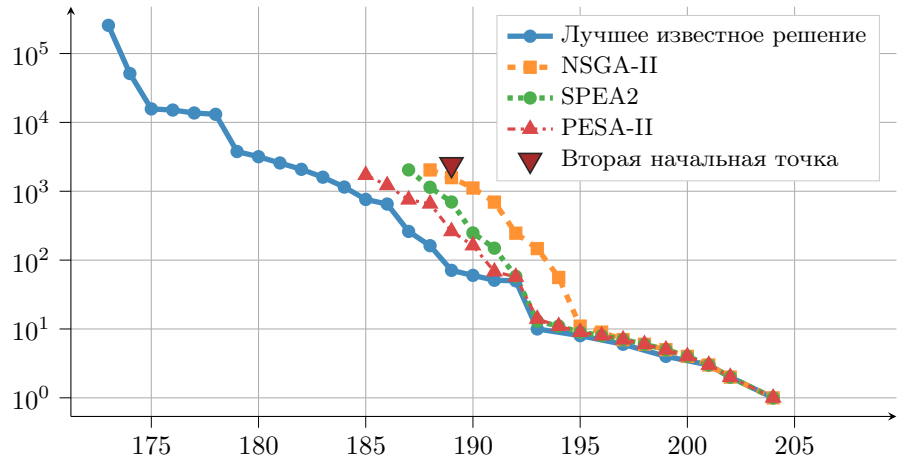


Рис. 2. Качество полученной границы Парето:
среднее $O_{\min}(\boldsymbol{w}^1)$, среднее $D(\boldsymbol{w}^1)$

используемых многокритериальных эволюционных алгоритмов. А именно, применяются следующие многокритериальные алгоритмы из Java-библиотеки MOEA framework [35]:

- NSGA-II — nondominated sorting genetic algorithm II [36];
- SPEA2 — strength Pareto evolutionary algorithm 2 [37];
- PESA-II — Pareto envelope region-based selection algorithm [38];
- PAES — Pareto archived evolutionary strategy [39].

Также протестированы другие эволюционные алгоритмы, но они показали результаты хуже, чем перечисленные выше.

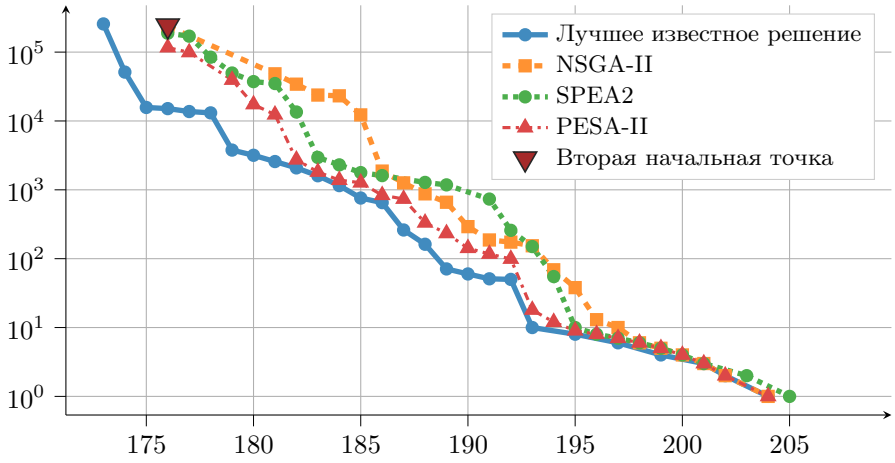


Рис. 3. Качество полученной границы Парето:
хорошее $O_{\min}(\boldsymbol{w}^1)$, среднее $D(\boldsymbol{w}^1)$

Стоит отметить, что алгоритмы, основанные на популяции, работают намного лучше, если им предоставляются несколько начальных решений $\{\boldsymbol{w}^0, \boldsymbol{w}^1, \ldots, \boldsymbol{w}^m\}$, а не только $\boldsymbol{w}^0$. На рис. 1–5 представлено поведение алгоритмов при двух начальных решениях $\{\boldsymbol{w}^0, \boldsymbol{w}^1\}$ для различных значений $\boldsymbol{w}^1$, при этом по горизонтальной оси отложено число перегруженных каналов, а по вертикальной — расстояние до границы Парето. Все результаты соответствуют исходному примеру.

Как видно из рис. 1–5, качество результатов, достигаемых с помощью алгоритмов, сильно зависит от исходных решений. Желательно, чтобы в начальной популяции было по возможности близкое к $\boldsymbol{w}^0$ решение, которое имеет как можно меньшее значение $O(\boldsymbol{w})$. Последнее необходимо для того, чтобы иметь возможность находить промежуточные потенциальные решения.

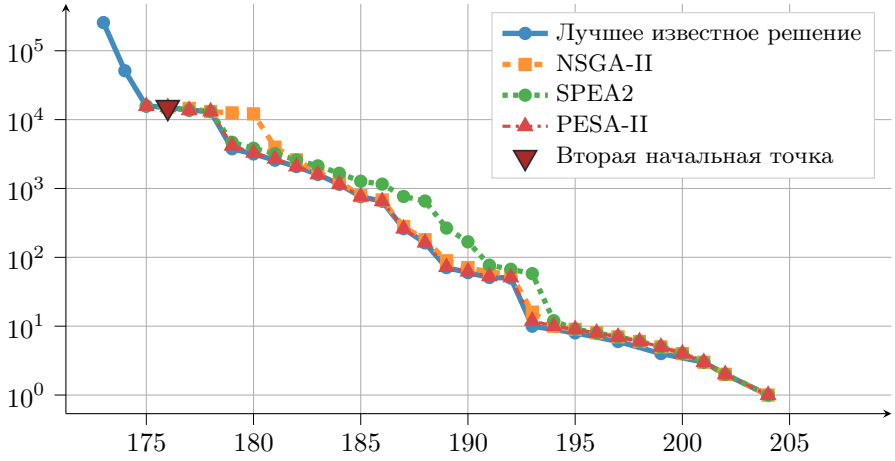


Рис. 4. Качество полученной границы Парето:
хорошее $O_{\min}(\boldsymbol{w}^1)$, хорошее $D(\boldsymbol{w}^1)$

Из-за присутствия ограничений в задаче эволюционным алгоритмам трудно исследовать пространство решений и находить хорошие отдалённые. Для повышения качества итоговых решения можно инициализировать популяцию с помощью решений, полученных при помощи метода, учитывающего эти ограничения, подобного тому, который представлен в разд. 2.

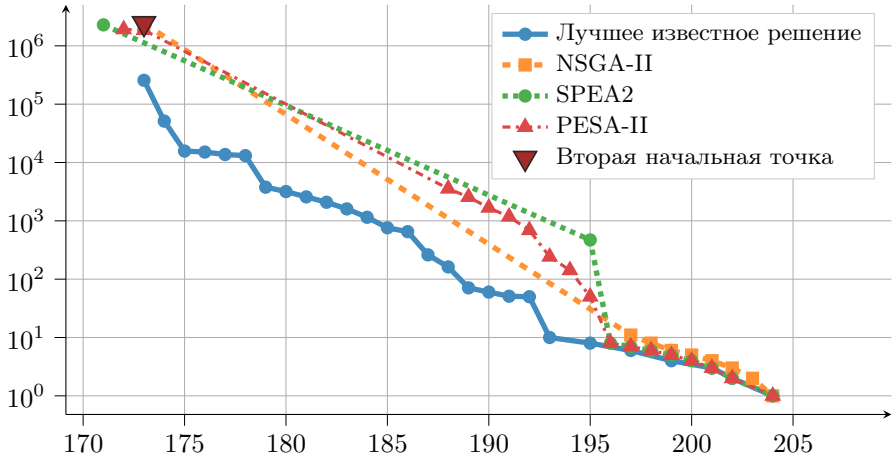
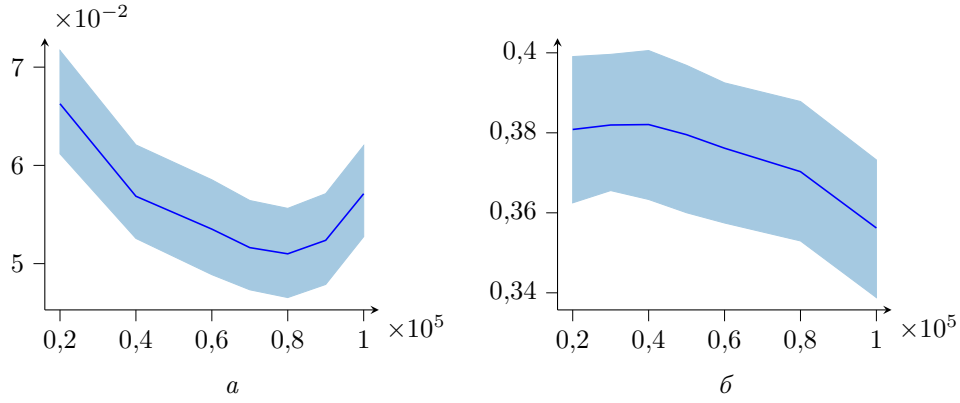


Рис. 5. Качество полученной границы Парето:
хорошее $O_{\min}(\boldsymbol{w}^1)$, плохое $D(\boldsymbol{w}^1)$

В предыдущей работе [30] было показано, что алгоритм PAES наилучшим образом среди эволюционных алгоритмов подходит для нахождения решений с малым числом перегруженных дуг. Там же было показано, что гибридизация других популяционных алгоритмов с PAES улучшает качество найденных решений, а среди таких вариантов выигрывает схема, в которой на 50 000 оцениваний целевой функции запускается PAES, после чего запускается алгоритм PESA-II с бюджетом 70 000 оцениваний целевой функции.

3.3. Выбор параметров. Чтобы определить хорошие значения параметров схемы VNMS, было решено использовать инструмент оптимизации гиперпараметров SMAC3 [42]. Так как схема может использоваться в двух вариантах — как самостоятельный алгоритм и в связке с PESA-II, были найдены два набора параметров: $\texttt{RT} = \texttt{exp}$, $k_{\max} = 8$, $p = 0{,}33$ с разделением на группы для первого варианта и $\texttt{RT} = \texttt{decremental}$, $k_{\max} = 4$, $p = 0{,}5$ без использования групп для второго. Схемы с этими параметрами будем называть $\text{VNMS}_{\text{fast}}$ и $\text{VNMS}_{\text{long}}$ соответственно.



а *б*

Рис. 6. Зависимость показателей качества от количества оцениваний целевой функции, выделенных на эволюционный алгоритм: *а* — расстояние от эталона, *б* — гиперобъём

3.4. Распределение бюджета между этапами. В этом эксперименте производится проверка, что соотношение вычислительных бюджетов, выделенных на построение решений с помощью схемы VNMS и на их последующее улучшение с помощью эволюционного алгоритма, выбрано верно. Для этого выполнена серия запусков с одинаковым суммарным бюджетом, равным, как и ранее, 120 000, но с разным соотношением бюджетов между этапами. На рис. 6 отражены зависимости среднего расстояния от эталона и среднего гиперобъёма от количества оцениваний

целевой функции, выделенных на эволюционный алгоритм. Остальной бюджет потрачен предложенной схемой на генерацию начальных решений. Закрашенная полоса обозначает доверительный интервал для уровня доверия 0,95.

Из графиков видно, что минимум расстояния, как и максимум объёма, достигается при бюджете, выделенном на эволюционный алгоритм, равном 80 000. Это говорит о том, что соотношение бюджетов, использованное ранее, близко к оптимальному, хотя можно добиться небольшого улучшения, если увеличить бюджет на улучшение решений эволюционным алгоритмом.

3.5. Сравнение схем. В этом пункте сравниваются схемы, выбранные ранее, а именно: PAES+PESA-II, $\text{VNMS}_{\text{fast}}$+PESA-II и $\text{VNMS}_{\text{long}}$. Первые две схемы двухэтапные, где часть бюджета выделяется на построение начальных решений, а оставшийся бюджет расходуется PESA-II, использующим эти решения в качестве стартовых. Для краткости обозначений назовём двухэтапные схемы PPESA и VPESA соответственно, а для алгоритма $\text{VNMS}_{\text{long}}$ будем также использовать просто обозначение VNMS. Общий объём вычислений для всех трёх схем примерно одинаков и составляет 12 минут или 120 000 вычислений целевой функции.

Каждый алгоритм запущен по 10 раз, а затем с использованием результатов этих запусков применены два U-критерия Манна — Уитни [40] для каждого примера, каждой пары вариантов запусков и всех индикаторов, за исключением индикаторов R_1 и R_2. Нулевая гипотеза состоит в том, что вероятность того, что значение показателя для первого алгоритма в попарном сравнении будет лучше значения для второго алгоритма, не превышает вероятности того, что значение показателя для

Таблица 1

Число побед в попарных сравнениях выбранных схем

Показатель	PPESA:VPESA	VPESA:VNMS	VNMS:PPESA
Гиперобъём	1:11	11:0	6:6
Вклад	1:7	11:0	1:8
Расст. до эталона	3:7	12:0	1:11
Расст. от эталона	1:12	11:0	9:3
ε-индикатор	0:11	2:2	0:12
Макс. ошибка	5:4	9:0	1:7
R_1	0:11	2:2	10:0
R_2	0:11	2:2	11:0
$O_{\min}$	0:12	0:3	13:0
Число решений	0:10	13:0	2:10

второго варианта будет лучше значения для первого варианта. Для индикаторов R_1 и R_2 проверены критерии знаковых рангов Уилкоксона [41] с нулевой гипотезой о том, что один вариант не лучше другого с точки зрения значений индикаторов R_1, R_2 (п. 3.1).

Говорим, что первый алгоритм выигрывает на данном примере по данному показателю, если нулевая гипотеза о том, что второй алгоритм не лучше первого, отвергается и принимается альтернативная гипотеза о том, что он лучше. Аналогично говорим, что первый алгоритм проигрывает, если принимается альтернативная гипотеза о том, что второй алгоритм лучше в этом случае и по данному показателю. В случае, если не принимается ни одна из альтернативных гипотез, говорим, что эти варианты эквиваленты. Результаты сравнений представлены в табл. 1. Первое число пары, разделённое двоеточием — это число побед первого алгоритма в паре, а второе число — число побед второго.

Как видно из табл. 1, двухэтапная схема с использованием $\mathrm{VNMS}_{\mathrm{fast}}$ для генерации исходных решений работает наилучшим образом из проверенных вариантов. Схема $\mathrm{VNMS}_{\mathrm{long}}$ также даёт хорошие результаты. Хотя гибридная схема, использующая эволюционные алгоритмы, аппроксимирует границу Парето вблизи исходного решения намного лучше, чем $\mathrm{VNMS}_{\mathrm{long}}$, последняя значительно превосходит эволюционные методы (включая PAES) в поиске решений с малыми значениями $O(\boldsymbol{w})$. Это приводит к улучшению расстояния от эталона, ε-индикатора и $O_{\min}$ и сопоставимым результатам с точки зрения гиперобъёма. Схема VPESA использует преимущества обоих подходов, что приводит к получению более качественных решений.

Таблица 2

Средние значения показателей и относительное улучшение алгоритмов

Показатель	PPESA	VNMS	VPESA	Улучш. VNMS	Улучш. VPESA
Гиперобъём	0,336	0,345	0,381	0,043	0,153
Вклад	0,164	0,113	0,211	−0,133	0,392
Расст. до эталона	0,010	0,020	0,008	−0,914	0,201
Расст. от эталона	0,102	0,070	0,046	0,222	0,494
ε-индикатор	0,299	0,131	0,135	0,511	0,492
Макс. ошибка	0,114	0,169	0,106	−1,028	−0,240
$O_{\min}$	177,163	166,061	166,783	0,063	0,060
Число решений	32,489	25,207	42,990	−0,198	0,316
Расстояние	0,537	1,529	0,505	—	—

В табл. 2 представлены средние значения показателей и относительные улучшения этих показателей для предложенных схем относительно эволюционного алгоритма. Для показателя «Расстояние между решениями» не приведены значения улучшения, так как он не отражает напрямую качество решений.

Видно, что хотя алгоритм $\mathrm{VNMS}_{\mathrm{long}}$ проигрывает по некоторым показателям, двухэтапная схема VPESA превосходит эволюционные алгоритмы почти по всем показателям на 15–49%.

3.6. Дисперсия схемы. Наконец, проведены эксперименты с целью установить разброс качества получаемых решений, для чего схема была запущена 80 раз на каждом примере. В табл. 3 представлены результаты этих экспериментов. Колонка «Стандартное отклонение» содержит значение среднеквадратического отклонения для каждого параметра, усреднённого по всем примерам, а колонка «Относительное стандартное отклонение» — величину стандартного отклонения, поделённого на среднее значение показателя, также усреднённую по всем примерам.

Таблица 3

Статистики показателей качества решений

Показатель	Среднее	Станд. отклон.	Относит. станд. отклон.
Гиперобъём	0,370	0,019	0,051
Вклад	0,109	0,041	0,498
Расст. до эталона	0,012	0,003	0,266
Расст. от эталона	0,060	0,014	0,239
ε-индикатор	0,140	0,040	0,303
Макс. ошибка	0,132	0,035	0,265
$O_{\min}$	165,786	2,627	0,016
Число решений	42,945	2,969	0,076
Расстояние	0,515	0,142	0,429

Из табл. 3 видно, что некоторые показатели имеют небольшой разброс, в то время как другие могут значительно отклоняться от среднего значения. Наибольший разброс имеет вклад в эталонное решение, так как эта метрика зависит от точного расположения решений в пространстве целевых функций: если хоть по одной целевой функции решение чуть хуже, то оно не засчитывается как решение, вносящее вклад. Также сильно меняется расстояние между решениями, хотя число решений на Парето-границе меняется несильно. Вместе с малым изменением гиперобъёма

это может говорить о том, что основные опорные точки находятся верно, но промежуточные точки могут находиться в разных частях Парето-границы. Это же может быть причиной средних разбросов расстояний от и до эталона, ε-индикатора и максимальной ошибки.

Заключение

В работе рассмотрена новая двухкритериальная задача оптимизации «чёрного ящика» для управления потоком трафика в сети. Задача заключается в поиске такой реконфигурации весов для сетевых каналов, используемых протоколом маршрутизации, при которой число перегруженных каналов сведено к минимуму, а разница между старыми и новыми весами минимальна. Новые веса не должны увеличивать общий поток и не должны создавать новые перегруженные каналы. В ходе работы разработана специализированная схема для решения этой задачи и проведены сравнительные эксперименты для этой схемы и метаэвристических алгоритмов общего назначения.

Эксперименты показали, что алгоритм PESA2 из библиотеки MOEA Framework работает наилучшим образом среди проверенных метаэвристик, часто встречающихся в литературе. Тесты показали, что хотя упомянутые алгоритмы могут находить хорошую границу Парето, им трудно находить решения с небольшим числом перегруженных каналов, поэтому они значительно выигрывают от хороших начальных точек. Эти алгоритмы могут эффективно заполнять пробелы между заданными точками.

Обнаружено, что изменение весов по одному не позволяет найти хорошие решения с точки зрения числа перегруженных каналов, а просмотр окрестности, состоящий в изменении нескольких весов, занимает слишком большое время. Ввиду этого в работе разработана модель целочисленного линейного программирования (6)–(11) для поиска наилучшего решения в аппроксимации большой окрестности. Для этой модели вычисляются изменения нагрузки на канал после изменения одного веса. Модель ищет комбинацию из нескольких модификаций, которая минимизирует число перегруженных каналов. Затем предложен итерационный алгоритм VNMS для исходной задачи, основанный на этой модели. Этот алгоритм изменяет параметры модели для получения более качественных итоговых решений.

Алгоритм VNMS может быть использован для двух целей: найти решение с небольшим числом перегруженных каналов за короткое время или найти всё множество Парето. Во втором случае алгоритм демонстрирует хорошие результаты при решении однокритериальной задачи

минимизации числа перегруженных каналов, которые близки к результатам, полученным с помощью гибридного алгоритма на основе популяционных методов и известного алгоритма PAES. Комбинация VNMS с алгоритмами, основанными на популяции, показывает статистически лучшие на 15–49% результаты для исходной задачи, поскольку она использует преимущества обоих подходов.

Финансирование работы

Исследование выполнено в рамках государственного задания Института математики им. С. Л. Соболева (проект № FWNF–2022–0019). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Altın A., Fortz B., Thorup M., Ümit H.** Intra-domain traffic engineering with shortest path routing protocols // Ann. Oper. Res. 2013. V. 204, No. 1. P. 65–95. DOI: 10.1007/s10479-012-1270-7.
2. **Elwalid A., Jin C., Low S., Widjaja I.** MATE: MPLS adaptive traffic engineering // Twenty years into the communications odyssey. Proc. 20th Annu. Joint Conf. IEEE Computer and Communications Societies (Anchorage, AK, Apr. 22–26, 2001). V. 3. Washington: IEEE Comput. Soc., 2001. P. 1300–1309. DOI: 10.1109/infcom.2001.916625.
3. **Abbasi M., Guleria A., Devi M.** Traffic engineering in software defined networks: A survey // J. Telecommun. Inf. Technol. 2016. V. 4. P. 3–14.
4. **Bhatia R., Hao F., Kodialam M., Lakshman T.** Optimized network traffic engineering using segment routing // Proc. 2015 IEEE Conf. Computer Communications (Hong Kong, China, Apr. 26 – May 1, 2015). Piscataway: IEEE, 2015. P. 657–665. DOI: 10.1109/INFOCOM.2015.7218434.
5. **Wang Y., Wang Z.** Explicit routing algorithms for Internet traffic engineering // Proc. 8th Int. Conf. Computer Communications and Networks (Boston, MA, Oct. 11–13, 1999). Piscataway: IEEE, 1999. P. 582–588. DOI: 10.1109/ICCCN.1999.805577.
6. **Poppe F., Van den Bosch S., de La Vallée-Poussin P., Van Hove H., De Neve H., Petit G.** Choosing the objectives for traffic engineering in IP backbone networks based on quality-of-service requirements // Quality of future Internet service. Proc. 1st COST 263 Int. Workshop (Berlin, Germany, Sept. 25–26, 2000). Heidelberg: Springer, 2000. P. 129–140. (Lect. Notes Comput. Sci.; V. 1922). DOI: 10.1007/3-540-39939-9_11.
7. **Audet C., Hare W.** Derivative-free and blackbox optimization. Cham: Springer, 2017. 302 p. DOI: 10.1007/978-3-319-68913-5.

8. **Yuskov A. D., Kulachenko I. N., Melnikov A. A., Kochetov Yu. A.** Stadium antennas deployment optimization // Mathematical optimization theory and operations research. Proc. 23rd Int. Conf. MOTOR 2024 (Omsk, Russia, June 30 – July 6, 2024). Cham: Springer, 2024. P. 449–461. (Lect. Notes Comput. Sci.; V. 14766). DOI: 10.1007/978-3-031-62792-7_30.
9. **Юськов А. Д., Кулаченко И. Н., Мельников А. А., Кочетов Ю. А.** Метод декомпозиции для управления запасами в двухэшелонной системе складов // Дискрет. анализ и исслед. операций. 2024. Т. 31, № 4. С. 186–212.
10. Internetworking technologies handbook. Indianapolis: Cisco Press, 2000. 1078 p.
11. **Fortz B., Thorup M.** Internet traffic engineering by optimizing OSPF weights // Reaching the Promised Land of communications. Proc. 20th Annu. Joint Conf. IEEE Computer and Communications Societies (Tel Aviv, Israel, Mar. 26–30, 2000). V. 2. Washington: IEEE Comput. Soc., 2000. P. 519–528. DOI: 10.1109/INFCOM.2000.832225.
12. **Ericsson M., Resende M., Pardalos P.** A genetic algorithm for the weight setting problem in OSPF routing // J. Comb. Optim. 2002. V. 6. P. 299–333. DOI: 10.1023/A:1014852026591.
13. **Fortz B., Thorup M.** Optimizing OSPF/IS-IS weights in a changing world // IEEE J. Sel. Areas Commun. 2002. V. 20. P. 756–767. DOI: 10.1109/JSAC.2002.1003042.
14. **Kodialam M. S., Lakshman T. V.** Network link weight setting: A machine learning based approach // Proc. IEEE Conf. Computer Communications (London, May 2–5, 2022). Piscataway: IEEE, 2022. P. 2048–2057. DOI: 10.1109/INFOCOM48880.2022.9796922.
15. **Pióro M., Szentesi Á., Harmatos J., Jüttner A., Gajowniczek P., Kozdrowski S.** On open shortest path first related network optimisation problems // Perform. Eval. 2002. V. 48, No. 1–4. P. 201–223. DOI: 10.1016/S0166-5316(02)00036-6.
16. **Balon S., Skivée F., Leduc G.** How well do traffic engineering objective functions meet TE requirements? // NETWORKING 2006. Networking technologies, services, protocols; Performance of computer and communication networks; Mobile and wireless communications systems. Proc. 5th Int. IFIP-TC6 Networking Conf. (Coimbra, Portugal, May 15–19, 2006). Heidelberg: Springer, 2006. P. 75–86. (Lect. Notes Comput. Sci.; V. 3976). DOI: 10.1007/11753810_7.
17. **Blanchy F., Melon L., Leduc G.** Routing in a MPLS network featuring preemption mechanisms // Proc. 10th Int. Conf. Telecommunications (Papeete, French Polynesia, Feb. 23 – Mar. 1, 2003). V. 1. Piscataway: IEEE, 2003. P. 253–260. DOI: 10.1109/ICTEL.2003.1191228.
18. **Athanasiou G., Tsagkaris K., Vlacheas P., Karvounas D., Demestichas P.** Multi-objective traffic engineering for future networks // IEEE Commun. Lett. 2012. V. 16, No. 1. P. 101–103. DOI: 10.1109/LCOMM.2011.110711.112071.

19. **El-Alfy E.-S. M.** Flow-based path selection for Internet traffic engineering with NSGA-II // Proc. 17th Int. Conf. Telecommunications (Doha, Qatar, Apr. 4–7, 2010). Piscataway: IEEE, 2010. P. 621–627. DOI: 10.1109/ICTEL.2010.5478839.
20. **Sousa P., Cortez P., Rio M., Rocha M.** Traffic engineering approaches using multicriteria optimization techniques // Wired/wireless internet communications. Proc. 9th IFIP TC 6 Int. Conf. (Vilanova i la Geltrú, Spain, June 15–17, 2011). Heidelberg: Springer, 2011. P. 104–115. (Lect. Notes Comput. Sci.; V. 6649). DOI: 10.1007/978-3-642-21560-5_9.
21. **Pereira V., Sousa P., Rocha M.** A comparison of multi-objective optimization algorithms for weight setting problems in traffic engineering // Nat. Comput. 2022. V. 21. P. 507–522. DOI: 10.1007/s11047-020-09807-1.
22. **Wang N., Ho K. H., Pavlou G., Howarth M.** An overview of routing optimization for internet traffic engineering // IEEE Commun. Surv. Tutor. 2008. V. 10, No. 1. P. 36–56. DOI: 10.1109/COMST.2008.4483669.
23. **Kaneda S., Uyematsu T., Nagatsu N., Sato K.** Network design and cost optimization for label switched multilayer photonic IP networks // IEEE J. Sel. Areas Commun. 2005. V. 23, No. 8. P. 1612–1619. DOI: 10.1109/JSAC.2005.851747.
24. **Zhang-Shen R., McKeown N.** Designing a predictable Internet backbone network // Proc. 3rd Workshop Hot Topics in Networks (HotNets-III) (San Diego, CA, Nov. 15–16, 2004). New York: ACM SIGCOMM, 2004. 6 p. URL: conferences.sigcomm.org/hotnets/2004/HotNets-III%20Proceedings/zhang-shen.pdf (accessed: 10.10.2025).
25. **Clark D. D.** Designing an Internet. Cambridge, MA: MIT Press, 2018. 432 p.
26. **Holmberg K., Yuan D.** Optimization of internet protocol network design and routing // Networks. 2004. V. 43, No. 1. P. 39–53. DOI: 10.1002/net.10102.
27. **Dehghani M., Vahdat V., Amiri M., Rabiei E., Salehi S.** A multi-objective optimization model for a reliable generalized flow network design // Comput. Ind. Eng. 2019. V. 138. Article ID 106074. 32 p. DOI: 10.1016/j.cie.2019.106074.
28. **Zhu H., Gupta V., Ahuja S. S., Tian Y., Zhang Y., Jin X.** Network planning with deep reinforcement learning // Proc. ACM SIGCOMM 2021 Conf. (Delft, Netherlands, Aug. 23–28, 2021). New York: ACM, 2021. P. 258–271. DOI: 10.1145/3452296.3472902.
29. **Wong R. T.** Telecommunications network design: Technology impacts and future directions // Networks. 2021. V. 77, No. 2. P. 205–224. DOI: 10.1002/net.21997.
30. **Yuskov A. D., Kulachenko I. N., Melnikov A. A., Kochetov Yu. A.** Two-stage algorithm for bi-objective black-box traffic engineering // Optimization and applications. Rev. Sel. Pap. 14th Int. Conf. OPTIMA 2023 (Petrovac, Montenegro, Sept. 18–22, 2023). Cham: Springer, 2023. P. 110–125. (Lect. Notes Comput. Sci.; V. 14395). DOI: 10.1007/978-3-031-47859-8_9.

31. Hansen P., Mladenović N., Todosijević R., Hanafi S. Variable neighborhood search: Basics and variants // EURO J. Comput. Optim. 2016. V. 5, No. 3. P. 423–454. DOI: 10.1007/s13675-016-0075-x.

32. Forrest J., Ralphs T., Vigerske S. [et al.]. COIN-OR Branch-and-Cut solver. Genève: CERN; Zenodo, 2023. DOI: 10.5281/zenodo.10041724.

33. Audet C., Bigeon J., Cartier D., Le Digabel S., Salomon L. Performance indicators in multiobjective optimization // Eur. J. Oper. Res. 2021. V. 292, No. 2. P. 397–422. DOI: 10.1016/j.ejor.2020.11.016.

34. Konak A., Coit D. W., Smith A. E. Multi-objective optimization using genetic algorithms: A tutorial // Reliab. Eng. Syst. Saf. 2006. V. 91, No. 9. P. 992–1007. DOI: 10.1016/j.ress.2005.11.018.

35. Hadka D. MOEA framework: A free and open source Java framework for multiobjective optimization. Version 5.1. 2025. URL: moeaframework.org (accessed: 10.10.2025).

36. Deb K., Pratap A., Agarwal S., Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA-II // IEEE Trans. Evolut. Comput. 2002. V. 6, No. 2. P. 182–197. DOI: 10.1109/4235.996017.

37. Zitzler E., Laumanns M., Thiele L. SPEA2: Improving the strength Pareto evolutionary algorithm. Inst. Tech. Inform. Kommun. rep. 103. Zürich: ETH Zürich, 2001. DOI: 10.3929/ethz-a-004284029.

38. Corne D. W., Jerram N. R., Knowles J. D., Oates M. J. PESA-II: Region-based selection in evolutionary multiobjective optimization // Proc. 3rd Annu. Conf. Genetic and Evolutionary Computation (San Francisco, CA, July 7–11, 2001). San Francisco: Morgan Kaufmann Publ., 2001. P. 283–290.

39. Knowles J. D., Corne D. W. Approximating the nondominated front using the Pareto archived evolution strategy // Evolut. Comput. 2000. V. 8, No. 2. P. 149–172. DOI: 10.1162/106365600568167.

40. Mann H. B., Whitney D. R. On a test of whether one of two random variables is stochastically larger than the other // Ann. Math. Stat. 1947. V. 18, No. 1. P. 50–60. DOI: 10.1214/aoms/1177730491.

41. Wilcoxon F. Individual comparisons by ranking methods // Biom. Bull. 1945. V. 1, No. 6. P. 80–83.

42. Lindauer M., Eggensperger K., Feurer M. [et al.]. SMAC3: A versatile Bayesian optimization package for hyperparameter optimization // J. Mach. Learn. Res. 2022. V. 23. Article ID 54. 9 p.

Юськов Александр Дмитриевич
Кулаченко Игорь Николаевич
Мельников Андрей Андреевич
Кочетов Юрий Андреевич

Статья поступила
3 февраля 2025 г.
После доработки —
23 мая 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 117–144

UDC 519.8 DOI: 10.33048/daio.2025.32.827

A HYBRID ALGORITHM FOR A TWO-OBJECTIVE TRAFFIC ENGINEERING PROBLEM

A. D. Yuskov[1, a], *I. N. Kulachenko*[2, b], *A. A. Melnikov*[2, c], and *Y. A. Kochetov*[2, d]

[1] Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia
[2] Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue, 630090 Novosibrsk, Russia
E-mail: [a] a.yuskov@g.nsu.ru, [b] ink@math.nsc.ru,
[c] melnikov@math.nsc.ru, [d] jkochet@math.nsc.ru

Abstract. We consider an Internet traffic routing problem. The paths for requests are assigned implicitly by setting link weights. The loads of links are generated by a simulator. If the load of a link is greater than its capacity, then the link is called congested. Our goal is to minimize two objective functions: the number of congested links and the distance between the initial and current weight vectors. The problem also includes two constraints: the total link flow in the network has an upper bound and new congested links are unwanted. We propose a new two-stage evolutionary scheme. The scheme employs a local search algorithm with a large neighbourhood to find an initial approximation of the Pareto set. The algorithm utilizes an integer linear programming model to determine the best solution in the neighbourhood. We compare the proposed scheme with well-known evolutionary algorithms using instances with 628 links and 1324 requests. According to the experiments, the proposed scheme constructs solutions statistically better at 15–49% for many performance indicators (9 out of 10). Tab. 3, illustr. 6, bibliogr. 42.

Keywords: black box optimization, matheuristic, variable neighbourhood search, OSPF, evolutionary algorithm.

References

1. **A. Altın, B. Fortz, M. Thorup,** and **H. Ümit,** Intra-domain traffic engineering with shortest path routing protocols, *Ann. Oper. Res.* **204** (1), 65–95 (2013), DOI: 10.1007/s10479-012-1270-7.

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

2. **A. Elwalid, C. Jin, S. Low,** and **I. Widjaja,** MATE: MPLS adaptive traffic engineering, in *Twenty Years into the Communications Odyssey*, Proc. 20th Annu. Joint Conf. IEEE Computer and Communications Societies (Anchorage, AK, Apr. 22–26, 2001), Vol. 3 (IEEE Comput. Soc., Washington, 2001), pp. 1300–1309, DOI: 10.1109/infcom.2001.916625.
3. **M. Abbasi, A. Guleria,** and **M. Devi,** Traffic engineering in software defined networks: A survey, *J. Telecommun. Inf. Technol.* **4**, 3–14 (2016).
4. **R. Bhatia, F. Hao, M. Kodialam,** and **T. Lakshman,** Optimized network traffic engineering using segment routing, in *Proc. 2015 IEEE Conf. Computer Communications* (Hong Kong, China, Apr. 26 – May 1, 2015) (IEEE, Piscataway, 2015), pp. 657–665, DOI: 10.1109/INFOCOM.2015.7218434.
5. **Y. Wang** and **Z. Wang,** Explicit routing algorithms for Internet traffic engineering, in *Proc. 8th Int. Conf. Computer Communications and Networks* (Boston, MA, Oct. 11–13, 1999) (IEEE, Piscataway, 1999), pp. 582–588, DOI: 10.1109/ICCCN.1999.805577.
6. **F. Poppe, S. Van den Bosch, P. de La Vallée-Poussin, H. Van Hove, H. De Neve,** and **G. Petit,** Choosing the objectives for traffic engineering in IP backbone networks based on quality-of-service requirements, in *Quality of Future Internet Service*, Proc. 1st COST 263 Int. Workshop (Berlin, Germany, Sept. 25–26, 2000) (Springer, Heidelberg, 2000), pp. 129–140 (Lect. Notes Comput. Sci., Vol. 1922), DOI: 10.1007/3-540-39939-9_11.
7. **C. Audet** and **W. Hare,** *Derivative-Free and Blackbox Optimization* (Springer, Cham, 2017), DOI: 10.1007/978-3-319-68913-5.
8. **A. D. Yuskov, I. N. Kulachenko, A. A. Melnikov,** and **Yu. A. Kochetov,** Stadium antennas deployment optimization, in *Mathematical Optimization Theory and Operations Research*, Proc. 23rd Int. Conf. MOTOR 2024 (Omsk, Russia, June 30 – July 6, 2024) (Springer, Cham, 2024), pp. 449–461 (Lect. Notes Comput. Sci., Vol. 14766), DOI: 10.1007/978-3-031-62792-7_30.
9. **A. D. Yuskov, I. N. Kulachenko, A. A. Melnikov,** and **Yu. A. Kochetov,** Decomposition approach for a two-echelon inventory management system, *Diskretn. Anal. Issled. Oper.* **31** (4), 186–212 (2024), DOI: 10.33048/daio.2024.31.794 [Russian] [*J. Appl. Ind. Math.* **18** (4) 918–934 (2024), DOI: 10.1134/S1990478924040239].
10. *Internetworking Technologies Handbook* (Cisco Press, Indianapolis, 2000).
11. **B. Fortz** and **M. Thorup,** Internet traffic engineering by optimizing OSPF weights, in *Reaching the Promised Land of Communications*, Proc. 20th Annu. Joint Conf. IEEE Computer and Communications Societies (Tel Aviv, Israel, Mar. 26–30, 2000), Vol. 2 (IEEE Comput. Soc., Washington, 2000), pp. 519–528, DOI: 10.1109/INFCOM.2000.832225.
12. **M. Ericsson, M. Resende,** and **P. Pardalos,** A genetic algorithm for the weight setting problem in OSPF routing, *J. Comb. Optim.* **6**, 299–333 (2002), DOI: 10.1023/A:1014852026591.
13. **B. Fortz** and **M. Thorup,** Optimizing OSPF/IS-IS weights in a changing world, *IEEE J. Sel. Areas Commun.* **20**, 756–767 (2002), DOI: 10.1109/JSAC.2002.1003042.

14. **M. S. Kodialam** and **T. V. Lakshman,** Network link weight setting: A machine learning based approach, in *Proc. IEEE Conf. Computer Communications* (London, May 2–5, 2022) (IEEE, Piscataway, 2022), pp. 2048–2057, DOI: 10.1109/INFOCOM48880.2022.9796922.
15. **M. Pióro, Á. Szentesi, J. Harmatos, A. Jüttner, P. Gajowniczek,** and **S. Kozdrowski,** On open shortest path first related network optimisation problems, *Perform. Eval.* **48** (1–4), 201–223 (2002), DOI: 10.1016/S0166-5316(02)00036-6.
16. **S. Balon, F. Skivée,** and **G. Leduc,** How well do traffic engineering objective functions meet TE requirements?, in *NETWORKING 2006. Networking Technologies, Services, Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems*, Proc. 5th Int. IFIP-TC6 Networking Conf. (Coimbra, Portugal, May 15–19, 2006) (Springer, Heidelberg, 2006), pp. 75–86 (Lect. Notes Comput. Sci., Vol. 3976), DOI: 10.1007/11753810_7.
17. **F. Blanchy, L. Melon,** and **G. Leduc,** Routing in a MPLS network featuring preemption mechanisms, in *Proc. 10th Int. Conf. Telecommunications* (Papeete, French Polynesia, Feb. 23 – Mar. 1, 2003), Vol. 1 (IEEE, Piscataway, 2003), pp. 253–260, DOI: 10.1109/ICTEL.2003.1191228.
18. **G. Athanasiou, K. Tsagkaris, P. Vlacheas, D. Karvounas,** and **P. Demestichas,** Multi-objective traffic engineering for future networks, *IEEE Commun. Lett.* **16** (1), 101–103 (2012), DOI: 10.1109/LCOMM.2011.110711.112071.
19. **E.-S. M. El-Alfy,** Flow-based path selection for Internet traffic engineering with NSGA-II, in *Proc. 17th Int. Conf. Telecommunications* (Doha, Qatar, Apr. 4–7, 2010) (IEEE, Piscataway, 2010), pp. 621–627, DOI: 10.1109/ICTEL.2010.5478839.
20. **P. Sousa, P. Cortez, M. Rio,** and **M. Rocha,** Traffic engineering approaches using multicriteria optimization techniques, in *Wired/Wireless Internet Communications*, Proc. 9th IFIP TC 6 Int. Conf. (Vilanova i la Geltrú, Spain, June 15–17, 2011) (Springer, Heidelberg, 2011), pp. 104–115 (Lect. Notes Comput. Sci., Vol. 6649), DOI: 10.1007/978-3-642-21560-5_9.
21. **V. Pereira, P. Sousa,** and **M. Rocha,** A comparison of multi-objective optimization algorithms for weight setting problems in traffic engineering, *Nat. Comput.* **21**, 507–522 (2022), DOI: 10.1007/s11047-020-09807-1.
22. **N. Wang, K. H. Ho, G. Pavlou,** and **M. Howarth,** An overview of routing optimization for internet traffic engineering, *IEEE Commun. Surv. Tutor.* **10** (1), 36–56 (2008), DOI: 10.1109/COMST.2008.4483669.
23. **S. Kaneda, T. Uyematsu, N. Nagatsu,** and **K. Sato,** Network design and cost optimization for label switched multilayer photonic IP networks, *IEEE J. Sel. Areas Commun.* **23** (8), 1612–1619 (2005), DOI: 10.1109/JSAC.2005.851747.
24. **R. Zhang-Shen** and **N. McKeown,** Designing a predictable Internet backbone network, in *Proc. 3rd Workshop Hot Topics in Networks (HotNets-III)* (San Diego, CA, Nov. 15–16, 2004) (ACM SIGCOMM, New

York, 2004), URL: conferences.sigcomm.org/hotnets/2004/HotNets-III%20Proceedings/zhang-shen.pdf (accessed: 10.10.2025).

25. **D. D. Clark,** *Designing an Internet* (MIT Press, Cambridge, MA, 2018).
26. **K. Holmberg** and **D. Yuan,** Optimization of internet protocol network design and routing, *Networks* **43** (1), 39–53 (2004), DOI: 10.1002/net.10102.
27. **M. Dehghani, V. Vahdat, M. Amiri, E. Rabiei,** and **S. Salehi,** A multi-objective optimization model for a reliable generalized flow network design, *Comput. Ind. Eng.* **138**, ID 106074 (2019), DOI: 10.1016/j.cie.2019.106074.
28. **H. Zhu, V. Gupta, S. S. Ahuja, Y. Tian, Y. Zhang,** and **X. Jin,** Network planning with deep reinforcement learning, in *Proc. ACM SIGCOMM 2021 Conf.* (Delft, Netherlands, Aug. 23–28, 2021) (ACM, New York, 2021), pp. 258–271, DOI: 10.1145/3452296.3472902.
29. **R. T. Wong,** Telecommunications network design: Technology impacts and future directions, *Networks* **77** (2), 205–224 (2021), DOI: 10.1002/net.21997.
30. **A. D. Yuskov, I. N. Kulachenko, A. A. Melnikov,** and **Yu. A. Kochetov,** Two-stage algorithm for bi-objective black-box traffic engineering, in *Optimization and Applications*, Rev. Sel. Pap. 14th Int. Conf. OPTIMA 2023 (Petrovac, Montenegro, Sept. 18–22, 2023) (Springer, Cham, 2023), pp. 110–125 (Lect. Notes Comput. Sci., Vol. 14395), DOI: 10.1007/978-3-031-47859-8_9.
31. **P. Hansen, N. Mladenović, R. Todosijević,** and **S. Hanafi,** Variable neighborhood search: Basics and variants, *EURO J. Comput. Optim.* **5** (3), 423–454 (2016), DOI: 10.1007/s13675-016-0075-x.
32. **J. Forrest, T. Ralphs, S. Vigerske,** [et al.], COIN-OR Branch-and-Cut solver (CERN; Zenodo, Genève, 2023), DOI: 10.5281/zenodo.10041724.
33. **C. Audet, J. Bigeon, D. Cartier, S. Le Digabel,** and **L. Salomon,** Performance indicators in multiobjective optimization, *Eur. J. Oper. Res.* **292** (2), 397–422 (2021), DOI: 10.1016/j.ejor.2020.11.016.
34. **A. Konak, D. W. Coit,** and **A. E. Smith,** Multi-objective optimization using genetic algorithms: A tutorial, *Reliab. Eng. Syst. Saf.* **91** (9), 992–1007 (2006), DOI: 10.1016/j.ress.2005.11.018.
35. **D. Hadka,** MOEA framework: A free and open source Java framework for multiobjective optimization. Version 5.1 (2025), URL: moeaframework.org (accessed: 10.10.2025).
36. **K. Deb, A. Pratap, S. Agarwal,** and **T. Meyarivan,** A fast and elitist multiobjective genetic algorithm: NSGA-II, *IEEE Trans. Evolut. Comput.* **6** (2), 182–197 (2002), DOI: 10.1109/4235.996017.
37. **E. Zitzler, M. Laumanns,** and **L. Thiele,** SPEA2: Improving the strength Pareto evolutionary algorithm, *Inst. Tech. Inform. Kommun. rep. 103* (ETH Zürich, Zürich, 2001), DOI: 10.3929/ethz-a-004284029.
38. **D. W. Corne, N. R. Jerram, J. D. Knowles,** and **M. J. Oates,** PESA-II: Region-based selection in evolutionary multiobjective optimization, in *Proc. 3rd Annu. Conf. Genetic and Evolutionary Computation* (San Francisco, CA, July 7–11, 2001) (Morgan Kaufmann Publ., San Francisco, 2001), pp. 283–290.

39. J. D. Knowles and **D. W. Corne,** Approximating the nondominated front using the Pareto archived evolution strategy, *Evolut. Comput.* **8** (2), 149–172 (2000), DOI: 10.1162/106365600568167.

40. H. B. Mann and **D. R. Whitney,** On a test of whether one of two random variables is stochastically larger than the other, *Ann. Math. Stat.* **18** (1), 50–60 (1947), DOI: 10.1214/aoms/1177730491.

41. F. Wilcoxon, Individual comparisons by ranking methods, *Biom. Bull.* **1** (6), 80–83 (1945).

42. M. Lindauer, K. Eggensperger, M. Feurer, [et al.], SMAC3: A versatile Bayesian optimization package for hyperparameter optimization, *J. Mach. Learn. Res.* **23**, ID 54 (2022).

Aleksandr D. Yuskov
Igor N. Kulachenko
Andrey A. Melnikov
Yury A. Kochetov

Received February 3, 2025
Revised May 23, 2025
Accepted June 22, 2025

ДИСКРЕТНЫЙ АНАЛИЗ
И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

2025. Том 32, № 3

Зав. редакцией Е. В. Горкунов

Журнал подготовлен с использованием макропакета LaTeX 2_ε.
The present publication has been typeset using LaTeX 2_ε.

Журнал зарегистрирован в Федеральной службе по надзору
в сфере связи, информационных технологий и массовых коммуникаций.
Свидетельство о регистрации ЭЛ № ФС77-85978 от 26.09.2023 г.
Размещение в сети Интернет: `math-sobolev.ru`.

Дата размещения в сети Интернет 30.01.2026 г.
Формат $70 \times 100\,1/16$. Усл. печ. л. 11,7. Объём 1,56 МБ.

Издательство Института математики,
пр. Академика Коптюга, 4, 630090 Новосибирск, Россия