БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

ЖУРНАЛ
БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

МАТЕМАТИКА
ИНФОРМАТИКА

JOURNAL
OF THE BELARUSIAN STATE UNIVERSITY

MATHEMATICS
and
INFORMATICS

Издается с января 1969 г.
(до 2017 г. – под названием «Вестник БГУ.
Серия 1, Физика. Математика. Информатика»)

Выходит три раза в год

3

2021

МИНСК
БГУ

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

УДК 517.5

О РАЦИОНАЛЬНЫХ СУММАХ АБЕЛЯ – ПУАССОНА НА ОТРЕЗКЕ И АППРОКСИМАЦИЯХ ФУНКЦИЙ МАРКОВА

П. Г. ПОЦЕЙКО[1]***, Е. А. РОВБА***[1]

[1]*Гродненский государственный университет им. Янки Купалы, ул. Ожешко, 22, 230023, г. Гродно, Беларусь*

Исследованы приближения на отрезке $[-1, 1]$ функций Маркова суммами Абеля – Пуассона рационального интегрального оператора типа Фурье, ассоциированного с системой алгебраических дробей Чебышева – Маркова, в случае фиксированного числа геометрически различных полюсов. Найдены интегральное представление приближений и оценка равномерных приближений. Изучены приближения функций Маркова в случае, когда мера μ удовлетворяет условиям $\operatorname{supp}\mu = [1, a]$, $a > 1$, $d\mu(t) = \varphi(t)dt$ и $\varphi(t) \asymp (t-1)^{\alpha}$ на $[1, a]$. Получены оценки поточечных и равномерных приближений и асимптотическое выражение мажоранты равномерных приближений. Найдены оптимальные значения параметров, при которых мажоранта имеет наибольшую скорость убывания. В качестве следствия приведены асимптотические оценки приближений на отрезке $[-1, 1]$ исследуемым методом рациональной аппроксимации некоторых элементарных функций Маркова.

Ключевые слова: функции Маркова; рациональные интегральные операторы; суммы Абеля – Пуассона; алгебраические дроби Чебышева – Маркова; наилучшие приближения; асимптотические оценки; точные константы.

Образец цитирования:
Поцейко ПГ, Ровба ЕА. О рациональных суммах Абеля – Пуассона на отрезке и аппроксимациях функций Маркова. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:6–24.
https://doi.org/10.33581/2520-6508-2021-3-6-24

For citation:
Patseika PG, Rouba YA. On rational Abel – Poisson means on a segment and approximations of Markov functions. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:6–24. Russian.
https://doi.org/10.33581/2520-6508-2021-3-6-24

Авторы:
Павел Геннадьевич Поцейко – кандидат физико-математических наук; доцент кафедры фундаментальной и прикладной математики факультета математики и информатики.
Евгений Алексеевич Ровба – доктор физико-математических наук, профессор; заведующий кафедрой фундаментальной и прикладной математики факультета математики и информатики.

Authors:
Pavel G. Patseika, PhD (physics and mathematics); associate professor at the department of fundamental and applied mathematics, faculty of mathematics and informatics.
pahamatby@gmail.com
https://orcid.org/0000-0001-7835-0500
Yauheni A. Rouba, doctor of science (physics and mathematics), full professor; head of the department of fundamental and applied mathematics, faculty of mathematics and informatics.
rovba.ea@gmail.com
https://orcid.org/0000-0002-1265-1965

ON RATIONAL ABEL – POISSON MEANS ON A SEGMENT AND APPROXIMATIONS OF MARKOV FUNCTIONS

P. G. PATSEIKA[a]**,** ***Y. A. ROUBA***[a]

[a]*Yanka Kupala State University of Grodno, 22 Ažeška Street, Hrodna 230023, Belarus*
Corresponding author: P. G. Patseika (pahamatby@gmail.com)

Approximations on the segment $[-1, 1]$ of Markov functions by Abel – Poisson sums of a rational integral operator of Fourier type associated with the Chebyshev – Markov system of algebraic fractions in the case of a fixed number of geometrically different poles are investigated. An integral representation of approximations and an estimate of uniform approximations are found. Approximations of Markov functions in the case when the measure μ satisfies the conditions $\operatorname{supp}\mu = [1, a]$, $a > 1$, $d\mu(t) = \varphi(t)dt$ and $\varphi(t) \asymp (t-1)^{\alpha}$ on $[1, a]$ are studied and estimates of pointwise and uniform approximations and the asymptotic expression of the majorant of uniform approximations are obtained. The optimal values of the parameters at which the majorant has the highest rate of decrease are found. As a corollary, asymptotic estimates of approximations on the segment $[-1, 1]$ are given by the method of rational approximation of some elementary Markov functions under study.

Keywords: Markov functions; rational integral operators; Abel – Poisson means; Chebyshev – Markov algebraic fractions; best approximations; asymptotic estimates; exact constants.

Введение

Приближение непрерывных 2π-периодических функций суммами Абеля – Пуассона является хорошо известной задачей. И. П. Натансон [1] установил асимптотическое выражение точной верхней грани уклонений на классах $H_{2\pi}^{(\alpha)}$ 2π-периодических функций, удовлетворяющих условию Липшица порядка α, $\alpha \in (0, 1]$, с константой, равной единице. А. Ф. Тиман [2] уточнил остаточный член в асимптотическом равенстве, полученном И. П. Натансоном. Полное асимптотическое разложение верхних граней уклонений на классе $H_{2\pi}^{(1)}$ было установлено Э. Л. Штарком [3]. В. В. Жук [4] получил оценки сверху уклонений сумм Пуассона от функций $f \in C_{2\pi}$ в терминах модулей непрерывности.

Для функций $f \in C[-1, 1]$ точные верхние грани уклонений сумм Абеля – Пуассона на классах $H^{(\alpha)}[-1, 1]$, $\alpha \in (0, 1]$, были установлены Ю. И. Русецким [5]. Т. В. Жигалло [6] уточнила остаточный член в асимптотической формуле, полученной Ю. И. Русецким.

В 1956 г. М. М. Джрбашян [7] ввел рациональные ряды Фурье, обобщающие соответствующие классические тригонометрические ряды. В частности, в этой работе было найдено компактное представление ядра Дирихле рациональных рядов Фурье. В 1963 г. А. А. Китбалян [8] предложил подход к построению сумм Абеля – Пуассона тригонометрических рядов Фурье, введенных М. М. Джрбашяном. В его работе был установлен ряд теорем о сходимости при $r \to 1-0$ сумм Абеля – Пуассона рациональных рядов Фурье к функциям $f \in L_p(-\pi, \pi)$, $p > 1$.

Пусть μ – положительная борелевская мера с компактным носителем $F = \operatorname{supp}\mu \subset \mathbb{R}$. Преобразование Коши меры μ

$$\hat{\mu}(z) = \int_F \frac{d\mu(t)}{t-z}, \; z \in \overline{\mathbb{C}} \backslash F,$$

называется функцией Маркова [9].

Функции Маркова голоморфны в $\overline{\mathbb{C}} \backslash F$, и их рациональная аппроксимация является хорошо известной классической задачей. Данной тематике посвятили свои статьи А. А. Гончар [10], Т. Ганелиус [11], Я.-Э. Андерссон [12], А. А. Пекарский [13]. Отметим работу Н. С. Вячеславова и Е. П. Мочалиной [14], в которой изучаются аппроксимации функций Маркова в пространствах Харди H_p, $p \in (0, +\infty)$, при определенных условиях на меру μ, а также работу А. П. Старовойтова и Ю. А. Лабыч [15], где для функции Маркова, порожденной положительными борелевскими мерами степенного типа, установлена асимптотика поведения строчных последовательностей ее таблицы Паде. Последнее позволило найти точные порядки убывания наилучших приближений функций Маркова рациональными функциями с фиксированным числом полюсов.

Среди методов рациональной аппроксимации выделяются интегральные операторы, восходящие своими корнями к рядам Фурье и методам их суммирования. В работе [16] исследованы аппроксимации функций Маркова в единичном круге частичными суммами рядов Фурье по системам рациональных функций, введенных С. Такенакой [17] и Ф. Мальмквистом [18], а также на отрезке $[-1, 1]$ по системам рациональных функций, введенных М. М. Джрбашяном и А. А. Китбаляном [19]. Эти исследования были продолжены в [20], где найдены асимптотические оценки равномерных приближений указанными методами при фиксированном числе геометрически различных полюсов аппроксимирующей функции.

Заметим, что приближения непрерывных функций с характерными особенностями рациональными функциями с фиксированным числом геометрически различных полюсов впервые были рассмотрены в работах К. Н. Лунгу [21; 22].

В 1979 г. Е. А. Ровба [23] ввел интегральный оператор на основании системы рациональных функций Чебышева – Маркова, который является естественным обобщением частичных сумм полиномиальных рядов Фурье – Чебышева. Пусть задано произвольное множество чисел $\{a_k\}_{k=1}^{n}$, где a_k являются либо действительными ($|a_k| < 1$), либо попарно комплексно-сопряженными. На множестве суммируемых на отрезке $[-1, 1]$ с весом $\frac{1}{\sqrt{1-x^2}}$ функций $f(x)$ рассмотрим рациональный интегральный оператор Фурье – Чебышева порядка не выше n (см. [23]):

$$s_n(f, x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(\cos v)\frac{\sin\lambda_n(v, u)}{\sin\frac{v-u}{2}}dv, \ x = \cos u, \tag{1}$$

где

$$\lambda_n(v, u) = \int_u^v \lambda_n(y)dy, \ \lambda_n(y) = \frac{1}{2} + \sum_{k=1}^{n}\frac{1-\alpha_k^2}{1+2\alpha_k\cos y+\alpha_k^2}, \ \alpha_k = \frac{a_k}{1+\sqrt{1-a_k^2}}, \ |\alpha_k| < 1.$$

Оператор

$$s_n : f \to \frac{p_n(x)}{\prod_{k=1}^{n}(1+a_k x)},$$

где $p_n(x)$ – некоторый многочлен степени не выше n, коэффициенты которого зависят от a_k, и $s_n(1, x) = 1$. В частности, если положить $a_k = 0$, $k = 1, 2, \ldots, n$, то $s_n(f, x)$ есть частичная сумма полиномиального ряда Фурье – Чебышева.

Целью настоящей работы является изучение аппроксимационных свойств сумм Абеля – Пуассона рациональных интегральных операторов (1) в случае ограничений на количество геометрически различных полюсов. Представляет интерес исследовать данным методом скорость рациональной аппроксимации функций Маркова.

Суммы Абеля – Пуассона рациональных интегральных операторов Фурье – Чебышева и приближения функций Маркова

Пусть q – произвольное натуральное число, A_q есть множество точек $a = (a_1, \ldots, a_q)$ таких, что все a_i, $i = 1, 2, \ldots, q$, различны. В этом случае значения интегрального оператора (1) представляют собой рациональные функции вида

$$s_{mq}(f, x) = \frac{p_{mq}(x)}{\left(\prod_{k=1}^{q}(1+a_k x)\right)^m}, \ m = 0, 1, \ldots.$$

Другими словами, будем вести речь об аппроксимации рациональными функциями с q геометрически различными полюсами в расширенной комплексной плоскости.

Составим суммы:

$$P_{r,q}(f, x) = (1-r)\sum_{k=0}^{+\infty} r^k s_{kq}(f, x), \ x \in [-1, 1], \ r \in (0, 1). \tag{2}$$

Выражение (2) естественно назвать суммами Абеля – Пуассона рациональных интегральных операторов Фурье – Чебышева с q геометрически различными полюсами. Из представления (2) очевидно также, что $P_{r,q}(1, x) = 1$.

Заметим, что формула, выражающая зависимость между суммами Абеля – Пуассона и частичными суммами в случае числовых рядов, содержится, например, в [24, с. 403].

Изучим приближения функций Маркова суммами Абеля – Пуассона (2). С этой целью введем следующие обозначения:

$$\varepsilon_{r,q}(x, A_q) = \hat{\mu}(x) - P_{r,q}(\hat{\mu}(\cdot), x), \; x \in [-1, 1], \tag{3}$$

$$\varepsilon_{r,q}(A_q) = \left\| \hat{\mu}(x) - P_{r,q}(\hat{\mu}(\cdot), x) \right\|_{C[-1,1]}, \; r \in (0, 1). \tag{4}$$

Будем полагать, что $\operatorname{supp}\mu \subset [1, +\infty)$,

$$\int \frac{d\mu(t)}{t-1} < \infty. \tag{5}$$

Справедлива следующая теорема.

Теорема 1. *Пусть мера* μ *удовлетворяет условию (5), а мера* ν *определяется соотношением*

$$d\nu(y) = \frac{4y^2}{1-y^2} d\mu(\eta(y)), \; y \in (0, 1], \tag{6}$$

где

$$\eta(y) = \frac{1}{2}\left(y + \frac{1}{y}\right).$$

Тогда для приближений функций Маркова $\hat{\mu}(x)$ *на отрезке* $[-1, 1]$ *суммами Абеля – Пуассона (2) имеют место:*

1) интегральное представление

$$\varepsilon_{r,q}(x, A_q) = (1-r) \int\limits_{\operatorname{supp}\nu} \frac{\cos\psi_r(y, u, A_q)\, d\nu(y)}{\sqrt{1 - 2y\cos u + y^2}\,\sqrt{1 - 2r\omega_q(y)\cos\arg\omega_q(\xi) + r^2\omega_q^2(y)}}; \tag{7}$$

2) оценка равномерных приближений

$$\varepsilon_{r,q}(A_q) \le (1-r) \max_{x \in [-1,1]} \int\limits_{\operatorname{supp}\nu} \frac{|d\nu(y)|}{\sqrt{1 - 2y\cos u + y^2}\,\sqrt{1 - 2r\omega_q(y)\cos\arg\omega_q(\xi) + r^2\omega_q^2(y)}},$$

где

$$\psi_r(y, u, A_q) = \arg\frac{\xi - y}{1 - r\omega_q(\xi)\omega_q(y)}, \;\; \omega_q(y) = \prod_{j=1}^{q} \frac{y + \alpha_j}{1 + \alpha_j y}, \;\; x = \cos u, \;\; \xi = e^{iu}. \tag{8}$$

Д о к а з а т е л ь с т в о. С учетом точности сумм Абеля – Пуассона (2) на константах из (3) получим

$$\varepsilon_{r,q}(x, A_q) = (1-r) \sum_{k=0}^{+\infty} r^k \delta_{k,q}(x, A_q), \;\; x \in [-1, 1], \tag{9}$$

где $\delta_{k,q}(x, A_q)$ – приближения функций Маркова рациональным интегральным оператором Фурье – Чебышева (1) с q геометрически различными полюсами в расширенной комплексной плоскости. С другой стороны, известно, что интегральный оператор (1) является частным случаем рационального интегрального оператора на отрезке, введенного в [25]. Из результатов этой работы следует, что

$$\delta_{k,q}(x, A_q) = \frac{1}{2} \int\limits_{\operatorname{supp}\nu} \left[\frac{1 - \xi y}{\xi} \overline{\omega_q^k(\xi)} + (\xi - y)\omega_q^k(\xi) \right] \frac{\omega_q^k(y)\, d\nu(y)}{1 - 2y\cos u + y^2},$$

где $\xi = e^{iu}$, $x = \cos u$, $k = 0, 1, \ldots$, $\nu(y)$ из (6).

Подставим последнее соотношение в (9) и поменяем порядок суммирования и интегрирования. Указанная операция оправданна, поскольку ряд в правой части (9) равномерно сходится при всех $x \in [-1, 1]$ для любого фиксированного r, $r \in (0, 1)$. Тогда

$$\varepsilon_{r,q}(x, A_q) = \frac{1-r}{2} \int\limits_{\operatorname{supp}\nu} \left[(\bar{\xi} - y) \sum_{k=0}^{+\infty} r^k \overline{\omega_q^k(\xi)} \omega_q^k(y) + (\xi - y) \sum_{k=0}^{+\infty} r^k \omega_q^k(\xi) \omega_q^k(y) \right] \frac{d\nu(y)}{1 - 2y\cos u + y^2}.$$

Ряды в квадратных скобках представляют собой суммы геометрических прогрессий со знаменателями $\left| r\overline{\omega_q(\xi)}\omega_q(y) \right| < 1$ и $\left| r\omega_q(\xi)\omega_q(y) \right| < 1$ соответственно. Следовательно,

$$\varepsilon_{r,q}(x, A_q) = \frac{1-r}{2} \int\limits_{\operatorname{supp}\nu} \left[\frac{\bar{\xi} - y}{1 - r\overline{\omega_q(\xi)}\omega_q(y)} + \frac{\xi - y}{1 - r\omega_q(\xi)\omega_q(y)} \right] \frac{d\nu(y)}{1 - 2y\cos u + y^2}, \ x = \cos u.$$

Выражение в квадратных скобках представляет собой сумму взаимно комплексно-сопряженных слагаемых, т. е. является действительно значной функцией. Используя первое из обозначений в (8), после соответствующих преобразований придем к (7).

Второе утверждение теоремы 1 легко следует из (7). Теорема 1 доказана.

Оценки приближений функций Маркова в случае меры специального вида

При исследовании приближений функций Маркова часто рассматривается случай, когда производная меры $\mu(t)$ слабо эквивалентна некоторой степенной функции (см., например, [12; 13]). Такой случай изучается нами далее. При этом в определении рационального интегрального оператора (1) для удобства сделаем замену $\alpha_k \mapsto -\alpha_k$, $k = 1, 2, \ldots, q$, и будем полагать, что $\alpha_k \in [0, 1)$.

Теорема 2. *Пусть* $d\mu(t) = \varphi(t)dt$ *и* $\varphi(t) \asymp (t-1)^\gamma$, $t \in [1, a]$, $\gamma > 0$. *Тогда в условиях теоремы 1 для приближений функции* $\hat{\mu}(x)$ *на отрезке* $[-1, 1]$ *суммами Абеля – Пуассона (2) справедливы оценки:*

1) поточечных приближений

$$\left|\varepsilon_{r,q}(x, A_q)\right| \le \frac{1-r}{2^{\gamma-1}} \int\limits_d^1 \frac{(1-y)^{2\gamma} dy}{y^\gamma \sqrt{1 - 2y\cos u + y^2} \sqrt{1 - 2r\omega_q(y)\cos\arg\omega_q(\xi) + r^2\omega_q^2(y)}}; \tag{10}$$

2) равномерных приближений

$$\varepsilon_{r,q}(A_q) \le \varepsilon_{r,q}^*(A_q), \ n \in \mathbb{N}, \tag{11}$$

где

$$\varepsilon_{r,q}^*(A_q) = \frac{1-r}{2^{\gamma-1}} \int\limits_d^1 \frac{(1-y)^{2\gamma-1}}{y^\gamma} \frac{dy}{1 - r\left|\omega_q(y)\right|}, \tag{12}$$

$d = a - \sqrt{a^2 - 1}$, $d \in (0, 1]$, $\omega_q(y)$ *из (8).*

Доказательство. Из (6) и (7) следует, что в случае $d\mu(t) = \varphi(t)dt$ и $\varphi(t) \asymp (t-1)^\gamma$ естественно рассматривать приближения (3) в виде

$$\varepsilon_{r,q}(x, A_q) = \frac{1-r}{2^{\gamma-1}} \int\limits_d^1 \frac{(1-y)^{2\gamma} \cos\psi_r(y, u, A_q) dy}{y^\gamma \sqrt{1 - 2y\cos u + y^2} \sqrt{1 - 2r\omega_q(y)\cos\arg\omega_q(\xi) + r^2\omega_q^2(y)}},$$

где d определено в формулировке теоремы, $x = \cos u$, $\omega_q(y)$, $\psi_r(y, u, A_q)$ из (8). Учитывая, что $\left|\cos\psi_r(y, u, A_q)\right| \le 1$, из последнего соотношения следует оценка (10).

Воспользовавшись известным неравенством

$$\sqrt{1 - 2y\cos u + y^2} \ge 1 - y, \ y \in [0, 1], \ u \in \mathbb{R},$$

а также заметив, что

$$\sqrt{1 - 2r\omega_q(y)\cos\arg\omega_q(\xi) + r^2\omega_q^2(y)} \ge 1 - r\left|\omega_q(y)\right|, \ r \in (0, 1),$$

из (10) приходим к (11). Доказательство теоремы 2 завершено.

Замечание. Теорема 2 имеет место и при $d = 0$, что соответствует случаю, когда носитель функции Маркова $F = [1, +\infty)$. Тогда полагаем $\gamma \in (0, 1)$.

Положим в соотношениях (10) и (11) значения параметров $\alpha_k = 0$, $k = 1, 2, \ldots, q$. Тогда $\varepsilon_{r,1}(x, O) = \varepsilon_r^{(0)}(x)$, $\varepsilon_{r,1}(O) = \varepsilon_r^{(0)}$, $O = (0, \ldots, 0)$, – соответственно поточечные и равномерные приближения функций Маркова $\hat{\mu}(x)$ на отрезке $[-1, 1]$ суммами Абеля – Пуассона рядов Фурье по системе многочленов Чебышева первого рода, когда мера $\mu(t)$ удовлетворяет условиям в формулировке теоремы 2.

Следствие 1. *Имеют место соотношения*

$$\left|\varepsilon_r^{(0)}(x)\right| \leq \frac{1-r}{2^{\gamma-1}} \int_d^1 \frac{(1-y)^{2\gamma}\, dy}{y^\gamma \sqrt{1 - 2y\cos u + y^2}\sqrt{1 - 2ry\cos u + r^2y^2}}, \quad x = \cos u, \quad x \in [-1, 1],$$

$$\varepsilon_r^{(0)} = \frac{1-r}{2^{\gamma-1}} \int_d^1 \frac{(1-y)^{2\gamma-1}\, dy}{y^\gamma (1-ry)}, \quad r \in (0, 1). \tag{13}$$

Асимптотика мажоранты равномерных приближений

Исследуем асимптотическое поведение величины (12) при $r \to 1$. С этой целью в интеграле выполним замену переменного по формуле $y = \dfrac{1-u}{1+u}$, $dy = \dfrac{-2du}{(1+u)^2}$. Тогда

$$\varepsilon_{r,q}^*(A_q) = 2^{\gamma+1}(1-r)\int_0^D \Omega_r^{(\gamma)}(u, A_q)\, du, \quad D = \frac{1-d}{1+d} = \sqrt{\frac{a-1}{a+1}}, \quad D \in [0, 1), \quad r \in (0, 1), \tag{14}$$

где

$$\Omega_r^{(\gamma)}(u, A_q) = \frac{u^{2\gamma-1}}{(1+u)(1-u^2)^\gamma \left(1 - r|\pi_q(u)|\right)}, \quad \pi_q(u) = \prod_{j=1}^q \frac{\beta_j - u}{\beta_j + u}, \quad \beta_j = \frac{1-\alpha_j}{1+\alpha_j}. \tag{15}$$

Отметим, что в рассматриваемом нами случае для каждого значения $r \in (0, 1)$ может выбираться соответствующее множество точек $A_q = (\alpha_1, \ldots, \alpha_q)$ и $\alpha_k = \alpha_k(r) \to 1$ при $r \to 1$, $k = 1, 2, \ldots, q$. При этом будем полагать, что выполняются условия

$$\lim_{r \to 1} \frac{1-\alpha_k}{1-r} = \infty, \quad k = 1, 2, \ldots, q.$$

Из сказанного следует, что для любого значения $d = a - \sqrt{a^2 - 1}$ существует такое r_0, $r_0 \in (0, 1)$, что при $r \in (r_0, 1)$ $\alpha_k \in [d, 1)$, $k = 1, 2, \ldots, q$. Эти ограничения будем учитывать в дальнейших рассуждениях. В этом случае без нарушения общности можно полагать параметры упорядоченными следующим образом: $0 < \beta_q < \ldots < \beta_1 < D \leq 1$. Справедлива нижеприведенная теорема.

Теорема 3. *При* $r \to 1$ *имеют место асимптотические равенства*

$$\varepsilon_{r,q}^*(A_q) \sim \begin{cases} \dfrac{2^{1-\gamma}(1-r)^{2\gamma}\pi}{\sin 2\pi\gamma \left(\displaystyle\sum_{k=1}^q \frac{1}{\beta_k}\right)^{2\gamma}} + \Phi_r^{(\gamma)}(q, A_q), & \gamma \in \left(0, \dfrac{1}{2}\right), \\[2ex] \dfrac{\sqrt{2}(1-r)}{\displaystyle\sum_{k=1}^q \frac{1}{\beta_k}} \ln\left(1 + \dfrac{2r\beta_q}{1-r}\displaystyle\sum_{k=1}^q \frac{1}{\beta_k}\right) + \Phi_r^{(1/2)}(q, A_q), & \gamma = \dfrac{1}{2}, \\[2ex] 2^{\gamma+1}(1-r)\displaystyle\int_0^{\beta_q} \frac{u^{2\gamma-1}\, du}{(1+u)(1-u^2)^\gamma (1-\pi_q(u))} + \Phi_r^{(\gamma)}(q, A_q), & \gamma > \dfrac{1}{2}. \end{cases} \tag{16}$$

Здесь

$$\Phi_r^{(\gamma)}\left(q,\, A_q\right) = 2^{\gamma+1}(1-r)\left[\sum_{k=1}^{q-1}\int_{\beta_{k+1}}^{\beta_k}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-\pi_{q,\,k}(u)\right)} + \int_{\beta_1}^{D}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-\left|\pi_q(u)\right|\right)}\right], \quad (17)$$

$$\pi_{q,\,k}(u) = \prod_{j=1}^{k}\frac{\beta_j-u}{\beta_j+u}\prod_{j=k+1}^{q}\frac{u-\beta_j}{u+\beta_j}. \quad (18)$$

Доказательство. Представим интеграл в (14) в виде

$$\varepsilon_{r,\,q}^{*}\left(A_q\right) = 2^{\gamma+1}\left[I_1\left(r,\, A_q\right) + I_2\left(r,\, A_q\right) + I_3\left(r,\, A_q\right)\right], \quad (19)$$

где

$$I_1\left(r,\, A_q\right) = (1-r)\int_0^{\beta_q}\Omega_r^{(\gamma)}\left(u,\, A_q\right)du,$$

$$I_2\left(r,\, A_q\right) = (1-r)\sum_{k=1}^{q-1}\int_{\beta_{k+1}}^{\beta_k}\Omega_r^{(\gamma)}\left(u,\, A_q\right)du,$$

$$I_3\left(r,\, A_q\right) = (1-r)\int_{\beta_1}^{D}\Omega_r^{(\gamma)}\left(u,\, A_q\right)du,$$

функция $\Omega_r^{(\gamma)}\left(u,\, A_q\right)$ определена в (15).

Изучим асимптотическое поведение при $r \to 1$ каждого из трех интегралов в отдельности. Дальнейшему изложению предпошлем три леммы.

Лемма 1. *При* $r \to 1$ *справедливы асимптотические равенства*

$$I_1\left(r,\, A_q\right) \sim \begin{cases} \dfrac{(1-r)^{2\gamma}\pi}{\sin 2\pi\gamma\left(2r\sum\limits_{k=1}^{q}\dfrac{1}{\beta_k}\right)^{2\gamma}}, \ \gamma \in \left(0,\, \dfrac{1}{2}\right), \\ \dfrac{1-r}{2r\sum\limits_{k=1}^{q}\dfrac{1}{\beta_k}}\ln\left(1 + \dfrac{2r\beta_q}{1-r}\sum\limits_{k=1}^{q}\dfrac{1}{\beta_k}\right), \ \gamma = \dfrac{1}{2}, \\ (1-r)\displaystyle\int_0^{\beta_q}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-\pi_q(u)\right)}, \ \gamma > \dfrac{1}{2}. \end{cases} \quad (20)$$

Доказательство. Из (14) следует, что

$$I_1\left(r,\, A_q\right) = (1-r)\int_0^{\beta_q}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-r\pi_q(u)\right)}.$$

Очевидно, что асимптотическое поведение интеграла $I_1\left(r,\, A_q\right)$ при $r \to 1$ определяется сколь угодно малой окрестностью нуля переменной интегрирования. Используя разложение в ряд Тейлора

$$\pi_q(u) = 1 - 2u\sum_{k=1}^{q}\frac{1}{\beta_k} + o(u), \ u \to 0,$$

а также очевидное асимптотическое равенство

$$\frac{u^{2\gamma-1}}{(1+u)\left(1-u^2\right)^{\gamma}} \sim u^{2\gamma-1}, \ u \to 0,$$

находим, что

$$I_1(r, A_q) \sim \int\limits_0^{\beta_q} \frac{u^{2\gamma-1}du}{1+\frac{2ru}{1-r}\sum\limits_{k=1}^{q}\frac{1}{\beta_k}}, \ r \to 1.$$

В интеграле выполним замену переменного по формуле $\dfrac{2ru\sum\limits_{k=1}^{q}\frac{1}{\beta_k}}{1-r} \mapsto u.$ Тогда

$$I_1(r, A_q) \sim \frac{(1-r)^{2\gamma}}{\left(2r\sum\limits_{k=1}^{q}\frac{1}{\beta_k}\right)^{2\gamma}} \int\limits_0^{\varphi(r, A_q)} \frac{u^{2\gamma-1}du}{1+u}, \ \varphi(r, A_q) = \frac{2r\beta_q}{1-r}\sum_{k=1}^{q}\frac{1}{\beta_k} \to \infty, \ r \to 1.$$

Пусть $\gamma \in \left(0, \frac{1}{2}\right)$. Тогда, учитывая, что

$$\int\limits_0^{+\infty} \frac{u^{2\gamma-1}du}{1+u} = \frac{\pi}{\sin 2\pi\gamma},$$

получим

$$I_1(r, A_q) \sim \frac{(1-r)^{2\gamma}\pi}{\sin 2\pi\gamma\left(2r\sum\limits_{k=1}^{q}\frac{1}{\beta_k}\right)^{2\gamma}}, \ r \to 1. \tag{21}$$

Если $\gamma = \frac{1}{2}$, то из (21) находим

$$I_1(r, A_q) \sim \frac{1-r}{2r\sum\limits_{k=1}^{q}\frac{1}{\beta_k}} \int\limits_0^{\varphi(r, A_q)} \frac{du}{1+u} = \frac{1-r}{2r\sum\limits_{k=1}^{q}\frac{1}{\beta_k}} \ln\left(1+\varphi(r, A_q)\right), \ r \to 1. \tag{22}$$

Наконец, при $\gamma > \frac{1}{2}$ подынтегральная функция интегрируема при каждом значении $r \in (0, 1)$ и мажорируется интегрируемой функцией. Следовательно, оправдан предельный переход под знаком интеграла $I_1(r, A_q)$ при $r \to 1$, и, значит,

$$I_1(r, A_q) \sim (1-r)\int\limits_0^{\beta_q} \frac{u^{2\gamma-1}du}{(1+u)(1-u^2)^{\gamma}(1-\pi_q(u))}, \ r \to 1. \tag{23}$$

Из (21)–(23) следует (20). Лемма 1 доказана.

Лемма 2. *Справедливы асимптотические равенства*

$$I_2(r, A_q) \sim (1-r)\sum_{k=1}^{q-1}\int\limits_{\beta_{k+1}}^{\beta_k} \frac{u^{2\gamma-1}du}{(1+u)(1-u^2)^{\gamma}(1-\pi_{q,k}(u))}, \quad r \to 1, \tag{24}$$

где $\pi_{q,k}(u)$ *из (18).*

Доказательство. Из (15) следует, что

$$I_2(r, A_q) = (1-r)\sum_{k=1}^{q-1}\int\limits_{\beta_{k+1}}^{\beta_k} \frac{u^{2\gamma-1}du}{(1+u)(1-u^2)^{\gamma}(1-r\pi_{q,k}(u))}.$$

Каждая из $q-1$ подынтегральных функций в сумме справа суммируема на соответствующих интервалах $[\beta_{k+1}, \beta_k]$, $k = 1, 2, \ldots, q-1$, и при любом значении $r \in (0, 1)$ и выполнении условия (18) ограничена в совокупности суммируемой функцией. Выполнив в каждом из $q-1$ интегралов предельный переход при $r \to 1$, придем к равенству (24). Лемма 2 доказана.

Лемма 3. *Справедливы асимптотические равенства*

$$I_3\left(r, A_q\right) \sim (1-r)\int_{\beta_1}^{D} \frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-\left|\pi_q(u)\right|\right)}, \ r \to 1, \tag{25}$$

где $\pi_q(u)$ *из (15).*

Доказательство. Очевидно, что

$$I_3\left(r, A_q\right) = (1-r)\int_{\beta_1}^{D} \frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^{\gamma}\left(1-\left|\pi_q(u)\right|\right)}.$$

Далее доказательство проводится аналогично доказательству леммы 2.

Теперь вернемся к доказательству теоремы 3. Подставив (20), (24) и (25) в (19), придем к (16). Теорема 3 доказана.

Следствие 2. *В условиях теоремы 2 для равномерных приближений функций Маркова суммами Абеля – Пуассона рядов Фурье по системе полиномов Чебышева первого рода (13) при* $r \to 1$ *справедливы асимптотические равенства*

$$\varepsilon_r^{(0)} \sim \begin{cases} \dfrac{2^{1-\gamma}\pi(1-r)^{2\gamma}}{\sin 2\pi\gamma}, \ \gamma \in \left(0, \dfrac{1}{2}\right), \\ \sqrt{2}(1-r)\ln\dfrac{2}{1-r}, \ \gamma = \dfrac{1}{2}, \\ \dfrac{2^{\gamma}D^{2\gamma-1}(1-r)}{2\gamma-1}, \ \gamma > \dfrac{1}{2}. \end{cases} \tag{26}$$

Положим в формулировке теоремы 3 значение $q = 1$. Тогда $\varepsilon_{r,1}^{*}\left(A_1\right)$ – мажоранта равномерных приближений функций Маркова рациональными суммами Абеля – Пуассона с одним полюсом в открытой комплексной плоскости.

Следствие 3. *Справедливы асимптотические равенства*

$$\varepsilon_{r,1}^{*}\left(A_1\right) \sim \begin{cases} \dfrac{2^{1-\gamma}(1-r)^{2\gamma}\pi\beta^{2\gamma}}{\sin 2\pi\gamma} + \dfrac{2^{\gamma}(1-r)}{\beta}\displaystyle\int_{\beta}^{D}\frac{u^{2\gamma-1}(u+\beta)du}{(1+u)\left(1-u^2\right)^{\gamma}}, \ \gamma \in \left(0, \dfrac{1}{2}\right), \\ \sqrt{2}(1-r)\beta\ln\dfrac{2}{1-r} + \dfrac{\sqrt{2}(1-r)}{\beta}\displaystyle\int_{\beta}^{D}\frac{(u+\beta)du}{(1+u)\left(1-u^2\right)^{1/2}}, \ \gamma = \dfrac{1}{2}, \\ 2^{\gamma}\left[\displaystyle\int_{0}^{\beta}\frac{u^{2\gamma-2}(u+\beta)du}{(1+u)\left(1-u^2\right)^{\gamma}} + \dfrac{1}{\beta}\displaystyle\int_{\beta}^{D}\frac{u^{2\gamma-1}(u+\beta)du}{(1+u)\left(1-u^2\right)^{\gamma}}\right](1-r), \ \gamma > \dfrac{1}{2}. \end{cases}$$

Заметим, что параметр d в формулировке теоремы 3 может принимать и нулевое значение. В этом случае $\gamma \in (0, 1)$.

Наилучшая мажоранта равномерных приближений

Представляет интерес минимизировать правую часть асимптотического равенства (16) посредством выбора оптимального для этой задачи множества $A_q^{*} = \left(\alpha_1^{*}, \ldots, \alpha_q^{*}\right)$. Другими словами, будем искать оценку наилучшего равномерного приближения функций Маркова в условиях теоремы 2 суммами (2). Положим

$$\varepsilon_{r,q} = \inf_{A_q} \varepsilon_{r,q}\left(A_q\right), \ \varepsilon_{r,q}^{*} = \inf_{A_q} \varepsilon_{r,q}^{*}\left(A_q\right),$$

где $\varepsilon_{r,\,q}\left(A_q\right)$ – равномерные приближения функций Маркова суммами Абеля – Пуассона (2), определенные в (4). Отметим очевидное неравенство, следующее из (11):

$$\varepsilon_{r,\,q} \le \varepsilon^*_{r,\,q},\ \ r \in (0,\,1).$$

Теорема 4. *При* $r \to 1$ *справедливы асимптотические равенства*

$$\varepsilon^*_{r,\,q} \sim \begin{cases} \mu(q,\,\gamma)(1-r)^{1-\frac{(1-2\gamma)^q}{1+2\gamma}},\ \gamma \in \left(0,\,\frac{1}{2}\right), \\ 2\sqrt{2c\left(\frac{1}{2}\right)}(1-r)\sqrt{\ln_q \frac{2}{1-r}},\ \gamma = \frac{1}{2}, \\ 2^{\gamma+1}\inf\limits_{A_q} F_\gamma\left(A_q\right)(1-r),\ \gamma > \frac{1}{2}, \end{cases} \tag{27}$$

где

$$\mu(q,\,\gamma) = (1+2\gamma)\left[\frac{2^{(1-\gamma)\left(2(1-2\gamma)^{q-1}-(1+2\gamma)\right)}\left(c(\gamma)\right)^{2\gamma}}{(1-2\gamma)^{\frac{1-(1-2\gamma)^{q-1}}{2\gamma}}\gamma^{1+2\gamma-(1-2\gamma)^{q-1}}}\left(\frac{\pi}{\sin 2\pi\gamma}\right)^{(1-2\gamma)^{q-1}}\right]^{\frac{1}{1+2\gamma}},$$

$$c(\gamma) = \begin{cases} \int\limits_0^D \frac{u^{2\gamma}du}{(1+u)\left(1-u^2\right)^\gamma},\ \gamma > 0,\ d \in (0,\,1],\ D = \frac{1-d}{1+d}, \\ \int\limits_0^1 \frac{u^{2\gamma}du}{(1+u)\left(1-u^2\right)^\gamma},\ \gamma \in (0,\,1),\ d = 0, \end{cases} \tag{28}$$

$$\ln_q \frac{2}{1-r} = \underbrace{1+\ln\left(1+\ln\left(1+\ldots+\ln\ln\frac{2}{1-r}\right)\right)}_{q \text{ раз}}, \tag{29}$$

$$F_\gamma\left(A_q\right) = \int\limits_0^{\beta_q} \frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^\gamma\left(1-\pi_q(u)\right)} +$$
$$+\sum_{k=1}^{q-1}\int\limits_{\beta_{k+1}}^{\beta_k}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^\gamma\left(1-\pi_{q,\,k}(u)\right)} + \int\limits_{\beta_1}^{D}\frac{u^{2\gamma-1}du}{(1+u)\left(1-u^2\right)^\gamma\left(1-\left|\pi_q(u)\right|\right)}, \tag{30}$$

здесь $\pi_q(u)$ *из (15),* $\pi_{q,\,k}(u)$ *из (18).*

Доказательство. Исследуем асимптотические равенства (16). При фиксированных β_j, $j = 1, 2, \ldots, q$, порядок в указанном соотношении, очевидно, не отличается от полиномиального, полученного нами в (26).

Пусть $\gamma \in \left(0,\,\frac{1}{2}\right]$. В этом случае будем полагать, что $\beta_j = \beta_j(r) \to 0$, $r \to 1$, причем $\beta_{j+1} = o\left(\beta_j\right)$, $j = 1, 2, \ldots, q$, $r \to 1$. При этом из (17) находим, что

$$\Phi_r^{(\gamma)}\left(q,\,A_q\right) \sim 2^\gamma(1-r)\begin{cases} \frac{1}{1-2\gamma}\sum\limits_{k=1}^{q-1}\frac{\beta_k}{\beta_{k+1}^{1-2\gamma}} + \frac{c(\gamma)}{\beta_1},\ \gamma \in \left(0,\,\frac{1}{2}\right), \\ \sum\limits_{k=1}^{q-1}\beta_k\ln\frac{\beta_k}{\beta_{k+1}} + \frac{c\left(\frac{1}{2}\right)}{\beta_1},\ \gamma = \frac{1}{2}, \end{cases}$$

где $c(\gamma)$ определена в (27).

Тогда первые два асимптотических равенства из (16) при $r \to 1$ примут вид

$$\varepsilon_{r,\,q}^{*}\left(A_q\right) \sim \frac{2^{\gamma}(1-r)}{1-2\gamma}\left[\frac{2^{1-2\gamma}\pi(1-2\gamma)(1-r)^{2\gamma-1}\beta_q^{2\gamma}}{\sin 2\pi\gamma} + \sum_{k=1}^{q-1}\frac{\beta_k}{\beta_{k+1}^{1-2\gamma}} + \frac{(1-2\gamma)c(\gamma)}{\beta_1}\right],\ \gamma \in \left(0, \frac{1}{2}\right), \tag{31}$$

$$\varepsilon_{r,\,q}^{*}\left(A_q\right) \sim \sqrt{2}(1-r)\left[\ln\frac{2\beta_q}{1-r} + \sum_{k=1}^{q-1}\beta_k \ln\frac{\beta_k}{\beta_{k+1}} + \frac{c\left(\frac{1}{2}\right)}{\beta_1}\right],\ \gamma = \frac{1}{2}. \tag{32}$$

При каждом фиксированном $\gamma \in \left(0, \frac{1}{2}\right]$ правые части асимптотических равенств (31) и (32) представляют собой функции переменных $\beta_1, \ldots, \beta_q$, непрерывные в каждой точке q-мерного куба $[\delta, 1]^q$, $\delta = \delta(r) > 0$, следовательно, имеют строгий минимум при некотором $\beta^* = \left(\beta_1^*, \ldots, \beta_q^*\right) \in [\delta, 1]^q$. Если $\beta_k = 1$, $k = 1, \ldots, q$, то получим полиномиальный случай. Можно предположить, что β^* – внутренняя точка куба $[\delta, 1]^q$. Для того чтобы найти оптимальный набор β^* для соответствующего асимптотического равенства, решим экстремальную задачу

$$\varepsilon_{r,\,q}^{*}\left(A_q\right) \underset{A_q}{\to} \inf.$$

Рассмотрим каждый случай в отдельности. Так, исходя из асимптотического равенства (31), приходим к задаче

$$\Psi^{(\gamma)}\left(A_q\right) = c_q\beta_q^{2\gamma} + \frac{\beta_{q-1}}{\beta_q^{1-2\gamma}} + \frac{\beta_{q-2}}{\beta_{q-1}^{1-2\gamma}} + \ldots + \frac{\beta_2}{\beta_3^{1-2\gamma}} + \frac{\beta_1}{\beta_2^{1-2\gamma}} + \frac{c_1}{\beta_1} \underset{A_q}{\to} \inf,$$

где для краткости положено

$$c_q = \frac{2^{1-2\gamma}\pi(1-2\gamma)(1-r)^{2\gamma-1}}{\sin 2\pi\gamma},\ c_1 = (1-2\gamma)c(\gamma).$$

Функция $\Psi^{(\gamma)}\left(A_q\right)$ переменных $\beta_1, \beta_2, \ldots, \beta_q$ непрерывно дифференцируема в кубе $(0, 1)^q$. Естественно искать точку минимума этой функции там, где выполняется необходимое условие экстремума $\frac{\partial\Psi^{(\gamma)}\left(A_q\right)}{\partial\beta_j} = 0$, $j = 1, 2, \ldots, q$. Несложные вычисления приводят к системе уравнений

$$\begin{cases} 2\gamma c_q\beta_q^{2\gamma-1} - (1-2\gamma)\dfrac{\beta_{q-1}}{\beta_q^{2-2\gamma}} = 0, \\ \dfrac{1}{\beta_q^{1-2\gamma}} - (1-2\gamma)\dfrac{\beta_{q-2}}{\beta_{q-1}^{2-2\gamma}} = 0, \\ \dfrac{1}{\beta_{q-1}^{1-2\gamma}} - (1-2\gamma)\dfrac{\beta_{q-3}}{\beta_{q-2}^{2-2\gamma}} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \dfrac{1}{\beta_3^{1-2\gamma}} - (1-2\gamma)\dfrac{\beta_1}{\beta_2^{2-2\gamma}} = 0, \\ \dfrac{1}{\beta_2^{1-2\gamma}} - \dfrac{c_1}{\beta_1^2} = 0, \end{cases} \tag{33}$$

из которой последовательно находим

$$\frac{\beta_1}{\beta_2^{1-2\gamma}} = \frac{c_1}{\beta_1},\ \frac{\beta_k}{\beta_{k+1}^{1-2\gamma}} = (1-2\gamma)^{k-1}\frac{c_1}{\beta_1},\ k = 2, 3, \ldots, q-1.$$

С другой стороны, из первого уравнения системы (33) получаем

$$2\gamma c_q \beta_q^{2\gamma} = (1-2\gamma)\frac{\beta_{q-1}}{\beta_q^{1-2\gamma}} = (1-2\gamma)^{q-1}\frac{c_1}{\beta_1}.$$

Таким образом, с оптимальным набором параметров функция $\Psi^{(\gamma)}(A_q)$ имеет вид

$$\Psi^{(\gamma)}(A_q^*) = \frac{(1-2\gamma)^{q-1}}{2\gamma}\frac{c_1}{\beta_1^*} + (1-2\gamma)^{q-2}\frac{c_1}{\beta_1^*} + $$

$$+ (1-2\gamma)^{q-3}\frac{c_1}{\beta_1^*} + \ldots + \frac{c_1}{\beta_1^*} + \frac{c_1}{\beta_1^*} = \frac{1+2\gamma}{2\gamma}\frac{c_1}{\beta_1^*}. \quad (34)$$

Осталось найти параметр β_1^*. С этой целью снова обратимся к системе (33). Последовательно находим

$$\begin{cases} \dfrac{\beta_{q-1}}{\beta_q} = \dfrac{2\gamma c_q}{1-2\gamma}, \\ \dfrac{\beta_{q-2}}{\beta_{q-1}} = \dfrac{1}{1-2\gamma}\left(\dfrac{\beta_{q-1}}{\beta_q}\right)^{1-2\gamma} = \dfrac{1}{1-2\gamma}\left(\dfrac{2\gamma c_q}{1-2\gamma}\right)^{1-2\gamma}, \\ \dfrac{\beta_{q-3}}{\beta_{q-2}} = \dfrac{1}{1-2\gamma}\left(\dfrac{\beta_{q-2}}{\beta_{q-1}}\right)^{1-2\gamma} = \dfrac{(2\gamma c_q)^{(1-2\gamma)^2}}{(1-2\gamma)(1-2\gamma)^{1-2\gamma}(1-2\gamma)^{(1-2\gamma)^2}}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \dfrac{\beta_1}{\beta_2} = \dfrac{(2\gamma c_q)^{(1-2\gamma)^{(q-2)}}}{(1-2\gamma)^{\left[1+(1-2\gamma)+(1-2\gamma)^2+\ldots+(1-2\gamma)^{(q-2)}\right]}} = \dfrac{(2\gamma c_q)^{(1-2\gamma)^{(q-2)}}}{(1-2\gamma)^{\frac{1-(1-2\gamma)^{(q-1)}}{2\gamma}}}. \end{cases} \quad (35)$$

С другой стороны, из последнего уравнения в (33) имеем

$$\beta_2 = \frac{\beta_1^{\frac{2}{1-2\gamma}}}{c_1^{\frac{1}{1-2\gamma}}}.$$

Подставив полученное выражение для β_2 в последнее равенство системы (35), после необходимых преобразований будем иметь

$$\beta_1^* = c_1^{\frac{1}{1+2\gamma}}\left(\frac{(1-2\gamma)^{\frac{1-(1-2\gamma)^{(q-1)}}{2\gamma}}}{(2\gamma c_q)^{(1-2\gamma)^{(q-2)}}}\right)^{\frac{1-2\gamma}{1+2\gamma}}, \quad \gamma \in \left(0, \frac{1}{2}\right).$$

При найденном β_1^* в (34) получим

$$\Psi^{(\gamma)}(A_q^*) = \frac{1+2\gamma}{2\gamma} c_1^{\frac{2\gamma}{1+2\gamma}}\left(\frac{(2\gamma c_q)^{(1-2\gamma)^{(q-2)}}}{(1-2\gamma)^{\frac{1-(1-2\gamma)^{(q-1)}}{2\gamma}}}\right)^{\frac{1-2\gamma}{1+2\gamma}}, \quad \gamma \in \left(0, \frac{1}{2}\right).$$

Возвращаясь к первоначальным значениям параметров c_1 и c_q, из последнего соотношения и формулы (31) находим, что

$$\varepsilon_{r,q}^* \sim \mu(q,\gamma)(1-r)^{1-\frac{(1-2\gamma)^q}{1+2\gamma}}, \quad r \to 1, \quad (36)$$

где $\mu(q,\gamma)$ определена в формулировке теоремы 4.

Займемся теперь асимптотическим равенством (32). Здесь приходим к следующей задаче оптимизации:

$$\Psi^{(1/2)}\left(A_q\right) = \ln\frac{2\beta_q}{1-r} + \beta_{q-1}\ln\frac{\beta_{q-1}}{\beta_q} + \beta_{q-2}\ln\frac{\beta_{q-2}}{\beta_{q-1}} + \ldots + \beta_1\ln\frac{\beta_1}{\beta_2} + \frac{c\left(\frac{1}{2}\right)}{\beta_1} \underset{A_q}{\rightarrow} \inf, \tag{37}$$

где $c\left(\frac{1}{2}\right)$ определено в (28). Рассуждая аналогичным образом, заключаем, что оптимальный набор $\beta^* = \left(\beta_1^*, \beta_2^*, \ldots, \beta_q^*\right)$ является решением системы уравнений

$$\begin{cases} \ln\frac{2}{1-r} - \frac{\beta_{q-1}}{\beta_q} = 0, \\ \ln\frac{\beta_{q-1}}{\beta_q} + 1 - \frac{\beta_{q-2}}{\beta_{q-1}} = 0, \\ \ln\frac{\beta_{q-2}}{\beta_{q-1}} + 1 - \frac{\beta_{q-3}}{\beta_{q-2}} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ln\frac{\beta_2}{\beta_3} + 1 - \frac{\beta_1}{\beta_2} = 0, \\ \ln\frac{\beta_1}{\beta_2} + 1 - \frac{c\left(\frac{1}{2}\right)}{\beta_1^2} = 0. \end{cases} \tag{38}$$

Из последней системы находим, что с оптимальным набором параметров функция $\Psi^{(1/2)}\left(A_q^*\right)$ из (37) имеет вид

$$\Psi^{(1/2)}\left(A_q^*\right) = \ln\frac{2\beta_q^*}{1-r} + \beta_{q-1}^*\left(\frac{\beta_{q-2}^*}{\beta_{q-1}^*} - 1\right) + \beta_{q-2}^*\left(\frac{\beta_{q-3}^*}{\beta_{q-2}^*} - 1\right) + \ldots$$

$$\ldots + \beta_2^*\left(\frac{\beta_1^*}{\beta_2^*} - 1\right) + \beta_1^*\left(\frac{c\left(\frac{1}{2}\right)}{\beta_1^{*2}} - 1\right) + \frac{c\left(\frac{1}{2}\right)}{\beta_1^*} = \frac{2c\left(\frac{1}{2}\right)}{\beta_1^*}. \tag{39}$$

Осталось найти значение параметра β_1^*. С этой целью снова обратимся к системе (38). Последовательно получим

$$\begin{cases} \frac{\beta_{q-1}}{\beta_q} = \ln\frac{2}{1-r}, \\ \frac{\beta_{q-2}}{\beta_{q-1}} = 1 + \ln\ln\frac{2}{1-r}, \\ \frac{\beta_{q-3}}{\beta_{q-2}} = 1 + \ln\left(1 + \ln\ln\frac{2}{1-r}\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \frac{\beta_1}{\beta_2} = \underbrace{1 + \ln\left(1 + \ln\left(1 + \ldots + \ln\ln\frac{2}{1-r}\right)\right)}_{q-1\ \text{раз}}, \\ \frac{c\left(\frac{1}{2}\right)}{\beta_1^2} = \underbrace{1 + \ln\left(1 + \ln\left(1 + \ldots + \ln\ln\frac{2}{1-r}\right)\right)}_{q\ \text{раз}}. \end{cases}$$

Из последнего равенства системы имеем

$$\beta_1^* = \frac{\sqrt{c\left(\frac{1}{2}\right)}}{\sqrt{\ln_q \frac{2}{1-r}}},$$

где выражение $\ln_q \dfrac{2}{1-r}$ определено в (29). Для оптимального β_1^* из (39) находим

$$\Psi^{(1/2)}\left(A_q^*\right) = 2\sqrt{c\left(\frac{1}{2}\right)}\sqrt{\ln_q \frac{2}{1-r}}.$$

Подставив последнее соотношение в (32), будем иметь

$$\varepsilon_{r,\,q}^* \sim 2\sqrt{2c\left(\frac{1}{2}\right)}(1-r)\sqrt{\ln_q \frac{2}{1-r}},\ \gamma = \frac{1}{2},\ r \to 1. \tag{40}$$

Пусть $\gamma > \dfrac{1}{2}$. В этом случае из (16) и (17) находим

$$\varepsilon_{r,\,q}^*\left(A_q\right) \sim 2^{\gamma+1} F_\gamma\left(A_q\right)(1-r),\ r \to 1,$$

где $F_\gamma\left(A_q\right)$ определена в (30). На основании этого представления заключаем, что в данном случае оптимальный набор параметров $\beta^* = \left(\beta_1^*,\ \beta_2^*,\ \ldots,\ \beta_q^*\right)$ не зависит от r и не влияет на скорость убывания мажоранты. Следовательно,

$$\varepsilon_{n,\,q}^* \sim 2^{\gamma+1} \inf_{A_q} F_\gamma\left(A_q\right)(1-r),\ \gamma > \frac{1}{2},\ r \to 1. \tag{41}$$

Из асимптотических равенств (36), (40) и (41) приходим к (27). Теорема 4 доказана.

Следствие 4. *Пусть $q = 1$. Тогда в условиях теоремы 2 для наилучшей мажоранты равномерных приближений при $r \to 1$ справедливо асимптотическое равенство*

$$\varepsilon_{n,1}^* \sim \begin{cases} (1+2\gamma)\left[\dfrac{2^{(1-\gamma)(1-2\gamma)}\left[c(\gamma)\right]^{2\gamma}\pi}{(1-2\gamma)^{\frac{1}{2\gamma}}\sin 2\pi\gamma}\right]^{\frac{1}{1+2\gamma}}(1-r)^{\frac{4\gamma}{1+2\gamma}},\ \gamma \in \left(0,\ \dfrac{1}{2}\right), \\ 2\sqrt{2c\left(\dfrac{1}{2}\right)}(1-r)\sqrt{\ln \dfrac{2}{1-r}},\ \gamma = \dfrac{1}{2}, \\ 2^\gamma \inf\limits_{\beta \in (0,1]}\left[\displaystyle\int_0^\beta \frac{u^{2\gamma-2}(\beta+u)\,du}{(1+u)\left(1-u^2\right)^\gamma} + \frac{1}{\beta}\int_\beta^D \frac{u^{2\gamma-1}\,du}{(1+u)\left(1-u^2\right)^\gamma}\right](1-r),\ \gamma > \dfrac{1}{2}, \end{cases}$$

где $c(\gamma)$ определена в формулировке теоремы 4.

Аппроксимация некоторых элементарных функций

Известно (см., например, [11]), что многие элементарные функции можно представить в виде комбинаций функций Маркова. Рассмотрим функцию $f(z) = (z-1)^\gamma,\ \gamma \in (0,\ +\infty)\backslash\mathbb{N}$. Она является голоморфной в области $\mathbb{C}\backslash(1,\ +\infty)$. Стандартное применение интегральной формулы Коши приводит к соотношению

$$(w-1)^\gamma = \frac{1}{2\pi i}\int_{\partial\Omega} \frac{(z-1)^\gamma}{z-w}dz,\ w \in \Omega,$$

где Ω – круг радиусом $a > 1$ с центром в начале координат и разрезом по отрезку $[1,\ a]$. Из последней формулы легко получить (см., например, [12]), что при $|w| < a,\ w \,\overline{\in}\, (1,\ a)$, справедливо равенство

$$(1-x)^\gamma = \hat{\mu}_1(x) + g(x),\ x \in [0,\ 1], \tag{42}$$

где

$$\hat{\mu}_1(x) = -\frac{\sin\pi\gamma}{\pi}\int_1^a \frac{(t-1)^\gamma}{t-x}dt,\ g(x) = \frac{1}{2\pi i}\int_{|z|=a}\frac{(1-z)^\gamma}{z-x}dz.$$

Функция $\hat{\mu}_1(x),\ x\in[0,1]$, удовлетворяет условию теоремы 4. Следовательно,

$$\varepsilon^*_{r,q}\left(\hat{\mu}_1(x)\right) \sim \frac{\sin\pi\gamma}{\pi}\begin{cases}\mu(q,\gamma)(1-r)^{1-\frac{(1-2\gamma)^q}{1+2\gamma}},\ \gamma\in\left(0,\frac{1}{2}\right),\\ 2\sqrt{\pi-2}(1-r)\sqrt{\ln_q\frac{2}{1-r}},\ \gamma=\frac{1}{2},\\ 2^{\gamma+1}\inf\limits_{A_q}F_\gamma\left(A_q\right)(1-r),\ \gamma\in\left(\frac{1}{2},1\right),\end{cases}$$

где $\mu(q,\gamma)$ определена в теореме 4; $F_\gamma\left(A_q\right)$ из (30). Исследуем приближения функции $g(x)$ суммами Абеля – Пуассона (2). В обозначениях (3) имеем

$$\varepsilon_{r,q}\left(g,x,A_q\right) = (1-r)\sum_{k=0}^{+\infty} r^k\delta_{k,q}\left(g,x,A_q\right),\ x\in[-1,1], \tag{43}$$

где

$$\delta_{k,q}\left(g,x,A_q\right) = g(x) - s_n(g,x) = \frac{1}{(2\pi)^2 i}\int_{|z|=a}\frac{(1-z)^\gamma}{z-x}I_k(x,z)dz \tag{44}$$

– приближения функции $g(x)$ интегральным рациональным оператором Фурье – Чебышева (1) с набором параметров A_q,

$$I_k(x,z) = \int_{-\pi}^{\pi}\frac{\cos u-\cos v}{z-\cos v}\left(\zeta\frac{\omega_q^k(\zeta)}{\omega_q^k(\xi)} - \xi\frac{\omega_q^k(\xi)}{\omega_q^k(\zeta)}\right)\frac{dv}{\zeta-\xi},\ \zeta = \mathrm{e}^{iv},\ \xi = \mathrm{e}^{iu},\ x = \cos u,$$

$\omega_q(\xi)$ определена в (8). Выполнив в интеграле $I_k(x,z)$ замену переменных по формулам $\zeta = \mathrm{e}^{iv}$, $\xi = \mathrm{e}^{iu}$, получим

$$I_k(x,z) = -\frac{1}{i\xi}\left(\overline{\omega_q^k(\xi)}J_1 - \xi\omega_q^k(\xi)J_2\right),\ \xi = \mathrm{e}^{iu},\ x = \cos u, \tag{45}$$

где

$$J_1 = \int_{|\zeta|=1}\frac{1-\xi\zeta}{(\zeta-a_1)(\zeta-a_2)}\omega_q^k(\zeta)d\zeta,\ J_2 = \int_{|\zeta|=1}\frac{1-\xi\zeta}{(\zeta-a_1)(\zeta-a_2)}\frac{d\zeta}{\zeta\omega_q^k(\zeta)},$$

$$a_1 = z-\sqrt{z^2-1},\ a_2 = z+\sqrt{z^2-1},\ |z| = a > 1.$$

Величины a_1 и a_2 представляют собой функции переменного z, обратные к функции Жуковского, причем $|a_1|<1,\ |a_2|>1$. Следовательно, подынтегральная функция интеграла J_1 внутри единичного круга имеет в точке $\zeta = a_1$ простой полюс. Применяя теорему Коши о вычетах, находим, что

$$J_1 = 2\pi i\frac{1-\xi a_1}{a_1-a_2}\omega_q^k(a_1). \tag{46}$$

Подынтегральная функция интеграла J_2 во внешности единичного круга имеет в точке $\zeta = a_2$ простой полюс, а на бесконечности – нуль не ниже второго порядка. Применяя теорему Коши о вычетах, получаем

$$J_2 = -2\pi i\frac{1-\xi a_2}{(a_2-a_1)a_2\omega_q^k(a_2)} = 2\pi i\frac{a_1-\xi}{a_1-a_2}\omega_q^k(a_1). \tag{47}$$

Подставив (46) и (47) в (45), будем иметь

$$I_k(x,z) = \frac{2\pi}{\sqrt{z^2-1}}\left(\overline{\omega_q^k(\xi)}\left(\bar{\xi}-a_1\right) + \omega_q^k(\xi)(\xi-a_1)\right)\omega_q^k(a_1),\ \xi = \mathrm{e}^{iu},\ x = \cos u.$$

Из (44) при этом находим

$$\delta_{k,q}\left(g,\ x,\ A_q\right)=\frac{1}{2\pi i}\int\limits_{|z|=a}\frac{(1-z)^{\gamma}\left(\overline{\omega_q^k(\xi)}\left(\overline{\xi}-a_1\right)+\omega_q^k(\xi)(\xi-a_1)\right)}{(z-x)\sqrt{z^2-1}}\omega_q^k(a_1)\,dz,\ \ \xi=\mathrm{e}^{iu},\ \ x=\cos u.$$

Оценим полученное выражение. Выполнив в интеграле справа замену переменного по формуле $z=a\mathrm{e}^{i\theta}$, будем иметь

$$\left|\delta_{k,q}\left(g,\ x,\ A_q\right)\right|=\frac{a}{2\pi}\left|\int\limits_0^{2\pi}\frac{\left(1-a\mathrm{e}^{i\theta}\right)^{\gamma}\left(\overline{\omega_q^k(\xi)}\left(\overline{\xi}-b_1\right)+\omega_q^k(\xi)(\xi-b_1)\right)}{\left(a\mathrm{e}^{i\theta}-x\right)\sqrt{a^2\mathrm{e}^{2i\theta}-1}}\omega_q^k(a_1)\,i\mathrm{e}^{i\theta}d\theta\right|\le$$

$$\le\frac{a}{2\pi}\int\limits_0^{2\pi}\frac{\left|1-a\mathrm{e}^{i\theta}\right|^{\gamma}\left(\left|\overline{\xi}-b_1\right|+\left|\xi-b_1\right|\right)}{\left|a\mathrm{e}^{i\theta}-x\right|\sqrt{\left|a^2\mathrm{e}^{2i\theta}-1\right|}}\left|\omega_q(b_1)\right|^k d\theta,$$

где $b_1=a\mathrm{e}^{i\theta}-\sqrt{a^2\mathrm{e}^{2i\theta}-1}$, $|b_1|<1$, $\xi=\mathrm{e}^{iu}$, $x=\cos u$. Заметив, что $\left|\omega_q(b_1)\right|\le\lambda<1$, получим

$$\left|\delta_{k,q}\left(g,\ x,\ A_q\right)\right|\le\frac{a}{2\pi}\lambda^k\int\limits_0^{2\pi}\Phi(\theta,\ x,\ a)\,d\theta, \tag{48}$$

где

$$\Phi(\theta,\ x,\ a)=$$

$$=\frac{\left(1-2a\cos\theta+a^2\right)^{\gamma/2}\left(\sqrt{1-2a\cos(u-\theta)+a^2}+\sqrt{1-2a\cos(u+\theta)+a^2}+2\left(1-2a^2\cos2\theta+a^4\right)^{1/4}\right)}{\sqrt{a^2-2ax\cos\theta+x^2}\left(1-2a^2\cos2\theta+a^4\right)^{1/4}}.$$

Поскольку равномерно по $x\in[0,\ 1]$ и $\theta\in[0,\ 2\pi]$

$$\Phi(\theta,\ x,\ a)\le\frac{2(1+a)^{\gamma}\left(1+a+\sqrt{1+a^2}\right)}{(a-x)\sqrt{a^2-1}},\ \ a>1,$$

то из (48) находим, что

$$\left|\delta_{k,q}\left(g,\ x,\ A_q\right)\right|\le\frac{2a(1+a)^{\gamma}\left(1+a+\sqrt{1+a^2}\right)}{(a-x)\sqrt{a^2-1}}\lambda^k,\ \ k=0,\ 1,\ 2,\ \ldots.$$

Из последней оценки и формулы (43) получим

$$\left|\varepsilon_{r,q}\left(g,\ x,\ A_q\right)\right|\le(1-r)\sum_{k=0}^{+\infty}r^k\left|\delta_{k,q}\left(g,\ x,\ A_q\right)\right|=$$

$$=(1-r)\frac{2a(1+a)^{\gamma}\left(1+a+\sqrt{1+a^2}\right)}{(a-1)\sqrt{a^2-1}}\sum_{k=0}^{+\infty}r^k\lambda^k=$$

$$=(1-r)\frac{2a(1+a)^{\gamma}\left(1+a+\sqrt{1+a^2}\right)}{(a-1)\sqrt{a^2-1}(1-r\lambda)}\le(1-r)\frac{2a(1+a)^{\gamma}\left(1+a+\sqrt{1+a^2}\right)}{(a-1)\sqrt{a^2-1}(1-\lambda)},\ \lambda<1,\ a>1.$$

Другими словами, для любого набора параметров A_q равномерно по $r\in(0,\ 1)$ справедлива оценка $\left\|\varepsilon_{r,q}\left(g,\ x,\ A_q\right)\right\|_{C[-1,1]}=O(1-r)$. Из представления (42) и последних рассуждений мы получаем нижеприведенное следствие.

Следствие 5 (аппроксимация функции $(1-x)^{\gamma}$, $\gamma\in(0,\ 1)$). *Для любого натурального q справедливо соотношение*

$$\varepsilon^{*}_{r,\,q}\left((1-x)^{\gamma},\ [0,1]\right)=\begin{cases}\dfrac{\sin\pi\gamma}{\pi}\mu(q,\gamma)(1-r)^{1-\frac{(1-2\gamma)^{q}}{1+2\gamma}}+O(1-r),\ \gamma\in\left(0,\ \dfrac{1}{2}\right),\\ \dfrac{2\sqrt{\pi-2}}{\pi}(1-r)\sqrt{\ln_{q}\dfrac{2}{1-r}}+O(1-r),\ \gamma=\dfrac{1}{2},\\ O(1-r),\ \gamma\in\left(\dfrac{1}{2},1\right).\end{cases}\tag{49}$$

Следствие 6. *Для наилучших равномерных приближений функции* $(1-x)^{\gamma},\ \gamma\in(0,1)$, *на отрезке* $[0,1]$ *суммами Абеля – Пуассона полиномиальных рядов Фурье – Чебышева при* $r\to1$ *справедливо асимптотическое равенство*

$$\varepsilon^{(0)}_{r}\left((1-x)^{\gamma},\ [0,1]\right)=\begin{cases}\dfrac{(1-r)^{2\gamma}}{2^{\gamma}\cos\pi\gamma}+O(1-r),\ \gamma\in\left(0,\ \dfrac{1}{2}\right),\\ \dfrac{\sqrt{2}}{\pi}(1-r)\ln\dfrac{2}{1-r}+O(1-r),\ \gamma=\dfrac{1}{2},\\ O(1-r),\ \gamma\in\left(\dfrac{1}{2},1\right).\end{cases}$$

Доказательство. Оно следует непосредственно из (26) и предыдущих рассуждений. Обратим внимание, что в полиномиальном случае имеем асимптотическую оценку равномерных приближений.

Известно [26, c. 96], что для наилучших равномерных полиномиальных приближений справедливо равенство

$$E_{2n}\left(|x|^{2\gamma},\ [-1,1]\right)=\frac{1}{2^{\gamma}}E_{n}\left((1-x)^{\gamma},\ [0,1]\right).$$

Используя аналогичные рассуждения, после соответствующих преобразований из (49) находим, что

$$\varepsilon^{*}_{r,\,2q}\left(|x|^{s},\ [-1,1]\right)=\begin{cases}\dfrac{1}{\pi}\sin\dfrac{\pi s}{2}\mu_{1}(q,s)(1-r)^{1-\frac{(1-s)^{q}}{1+s}}+O(1-r),\ s\in(0,1),\\ \dfrac{2\sqrt{\pi-2}}{\pi}(1-r)\sqrt{\ln_{q}\dfrac{2}{1-r}}+O(1-r),\ s=1,\\ O(1-r),\ s\in(1,\ 2),\ r\to1,\end{cases}$$

где

$$\mu_{1}(q,s)=\frac{2^{\frac{s}{2}}(1+s)}{s}\left[\frac{2^{(1-s)^{q}}s^{(1-s)^{q-1}}\left[c\left(\frac{s}{2}\right)\right]^{s}}{(1-s)^{\frac{1-(1-s)^{q-1}}{s}}}\left(\frac{\pi}{\sin\pi s}\right)^{(1-s)^{q-1}}\right]^{\frac{1}{1+s}},\ s\in(0,1).$$

Заключение

В работе изучены аппроксимации функций Маркова суммами Абеля – Пуассона интегральных операторов Фурье – Чебышева, ассоциированных с системой рациональных функций Чебышева – Маркова, при фиксированном числе геометрически различных полюсов у аппроксимирующей функции. Найдены интегральное представление приближений и оценка равномерных приближений. В случае, когда мера μ удовлетворяет условиям $d\mu(t)=\varphi(t)dt$ и $\varphi(t)\asymp(t-1)^{\gamma},\ \gamma>0$, получены оценки поточечных и равномерных приближений, асимптотическое выражение мажоранты равномерных приближений, оптимальные значения параметров, при которых мажоранта имеет наибольшую скорость убывания. Отмечено, что при $\gamma\in\left(0,\ \frac{1}{2}\right]$ порядок стремления к нулю равномерных приближений функций Маркова рациональными суммами Абеля – Пуассона даже с одним полюсом в открытой комплексной плоскости выше в сравнении с полиномиальным случаем. При $\gamma > \frac{1}{2}$ скорость убывания мажоранты имеет тот же порядок малости, что и в полиномиальном случае.

На основании проведенных исследований можно заключить, что суммы Абеля – Пуассона рациональных интегральных операторов типа Фурье – Чебышева отражают особенности рациональной аппроксимации функций Маркова в условиях теоремы 2.

Следствием полученных результатов являются асимптотические оценки равномерных приближений некоторых элементарных функций со степенной особенностью.

Библиографические ссылки

1. Натансон ИП. О порядке приближения непрерывной 2π-периодической функции при помощи ее интеграла Пуассона. *Доклады Академии наук СССР.* 1950;72(1):11–14.
2. Тиман АФ. Точная оценка остатка при приближении периодических дифференцируемых функций интегралами Пуассона. *Доклады Академии наук СССР.* 1950;74(1):17–20.
3. Штарк ЭЛ. Полное асимптотическое разложение для верхней грани уклонения функций из Lip1 от сингулярного интеграла Абеля – Пуассона. *Математические заметки.* 1973;13(1):21–28.
4. Жук ВВ. О порядке приближения непрерывной 2π-периодической функции при помощи средних Фейера и Пуассона ее ряда Фурье. *Математические заметки.* 1968;4(1):21–32.
5. Русецкий ЮИ. О приближении непрерывных на отрезке функций суммами Абеля – Пуассона. *Сибирский математический журнал.* 1968;9(1):136–144.
6. Жигалло ТВ. Приближение функций, удовлетворяющих условию Липшица на конечном отрезке вещественной оси, интегралами Пуассона – Чебышева. *Проблемы управления и информатики.* 2018;3:46–58.
7. Джрбашян ММ. К теории рядов Фурье по рациональным функциям. *Известия Академии наук Армянской ССР. Серия: Математика.* 1956;9(7):3–28.
8. Китбалян АА. Разложения по обобщенным тригонометрическим системам. *Известия Академии наук Армянской ССР. Серия: Математика.* 1963;16(6):3–24.
9. Марков АА. Два доказательства сходимости некоторых непрерывных дробей. В: *Избранные труды по теории непрерывных дробей и теории функций, наименее уклоняющихся от нуля.* Москва: Государственное издательство технико-теоретической литературы; 1948. с. 106–119.
10. Гончар АА. О скорости рациональной аппроксимации некоторых аналитических функций. *Математический сборник.* 1978;105(2):147–163.
11. Ganelius T. Ortogonal polynomials and rational approximation of holomorphic function. In: Erdős P, Alpár L, Halász G, Sárközy A, editors. *Studies in pure mathematics. To the memory of Paul Turán.* Basel: Birkhäuser; 1978. p. 237–243.
12. Andersson J-E. Best rational approximation to Markov functions. *Journal of Approximation Theory*. 1994;76(2):219–232. DOI: 10.1006/jath.1994.1015.
13. Пекарский АА. Наилучшие равномерные рациональные приближения функций Маркова. *Алгебра и анализ.* 1995;7(2): 121–132.
14. Vyacheslavov NS, Mochalina EP. Rational approximations of functions of Markov – Stieltjes type in Hardy spaces H_p, $0 < p \leq \infty$. *Moscow University Mathematics Bulletin*. 2008;63(4):125–134. DOI: 10.3103/S0027132208040013.
15. Старовойтов АП, Лабыч ЮА. Рациональная аппроксимация функций Маркова, порожденных борелевскими мерами степенного типа. *Проблемы физики, математики и техники.* 2009;1:69–73.
16. Пекарский АА, Ровба ЕА. Равномерные приближения функций Стилтьеса посредством ортопроекции на множество рациональных функций. *Математические заметки.* 1999;65(3):362–368.
17. Takenaka S. On the orthogonal functions and a new formula of interpolations. *Japanese Journal of Mathematics: Transactions and Abstracts.* 1925;2:129–145. DOI: 10.4099/jjm1924.2.0_129.
18. Malmquist F. Sur la determination d'une classe functions analytiques par leurs dans un ensemble donne de points. In: *Comptes rendus du Sixtiéme Congrés des mathématiciens scandinaves*. Copenhagen: [s. n.]; 1926. p. 253–259.
19. Джрбашян ММ, Китбалян АА. Об одном обобщении полиномов Чебышева. *Доклады Академии наук Армянской ССР.* 1964;38(5):263–270.
20. Ровба ЕА, Микулич ЕГ. Константы в рациональной аппроксимации функций Маркова – Стилтьеса с фиксированным числом полюсов. *Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 2. Матэматыка. Фізіка. Інфарматыка, вылічальная тэхніка і кіраванне.* 2013;1:12–20.
21. Лунгу КН. О наилучших приближениях рациональными функциями с фиксированным числом полюсов. *Математический сборник.* 1971;86(2):314–324.
22. Лунгу КН. О наилучших приближениях рациональными функциями с фиксированным числом полюсов. *Сибирский математический журнал.* 1984;25(2):151–160.
23. Ровба ЕА. Об одном прямом методе в рациональной аппроксимации. *Доклады Академии наук БССР.* 1979;23(11):968–971.
24. Фихтенгольц ГМ. *Курс дифференциального и интегрального исчисления. Том 2.* Москва: Физматлит; 2003. 864 с.
25. Поцейко ПГ, Ровба ЕА, Смотрицкий КА. Об одном рациональном интегральном операторе типа Фурье – Чебышева и аппроксимации функций Маркова. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;2:6–27.
26. Бернштейн СН. *Экстремальные свойства полиномов и наилучшее приближение непрерывных функций одной вещественной переменной. Часть 1.* Москва: Главная редакция общетехнической литературы; 1937. 200 с. (Математика в монографиях).

References

1. Natanson IP. [On the order of approximation of a continuous 2π-periodic function using its Poisson integral]. *Doklady Akademii nauk SSSR.* 1950;72(1):11–14. Russian.

2. Timan AF. [Exact estimation of the remainder in the approximation of periodic differentiable functions by Poisson integrals]. *Doklady Akademii nauk SSSR.* 1950;74(1):17–20. Russian.

3. Stark EL. [Complete asymptotic decomposition for the upper face of the deviation of functions from Lip1 from the singular Abel – Poisson integral]. *Matematicheskie zametki.* 1973;13(1):21–28. Russian.

4. Zhuk VV. [On the order of approximation of a continuous 2π-periodic function using Feyer and Poisson averages of its Fourier series]. *Matematicheskie zametki.* 1968;4(1):21–32. Russian.

5. Rusetsky YuI. [On the approximation of continuous functions on a segment by Abel – Poisson means]. *Sibirskii matematicheskii zhurnal.* 1968;9(1):136–144. Russian.

6. Zhyhallo TV. Approximation of functions satisfying the Lipschitz condition on a finite segment of the real axis by Poisson – Chebyshev's integrals. *Problemy upravleniya i informatiki.* 2018;3:46–58. Russian.

7. Dzhrbashyan MM. [On the theory of Fourier series in terms of rational functions]. *Izvestiya Akademii nauk Armyanskoi SSR. Seriya: Matematika.* 1956;9(7):3–28. Russian.

8. Kitbalyan AA. [Decompositions by generalised trigonometric systems]. *Izvestiya Akademii nauk Armyanskoi SSR. Seriya: Matematika.* 1963;16(6):3–24. Russian.

9. Markov AA. [Two proofs of convergence of some continuous fractions]. In: *Izbrannye trudy po teorii nepreryvnykh drobei i teorii funktsii, naimenee uklonyayushchikhsya ot nulya* [Selected works on the theory of continuous fractions and the theory of functions least deviating from zero]. Moscow: Gosudarstvennoe izdatel'stvo tekhniko-teoreticheskoi literatury; 1948. p. 106–119. Russian.

10. Gonchar AA. [On the speed of rational approximation of some analytical functions]. *Matematicheskii sbornik.* 1978;105(2):147–163. Russian.

11. Ganelius T. Ortogonal polynomials and rational approximation of holomorphic function. In: Erdős P, Alpár L, Halász G, Sárközy A, editors. *Studies in pure mathematics. To the memory of Paul Turán.* Basel: Birkhäuser; 1978. p. 237–243.

12. Andersson J-E. Best rational approximation to Markov functions. *Journal of Approximation Theory.* 1994;76(2):219–232. DOI: 10.1006/jath.1994.1015.

13. Pekarskii AA. [Best uniform rational approximations to Markov functions]. *Algebra i analiz.* 1995;7(2):121–132. Russian.

14. Vyacheslavov NS, Mochalina EP. Rational approximations of functions of Markov – Stieltjes type in Hardy spaces H_p, $0 < p \leq \infty$. *Moscow University Mathematics Bulletin*. 2008;63(4):125–134. DOI: 10.3103/S0027132208040013.

15. Starovoitov AP, Labych YuA. [Rational approximation of Markov functions generated by Borel measures of power type]. *Problemy fiziki, matematiki i tekhniki.* 2009;1:69–73. Russian.

16. Pekarskii AA, Rouba EA. [Uniform approximations of Stieltjes functions by orthogonal projection on the set of rational functions]. *Matematicheskie zametki.* 1999;65(3):362–368. Russian.

17. Takenaka S. On the orthogonal functions and a new formula of interpolations. *Japanese Journal of Mathematics: Transactions and Abstracts.* 1925;2:129–145. DOI: 10.4099/jjm1924.2.0_129.

18. Malmquist F. Sur la determination d'une classe functions analytiques par leurs dans un ensemble donne de points. In: *Comptes rendus du Sixtiéme Congrés des mathématiciens scandinaves.* Copenhagen: [s. n.]; 1926. p. 253–259.

19. Dzhrbashyan MM, Kitbalyan AA. [On a generalisation of Chebyshev polynomials]. *Doklady Akademii nauk Armyanskoi SSR.* 1964;38(5):263–270. Russian.

20. Rovba EA, Mikulich EG. Constants in rational approximation of Markov – Stieltjes functions with fixed number of poles. *Vesnik of Yanka Kupala State University of Grodno. Series 2. Mathematics. Physics. Informatics, Computer Technology and its Control.* 2013;1:12–20.

21. Lungu KN. [On best approximations by rational functions with a fixed number of poles]. *Matematicheskii sbornik.* 1971;86(2):314–324. Russian.

22. Lungu KN. [On the best approximations by rational functions with a fixed number of poles]. *Sibirskii matematicheskii zhurnal.* 1984;25(2):151–160. Russian.

23. Rouba YA. [On a direct method in a rational approximation]. *Doklady Akademii nauk BSSR.* 1979;23(11):968–971. Russian.

24. Fichtenholz GM. *Kurs differentsial'nogo i integral'nogo ischisleniya. Tom 2* [Course of differential and integral calculus. Volume 2]. Moscow: Fizmatlit; 2003. 864 p. Russian.

25. Patseika PG, Rouba YA, Smatrytski KA. On one rational integral operator of Fourier – Chebyshev type and approximation of Markov functions. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;2:6–27.

26. Bernshtein SN. *Ekstremal'nye svoistva polinomov i nailuchshee priblizhenie nepreryvnykh funktsii odnoi veshchestvennoi peremennoi. Chast' 1* [Extremal properties of polynomials and the best approximation of continuous functions of one real variable. Part 1]. Moscow: Glavnaya redaktsiya obshchetekhnicheskoi literatury; 1937. 200 p. (Matematika v monografiyakh). Russian.

Получена 05.10.2021 / исправлена 08.10.2021 / принята 12.10.2021.
Received 05.10.2021 / revised 08.10.2021 / accepted 12.10.2021.

Математическая логика, алгебра и теория чисел

Mathematical logic, algebra and number theory

УДК 512.542

КОНЕЧНЫЕ ГРУППЫ С ЗАДАННЫМИ СИСТЕМАМИ ОБОБЩЕННЫХ σ-ПЕРЕСТАНОВОЧНЫХ ПОДГРУПП

В. С. ЗАКРЕВСКАЯ[1)]

[1)]*Гомельский государственный университет им. Франциска Скорины, ул. Советская, 104, 246019, г. Гомель, Беларусь*

Пусть $\sigma = \{\sigma_i | i \in I\}$ – разбиение множества всех простых чисел $\mathbb{P}$, а G – конечная группа. Множество $\mathcal{H}$ подгрупп группы G называется *полным холловым* σ-*множеством* группы G, если каждый член $\neq 1$ из $\mathcal{H}$ является холловой σ_i-подгруппой группы G для некоторого $i \in I$ и $\mathcal{H}$ содержит ровно одну холлову σ_i-подгруппу группы G для всех i таких, что $\sigma_i \cap \pi(G) \neq \varnothing$. Группа считается σ-*примарной*, если она есть конечная σ_i-группа для некоторого i. Подгруппа A группы G называется σ-*перестановочной* в G, если G содержит полное холлово σ-множество $\mathcal{H}$ такое, что $AH^x = H^xA$ для любого $H \in \mathcal{H}$ и любого $x \in G$; σ-*субнормальной* в G, если существует подгруппа цепи $A = A_0 \leq A_1 \leq \ldots \leq A_t = G$ такая, что либо $A_{i-1} \trianglelefteq A_i$, либо $A_i/\left(A_i - 1\right)_{A_i}$ является σ-примарной для всех $i = 1, \ldots, t$; $\mathfrak{U}$-*нормальной* в G, если каждый главный фактор группы G между A_G и A^G циклический. Мы говорим, что подгруппа H группы G является: (i) *частично* σ-*перестановочной* в G, если существуют $\mathfrak{U}$-нормальная подгруппа A и σ-перестановочная подгруппа B из G такие, что $H = <A, B>$; (ii) $(\mathfrak{U}, \sigma)$-*вложенной* в G, если существуют частично σ-перестановочная подгруппа S и σ-субнормальная подгруппа T из G такие, что $G = HT$

Образец цитирования:
Закревская ВС. Конечные группы с заданными системами обобщенных σ-перестановочных подгрупп. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:25–33 (на англ.).
https://doi.org/10.33581/2520-6508-2021-3-25-33

For citation:
Zakrevskaya VS. Finite groups with given systems of generalised σ-permutable subgroups. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:25–33.
https://doi.org/10.33581/2520-6508-2021-3-25-33

Автор:
Виктория Сергеевна Закревская – аспирантка кафедры алгебры и геометрии факультета математики и технологий программирования. Научный руководитель – доктор физико-математических наук А. Н. Скиба.

Author:
Viktoria S. Zakrevskaya, postgraduate student at the department of algebra and geometry, faculty of mathematics and technologies of programming.
tory.zakreuskaya@gmail.com

и $H \cap T \leq S \leq H$. Мы изучаем G, предполагая, что некоторые подгруппы группы G являются частично σ-перестановочными или $(\mathfrak{U}, \sigma)$-вложенными в G. Некоторые известные результаты обобщены.

Ключевые слова: конечная группа; σ-разрешимые группы; σ-нильпотентная группа; частично σ-перестановочная подгруппа; $(\mathfrak{U}, \sigma)$-вложенная подгруппа; $\mathfrak{U}$-нормальная подгруппа.

FINITE GROUPS WITH GIVEN SYSTEMS OF GENERALISED σ-PERMUTABLE SUBGROUPS

V. S. ZAKREVSKAYA[a]

[a]*Francisk Skorina Gomel State University, 104 Savieckaja Street, Homieĺ 246019, Belarus*

Let $\sigma = \{\sigma_i | i \in I\}$ be a partition of the set of all primes $\mathbb{P}$ and G be a finite group. A set $\mathcal{H}$ of subgroups of G is said to be a *complete Hall* σ-*set* of G if every member $\neq 1$ of $\mathcal{H}$ is a Hall σ_i-subgroup of G for some $i \in I$ and $\mathcal{H}$ contains exactly one Hall σ_i-subgroup of G for every i such that $\sigma_i \cap \pi(G) \neq \varnothing$. A group is said to be σ-*primary* if it is a finite σ_i-group for some i. A subgroup A of G is said to be: σ-*permutable* in G if G possesses a complete Hall σ-set $\mathcal{H}$ such that $AH^x = H^xA$ for all $H \in \mathcal{H}$ and all $x \in G$; σ-*subnormal* in G if there is a subgroup chain $A = A_0 \leq A_1 \leq \ldots \leq A_t = G$ such that either $A_{i-1} \trianglelefteq A_i$ or $A_i / (A_i - 1)_{A_i}$ is σ-primary for all $i = 1, \ldots, t$; $\mathfrak{U}$-*normal* in G if every chief factor of G between A_G and A^G is cyclic. We say that a subgroup H of G is: (i) *partially* σ-*permutable* in G if there are a $\mathfrak{U}$-normal subgroup A and a σ-permutable subgroup B of G such that $H = \langle A, B \rangle$; (ii) $(\mathfrak{U}, \sigma)$-*embedded* in G if there are a partially σ-permutable subgroup S and a σ-subnormal subgroup T of G such that $G = HT$ and $H \cap T \leq S \leq H$. We study G assuming that some subgroups of G are partially σ-permutable or $(\mathfrak{U}, \sigma)$-embedded in G. Some known results are generalised.

Keywords: finite group; σ-soluble groups; σ-nilpotent group; partially σ-permutable subgroup; $(\mathfrak{U}, \sigma)$-embedded subgroup; $\mathfrak{U}$-normal subgroup.

Introduction

Throughout this paper, all groups are finite and G always denotes a finite group. Moreover, $\mathbb{P}$ is the set of all primes, $\pi \subseteq \mathbb{P}$ and $\pi' = \mathbb{P} \setminus \pi$. If n is an integer, the symbol $\pi(n)$ denotes the set of all primes dividing n; as usual, $\pi(G) = \pi(|G|)$, the set of all primes dividing the order of G.

A subgroup A of G is said to be $\mathfrak{U}$-*normal* in G [1] if either $A \trianglelefteq G$ or $A_G \neq A^G$ and every chief factor of G between A_G and A^G is cyclic.

Following L. Shemetkov [2], we use σ to denote some partition of $\mathbb{P}$. Thus $\sigma = \{\sigma_i | i \in I\}$, where $\mathbb{P} = \bigcup_{i \in I} \sigma_i$ and $\sigma_i \cap \sigma_j = \varnothing$ for all $i \neq j$. The symbol $\sigma(n)$ denotes the set $\{\sigma_i | \sigma_i \cap \pi(n) \neq \varnothing\}$; $\sigma(G) = \sigma(|G|)$.

The group G is said to be [3–5]: σ-*primary* if G is a σ_i-group for some $i \in I$; σ-*nilpotent* if $G = G_1 \times \ldots \times G_n$ for some σ-primary groups $G_1, \ldots, G_n$; σ-*soluble* if every chief factor of G is σ-primary.

A set $\mathcal{H}$ of subgroups of G is said to be a *complete Hall* σ-*set* of G [6; 7] if every member $\neq 1$ of $\mathcal{H}$ is a Hall σ_i-subgroup of G for some $i \in I$ and $\mathcal{H}$ contains exactly one Hall σ_i-subgroup of G for every i such that $\sigma_i \cap \pi(G) \neq \varnothing$.

A subgroup A of G is said to be [3]: σ-*permutable* in G if G possesses a complete Hall σ-set $\mathcal{H}$ such that $AH^x = H^xA$ for all $H \in \mathcal{H}$ and all $x \in G$; σ-*subnormal* in G if there is a subgroup chain $A = A_0 \leq A_1 \leq \ldots \leq A_t = G$ such that either $A_{i-1} \trianglelefteq A_i$ or $A_i / (A_i - 1)_{A_i}$ is σ-primary for all $i = 1, \ldots, t$.

Note that in the classical case when $\sigma = \{\{2\}, \{3\}, \ldots\}$, σ-permutable subgroups are also called *S-permutable* [8; 9], and in this case A is σ-subnormal in G if and only if it is subnormal in G.

The σ-permutable and σ-subnormal subgroups were studied by a lot of authors (see, in particular, the papers [3–6; 10–29]).

In this paper we consider some applications of the following generalisation of σ-subnormal and σ-permutable subgroups.

Definition 1. We say that a subgroup H of G is

(i) *partially* σ*-permutable* in G if there are a $\mathfrak{U}$-normal subgroup A and a σ-permutable subgroup B of G such that $H = \langle A, B\rangle$;

(ii) $(\mathfrak{U}, \sigma)$*-embedded* in G if there are a partially σ-permutable subgroup S and a σ-subnormal subgroup T of G such that $G = HT$ and $H \cap T \leq S \leq H$.

Note that every $\mathfrak{U}$-normal subgroup $A = \langle A, 1\rangle$ and every σ-permutable subgroup $B = \langle 1, B\rangle$ are partially σ-permutable in G. Moreover, every partially σ-permutable subgroup S is $(\mathfrak{U}, \sigma)$-embedded in G since in this case we have $G = SG$ and $S \cap G = S \leq S$, where G is a σ-subnormal subgroup of G by definition.

Now we consider the following examples, which allow you to get various applications of the introduced concepts.

Example 1. (i) A subgroup H of G is said to be *weakly* σ*-permutable* [30] or *weakly* σ*-quasinormal* [31] in G if there is a σ-subnormal subgroup T and a σ-permutable subgroup S of G such that $G = HT$ and $H \cap T \leq S \leq H$. Every weakly σ-quasinormal subgroup is $(\mathfrak{U}, \sigma)$-embedded in the group.

(ii) A subgroup H of G is said to be *weakly S-permutable* in G [32] if there are an S-permutable subgroup S and a subnormal subgroup T of G such that $G = HT$ and $H \cap T \leq S \leq H$. It is clear that every weakly S-permutable subgroup is $(\mathfrak{U}, \sigma)$-embedded for every partition σ of $\mathbb{P}$.

(iii) Recall that a subgroup M of G is called *modular* in G if M is a modular element (in the sense of Kurosh [33, p. 43]) of the lattice $\mathcal{L}(G)$ of all subgroups of G, that is (i) $\langle X, M \cap Z\rangle = \langle X, M\rangle \cap Z$ for all $X \leq G$, $Z \leq G$ such that $X \leq Z$, and (ii) $\langle M, Y \cap Z\rangle = \langle M, Y\rangle \cap Z$ for all $Y \leq G$, $Z \leq G$ such that $M \leq Z$.

A subgroup H of G is called *m*-σ*-permutable* in G [34] if there are a modular subgroup A and a σ-permutable subgroup B of G such that $H = \langle A, B\rangle$. In view of [33, theorem 5.1.9], every modular subgroup is $\mathfrak{U}$-normal in the group. Therefore, every m-σ-permutable subgroup is partially σ-permutable.

(iv) A subgroup H of G is called *weakly m*-σ*-permutable* in G [34] if there are an m-σ-permutable subgroup S and a σ-subnormal subgroup T of G such that $G = HT$ and $H \cap T \leq S \leq H$. It is clear that every weakly m-σ-permutable subgroup is $(\mathfrak{U}, \sigma)$-embedded.

(v) A subgroup A of G is said to be *c-normal* in G [35] if for some normal subgroup T of G we have $AT = G$ and $A \cap T \leq A_G$. Every c-normal subgroup is $(\mathfrak{U}, \sigma)$-embedded.

Our first observation generalises corresponding results in [34; 35].

Theorem A. *(i) If every non-nilpotent maximal subgroup of G is* $(\mathfrak{U}, \sigma)$*-embedded in G, then G is* σ*-soluble.*

(ii) G is soluble if and only if every maximal subgroup of G is $(\mathfrak{U}, \sigma)$*-embedded in G and G possesses a complete Hall* σ*-set* $\mathcal{H}$ *whose members are soluble groups.*

In view of example 1 (iii), we get also from theorem A the following corollary.

Corollary 1 [34, theorem B]. *If every non-nilpotent maximal subgroup of G is weakly m-*σ*-permutable in G, then G is* σ*-soluble.*

In the case when $\sigma = \{\{2\}, \{3\}, \ldots\}$ we get from theorem A (ii) the following know result.

Corollary 2 [35, theorem 3.1]. *If every maximal subgroup of G is c-normal in G, then G is soluble.*

Now, recall that if $M_2 < M_1 < G$ where M_2 is a maximal subgroup of M_1 and M_1 is a maximal subgroup of G, then M_2 is said to be a 2*-maximal subgroup* of G.

Our next theorem generalises a well-known Agrawal's result on supersolubility of groups with S-permutable 2-maximal subgroups.

Theorem B. *If every* 2*-maximal subgroup of G is partially* σ*-permutable in G and G possesses a complete Hall* σ*-set* $\mathcal{H}$ *whose members are supersoluble, then G is supersoluble.*

Corollary 3. *If every* 2*-maximal subgroup of G is* σ*-permutable in G and G possesses a complete Hall* σ*-set* $\mathcal{H}$ *whose members are supersoluble, then G is supersoluble.*

In the case when $\sigma = \{\{2\}, \{3\}, \ldots\}$ we get from theorem B the following known results.

Corollary 4 [36; 37, chapter 1, theorem 6.5]. *If every* 2*-maximal subgroup of G is S-permutable in G, then G is supersoluble.*

Corollary 5 [38]. *If every* 2*-maximal subgroup of G is modular in G, then G is supersoluble.*

Recall that G is *meta-*σ*-nilpotent* [7] if G is an extension of a σ-nilpotent group by a σ-nilpotent group. An analysis of many open questions leads to the necessity of studying various classes of meta-σ-nilpotent groups (see, for example, the recent papers [3; 11–18; 30] and the survey [7]).

Out next result gives the following characterisation of meta-σ-nilpotent groups.

Theorem C. *(i) The following conditions are equivalent:*

(a) G possesses a complete Hall σ*-set* $\mathcal{H}$ *whose members are* $(\mathfrak{U}, \sigma)$*-embedded in G;*

(b) G is meta-σ*-nilpotent;*

(c) G is σ*-soluble and every* σ*-Hall subgroup H of G (that is* $\sigma(H) \cap \sigma(|G:H|) = \varnothing$*) is c-normal in G.*

(ii) If G possesses a complete Hall σ*-set* $\mathcal{H}$ *whose members are partially* σ*-permutable in G, then the derived subgroup G′ of G is* σ*-nilpotent.*

A group G is said to be: a D_π*-group* if G possesses a Hall π-subgroup E and every π-subgroup of G is contained in some conjugate of E; a σ*-full group of Sylow type* [3] if every subgroup E of G is a D_{σ_i}-group for each $\sigma_i \in \sigma(E)$.

In view of example 1 (ii) we get from theorem C the following corollary.

Corollary 6 [30, theorem 1.4]. *Let G be a* σ*-full group of Sylow type. If every Hall* σ_i*-subgroup of G is weakly* σ*-permutable in G for all* $\sigma_i \in \sigma(G)$*, then G is* σ*-soluble.*

In the case when $\sigma = \{\{2\}, \{3\}, \ldots\}$ we get from theorem C the following known result.

Corollary 7 [39, chapter I, theorem 3.49]. *G is metanilpotent if and only if every Sylow subgroup of G is c-normal.*

Proof of theorem A

First we prove the following two lemmas.

Lemma 1. *Let A, B and N be subgroups of G, where A is partially* σ*-permutable in G and N is normal in G. Then:*

(1) AN/N is partially σ*-permutable in G/N.*

(2) If G is σ*-full group of Sylow type and* $A \le B$*, then A is partially* σ*-permutable in B.*

(3) If G is σ*-full group of Sylow type,* $N \le B$ *and B/N is partially* σ*-permutable in G/N, then B is partially* σ*-permutable in G.*

(4) If G is σ*-full group of Sylow type and B is partially* σ*-permutable in G, then* $<A, B>$ *is partially* σ*-permutable in G.*

P r o o f. Let $A = <L, T>$, where L is $\mathfrak{U}$-normal and T is σ-permutable subgroups of G.

(1) $AN/N = <LN/N, TN/N>$, where LN/N is $\mathfrak{U}$-normal in G/N by [40, lemma 2.8 (2)] and TN/N is σ-permutable in G/N by [3, lemma 2.8 (2)]. Hence AN/N is partially σ-permutable in G/N.

(2) This follows from [3, lemma 2.8 (1); 40 lemma 2.8].

(3) Let $B/N = <V/N, W/N>$, where V/N is $\mathfrak{U}$-normal in G/N and W/N is σ-permutable in G/N. Then $B = <V, W>$, where V is $\mathfrak{U}$-normal in G by [40 lemma 2.8 (3)] and W is σ-permutable in G. Hence B is partially σ-permutable in G.

(4) Let $B = <V, W>$, where V is $\mathfrak{U}$-normal and W is a σ-permutable subgroups of G. Then

$$<A, B> = \ll L, T>, <V, W\gg = \ll L, V>, <T, W\gg,$$

where $<L, V>$ is $\mathfrak{U}$-normal in G by [40, lemma 2.8 (1)] and $<T, W>$ is σ-permutable in G by [3, lemma 2.8 (4)].

Hence $<A, B>$ is partially σ-permutable in G.

The lemma is proved.

Lemma 2. *Let A, B and N be subgroups of G, where A is* $(\mathfrak{U}, \sigma)$*-embedded in G and N is normal in G.*

(1) If either $N \le A$ *or* $(|A|, |N|) = 1$*, then AN/N is* $(\mathfrak{U}, \sigma)$*-embedded in G/N.*

(2) If G is σ*-full group of Sylow type and* $A \le B$*, then A is* $(\mathfrak{U}, \sigma)$*-embedded in B.*

(3) If G is σ*-full group of Sylow type,* $N \le B$ *and B/N is* $(\mathfrak{U}, \sigma)$*-embedded in G/N, then B is* $(\mathfrak{U}, \sigma)$*-embedded in G.*

P r o o f. Let T be a σ-subnormal subgroup of G such that $AT = G$ and $A \cap T \le S \le A$ for some partially σ-permutable subgroup S of G.

(1) First note that $NT \cap NA = (T \cap A)N$. Therefore $G/N = (AN/N)(TN/N)$ and

$$(AN/N) \cap (TN/N) = (AN \cap TN/N) = (A \cap T)N/N \le SN/N,$$

where SN/N is a partially σ-permutable subgroup of G/N by lemma 1 (1). Hence AN/N is $(\mathfrak{U}, \sigma)$-embedded in G/N.

(2) $B = A(B \cap T)$ and $(B \cap T) \cap A = T \cap A \le S \le A$, where S is partially σ-permutable in B by lemma 1 (2). Hence A is $(\mathfrak{U}, \sigma)$-embedded in B.

(3) See the proof of (1) and use lemma 1 (3).

The lemma is proved.

P r o o f o f t h e o r e m A. (i) Assume that this assertion is false and let G be a counterexample of minimal order. Let R be a minimal normal subgroup of G.

(1) G/R is σ-soluble. Hence R is not σ-primary and it is a unique minimal normal subgroup of G.

Note that if M/R is a non-nilpotent maximal subgroup of G/R, then M is a non-nilpotent maximal subgroup of G and so it is $(\mathfrak{U}, \sigma)$-embedded in G by hypothesis. Hence M/R is $(\mathfrak{U}, \sigma)$-embedded in G/R by lemma 2 (1). Therefore the hypothesis holds for G/R. Hence G/R is σ-soluble and so R is not σ-primary by the choice of G. Now assume that G has a minimal normal subgroup $N \neq R$. Then G/N is σ-soluble and N is not σ-primary. But, in view of the G-isomorphism $RN/R \simeq N$, the σ-solubility of G/R implies that N is σ-primary. This contradiction completes the proof of (1).

In view of claim (1), R is not abelian. Hence $|\pi(R)| > 1$. Let p be any odd prime dividing $|R|$ and R_p a Sylow p-subgroup of R.

(2) If G_p is a Sylow p-subgroup of G with $R_p = G_p \cap R$, then there is a maximal subgroup M of G such that $RM = G$ and $G_p \leq N_G(R_p) \leq M$.

It is clear that $G_p \leq N_G(R_p)$. The Frattini argument implies that $G = RN_G(R_p)$. Conversely, claim (1) implies that $N_G(R_p) \neq G$, so for some maximal subgroup M of G we have $RM = G$ and $G_p \leq N_G(R_p) \leq M$.

(3) M is not nilpotent and $M_G = 1$. Hence M is $(\mathfrak{U}, \sigma)$-embedded in G.

Assume that M is nilpotent, and let $D = M \cap R$. Then D is a normal subgroup of M and R_p is a Sylow p-subgroup of D since $R_p \leq G_p \leq M$. Hence R_p is characteristic in D and so it is normal in M. Therefore $Z(J(R_p))$ is normal in M. Claims (1) and (2) imply that $M_G = 1$. Hence $N_G(Z(J(R_p))) = M$ and so $N_R(Z(J(R_p))) = D$ is nilpotent. This implies that R is p-nilpotent by the Glauberman – Thompson theorem on the normal p-complements. But then R is a p-group, contrary to claim (1). Hence we have (3).

(4) There is a σ-subnormal subgroup T of G such that $MT = G$, $M \cap T = 1$ and p does not divide $|T|$.

By claim (3), there are a partially σ-permutable subgroup S and a σ-subnormal subgroup T of G such that $G = MT$ and $M \cap T \leq S \leq M$. Then $S = \langle A, B\rangle$ for some $\mathfrak{U}$-normal subgroup A and σ-permutable subgroup B of G. Moreover, from the definition $\mathfrak{U}$-normality and claim (1) it follows that, in fact, $S = B$ and $S_G = 1$. Suppose that $S \neq 1$. Then for every $\sigma_i \in \sigma(S)$ we have $S = O_{\sigma_i'}(S) \times O_{\sigma_i}(S)$ by [3, theorem B]. Therefore for every Hall σ_i-subgroup H of G from $SH = HS = O_{\sigma_i'}(S)H$ we get that $1 < O_{\sigma_i}(S) \leq H_G$, contrary to claim (1). Therefore $S = 1$, so $T \cap M = 1$. Hence $|T| = |G : M|$, so p does not divide $|T|$ since $G_p \leq M$ by claim (2).

The final contradiction for (i). Let L be a minimal σ-subnormal subgroup of G contained in T. Then L is a simple group. If L is a σ_i-group for some i, then $L \leq O_{\sigma_i}(G)$ by [12, lemma 2.2 (10)], which is impossible by claim (1).

Hence L is non-abelian, so it is subnormal in G by [12, lemma 2.2 (7)]. Suppose that $L \nleq R$. Then $L \cap R = 1$. Conversely, $R \leq N_G(L)$ by [41, chapter A, theorem 14.3]. Hence $LR = L \times R$, so $L \leq C_G(R)$. But claim (1) implies that $R \nleq C_G(R)$ and so $C_G(R) = 1$, a contradiction. Hence L is a minimal normal subgroup of R. It follows that p divides $|L|$ and hence p divides $|T|$, contrary to claim (4). Therefore assertion (i) is true.

(ii) In view of theorem A, it is enough to show that if G is soluble, then every maximal subgroup M of G is $(\mathfrak{U}, \sigma)$-embedded in G. If $M_G \neq 1$, then M/M_G is $(\mathfrak{U}, \sigma)$-embedded in G/M_G by induction, so M is $(\mathfrak{U}, \sigma)$-embedded in G by lemma 2 (3). Conversely, if $M_G = 1$ and R is a minimal normal subgroup of G, then R is abelian and so $G = R \rtimes M$. Hence M is $(\mathfrak{U}, \sigma)$-embedded in G.

The theorem is proved.

Proof of theorem B

Lemma 3 [6, theorem A]. *If G is σ-soluble, then G is a σ-full group of Sylow type.*

Lemma 4. *If G is σ-soluble and G possesses a complete Hall σ-set whose members are p-soluble, then G is p-soluble.*

P r o o f. Suppose that this lemma is false and let G be a counterexample of minimal order. Let $\mathcal{H} = \{H_1, \ldots, H_t\}$ be a complete Hall σ-set of G. Then H_i is p-soluble by lemma 3 for all i.

First show that if R is minimal normal subgroup of G, then G/R is p-soluble. It is enough to show that the hypothesis holds for G/R.

Note that for every chief factor $(H/R)/(K/R)$ of G/R we have that $(H/R)/(K/R) \simeq_G H/K$, where H/K is a chief factor of G and H/K is σ-primary since G is σ-soluble. So $(H/R)/(K/R)$ is σ-primary, hence G/R is σ-soluble.

Note also that $\{H_1R/R, \ldots, H_tR/R\}$ is a complete Hall σ-set of G/R, where $H_iR/R \simeq H_i/(H_i \cap R)$ is p-soluble since H_i is p-soluble. Therefore the hypothesis holds for G/R, so G/R is p-soluble by the choice of G.

Now show that R is p-soluble. Since G is σ-soluble, R is σ-primary, that is, σ_i-group for some i. Also, for every Hall σ_i-subgroup H of G we have $R \leq H$. So, R is p-soluble by the hypothesis, hence G is p-soluble.

The lemma is proved.

Proof of theorem B. Suppose that this theorem is false and let G be a counterexample of minimal order. Let $\mathcal{H} = \{H_1, \ldots, H_t\}$. Then $t > 1$ since H_1 is supersoluble by hypothesis.

(1) If R is minimal normal subgroup of G, then G/R is supersoluble. Hence R is the unique minimal normal subgroup of G, R is not cyclic and $R \nleq \Phi(G)$.

It is enough to show that the hypothesis holds for G/R. First note that $\{H_1R/R, \ldots, H_tR/R\}$ is a complete Hall σ-set of G/R, where $H_iR/R \simeq H_i/(H_i \cap R)$ is supersoluble since H_i is supersoluble by hypothesis.

Now assume that statement (1) is false. Then G/R is not nilpotent, so every Sylow p-subgroup in G/R is proper. Then for every Sylow p-subgroup P of G/R it follows that P is contained in some maximal subgroup of G/R. Hence R is contained in some 2-maximal subgroup T of G and so T is partially σ-permutable in G by the hypothesis. But then T/R is 2-maximal of G/R and partially σ-permutable in G/R by lemma 1 (1). Therefore the hypothesis holds for G/R, so G/R is supersoluble by the choice of G. Then we have a contradiction.

Moreover, it is well-known that the class of all supersoluble groups is a saturated formation [42 chapter VI, definition 8.6]. Hence the choice of G implies that R is the unique minimal normal subgroup of G, R is not cyclic and $R \nleq \Phi(G)$. Hence we have (1).

(2) G is soluble.

Every 2-maximal subgroup in G is partially σ-permutable and so, partially σ-subnormal in G by [3, theorem B]. Then, in view of theorem in [40], G is σ-soluble. Hence, from lemma 4 it follows that G is soluble. So we have (2).

(3) $R = O_p(G) \nleq \Phi(G)$ *for some prime* $p \in \sigma_i$. *Hence for some maximal subgroup M of G we have* $G = R \rtimes M$ *and* $M \neq M_G = 1$.

By claim (2), G is soluble and so R is a p-group for some $p \in \sigma_i$. Hence the choice of G and claim (1) imply that R is a unique minimal normal subgroup of G. Moreover, $R \nleq \Phi(G)$ by claim (1), so $R = C_G(R) = O_p(G)$ by [41, chapter A, lemma 15.2]. Hence for some maximal subgroup M of G we have $G = R \rtimes M$ and $M \neq M_G = 1$ by claim (1).

(4) If $1 < H \leq M$, *then H is not* $\mathfrak{U}$*-normal in G.*

Indeed, if H is $\mathfrak{U}$-normal in G, then $H^G/H_G \leq Z_{\mathfrak{U}}(G/H_G)$, where $H_G = 1$ by claim (3). Hence $R \leq H^G \leq Z_{\mathfrak{U}}(G)$ by claim (1). But then R is cyclic, contrary to claim (1). This contradiction completes the proof of the claim.

(5) M is not a group of prime order.

Suppose that $|M| = q$ for some prime q. Hence $|M| = |G : R|$ is a prime and so R is a maximal subgroup of G. Then every maximal subgroup V of R is 2-maximal in G, so V is partially σ-permutable in G by hypothesis. So $V = <A, B>$, where A is $\mathfrak{U}$-normal and B is σ-permutable in G. Assume $A \neq 1$. Note $A_G = 1$ by the minimality of R. Then $R \leq A^G \leq Z_{\mathfrak{U}}(G)$ and so R is cyclic, contrary to claim (1). Hence $V = B$ is σ-permutable in G. Therefore every maximal subgroups of R is σ-permutable in G.

Note that $R \leq H_i$ since R is σ_i-group by claim (3) and $H_i = R \rtimes (H_i \cap M)$, again by claim (3). Since H_i is supersoluble by hypothesis, some maximal subgroup W of R is normal in H_i. In addition, W is σ-permutable in G since it is a maximal subgroup of R. Hence for each $j \neq i$ we have $WH_j = H_jW$, which implies that $H_j \leq N_G(W)$ since $R \cap WH_j = W(R \cap H_j) = W$. Therefore W is normal in G, so the minimality of R implies that $W = 1$ and hence $|R| = p$, which is impossible by claim (3). Hence we have (5).

(6) If T is a maximal subgroup of M, then T^G *is a* σ_i*-subgroup of G.*

Indeed, T is partially σ-permutable in G by hypothesis, so $T = <A, B>$ for some $\mathfrak{U}$-normal subgroup A and some σ-permutable subgroup B of G. Note that $T \neq 1$ by claim (5). Conversely, $A = 1$ by claim (4) and so $T = B$ is σ-permutable in G. Therefore T^G/T_G is σ-nilpotent [3, theorem B (ii)]. We have $T_G \leq M_G = 1$, so $T^G/T_G \simeq T^G/1 \simeq T^G$ is σ-nilpotent group. Hence the subgroup $O_{\sigma_k}(T^G)$ is characteristic in T^G, so it is normal in G. By claim (3) we have that $O_{\sigma_k}(T^G) = 1$ for all $k \neq i$. Hence $T^G = O_{\sigma_i}(T^G)$ is a σ_i-subgroup of G.

(7) M is not $\sigma_{i'}$*-group.*

Suppose that this is false and let T be a maximal subgroup of M. Then $T \neq 1$ by claim (5). Conversely, T is a $\sigma_{i'}$-group by the hypothesis and T^G is a σ_i-subgroup of G by claim (6). Then we have a contradiction. Hence, M is not a $\sigma_{i'}$-group.

(8) M is not σ_i-group (this follows from the facts that $t > 1$ and R is a σ_i-group).

Final contradiction.

Let T be a maximal subgroup of M, containing a Hall $\sigma_{i'}$-subgroup of M. Then T^G is σ_i-group by claim (6). Therefore, a Hall $\sigma_{i'}$-subgroup of M is the identity group. Hence M is σ_i-group, contrary to claim (8). This contradiction completes the proof of the result.

Proof of theorem C

We use $\mathfrak{N}_\sigma$ to denote the class of all σ-nilpotent groups.

Lemma 5 [3, corollary 2.4 and lemma 2.5]. *(1) The class $\mathfrak{N}_\sigma$ is closed under taking products of normal subgroups, homomorphic images and subgroups.*

(2) If G/N and G/R are σ-nilpotent, then $G/(N \cap R)$ is σ-nilpotent.

(3) If E is a normal subgroup of G and $E/(E \cap \Phi(G))$ is σ-nilpotent, then E is σ-nilpotent.

Recall that $G^{\mathfrak{N}_\sigma}$ denotes the σ-*nilpotent residual* of G, that is, the intersection of all normal subgroups N of G with σ-nilpotent quotient G/N. In view of [43, proposition 2.2.8], we get from lemma 5 (1) the following result.

Lemma 6. *If N is a normal subgroup of G, then $(G/N)^{\mathfrak{N}_\sigma} = G^{\mathfrak{N}_\sigma}N/N$.*

The next lemma is proved by the direct verifications on the basis of lemmas 5 and 6.

Lemma 7. *(1) G is meta-σ-nilpotent if and only if $G^{\mathfrak{N}_\sigma}$ is σ-nilpotent.*

(2) If G is meta-σ-nilpotent, then every quotient G/N of G is meta-σ-nilpotent.

(3) If G/N and G/R are meta-σ-nilpotent, then $G/(N \cap R)$ is meta-σ-nilpotent.

(4) If E is a normal subgroup of G and $E/(E \cap \Phi(G))$ is meta-σ-nilpotent, then E is meta-σ-nilpotent.

Lemma 8. *Let A, B and N be subgroups of G, where A is c-normal in G and N is normal in G.*

(1) If either $N \leq A$ or $(|A|, |N|) = 1$, then AN/N is c-normal in G/N.

(2) If $N \leq B$ and B/N is c-normal in G/N, then B is c-normal in G.

P r o o f. See the proof of lemma 2.

A natural number n is said to be a Π-*number* if $\sigma(n) \subseteq \Pi$. A subgroup A of G is said to be: a *Hall* Π-*subgroup* of G [6; 7] if $|A|$ is a Π-number and $|G : A|$ is a Π′-number; a σ-*Hall subgroup* of G if A is a Hall Π-subgroup of G for some $\Pi \subseteq \sigma$.

Recall also that a normal subgroup E of G is called *hypercyclically embedded* in G [33, p. 217] if every chief factor of G below E is cyclic.

P r o o f o f t h e o r e m C. Let $D = G^{\mathfrak{N}_\sigma}$ be the σ-nilpotent residual of G.

(i) (a) ⇒ (b). Assume that this is false and let G be a counterexample of minimal order. Then D is not σ-nilpotent since G/D is σ-nilpotent by lemma 5 (2). Let $\mathcal{H} = \{H_1, \ldots, H_t\}$. We can assume without loss of generality that H_i is a σ_i-group for all $i = 1, \ldots, t$. Let S_i be a partially σ-permutable subgroup and T_i be a σ-subnormal subgroup of G such that $S_i \leq H_i$, $H_iT_i = G$ and $H_i \cap T_i \leq S_i$ for all $i = 1, \ldots, t$. Then, for every i, $S_i = \langle A_i, B_i \rangle$ for some $\mathfrak{U}$-normal subgroup A_i and σ-permutable subgroup B_i of G.

(1) If R is a σ-primary minimal normal subgroup of G, then G/R is meta-σ-nilpotent and so G is σ-soluble. Moreover, R is a unique minimal normal subgroup of G, $C_G(R) \leq R$ and R is not cyclic.

First we show that G/R is meta-σ-nilpotent. In view of the choice of G, it is enough to show that the hypothesis holds for G/R. Since R is σ-primary, for some i we have $R \leq H_i$ and $(|R|, |H_j|) = 1$ for all $j \neq i$. Therefore $\{H_1R/R, \ldots, H_tR/R\}$ is a complete Hall σ-set of G/R whose members are $(\mathfrak{U}, \sigma)$-embedded in G/R by lemma 2 (1). Hence the hypothesis holds for G/R, so G/R is meta-σ-nilpotent and G is σ-soluble. Hence every minimal normal subgroup of G is σ-primary, so R is a unique minimal normal subgroup of G and $R \not\leq \Phi(G)$ by lemma 7 (4). Hence $C_G(R) \leq R$ by [41, chapter A, lemma 15.6]. Finally, note that in the case when R is cyclic we have $|R| = p$ for some prime p and so $G/C_G(R) = G/R$ is cyclic, which implies that G is metanilpotent and so it is meta-σ-nilpotent. Therefore we have (1).

(2) For some i, $i = 1$ say, we have $S_i = S_1 \neq 1$. Moreover, if for some k we have $S_k = 1$, then T_k is a normal complement to H_k in G.

Assume that $S_i = 1$. Then $H_i \cap T_i = 1$, so T_i is a σ-subnormal Hall σ_i'-subgroup of G. Hence T_i is a normal complement to H_i in G by [3, lemma 2.6 (10)]. Moreover, $G/T_i \simeq H_i$ is σ-nilpotent. Suppose that $S_i = 1$ for all $i = 1, \ldots, t$. Then $T_1 \cap \ldots \cap T_t = 1$ by [41, chapter A, theorem 1.6 (b)], so

$$G \simeq G/1 = G/(T_1 \cap \ldots \cap T_t)$$

is σ-nilpotent by lemma 5 (2). Then we have a contradiction. Hence for some i we have $S_i \neq 1$.

(3) If $S_i \neq 1$*, then* $(H_i)_G \neq 1$.

Assume that this is false. Then every non-identity subgroup L of H_i is not σ-permutable in G since otherwise for every $x \in G$ we have $LH_i^x = H_i^x L = H_i^x$ which implies that $1 < L \leq (H_i)_G = 1$.

Therefore $B_i = 1$ and so $S_i = A_i$ is a $\mathfrak{U}$-normal subgroup of G with $(S_i)_G = 1$. But then we have $1 < (S_i)^G$ is hypercyclically embedded in G by the definition $\mathfrak{U}$-normality and so R is cyclic, contrary to claim (1). Hence we have (3).

(4) G possesses a σ-primary minimal normal subgroup, R say.

Claims (2) and (3) imply that $(H_1)_G \neq 1$. Therefore, if R is a minimal normal subgroup of G contained in $(H_1)_G$, then R is σ-primary.

The final contradiction for the implication (a) ⇒ (b). Claims (1) and (4) imply that G is σ-soluble, so R is a unique minimal normal subgroup of G by claim (1). Hence claims (2) and (3) imply that $T_2, \ldots, T_t$ are normal subgroups of G and $G/T_k \simeq H_k$ for all $k = 2, \ldots, t$. Hence $G/(T_2 \cap \ldots \cap T_t)$ is σ-nilpotent by lemma 5 (2). Conversely, $T_2 \cap \ldots \cap T_t = H_1$ by [41, chapter A, theorem 1.6 (b)] and so G is meta-σ-nilpotent, contrary to the choice of G. This contradiction completes the proof of the (a) ⇒ (b).

(b) ⇒ (c). The subgroup D is σ-nilpotent by lemma 7 (1). Let $\Pi = \sigma(H)$. Then H is a Hall Π-subgroup of G.

Suppose that $H_G \neq 1$. Then H/H_G is c-normal in G by induction since the hypothesis holds for G/H_G by lemma 7 (2). Hence H is c-normal in G by lemma 8 (2).

Now assume that $H_G = 1$. Then, since D is σ-nilpotent, it follows that $D \cap H = 1$. Conversely, G/D is σ-nilpotent by lemma 5 (2) and $H \simeq HD/D$ is a Hall Π-subgroup of G/D, so HD/D has a normal complement T/D in G/D. Then T is a normal subgroup of G such that $HT = G$ and $T \cap H \leq T \cap HD \cap H \leq D \cap H = 1$. Hence H is c-normal in G. Therefore the implication (b) ⇒ (c) holds.

(c) ⇒ (b). In view of example 1 (v), this application is a corollary of the implication (a) ⇒ (b).

(ii) Suppose that this assertion is false and let G be a counterexample of minimal order. Then G is not σ-nilpotent, so $|\sigma(G)| > 1$. Moreover, from part (i) we know that D is σ-nilpotent and so G is σ-soluble. Let $\mathcal{H} = \{H_1, \ldots, H_t\}$.

Let R be a minimal normal subgroup of G. Then R is a σ_i-group for some i, so the hypothesis holds for G/R by lemma 1 (1). Hence $(G/R)' = G'R/R = G'/(G' \cap R)$ is σ-nilpotent by the choice of G. Therefore $R \leq G'$ and $R \nleq \Phi(G)$ by lemma 5 (3). Moreover, if G has a minimal normal subgroup $N \neq R$ of G, then $N \leq G'$ and $G' \simeq G'/1 = G'/(R \cap N)$ is σ-nilpotent, contrary to the choice of G. Therefore R is a unique minimal normal subgroup of G and $C_G(R) \leq R$ by [41, chapter A, lemma 16.5]. We can assume without loss of generality that $R \leq H_1$.

Let M be a maximal subgroup of G such that $R \nleq M$. Then $M_G = 1$ and $|G : M|$ is a σ_i-number. Therefore for some $x \in G$ we have $H = H_2^x \leq M$. Then $H = \langle A, B\rangle$ for some $\mathfrak{U}$-normal subgroup A and σ-permutable subgroup B of G. Moreover, $A_G \leq M_G = 1$, so A^G is hypercyclically embedded in G by the definition $\mathfrak{U}$-normality. If $A \neq 1$, then $R \leq A^G$ and so $|R| = p$ for some prime p. But then $C_G(R) = R$ and $G/R = G/C_G(R)$ is cyclic. Hence G' is nilpotent. This contradiction shows that $A = 1$, so $H = B$ is σ-permutable in G. But then $HH^x = H^x H = H$ for all $x \in G$ since H is a Hall σ_i-subgroup of G for some i. Hence H is normal in G, so $1 < H \leq M_G$, a contradiction. Therefore assertion (ii) is true.

The theorem is proved.

References

1. Hu B, Huang J, Skiba AN. Finite groups with only $\mathfrak{F}$-normal and $\mathfrak{F}$-abnormal subgroups *Journal of Group Theory.* 2019;22(5): 915–926. DOI: 10.1515/jgth-2018-0199.

2. Shemetkov LA. *Formatsii konechnykh grupp* [Finite group formations]. Moscow: Nauka; 1978. 272 p. Russian.

3. Skiba AN. On σ-subnormal and σ-permutable subgroups of finite groups. *Journal of Algebra.* 2015;436:1–16. DOI: 10.1016/j.jalgebra.2015.04.010.

4. Skiba AN. Some characterizations of finite σ-soluble *PσT*-groups. *Journal of Algebra.* 2018;495:114–129. DOI: 10.1016/j.jalgebra.2017.11.009.

5. Skiba AN. On sublattices of the subgroup lattice defined by formation Fitting sets. *Journal of Algebra.* 2020;550:69–85. DOI: 10.1016/j.jalgebra.2019.12.013.

6. Skiba AN. A generalization of a Hall theorem. *Journal of Algebra and Its Applications.* 2016;15(5):1650085. DOI: 10.1142/S0219498816500857.

7. Skiba AN. On some results in the theory of finite partially soluble groups. *Communications in Mathematics and Statistics.* 2016; 4(3):281–309. DOI: 10.1007/s40304-016-0088-z.

8. Ballester-Bolinches A, Beidleman JC, Heineken H. Groups in which Sylow subgroups and subnormal subgroups permute. *Illinois Journal of Mathematics.* 2003;47(1–2):63–69. DOI: 10.1215/ijm/1258488138.

9. Ballester-Bolinches A, Esteban-Romero R, Asaad M. *Products of finite groups.* Berlin: De Gruyter; 2010. 334 p. (De Gruyter Expositions in Mathematics; volume 53). DOI: 10.1515/9783110220612.
10. Yi X, Skiba AN. Some new characterizations of PST-groups. *Journal of Algebra.* 2014;399:39–54. DOI: 10.1016/j.jalgebra.2013.10.001.
11. Beidleman JC, Skiba AN. On τσ-quasinormal subgroups of finite groups. *Journal of Group Theory.* 2017;20(5):955–969. DOI: 10.1515/jgth-2017-0016.
12. Al-Sharo KA, Skiba AN. On finite groups with σ-subnormal Schmidt subgroups. *Communications in Algebra*. 2017;45(10):4158–4165. DOI: 10.1080/00927872.2016.1236938.
13. Guo W, Skiba AN. Groups with maximal subgroups of Sylow subgroups σ-permutably embedded. *Journal of Group Theory.* 2017;20(1):169–183. DOI: 10.1515/jgth-2016-0032.
14. Huang J, Hu B, Wu X. Finite groups all of whose subgroups are σ-subnormal or σ-abnormal. *Communications in Algebra.* 2017;45(10):4542–4549. DOI: 10.1080/00927872.2016.1270956.
15. Hu B, Huang J, Skiba AN. Groups with only σ-semipermutable and σ-abnormal subgroups. *Acta Mathematica Hungarica.* 2017;153(1):236–248. DOI: 10.1007/s10474-017-0743-1.
16. Bin Hu, Jianhong Huang. On finite groups with generalized σ-subnormal Schmidt subgroups. *Communications in Algebra.* 2018;46(7):3127–3134. DOI: 10.1080/00927872.2017.1404091.
17. Guo W, Zhang C, Skiba AN, Sinitsa DA. On H_σ-permutable embedded subgroups of finite groups. *Rendiconti del Seminario Matematico della Università di Padova.* 2018;139:143–158. DOI: 10.4171/RSMUP/139-4.
18. Hu B, Huang J, Skiba AN. Finite groups with given systems of σ-semipermutable subgroups. *Journal of Algebra and Its Applications.* 2017;17(2):1850031. DOI: 10.1142/S0219498818500317.
19. Guo W, Skiba AN. Finite groups whose *n*-maximal subgroups are σ-subnormal. *Science China Mathematics.* 2019;62(7):1355–1372. DOI: 10.1007/s11425-016-9211-9.
20. Kovaleva VA. A criterion for a finite group to be σ-soluble. *Communications in Algebra.* 2018;46(12):5410–5415. DOI: 10.1080/00927872.2018.1468907.
21. Hu B, Huang J, Skiba A. On σ-quasinormal subgroups of finite groups. *Bulletin of the Australian Mathematical Society.* 2019;99(3):413–420. DOI: 10.1017/S0004972718001132.
22. Skiba AN. On some classes of sublattices of the subgroup lattice. *Journal of the Belarusian State University. Mathematics and Informatics.* 2019;3:35–47. DOI: 10.33581/2520-6508-2019-3-35-47.
23. Heliel AE-R, Al-Shomrani M, Ballester-Bolinches A. On the σ-length of maximal subgroups of finite σ-soluble groups. *Mathematics.* 2020;8(12):2165. DOI: 10.3390/math8122165.
24. Al-Shomrani MM, Heliel AA, Ballester-Bolinches A. On σ-subnormal closure. *Communications in Algebra.* 2020;48(8):3624–3627. DOI: 10.1080/00927872.2020.1742348.
25. Ballester-Bolinches A, Kamornikov SF, Pedraza-Aguilera MC, Perez-Calabuig V. On σ-subnormality criteria in finite σ-soluble groups. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A: Matemáticas.* 2020;114(2):94. DOI: 10.1007/s13398-020-00824-4.
26. Ballester-Bolinches A, Kamornikov SF, Pedraza-Aguilera MC, Yi X. On σ-subnormal subgroups of factorised finite groups. *Journal of Algebra.* 2020;559:195–202. DOI: 10.1016/j.jalgebra.2020.05.002.
27. Kamornikov SF, Tyutyanov VN. On σ-subnormal subgroups of finite groups. *Siberian Mathematical Journal.* 2020;61(2):266–270. DOI: 10.1134/S0037446620020093.
28. Kamornikov SF, Tyutyanov VN. On σ-subnormal subgroups of finite 3′-groups. *Ukrainian Mathematical Journal.* 2020;72(6):935–941. DOI: 10.1007/s11253-020-01833-7.
29. Yi X, Kamornikov SF. Finite groups with σ-subnormal Schmidt subgroups. *Journal of Algebra.* 2020;560:181–191. DOI: 10.1016/j.jalgebra.2020.05.021.
30. Chi Zhang, Zhenfeng Wu, Wenbin Guo. On weakly σ-permutable subgroups of finite groups. *Publicationes Mathematicae Debrecen.* 2017;91(3–4):489–502.
31. Hu B, Huang J, Skiba AN. On weakly σ-quasinormal subgroups of finite groups. *Publicationes Mathematicae Debrecen.* 2018;92(1–2):12.
32. Skiba AN. On weakly *s*-permutable subgroups of finite groups. *Journal of Algebra.* 2007;315(1):192–209. DOI: 10.1016/j.jalgebra.2007.04.025.
33. Schmidt R. *Subgroup lattices of groups.* Berlin: Walter de Gruyter; 1994 (De Gruyter Expositions in Mathematics; volume 14). 572 p. DOI: 10.1515/9783110868647.
34. Xianbiao Wei. On weakly *m*-σ-permutable subgroups of finite groups. *Communications in Algebra.* 2019;47(3):945–956. DOI: 10.1080/00927872.2018.1498874.
35. Yanming Wang. *c*-Normality of groups and its properties. *Journal of Algebra.* 1996;180(3):954–965. DOI: 10.1006/jabr.1996.0103.
36. Agrawal RK. Generalized center and hypercenter of a finite group. *Proceedings of the American Mathematical Society.* 1976;58(1):13–21. DOI: 10.1090/S0002-9939-1976-0409651-8.
37. Weinstein M. *Between nilpotent and solvable.* Passaic: Polygonal; 1982. 231 p.
38. Schmidt R. Endliche Gruppen mit vielen modularen Untergruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg.* 1969;34(12):115–125. DOI: 10.1007/BF02992891.
39. Guo W. *Structure theory for canonical classes of finite groups.* Heidelberg: Springer; 2015. 359 p.
40. Zakrevskaya VS. Finite groups with partially σ-subnormal subgroups in short maximal chains. *Advances in Group Theory and Application.* 2020;12:91–106. DOI: 10.32037/agta-2021-014.
41. Doerk K, Hawkes TO. *Finite soluble groups.* Berlin: De Gruyter; 1992. 891 p. (De Gruyter Expositions in Mathematics; volume 4). DOI: 10.1515/9783110870138.
42. Huppert B. *Endliche Gruppen I.* Berlin: Springer; 1967. 796 p. (Grundlehren der mathematischen Wissenschaften; volume 134). DOI: 10.1007/978-3-642-64981-3.
43. Ballester-Bolinches A, Ezquerro LM. *Classes of finite groups.* Dordrecht: Springer; 2006. 381 p. DOI: 10.1007/1-4020-4719-3.

Received 12.07.2021 / revised 01.09.2021 / accepted 05.10.2021.

УДК 511.42

ВКЛАД ЙОНАСА КУБИЛЮСА В МЕТРИЧЕСКУЮ ТЕОРИЮ ДИОФАНТОВЫХ ПРИБЛИЖЕНИЙ ЗАВИСИМЫХ ПЕРЕМЕННЫХ

***В. В. БЕРЕСНЕВИЧ*[1], *В. И. БЕРНИК*[2], *Ф. ГЁТЦЕ*[3], *Е. В. ЗАСИМОВИЧ*[2], *Н. И. КАЛОША*[2]**

[1]*Колледж им. Джеймса Рашолма, Йоркский университет, Западный кампус, YO10 5DD, г. Йорк, Великобритания*
[2]*Институт математики НАН Беларуси, ул. Сурганова, 11, 220072, г. Минск, Беларусь*
[3]*Билефельдский университет, Университетсштрассе, 25, D-33615, г. Билефельд, Германия*

Посвящается 100-летию со дня рождения академика Йонаса Кубилюса, который является основоположником метрической теории диофантовых приближений. Проводится обзор наиболее важных результатов, полученных в метрической теории диофантовых приближений. Отмечается, что за последние 70 лет в области диофантовых приближений сделано много выдающихся достижений. Упоминаются работы лауреатов Филдсовской премии Алана Бейкера и Григория Маргулиса, а также ученика Й. Кубилюса, академика АН БССР Владимира Спринджука, который в 1964 г. решил известную проблему Малера и стал основателем белорусской школы теории чисел.

Ключевые слова: Й. Кубилюс; диофантовы приближения; проблема Малера; метрическая теория чисел; трансцендентные и алгебраические числа.

Образец цитирования:
Береснсвич ВВ, Берник ВИ, Гётце Ф, Засимович ЕВ, Калоша НИ. Вклад Йонаса Кубилюса в метрическую теорию диофантовых приближений зависимых переменных. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:34–50 (на англ.).
https://doi.org/10.33581/2520-6508-2021-3-34-50

For citation:
Beresnevich VV, Bernik VI, Götze F, Zasimovich EV, Kalosha NI. Contribution of Jonas Kubilius to the metric theory of Diophantine approximation of dependent variables. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021; 3:34–50.
https://doi.org/10.33581/2520-6508-2021-3-34-50

Авторы:
Виктор Вячеславович Береснсвич – доктор физико-математических наук, профессор; профессор.
Василий Иванович Берник – доктор физико-математических наук, профессор; главный научный сотрудник отдела теории чисел.
Фридрих Гётце – доктор физико-математических наук, профессор; профессор.
Елена Васильевна Засимович – аспирантка отдела теории чисел. Научный руководитель – В. И. Берник.
Николай Иванович Калоша – кандидат физико-математических наук; старший научный сотрудник отдела теории чисел.

Authors:
Victor V. Beresnevich, doctor of science (physics and mathematics), full professor; professor.
victor.beresnevich@york.ac.uk
Vasily I. Bernik, doctor of science (physics and mathematics), full professor; chief researcher at the department of number theory.
bernik.vasili@mail.ru
Friedrich Götze, doctor of science (physics and mathematics), full professor; professor.
goetze@math.uni-bielefeld.de
Elena V. Zasimovich, postgraduate student at the department of number theory.
elena.guseva.96@yandex.by
Nikolai I. Kalosha, PhD (physics and mathematics); senior researcher at the department of number theory.
kalosha@im.bas-net.by

CONTRIBUTION OF JONAS KUBILIUS TO THE METRIC THEORY OF DIOPHANTINE APPROXIMATION OF DEPENDENT VARIABLES

V. V. BERESNEVICH[a], *V. I. BERNIK*[b], *F. GÖTZE*[c], *E. V. ZASIMOVICH*[b], *N. I. KALOSHA*[b]

[a]*James College, University of York, Campus West, YO10 5DD, York, United Kingdom*
[b]*Institute of Mathematics, National Academy of Sciences of Belarus, 11 Surhanava Street, Minsk 220072, Belarus*
[c]*Bielefeld University, 25 Universitätsstraße, Bielefeld D-33615, Germany*
Corresponding author: N. I. Kalosha (kalosha@im.bas-net.by)

The article is devoted to the latest results in metric theory of Diophantine approximation. One of the first major result in area of number theory was a theorem by academician Jonas Kubilius. This paper is dedicated to centenary of his birth. Over the last 70 years, the area of Diophantine approximation yielded a number of significant results by great mathematicians, including Fields prize winners Alan Baker and Grigori Margulis. In 1964 academician of the Academy of Sciences of BSSR Vladimir Sprindžuk, who was a pupil of academician J. Kubilius, solved the well-known Mahler's conjecture on the measure of the set of *S*-numbers under Mahler's classification, thus becoming the founder of the Belarusian academic school of number theory in 1962.

Keywords: J. Kubilius; Diophantine approximation; Mahler's conjecture; metric number theory; transcendence and algebraic numbers.

Dedicated to the centenary of academician Jonas Kubilius's birth

Introduction

Academician Jonas Kubilius devoted his life to research in theory of probability and number theory. He was one of the founders of metric theory of Diophantine approximation, obtaining one of the earliest major results in this field [1; 2] and influencing the work of his pupil Vladimir Sprindžuk, who in 1964 proved the famous Mahler's conjecture [3–5].

First results in metric theory of Diophantine approximation were obtained by Émile Borel in the beginning of the 20th century [6], and they were later significantly improved in a seminal work of Alexander Khintchine [7].

Let $\psi(x)$ be a monotonic decreasing function of $x > 0$, and let μB denote the Lebesgue measure of a measurable set $B \subset \mathbb{R}$. Let $\mathcal{L}_1(\psi)$ denote the set of real numbers in the interval $I \subset \mathbb{R}$ such that the inequality

$$\left| x - \frac{p}{q} \right| < \frac{\psi(q)}{q} \tag{1}$$

has infinitely many solutions in integers $p \in \mathbb{Z}$ and positive integers $q \in \mathbb{N}$.

Theorem 1 (Khintchine's theorem). *The Lebesque measure of the set* $\mathcal{L}_1(\psi)$ *satisfies*

$$\mu\mathcal{L}_1(\psi) = 0 \textit{ if } \sum_{q=1}^{\infty} \psi(q) < \infty, \tag{2}$$

$$\mu\mathcal{L}_1(\psi) = \mu I \textit{ if } \sum_{q=1}^{\infty} \psi(q) = \infty. \tag{3}$$

Note that in the case of convergence (2) the theorem also holds without the monotonicity requirement on the function $\psi(x)$. Khintchine's theorem was later generalised by A. V. Groshev for system of linear forms [8].

One important generalisation of the above setting considered by A. Khintchine concerns small values of integral polynomials, see articles [3; 5] and monographs [4; 9–11]. In particular, in [12] A. Khintchine proved the following theorem.

Theorem 2. *For all* $\varepsilon > 0$ *and an arbitrary interval I, the inequality*

$$\left|P(x)\right| < \varepsilon H^{-n} \tag{4}$$

has infinitely many solutions in polynomials

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ P(x) \in \mathbb{Z}[x],$$

of degree n and height $H = H(P) = \max_{0 \le j \le n} \left|a_j\right|$ *for almost all points* $x \in I$.

Clearly, we can find $x \in \mathbb{R}$ such that for $\varepsilon = \varepsilon(x)$ the inequality opposite to (4) is satisfied. Taking, for example, $x_1 = \sqrt[n+1]{2}$, we have

$$\left|P(x_1)\right| > c(n)H^{-n}$$

for an appropriate positive constant $c(n)$.

The inequality (4) can be viewed as the first result in metric Diophantine approximation of dependent variables since it relates to approximation of zero by values of an integer polynomial of an arbitrary degree.

In what follows, $c_1 = c_1(n),\ c_2,\ \ldots$ will denote quantities that depend on n and do not depend on H. Quantities A and B satisfy the inequality $A \ll B$, where $\ll$ is the Vinogradov symbol, if there exists a constant c such that $A < cB$.

In 1932 Kurt Mahler [13] proposed his classification of real and complex numbers based on the behaviour of best polynomial approximations of zero $P(\xi)$ and $P(z)$ as the height H tends to infinity at respectively real and complex points $\xi \in \mathbb{R}$, $z \in \mathbb{C}$. A detailed description of Mahler's classification can be found in Sprindžuk's [3; 4], Schmidt's [14] and Bugeaud's [15] monographs. K. Mahler divided the set of real numbers into four classes, namely the *A*-, *S*-, *T*- and *U*-numbers. He formulated the famous Mahler's conjecture, which became the main problem in metric theory of Diophantine approximations for several decades.

Let $M_n(w)$ be the set of real numbers $x \in I$ such that the inequality

$$\left|P(x)\right| < H^{-w},\ w > 0,$$

has infinitely many solutions in polynomials $P(x) \in \mathbb{Z}[x]$, $\deg P = n$.

Conjecture (Mahler's conjecture). For $w > n$ we have $\mu M_n(w) = 0$.

For complex numbers, conjecture 1 can be formulated as follows: define the set $\mathcal{K}_n(v)$ of $z \in \mathbb{C}$ such that the inequality $\left|P(z)\right| < H^{-v}$ has infinitely many solutions in $P(z) \in \mathbb{Z}[z]$, then for $v > \frac{n-1}{2}$ we have $\mu_2 \mathcal{K}_n(v) = 0$, where μ_2 is the two-dimensional Lebesgue measure on the complex plane $\mathbb{C}$.

Mahler's problem can also be formulated in terms of simultaneous Diophantine approximation: let $S_n(t)$, $t > 0$, be the set of real numbers x such that the inequality

$$\max_{1 \le l \le n} \left|qx^l - p_l\right| < q^{-t},\ t > n^{-1}, \tag{5}$$

has infinitely many solutions in integer vectors $\overline{m} = (q, p_1, \ldots, p_n)$, then $\mu S_n(t) = 0$.

The two formulations are equivalent by Khintchine's transference principle [10]; the equality $\mu M_n(w) = 0$ implies that $\mu S_n(t) = 0$ and vice versa.

K. Mahler was able to prove that $\mu M_n(w) = 0$ for $w > 4n$, with other researchers offering consecutive improvements: $w > 3n$ by Jurjen Koksma [16], $w \le 2$ by William LeVeque [17]; $w \le 2 - \frac{2}{n}$ by Friedrich Kasch and Bodo Volkmann [18]; $w \le 2 - \frac{7}{3n}$ by Wolfgang Schmidt [19]; $w \le \frac{3}{2}$, $w \le \frac{4}{3}$ by B. Volkmann [20] using Davenport's lemma [21].

The first proof of Mahler's conjecture for $n = 2$ was obtained by academician J. Kubilius for the inequality (5) using the method developed by academician Ivan Vinogradov [1; 22].

From Minkowski's linear forms theorem we see that the system of Diophantine inequalities

$$\max\left(\|xq\|,\ \left\|x^2 q\right\|\right) < q^{-1/2}$$

has infinitely many solutions for all $x \in \mathbb{R}$ and positive integers $q \in \mathbb{N}$. However, if we slightly reduce the order of the right-hand side to obtain

$$\max\left(\|xq\|,\ \left\|x^2 q\right\|\right) < q^{-1/2-\varepsilon},$$

then this new inequality has, for an arbitrarily small positive ε, only a finite number of solutions for almost all x. This result was proved by J. Kubilius in 1949 [1], thus proving Mahler's conjecture in the quadratic case. Soon thereafter John William Scott Cassels [23] obtained an improvement of Kubilius's result, proving that the system of inequalities

$$\|xq\| < \varphi(q), \ \|x^2q\| < f(q)$$

has a finite number of solutions in $q \in \mathbb{N}$ for almost all x if the series

$$\sum_{q=1}^{\infty} \varphi(q) f(q)$$

converges and

$$f(q) \geq \max\left(\varphi(q),\ q^{-1/2} \log q \sigma(q)\right),$$

where $\sigma(q)$ is the number of positive integer divisors of q. In 1959 J. Kubilius improved this result by relaxing the requirements on $\max\left(\varphi(q),\ f(q)\right)$, proving the following theorem [2].

Theorem 3. *The inequality*

$$\max\left(\|xq\|, \ \|x^2q\|\right) < \psi(q)$$

has only a finite number of solutions in $q \in \mathbb{N}$ for a positive function $\psi(q)$ if $q^{-1/2}\psi(q)$ is non-increasing and the series

$$\sum_{q=1}^{\infty} q^{-1/2} \psi(q)$$

converges.

In a private conversation with the V. Bernik, J. Kubilius mentioned that he had obtained the proof of Leveque's result prior to the publication of Leveque's paper, but J. Kubilius wasn't expedient in publishing this proof.

Mahler's problem was solved in 1964 by Belarusian mathematician V. Sprindžuk, a pupil of J. Kubilius. V. Sprindžuk proved Mahler's conjecture not only in the fields $\mathbb{R}$ and $\mathbb{C}$, but also reformulated and proved it for p-adic numbers and formal power series. V. Sprindžuk laid down the groundworks of metric theory of Diophantine approximation, publishing two monographs in Russian and English [4; 11].

The next few sections of this article will be devoted to solutions and generalisations of the problems that were posed in the 1950–60s and were related to Koksma's and Mahler's classifications, as well as the classical problems of Vladimir Sprindžuk, Alan Baker and Wolfgang Schmidt [24]. After that, we'll move on to applications of the methods of metric theory of Diophantine approximation to quantifying distributions of rational and algebraic numbers, as well as discriminants and resultants of integer polynomials.

To conclude the article, we will touch upon applications of Diophantine approximation in mathematical physics and wireless communications.

Generalisations of the Mahler – Sprindžuk problem

Several results related to Mahler's conjecture have been improved and generalised. In particular, a full analogue of Khintchine's theorem was proved for the inequalities (2) and (3). Let $\mathcal{L}_n(\psi)$ denote the set of $x \in I$ such that the inequality

$$|P(x)| < H^{-n+1}\psi(H)$$

has infinitely many solutions in polynomials $P(x) \in \mathbb{Z}[x]$ of degree n and height $H = H(P)$.

Theorem 4. *The Lebesgue measure of the set $\mathcal{L}_n(\psi)$ is*

$$\mu\mathcal{L}_n(\psi) = 0 \text{ if } \sum_{H=1}^{\infty} \psi(H) < \infty, \tag{6}$$

$$\mu\mathcal{L}_n(\psi) = \mu I \text{ if } \sum_{H=1}^{\infty} \psi(H) = \infty. \tag{7}$$

The equality (6) was proved by Vasili Bernik in the paper [25], and (7) was proved by Victor Beresnevich in [26]. In the case of convergence (6), theorem 4 also holds if the monotonicity requirement on $\psi(H)$ is omitted [27], as will be discussed later on. Analogues of theorem 4 also hold in the complex case [28], the p-adic case [29; 30], and in the case of approximation by algebraic numbers [15; 31; 32]. Many of these results have become parts of monographs [4; 11; 33].

Let $f_1(x), \ldots, f_n(x) \in C^{n+1}(I)$ be $n+1$ times continuously differentiable functions of the real variable $x \in I$ such that their Wronskian is non-zero,

$$W(x) = \begin{vmatrix} f_1'(x) & f_2'(x) & \ldots & f_n'(x) \\ f_1''(x) & f_2''(x) & \ldots & f_n''(x) \\ \ldots & \ldots & \ldots & \ldots \\ f_1^{(n)}(x) & f_2^{(n)}(x) & \ldots & f_n^{(n)}(x) \end{vmatrix} \neq 0, \tag{8}$$

for almost all $x \in I$. Let $\mathcal{K}_n(\psi)$ denote the set of $x \in I$ such that the inequality

$$|F(x)| = |a_n f_n(x) + \ldots + a_1 f_1(x) + a_0| < H^{-n+1}\psi_1(H)$$

has infinitely many solutions, where H is the «height» of the function $F(x)$ defined as $\max\limits_{0 \le j \le n} |a_j|$. W. Schmidt [19] proved that for $\psi_1(H) = H^{-\gamma}$, $\gamma > 1$, we have the equality $\mu\mathcal{K}_2(\psi_1) = 0$. The paper [34] proves this result for $n = 3$.

V. Sprindžuk conjectured [4] that for an arbitrary n and $\psi_1(H) = H^{-\gamma}$, $\gamma > 1$, we have $\mu\mathcal{K}_n(\psi_1) = 0$. This conjecture was proved by Dmitry Kleinbock and Grigori Margulis [35]. Soon thereafter, the following theorem was proved for a curve $S(x) = (f_1(x), \ldots, f_n(x))$ satisfying the condition (8).

Theorem 5. *The measure of $\mathcal{K}_n(\psi)$ is given as*

$$\mu\mathcal{K}_n(\psi) = 0 \textit{ if } \sum_{H=1}^{\infty} \psi(H) < \infty, \tag{9}$$

$$\mu\mathcal{K}_n(\psi) = \mu I \textit{ if } \sum_{H=1}^{\infty} \psi(H) = \infty. \tag{10}$$

The equality (9) was independently proved by V. Beresnevich [36] and V. Bernik, D. Kleinbock and G. Margulis [37], and (10) was proved by the latter authors in [38]. Several related results in metric theory of Diophantine approximation are presented in monographs [4; 11; 15; 33; 39–41] and the article [42].

Diophantine approximation and the Hausdorff dimension

A natural next step in metric theory of Diophantine approximation was generalisation of the inequalities (1) to $|xq - p| < q^{-s}$, $s > 1$, and $|P(x)| < H^{-w}$, $w > n$.

For $s > 1$ and $w > n$ theorems 4 and 5 yield the equality $\mu\mathcal{K}_n(\psi) = 0$, i. e. the sets $\mathcal{K}_n(\psi)$ are indistinguishable in terms of the Lebesgue measure. This motivated researchers to study the Hausdorff dimension of these sets.

Vojtěch Jarnik [43] and Abram Besicovitch [44] independently proved that

$$\dim \mathcal{K}_1(q^{-s}) = \frac{2}{s+1}.$$

In the paper [24] A. Baker and W. Schmidt considered, in addition to the set $\mathcal{K}_n(\psi)$, the set $\mathcal{T}_n(v)$, $v > n+1$, of real numbers $x \in I$ such that the inequality

$$|x - \alpha| < H^{-v}, \ v > n+1,$$

has infinitely many solutions in algebraic numbers α of degree at most n and height at most $H = H(\alpha)$. They introduced the concept of a regular system and proved the following theorem.

Theorem 6. *The following equalities hold*

$$\dim \mathcal{T}_n(v) = \frac{n+1}{v},$$

$$\frac{n+1}{w+1} \le \dim \mathcal{K}_n(w) \le 2\frac{n+1}{w+1}. \tag{11}$$

Theorem 6 was strengthened in [45], where the upper estimate in (11) was replaced by $\frac{n+1}{w+1}$, thus proving the equality

$$\dim \mathcal{K}_n(w) = \frac{n+1}{w+1}.$$

In the paper [46], Yuri Melnichuk obtained estimates for the Hausdorff dimension of the set of points in the unit circle and the unit sphere with a given order of approximation by rational numbers.

Theorem 6 was generalised for the field of p-adic numbers [47]. Later, regular systems have been constructed in the space $\mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p$ from the result [48] and its generalisations [49].

The concept of regular systems of points introduced by A. Baker and W. Schmidt in [24] led to lower bounds for the Hausdorff dimensions of sets of real numbers where an integer polynomial and its derivative provide a given order of approximation of zero. Note that problems related to the Hausdorff measure are closely related to Wirsing's conjecture [50; 51].

A collection of papers by Detta Dickinson, Maurice Dodson, Victor Beresnevich, Vasily Bernik and Sanju Velani [33; 52; 53] introduced the concept of ubiquitous systems, which are in many aspects similar to regular systems. This concept was used to prove lower bounds for the Hausdorff dimension of the sets of real points related to theorem 5.

Interesting facts related to Hausdorff measure of Diophantine sets were obtained by Bryan Rynne [54]. It turns out that in certain cases the Hausdorff dimension is independent of the measure of solutions of Diophantine inequalities.

Let $\overline{\tau} = (\tau_1, \ldots, \tau_n) \in \mathbb{R}_+^n$ and $\tau_1 \geq \ldots \geq \tau_n$, $\sum_{i=1}^{n} \tau_i \geq n$.

Let $W_n(\tau) = \left\{x \in \mathbb{R}^n : |qx_i - p_i| < q^{-\tau_i},\ 1 \leq i \leq n, \text{ for infinitely many } (p, q) \in \mathbb{Z}^n \times \mathbb{N}\right\}$.

Then

$$\dim W_n(\tau) = \min_{1 \leq j \leq n} \frac{n + 1 + \sum_{i=j+1}^{n} (\tau_j - \tau_i)}{\tau_j + 1}.$$

For $n = 2$, Rynne's theorem was generalised for rational approximation of the points of the curve $f \in C^{(3)}(I_0)$ defined on an interval I_0:

$$C_f = \left\{(x, f(x)) : x \in I_0\right\}.$$

Let $\overline{\tau} = (\tau_1, \tau_2)$, where τ_1 and τ_2 are positive numbers such that $0 < \min(\tau_1, \tau_2) < 1$ and $\tau_1 + \tau_2 \geq 1$. Assume that

$$\dim\left\{x \in I_0 : f''(x) = 0\right\} \leq \frac{2 - \min(\tau_1, \tau_2)}{1 + \max(\tau_1, \tau_2)}.$$

Then

$$\dim W_2(\overline{\tau}) \cap C_f = \frac{2 - \min(\tau_1, \tau_2)}{1 + \max(\tau_1, \tau_2)}.$$

Similar results have been obtained for approximation by real algebraic numbers [15; 55].

Victor Beresnevich and Evgeni Zorin proved the following fact [56].

Let M be a twice continuously differentiable submanifold of $\mathbb{R}^n$ of codimension m, and let

$$\frac{1}{n} \leq \tau \leq \frac{1}{m}.$$

Then

$$\dim S_n(\tau) \cap M \geq s := \frac{n+1}{\tau + 1} - m.$$

Furthermore,

$$H^s(S_n(\tau) \cap M) = H^s(M).$$

Recently, Victor Beresnevich, Robert Vaughan, Sanju Velani and Evgeni Zorin [57] worked on finding an upper bound on the quantity of rational points within a ψ-neighbourhood of manifolds. Using this result, they proved the following theorem.

Theorem 7. *Let $M_f \subset \mathbb{R}^n$ be a manifold defined on an open subset $U \subset \mathbb{R}^d$, and let*

$$H^s\left(\left\{\alpha \in U : \left|\det\left(\frac{\partial^2 f_j}{\partial\alpha_i \partial\alpha_j}\right)_{1 \le i,\, j \le n}\right| = 0\right\}\right) = 0$$

for $s = \dfrac{n+1}{\tau+1} - m.$

If $d > \dfrac{n+1}{2}$ *and* $\dfrac{1}{n} \le \tau \le \dfrac{1}{2m+1}$, *then*

$$\dim S_n(\tau) \cap M_f \le s.$$

Generalisations of this result have been obtained by David Simmons and Jing-Jing Huang [58; 59].

Theorem 8. *Let* $M := \left\{(x,\ f(x)) : x \in U \subset \mathbb{R}^d\right\}$, *where* $f : U \to \mathbb{R}^m,\ f \in C^{(2)}$. *Let* $\overline{\tau} = (\tau_1, \tau_2, \ldots, \tau_n) \in \mathbb{R}^n_{>0}$ *with*

$$\tau_1 \ge \ldots \ge \tau_d \ge \max_{d+1 \le i \le n}\left\{\tau_i,\ \frac{1 - \sum_{j=1}^{n-m}\tau_{j+d}}{d}\right\} \text{ and } \sum_{i=1}^{m}\tau_{d+i} < 1.$$

Then

$$\dim\left(W_n(\tau) \cap M\right) \ge \min_{1 \le j \le d}\left\{\frac{n + 1 + \sum_{i=j}^{m}\left(\tau_j - \tau_i\right)}{\tau_j + 1} - m\right\}.$$

Along with the result of V. Beresnevich and E. Zorin, this yields the exact value of $\dim\left(W_n(\tau) \cap M\right)$. The proofs are based on the mass transference principle developed by V. Beresnevich and S. Velani [60].

Let us note several other notable results on Hausdorff dimension of sets of numbers with various Diophantine properties. Irina Morotskaya generalised the Baker – Schmidt – Bernik theorem for the field of *p*-adic numbers [47], and Dickinson and Dodson proved a generalisation of this theorem for non-degenerate curves [53]. In 2017 Victor Beresnevich, Jung-Jo Lee and Robert Vaughan proved a sharp lower bound for a set of τ-approximable numbers in a C^2 submanifold of $\mathbb{R}^n$ for $\dfrac{1}{n} \le \tau < \dfrac{1}{m}$. Rynne's result was improved in a paper by Konstantin Yavid [61].

Results of this section were strengthened and generalised over the last few years [54; 59; 60; 62–71].

Diophantine approximation in complex and *p*-adic cases

In Sprindžuk's monograph [4], Mahler's problem was generalised to the fields of complex and *p*-adic numbers. Generalisations of Khintchine's theorem for complex numbers were obtained by Denis Vasilyev [28]. Diophantine approximation in the field $\mathbb{C}$ was studied in the papers by Irina Morozova [72], Dmitry Kleinbock and George Tomanov [73], Natalia Sakovich [74]. An in-depth discussion of simultaneous Diophantine approximation can be found in [62]. The main results of these papers are complete analogues of Khintchine's theorem and the Jarnik – Besicovitch theorem for weighted simultaneous Diophantine approximation in the *p*-adic case, as well as a lower bound for the Hausdorff dimension of weighted simultaneously approximable points on *p*-adic curves [75].

Simultaneous Diophantine approximation

The results that gave rise to metric theory of Diophantine approximation were the Khintchine – Groshev theorem and Mahler's problem. J. Kubilius obtained a complete solution of Mahler's problem for $n = 2$ by first considering simultaneous approximation of a parabola by rational points in $\mathbb{R}^2$ and applying Khintchine's transference principle [10].

The next major problem in simultaneous approximation was posed by V. Sprindžuk [3; 4].

For a fixed vector $\overline{x} = (x_1, \ldots, x_k) \in \mathbb{R}^k$, $1 \le k \le n$, let $w \le w_n(x)$ be the exact upper bound of positive $w_1 > 0$ such that the system of inequalities

$$\max_{1 \le j \le k}\left(\left|P\left(x_j\right)\right| < H^{-w_1}\right)$$

has infinitely many solutions in polynomials $P(t) \in \mathbb{Z}[x]$ of degree $\deg P = n$ and height $H(P) = H$. V. Sprindžuk conjectured that $w = \frac{n-k+1}{k}$, which was proved in [76]. In 1980 V. Sprindžuk [5] posed a problem of approximating points in the space $\Omega = \mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p = \{(x, z, \omega)\}$ by algebraic numbers from $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}_p$. He assumed that the following statement was true. Let μ_1 be the Lebesgue measure in $\mathbb{R}$ and $\mathbb{C}$, and μ_2 be the Haar measure in $\mathbb{Q}_p$. For almost all $\bar{u} = (x, z, \omega)$ (with respect to the product measure $\mu_1 \times \mu_2$) the system of inequalities

$$|P(x)| < H^{-v_1},\ |P(z)| < H^{-v_2},\ |P(\omega)| < H^{-v_3},$$

where $v_j \geq -1$, $j = 1, 2$, $v_3 \geq 0$, has only a finite number of solutions in polynomials $P(t) \in \mathbb{Z}[t]$.

This conjecture was proved by Frantz Želudevič [77]. The next major step was generalisation of the Želudevič's results to systems of inequalities where the right-hand sides are arbitrary functions $\psi(H)$. Analogues of Khintchine's theorem were proved for both convergence and divergence cases [78–80].

Of particular interest is the paper [81] that made use of Kleinbock and Margulis's method [49; 68; 70; 71; 76; 78; 79; 82–92].

A number of papers in theory of Diophantine approximations are devoted to studying the distances between conjugate algebraic numbers. The papers [88; 92] can be considered as an introduction to this topic. In the paper [93] Victor Beresnevich, Vasili Bernik and Friedrich Götze applied methods of metric theory of Diophantine approximation to such problems. It was proved that the inequality $|\alpha_1 - \alpha_2| \ll Q^{(n+1)/3}$ not only has a solution in algebraic conjugate numbers α_1 and α_2 of degree n and height $H(\alpha_1) = H(\alpha_2) = Q$, but also the number of the respective minimal polynomials was estimated from below by $c(n)Q^{(n+1)/3}$. This method was generalised for the distribution of polynomial root clusters [93; 94].

Distribution of rational points close to curves and surfaces

In [1; 2] J. Kubilius showed how estimates of the number of rational points close to a parabola $G_2 = (x, x^2)$ lead to a proof of Mahler's conjecture for $n = 2$. The proof was based on Khintchine's transference principle [10]. It turned out that metric theorems concerned with estimation of a dot product between an integer vector $\bar{a} = (a_n, \ldots, a_1, a_0)$ and a vector-function $F(x) = (f_n(x), \ldots, f_1(x), 1)$ are stronger than metric theorems in simultaneous Diophantine approximation, which is implied by certain results from geometry of numbers and dynamical system theory [35]. In 1994 Martin Huxley [95] proved a theorem on distribution of rational numbers close to smooth curves, estimating the number $N_f(Q, \delta, J) := \#\left\{\left(\frac{p_1}{q}, \frac{p_2}{q}\right) \in \mathbb{Q}^2 : \frac{p_1}{q} \in J, \left|f\left(\frac{p_1}{q}\right) - \frac{p_2}{q}\right| \leq \delta, 0 < q < Q\right\}$.

Let $I \subset \mathbb{R}$ be a compact interval, c_1 and c_2 be positive constants, and let $F(I; c_1, c_2)$ be the set of functions $f: I \to \mathbb{R}$, $f \in C^{(2)}$, such that

$$c_1 \leq |f''(x)| \leq c_2 \ \forall x \in I.$$

M. Huxley proved that

$$N_f(Q, \delta, I) \ll_\delta c^{10/3}\delta^{1-\delta}Q^2 + c^{1/3},\ c = \max(c_2, c_1^{-1}).$$

For $\delta > Q^{2/3}$, Huxley's result was improved in [52; 55; 56], where it was shown that for any $f \in F(I; c_1, c_2)$, any $Q > 1$ and $0 < \delta < \frac{1}{2}$, we have

$$N_f(Q, \delta, I) \ll \delta Q^2 + \delta^{-1/2}Q.$$

Later the quantity $N_f(Q, \delta, I)$ was estimated from below, and from above and below in the non-homogeneous case [1; 52; 53; 81].

Distribution of algebraic numbers

Distribution of rational numbers in real intervals is quite well-studied and can be described through Farey sequences. However, until recently, not much was known about distribution of algebraic numbers, even if their degrees were small. In 1985 V. Bernik was shown a letter from K. Mahler to V. Sprindžuk, where K. Mahler expressed his surprise about the many unanswered questions related to distribution of algebraic numbers both on the real line and in the complex plane. It wasn't until the 2010s that Denis Koleda began to solve the problems posed by K. Mahler [96–100]. Let us discuss the main results that he obtained.

Let A_n be the set of real algebraic numbers of degree n, and let the counting function of such algebraic numbers of height at most Q in the interval I be defined as

$$\Phi_n(Q, I) := \#\{\alpha \in A_n \cap I : H(\alpha) \leq Q\}.$$

Theorem 9 [99; 100]. *There exists a continuous positive function* $\varphi_n(x)$ *such that for any interval* $I \subseteq \mathbb{R}$, *we have*

$$\Phi_n(Q,\ I) = \frac{Q^{n+1}}{2\zeta(n+1)} \int_I \varphi_n(x)\,dx + O\left(Q^n (\ln Q)^{l(n)}\right),$$

where $l(n) = 0$ *for* $n \geq 3$, $l(n) = 1$ *for* $n = 2$ *and the implicit constant in the big-O notation only depends on n.*

The function $\varphi_n(x)$ can be defined explicitly. The remainder term in theorem 9 was shown to be sharp [96], up to a constant, for all n. Further studies of the distribution of algebraic numbers by Denis Koleda, Friedrich Götze and Dmitri Zaporozhets [97] led to the following description of the density of points with algebraically conjugate coordinates in the space $\mathbb{R}^k \times \mathbb{C}^l$.

Let $A_n(k,\ l)$ be the set of points in the space $\mathbb{R}^k \times \mathbb{C}^l$ such that their coordinates are roots of the same irreducible integral polynomial of degree n (i. e. k real and l complex conjugate algebraic numbers of degree n over $\mathbb{Q}$). Let us define a function

$$\Phi_{k,\,l}(Q,\ B) := \{\alpha \in A_n(k,\ l) \cap B : H(\alpha) \leq Q\}$$

for $Q \geq 1$ and $B \subset \mathbb{R}^k \times \mathbb{C}^l$.

Theorem 10 [97]. *Let* $B \subset \mathbb{R}^k \times \mathbb{C}^l$ *be a region such that its boundary* ∂B *is contained in a finite union of Lipschitz transformations of the cube* $[0,\ 1]^{k+2l-1}$. *Then*

$$\left| \frac{\Phi_{k,\,l}(Q,\ B)}{Q^{n+1}} - \frac{\mathrm{Vol}(B_H)}{2\zeta(n+1)} \int_B \rho_{k,\,l}(v)\,dv \right| \leq \begin{cases} cQ^{-1} \log Q, \text{ if } n = 2 \text{ and } l = 0, \\ cQ^{-1} \text{ otherwise,} \end{cases}$$

where $\rho_{k,\,l} : \mathbb{R}^k \times \mathbb{C}^l \to \mathbb{R}$ *is an explicitly defined continuous non-negative function, dv is a volume element in the space* $\mathbb{R}^k \times \mathbb{C}^l$ *(considered as* $\mathbb{R}^{k+2l}$*),* $\zeta(\cdot)$ *is the Riemann zeta function, and* $\mathrm{Vol}(B_H)$ *is the volume of an* $(n+1)$*-dimensional region* B_H *which is the cube* $[-1,\ 1]^{n+1}$ *in the case when H is the naive height.*

Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a continuously differentiable function on a finite interval $J \subset \mathbb{R}$, and let $\alpha = (\alpha_1,\ \alpha_2)$ be a point with algebraically conjugate coordinates such that the minimal polynomial of α_1, α_2 is of degree $\leq n$ and height $\leq Q$. Denote by $M_\varphi^n(Q,\ \gamma,\ J)$ the set of points α such that $|\varphi(\alpha_1) - \alpha_2| \leq c_1(n) Q^{-\gamma}$. We show for $0 < \gamma < 1$ and any sufficiently large Q there exist positive values $c_2 < c_3$, where $c_i = c_i(n)$, $i = 2, 3, \ldots$, that are independent of Q and the following estimate holds [22; 24; 94; 98–103]

$$c_2 Q^{n+1-\gamma} < \# M_\varphi^n(Q,\ \gamma,\ J) < c_3 Q^{n+1-\gamma}.$$

The Mahler – Sprindžuk problem with a non-monotonic right-hand side

It is well known that in the case of convergence, the Khintchine – Groshev theorem also holds for non-monotonic functions $\psi(q)$. A number of researchers have posed other problems in Diophantine approximation with non-monotonic functions in the right-hand side. Generally, the solution then depends on convergence or divergence of the Khintchine-type series with $\psi(q)$ replaced by a different function. For the Mahler – Sprindžuk problem, V. Beresnevich showed in 2005 [27] that the theorem holds for a non-monotonic function $\psi(q)$.

In the papers [104; 105] Natalia Budarina generalised Beresnevich's result for the fields of complex and p-adic numbers, as well as non-degenerate curves. She used Sprindžuk's method, imposing progressively lower bounds on the size of the derivative, and finally applying Kleinbock and Marguli's method for the smallest derivatives [106].

Inhomogeneous Diophantine approximation

The results of the previous sections may be viewed as approximation of zero by values of linear combinations of the form $F(x) = a_n f_n(x) + \ldots + a_1 f_1(x) + a_0 \cdot 1$ that are homogeneous with respect to functions $f_n(x), \ldots, f_1(x), f_0(x) \equiv 1$. Minkowski's theorems on linear forms and successive minima provide a powerful mechanism for solving this type of problems [10; 14; 15; 19]. However, these methods have very limited utility for derivation of upper and lower bounds if the function $F(x)$ assumes the form $P_1(x) = a_n x^n + \ldots + a_1 x + a_0 + \pi$ or $P_2(x) = a_n x^n + \ldots + a_1 x + a_0 + \sin x$. These latter problems are known as inhomogeneous Diophantine approximation. A number of metric theorems related to a wide range of functions of the form $P_1(x)$ and $P_2(x)$ have been proved to date [60; 106–110].

Applications of metric theory of Diophantine approximation

The earlies applications of Diophantine approximation to celestial mechanics are probably due to Karl Siegel, who mentions them in his lecture notes. Vladimir Arnold [111] used the Khintchine – Groshev theorem during the development of Kolmogorov – Arnold – Moser theory to prove that almost all celestial systems similar to the Solar system are stable. Systematic application of metric theory of Diophantine approximation in small denominator problems in equations of mathematical physics is described in Ptashnik's monograph [112].

In 2021 a textbook dedicated to applications of metric theory of Diophantine approximation in wireless communications is due to be published by Springer Verlag. Let us point out the articles [31; 113–116] which can be regarded as an introduction to this field of applications, as well as the article by Victor Beresnevich and Sanju Velani, Faustin Adiceam, Jason Levesley and Evgeni Zorin [31] explaining the main ideas behind applications of Diophantine approximation to radio engineering [117; 118].

Biography

Academician J. Kubilius was born in Fermos village, Jurbarkas district of Lithuania. In 1940 he graduated from a grammar school in Raseiniai, in 1946 graduated from Vilnius University, and finished his postgraduate studies at Leningrad University in 1951 under scientific supervision of academician Yuri Linnik. At the age of 36 J. Kubilius successfully defended his doctor of science thesis. Between 1958 and 1992 he was the rector of Vilnius University.

J. Kubilius was the scientific advisor of Belarusian mathematicians Vladimir Sprindžuk (full member of the Academy of Sciences of BSSR) and Nikolai Lazakovich (doctor of science). The academic school of number theory in Belarus, which has 5 doctor of science degree holders and over 40 PhDs degree holders, owes a lot to the work of J. Kubilius. He was the scientific advisor of Ramunė Sliesoraitiene [119], whose PhDs thesis was devoted to metric theory of Diophantine approximation. He was an opponent during thesis defenses of Belarusian mathematicians Vasili Bernik, Ella Kovalevskaya, Vladimir Mashanov.

A full list of scientific degrees and honors of academician J. Kubilius takes up an entire printed page. For more details, we refer the reader to the article [120].

Библиографические ссылки

1. Кубилюс ЙП. О применении метода академика Виноградова к решению одной задачи метрической теории чисел. *Доклады Академии наук СССР.* 1949;67:783–786.

2. Кубилюс ЙП. Об одной метрической проблеме теории диофантовых приближений. *Доклады Академии наук Литовской ССР.* 1959;2:3–7.

3. Спринджук ВГ. Доказательство гипотезы Малера о мере множества *S*-чисел. *Известия Академии наук СССР. Серия математическая.* 1965;29(2):379–436.

4. Спринджук ВГ. *Проблема Малера в метрической теории чисел.* Минск: Наука и техника; 1967. 181 с.

5. Спринджук ВГ. Достижения и проблемы теории диофантовых приближений. *Успехи математических наук.* 1980;35(4): 3–68.

6. Borel MÈ. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo (1884–1940).* 1909;27:247–271. DOI: 10.1007/bf03019651.

7. Khintchine A. Einige Sätze über Kettenbrüche, mit Anwendungen auf die Theorie der diophantischen Approximationen. *Mathematische Annalen.* 1924;92:115–125.

8. Грошев АВ. Теорема о системе линейных форм. *Доклады Академии наук СССР.* 1938;19:151–152.

9. Harman G. *Metric Number Theory.* Oxford: Clarendon Press; 1998. 297 p. (London Mathematical Society monographs; new series 18).

10. Cassels JWS. *An introduction to Diophantine approximation.* 1st edition. Cambridge: Cambridge University Press; 1957. 166 p. (Cambridge tracts in mathematics and mathematical physics; No. 45).

11. Sprindžuk VG. *Mahler's problem in metric number theory.* Volkmann B, translator. Providence: American Mathematical Society; 1969. 192 p. (Translations of mathematical monographs; volume 25).
12. Khintchine A. Zwei Bemerkungen zu einer Arbeit des Herrn Perron. *Mathematische Zeitschrift.* 1925;22:274–284. DOI: 10.1007/bf01479606.
13. Mahler K. Über das Maß der Menge aller *S*-Zahlen. *Mathematische Annalen.* 1932;106:131–139.
14. Schmidt WM. Bounds for certain sums; a remark on a conjecture of Mahler. *Transactions of the American Mathematical Society.* 1961;101(2):200–210. DOI: 10.1090/s0002-9947-1961-0132036-2.
15. Bugeaud Y. *Approximation by algebraic numbers*. Cambridge: Cambridge University Press; 2004. 290 p. (Cambridge tracts in mathematics; volume 160). DOI: 10.1017/CBO9780511542886.
16. Koksma JF. Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen. *Monatshefte für Mathematik.* 1939;48(1):176–189. DOI: 10.1007/bf01696176.
17. LeVeque WJ. Note on *S*-numbers. *Proceedings of the American Mathematical Society.* 1953;4:189–190. DOI: 10.1090/s0002-9939-1953-0054659-2.
18. Kasch F, Volkmann B. Zur Mahlerschen Vermutung über *S*-Zahlen. *Mathematische Annalen.* 1958;136(5):442–453. DOI: 10.1007/BF01347794.
19. Schmidt WM. Metrische Sätze über simultane Approximation abhängiger Größen. *Monatshefte für Mathematik.* 1964;68(2):154–166. DOI: 10.1007/bf01307118.
20. Volkmann B. The real cubic case of Mahler's conjecture. *Mathematika.* 1961;8(1):55–57. DOI: 10.1112/s0025579300002126.
21. Davenport H. A note on binary cubic forms. *Mathematika.* 1961;8(1):58–62. DOI: 10.1112/s0025579300002138.
22. Bernik V, Götze F, Gusakova A. On points with algebraically conjugate coordinates close to smooth curves. *Записки научных семинаров ПОМИ.* 2016;448:14–47.
23. Cassels JWS. Some metrical theorems in Diophantine approximation: v. on a conjecture of Mahler. *Mathematical Proceedings of the Cambridge Philosophical Society.* 1951;47(1):18–21. DOI: 10.1017/s0305004100026323.
24. Baker A, Schmidt WM. Diophantine approximation and Hausdorff dimension. *Proceedings of the London Mathematical Society.* 1970;s3-21(1):1–11. DOI: 10.1112/plms/s3-21.1.1.
25. Берник В. О точном порядке приближения нуля значениями целочисленных многочленов. *Acta Arithmetica.* 1989–1990; 53(1):17–28.
26. Beresnevich V. On approximation of real numbers by real algebraic numbers. *Acta Arithmetica.* 1999;90(2):97–112. DOI: 10.4064/aa-90-2-97-112.
27. Beresnevich V. On a theorem of V. Bernik in the metric theory of Diophantine approximation. *Acta Arithmetica.* 2005;117(1): 71–80. DOI: 10.4064/aa117-1-4.
28. Берник ВИ, Васильев ДВ. Теорема типа Хинчина для целочисленных многочленов комплексной переменной. *Труды Института математики НАН Беларуси.* 1999;3:10–20.
29. Beresnevich VV, Bernik VI, Kovalevskaya EI. On approximation of *p*-adic numbers by *p*-adic algebraic numbers. *Journal of Number Theory.* 2005;111(1):33–56. DOI: 10.1016/j.jnt.2004.09.007.
30. Mohammadi A, Golsefidy AS. *S*-arithmetic Khintchine-type theorem. *Geometric and Functional Analysis.* 2009;19(4):1147–1170. DOI: 10.1007/s00039-009-0029-z.
31. Adiceam F, Beresnevich V, Levesley J, Velani S, Zorin E. Diophantine approximation and applications in interference alignment. *Advances in Mathematics.* 2016;302:231–279. DOI: 10.1016/j.aim.2016.07.002.
32. Берник ВИ, Шамукова НВ. Приближение действительных чисел целыми алгебраическими числами и теорема Хинчина. *Доклады Национальной академии наук Беларуси.* 2006;50(3):30–32.
33. Bernik VI, Dodson MM. *Metric Diophantine approximation on manifolds*. Cambridge: Cambridge University Press; 1999. 172 p. (Cambridge tracts in mathematics; volume 137). DOI: 10.1017/CBO9780511565991.
34. Beresnevich V, Bernik V. On a metrical theorem of W. Schmidt. *Acta Arithmetica.* 1996;75(3):219–233. DOI: 10.4064/aa-75-3-219-233.
35. Kleinbock DY, Margulis GA. Flows on homogeneous spaces and Diophantine approximation on manifolds. *Annals of Mathematics.* 1998;148(1):339–360. DOI: 10.2307/120997.
36. Beresnevich V. A Groshev type theorem for convergence on manifolds. *Acta Mathematica Hungarica.* 2002;94(1–2):99–130. DOI: 10.1023/A:1015662722298.
37. Bernik V, Kleinbock D, Margulis G. Khintchine-type theorems on manifolds: the convergence case for standard and multiplicative versions. *International Mathematics Research Notices.* 2001;2001(9):453–486. DOI: 10.1155/S1073792801000241.
38. Beresnevich VV, Bernik VI, Kleinbock DYa, Margulis GA. Metric Diophantine approximation: the Khintchine – Groshev theorem for non-degenerate manifolds. *Moscow Mathematical Journal.* 2002;2(2):203–225. DOI: 10.17323/1609-4514-2002-2-2-203-225.
39. Baker A. On a theorem of Sprindžuk. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences.* 1966;292(1428):92–104. DOI: 10.1098/rspa.1966.0121.
40. Koksma JF. *Diophantische approximationen.* Berlin: Springer; 1974. 172 p. (Ergebnisse der Mathematik und ihrer Grenzgebiete; volume 4). DOI: 10.1007/978-3-642-65618-7.
41. Allen D, Beresnevich V. A mass transference principle for systems of linear forms and its applications. *Compositio Mathematica.* 2018;154(5):1014–1047. DOI: 10.1112/s0010437x18007121.
42. Берник ВИ, Васильев ДВ, Засимович ЕВ. Диофантовы приближения с постоянной правой частью неравенств на коротких интервалах. *Доклады Национальной академии наук Беларуси.* 2021;65(4):397–403. DOI: 10.29235/1561-8323-2021-65-4-397-403.
43. Jarnik V. Diophantische approximationen und Hausdorffsches mass. *Математический сборникъ.* 1929;36(3–4):371–382.
44. Besicovitch AS. Sets of fractional dimensions (IV): on rational approximation to real numbers. *Journal of the London Mathematical Society.* 1934;s1-9(2):126–131. DOI: 10.1112/jlms/s1-9.2.126.
45. Берник ВИ. Применение размерности Хаусдорфа в теории диофантовых приближений. *Acta Arithmetica.* 1983;42:219–253. DOI: 10.4064/aa-42-3-219-253.
46. Мельничук ЮВ. Диофантовы приближения на окружности и размерность Хаусдорфа. *Математические заметки.* 1979; 26(3):347–354.

47. Берник ВИ, Моротская ИЛ. Диофантовы приближения в $\mathbb{Q}_p$ и размерность Хаусдорфа. *Весцi Нацыянальнай акадэмii навук Беларусi. Серыя фiзiка-матэматычных навук.* 1986;3:3–9.
48. Берник ВИ, Калоша НИ. Приближение нуля значениями целочисленных полиномов в пространстве $\mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p$. *Весцi Нацыянальнай акадэмii навук Беларусi. Серыя фiзiка-матэматычных навук.* 2004;1:121–123.
49. Бударина НВ. Метрическая теория совместных диофантовых приближений в $\mathbb{R}^k \times \mathbb{C}^l \times \mathbb{Q}_p^m$. *Чебышевский сборник. Посвящается 65-й годовщине со дня рождения профессора Сергея Михайловича Воронина.* 2011;12(1):17–50.
50. Badziahin D, Schleischitz J. An improved bound in Wirsing's problem. *Transactions of the American Mathematical Society.* 2021;374:1847–1861. DOI: 10.1090/tran/8245.
51. Берник ВИ, Тищенко КИ. Целочисленные многочлены с перепадами высот коэффициентов и гипотеза Вирзинга. *Доклады Национальной академии наук Беларуси.* 1993;37(5):9–11.
52. Beresnevich V, Dickinson D, Velani S. Diophantine approximation on planar curves and the distribution of rational points (with an Appendix by R. C. Vaughan). *Annals of Mathematics.* 2007;166(2):367–426. DOI: 10.4007/annals.2007.166.367.
53. Dickinson H, Dodson MM. Extremal manifolds and Hausdorff dimension. *Duke Mathematical Journal.* 2000;101(2):271–281. DOI: 10.1215/S0012-7094-00-10126-3.
54. Rynne BP. Simultaneous Diophantine approximation on manifolds and Hausdorff dimension. *Journal of Number Theory.* 2003; 98(1):1–9. DOI: 10.1016/s0022-314x(02)00035-5.
55. Кудин АС, Луневич АВ. Аналог теоремы Хинчина в случае расходимости в полях действительных, комплексных и p-адических чисел. *Труды Института математики.* 2015;23(1):76–83.
56. Beresnevich V, Zorin E. Explicit bounds for rational points near planar curves and metric Diophantine approximation. *Advances in Mathematics.* 2010;225(6):3064–3087. DOI: 10.1016/j.aim.2010.05.021.
57. Beresnevich V, Vaughan RC, Velani S, Zorin E. Diophantine approximation on manifolds and the distribution of rational points: contributions to the convergence theory. *International Mathematics Research Notices.* 2017;2017(10):2885–2908. DOI: 10.1093/imrn/rnv389.
58. Huang J-J. The density of rational points near hypersurfaces. *Duke Mathematical Journal.* 2020;169(11):2045–2077. DOI: 10.1215/00127094-2020-0004.
59. Simmons D. Some manifolds of Khinchin type for convergence. *Journal de Théorie des Nombres de Bordeaux.* 2018;30(1): 175–193. DOI: 10.5802/jtnb.1021.
60. Beresnevich V, Velani S. An inhomogeneous transference principle and Diophantine approximation. *Proceedings of the London Mathematical Society.* 2010;101(3):821–851. DOI: 10.1112/plms/pdq002.
61. Явид КЮ. Оценка размерности Хаусдорфа множеств сингулярных векторов. *Доклады Академии наук БССР.* 1987; 31(9):777–780.
62. Beresnevich V, Levesley J, Ward B. A lower bound for the Hausdorff dimension of the set of weighted simultaneously approximable points over manifolds. *International Journal of Number Theory.* 2021;17(8):1795–1814. DOI: 10.1142/S1793042121500639.
63. Bernik VI. Applications of measure theory and Hausdorff dimension to the theory of Diophantine approximation. *New advances in transcendence theory.* 1988:25–36. DOI: 10.1017/CBO9780511897184.003.
64. Берник ВИ. Применение размерности Хаусдорфа в теории диофантовых приближений. *Acta Arithmetica*. 1983;42:219–253.
65. Beresnevich V, Lee L, Vaughan RC, Velani S. Diophantine approximation on manifolds and lower bounds for Hausdorff dimension. *Mathematika.* 2017;63(3):762–779. DOI: 10.1112/s0025579317000171.
66. Bernik VI, Pereverseva NA. The method of trigonometric sums and lower estimates of Hausdorff dimension. *Analytic and Probabilistic Methods in Number Theory.* 1992;2:75–81. DOI: 10.1515/9783112314234-011.
67. Bugeaud Y. Approximation by algebraic integers and Hausdorff dimension. *Journal of the London Mathematical Society.* 2002; 65(3):547–559. DOI: 10.1112/S0024610702003137.
68. Beresnevich VV, Velani SL. A note on simultaneous Diophantine approximation on planar curves. *Mathematische Annalen.* 2007;337(4):769–796. DOI: 10.1007/s00208-006-0055-1.
69. Бересневич ВВ. Применение понятия регулярных систем точек в метрической теории чисел. *Весцi Нацыянальнай акадэмii навук Беларусi. Серыя фiзiка-матэматычных навук.* 2000;1:35–39.
70. Бересневич ВВ. О построении регулярных систем точек с вещественными, комплексными и p-адическими алгебраическими координатами. *Весцi Нацыянальнай акадэмii навук Беларусi. Серыя фiзiка-матэматычных навук.* 2003;1:22–27.
71. Kovalevskaya EI, Bernik V. Simultaneous inhomogeneous Diophantine approximation of the values of integral polynomials with respect to Archimedean and non-Archimedean valuations. *Acta Mathematica Universitatis Ostraviensis.* 2006;14(1):37–42.
72. Бернiк ВI, Марозава IМ. Гiпотэза Бэйкера i рэгулярныя сiстэмы алгебраiчных лiчбаў з абмежаваннем на значэнне вытворнай. *Весцi Нацыянальнай акадэмii навук Беларусi. Серыя фiзiка-матэматычных навук.* 1996;3:109–113.
73. Kleinbock D, Tomanov G. Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation. *Commentarii Mathematici Helvetici.* 2007;82(3):519–581. DOI: 10.4171/cmh/102.
74. Берник ВИ, Сакович НВ. Регулярные системы комплексных алгебраических чисел. *Доклады Академии наук Беларуси.* 1994;38(5):10–13.
75. Бересневич ВВ, Ковалевская ЭИ. О диофантовых приближениях зависимых величин в p-адическом случае. *Математические заметки.* 2003;25(1):22–37. DOI: 10.4213/mzm165.
76. Берник ВИ. Метрическая теорема о совместном приближении нуля значениями целочисленных многочленов. *Известия Академии наук СССР. Серия математическая.* 1980;44(1):24–45.
77. Želudevič F. Simultane diophantische Approximationen abhängiger Größen in mehreren Metriken. *Acta Arithmetica.* 1986; 46(3):285–296. DOI: 10.4064/aa-46-3-285-296.
78. Bernik V, Budarina N, Dickinson D. A divergent Khintchine theorem in the real, complex, and p-adic fields. *Lithuanian Mathematical Journal.* 2008;48(2):158–173. DOI: 10.1007/s10986-008-9005-9.
79. Budarina N, Dickinson D, Bernik V. Simultaneous Diophantine approximation in the real, complex and p-adic fields. *Mathematical Proceedings of the Cambridge Philosophical Society.* 2010;149(2):193–216. DOI: 10.1017/s0305004110000162.
80. Домбровский ИР. Совместные приближения действительных чисел алгебраическими числами ограниченной степени. *Доклады Академии наук БССР.* 1989;33(3):205–208.
81. Beresnevich V. Rational points near manifolds and metric Diophantine approximation. *Annals of Mathematics.* 2012;175(1): 187–235. DOI: 10.4007/annals.2012.175.1.5.

82. Beresnevich VV, Velani SL. Simultaneous inhomogeneous Diophantine approximation on manifolds. *Journal of Mathematical Sciences*. 2012;180(5):531–541. DOI: 10.1007/s10958-012-0651-4.

83. Budarina N, Dickinson D, Levesley J. Simultaneous Diophantine approximation on polynomial curves. *Mathematika.* 2010; 56(1):77–85. DOI: 10.1112/s0025579309000382.

84. Budarina N. On a problem of Bernik, Kleinbock and Margulis. *Glasgow Mathematical Journal.* 2011;53(3):669–681. DOI: 10.1017/s0017089511000255.

85. Budarina N, Dickinson D. Simultaneous Diophantine approximation in two metrics and the distance between conjugate algebraic numbers in $\mathbb{R} \times \mathbb{Q}_p$. *Indagationes Mathematicae.* 2012;23(1–2):32–41. DOI: 10.1016/j.indag.2011.09.012.

86. Берник ВИ, Борбат ВН. Совместная аппроксимация нуля значениями целочисленных полиномов. *Труды Математического института имени В. А. Стеклова.* 1997;218:58–73.

87. Bernik VI, Budarina N, O'Donnell H. On regular systems of real algebraic numbers of third degree in short intervals. *Современные проблемы математики.* 2013;17:61–75. DOI: 10.4213/spm43.

88. Bugeaud Y, Mignotte M. Polynômes à coefficients entiers prenant des valeurs positives aux points réels. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie.* 2010;53(3):219–224.

89. Bernik V, Götze F. A new connection between metric theory of Diophantine approximations and distribution of algebraic numbers. *Contemporary Mathematics.* 2015;631:33–45. DOI: 10.1090/conm/631/12594.

90. Бударина НВ. Совместные диофантовы приближения с немонотонными правыми частями. *Доклады Академии наук.* 2011;437(4):441–443.

91. Bernik V, Mc Guire S. How small can polynomials be in an interval of given length? *Glasgow Mathematical Journal.* 2020; 62(2):261–280. DOI: 10.1017/S0017089519000077.

92. Bugeaud Y, Mignotte M. Polynomial root separation. *International Journal of Number Theory.* 2010;6(3):587–602. DOI: 10.1142/s1793042110003083.

93. Beresnevich V, Bernik V, Götze F. The distribution of close conjugate algebraic numbers. *Compositio Mathematica.* 2010; 146(5):1165–1179. DOI: 10.1112/S0010437X10004860.

94. Bernik V, Budarina N, O'Donnell H. Discriminants of polynomials in the Archimedean and non-Archimedean metrics. *Acta Mathematica Hungarica.* 2018;154(2):265–278. DOI: https://doi.org/10.1007/s10474-018-0794-y.

95. Huxley MN. The rational points close to a curve. *Annali della Scuola Normale Superiore di Pisa. Classe di Scienze. Série 4.* 1994;21(3):357–375.

96. Коледа ДВ. Об асимптотике распределения алгебраических чисел при возрастании их высот. *Чебышевский сборник.* 2015;16(1):191–204. DOI: 10.22405/2226-8383-2015-16-1-191-204.

97. Götze F, Koleda D, Zaporozhets D. Joint distribution of conjugate algebraic numbers: a random polynomial approach. *Advances in Mathematics.* 2020;359:106849. DOI: 10.1016/j.aim.2019.106849.

98. Лебедь ВВ, Берник ВИ. Алгебраические точки на плоскости. *Фундаментальная и прикладная математика.* 2005; 11(6):73–80.

99. Коледа ДВ. О распределении вещественных алгебраических чисел второй степени. *Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук.* 2013;3:54–63.

100. Koleda D. On the density function of the distribution of real algebraic numbers. *Journal de Théorie des Nombres de Bordeaux.* 2017;29(1):179–200. DOI: 10.5802/jtnb.975.

101. Берник ВИ, Гётце Ф, Калоша НИ. О количестве алгебраических чисел в коротких интервалах, содержащих рациональные точки. *Журнал Белорусского государственного университета. Математика. Информатика.* 2019;1:4–11. DOI: 10.33581/2520-6508-2019-1-4-11.

102. Бударина НВ, Диккинсон Д, Берник ВИ. Оценки снизу для количества векторов с алгебраическими координатами вблизи гладких поверхностей. *Доклады Национальной академии наук Беларуси.* 2020;64(1):7–12. DOI: 10.29235/1561-8323-2020-64-1-7-12.

103. Bernik VI, Götze F. Distribution of real algebraic numbers of arbitrary degree in short intervals. *Izvestiya: Mathematics.* 2015;79(1):18–39. DOI: 10.1070/im2015v079n01abeh002732.

104. Budarina N, Dickinson D. Diophantine approximation on non-degenerate curves with non-monotonic error function. *Bulletin of the London Mathematical Society.* 2009;41(1):137–146. DOI: 10.1112/blms/bdn116.

105. Budarina N. Diophantine approximation on the curves with non-monotonic error function in the *p*-adic case. *Чебышевский сборник.* 2010;11(1):74–80.

106. Badziahin D, Beresnevich V, Velani S. Inhomogeneous theory of dual Diophantine approximation on manifolds. *Advances in Mathematics.* 2013;232(1):1–35. DOI: 10.1016/j.aim.2012.09.022.

107. Badziahin D. Inhomogeneous Diophantine approximation on curves and Hausdorff dimension. *Advances in Mathematics.* 2010;223(1):329–351. DOI: 10.1016/j.aim.2009.08.005.

108. Bernik V, Dickinson H, Yuan J. Inhomogeneous Diophantine approximation on polynomials in $\mathbb{Q}_p$. *Acta Arithmetica.* 1999; 90(1):37–48. DOI: 10.4064/aa-90-1-37-48.

109. Beresnevich V, Ganguly A, Ghosh A, Velani S. Inhomogeneous dual Diophantine approximation on affine subspaces. *International Mathematics Research Notices.* 2020;12:3582–3613. DOI: 10.1093/imrn/rny124.

110. Beresnevich VV, Vaughan RC, Velani SL. Inhomogeneous Diophantine approximation on planar curves. *Mathematische Annalen.* 2011;349(4):929–942. DOI: 10.1007/s00208-010-0548-9.

111. Арнольд ВИ. Малые знаменатели и проблемы устойчивости движения в классической и небесной механике. *Успехи математических наук.* 1963;18(6):91–192.

112. Пташник БИ. *Некорректные граничные задачи для дифференциальных уравнений с частными производными.* Киев: Наукова думка; 1984. 264 с.

113. Cadambe VR, Jafar SA. Interference alignment and degrees of freedom of the *K*-user interference channel. *IEEE Transactions on Information Theory.* 2008;54(8):3425–3441. DOI: 10.1109/TIT.2008.926344.

114. Jafar SA. Interference alignment: a new look at signal dimensions in a communication network. *Foundations and Trends in Communications and Information Theory.* 2011;7(1):1–134. DOI: 10.1561/0100000047.

115. Jafar SA, Shamai Sh. Degrees of freedom region of the MIMO *X* channel. *IEEE Transactions on Information Theory.* 2008; 54(1):151–170. DOI: 10.1109/tit.2007.911262.

116. Beresnevich V, Velani S. Number theory meets wireless communications: an introduction for dummies like us. In: Beresnevich V, Burr A, Nazer B, Velani S, editors. *Number theory meets wireless communications.* [S. l.]: Springer International Publishing; 2020. p. 1–67. DOI: 10.1007/978-3-030-61303-7_1.

117. Budarina N, O'Donnell H. On a problem of Nesterenko: when is the closest root of a polynomial a real number? *International Journal of Number Theory.* 2012;8(3):801–811. DOI: 10.1142/s1793042112500455.

118. Motahari AS, Oveis-Gharan S, Maddah-Ali MA, Khandani AK. Real interference alignment: exploiting the potential of single antenna systems. *IEEE Transactions on Information Theory.* 2014;60(8):4799–4810. DOI: 10.1109/tit.2014.2329865.

119. Слесорайтене Р. Теорема Малера – Спринджука для полиномов третьей степени от двух переменных. (II). *Литовский математический сборник.* 1970;10:791–814.

120. Manstavičius E. Jonas Kubilius 1921–2011. *Lithuanian Mathematical Journal.* 2021;61:285–288. DOI: 10.1007/s10986-021-09522-z.

References

1. Kubilius JP. [On application of Academician Vinogradov's method to solving a certain problem in metric number theory]. *Doklady Akademii nauk SSSR.* 1949;67:783–786. Russian.

2. Kubilius JP. [On a metrical problem in Diophantine approximation theory]. *Doklady Akademii nauk Litovskoi SSR.* 1959;2:3–7. Russian.

3. Sprindžuk VG. [Proof of Mahler's conjecture on the measure of the set of *S*-numbers]. *Izvestiya Akademii nauk SSSR. Seriya matematicheskaya.* 1965;29(2):379–436. Russian.

4. Sprindžuk VG. *Problema Malera v metricheskoi teorii chisel* [Mahler's problem in metric number theory]. Minsk: Nauka i tekhnika; 1967. 181 p. Russian.

5. Sprindžuk VG. [Advances and problems in the theory of Diophantine approximation]. *Uspekhi matematicheskikh nauk.* 1980; 35(4):3–68. Russian.

6. Borel MÈ. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo (1884–1940).* 1909;27:247–271. DOI: 10.1007/bf03019651.

7. Khintchine A. Einige Sätze über Kettenbrüche, mit Anwendungen auf die Theorie der diophantischen Approximationen. *Mathematische Annalen.* 1924;92:115–125.

8. Groshev AV. [Theorem on a system of linear forms]. *Doklady Akademii nauk SSSR*. 1938;19:151–152. Russian.

9. Harman G. *Metric number theory.* Oxford: Clarendon Press; 1998. 297 p. (London Mathematical Society monographs; new series 18).

10. Cassels JWS. *An introduction to Diophantine approximation*. 1st edition. Cambridge: Cambridge University Press; 1957. 166 p. (Cambridge tracts in mathematics and mathematical physics; No. 45).

11. Sprindžuk VG. *Mahler's problem in metric number theory.* Volkmann B, translator. Providence: American Mathematical Society; 1969. 192 p. (Translations of mathematical monographs; volume 25).

12. Khintchine A. Zwei Bemerkungen zu einer Arbeit des Herrn Perron. *Mathematische Zeitschrift.* 1925;22:274–284. DOI: 10.1007/bf01479606.

13. Mahler K. Über das Maß der Menge aller *S*-Zahlen. *Mathematische Annalen.* 1932;106:131–139.

14. Schmidt WM. Bounds for certain sums; a remark on a conjecture of Mahler. *Transactions of the American Mathematical Society.* 1961;101(2):200–210. DOI: 10.1090/s0002-9947-1961-0132036-2.

15. Bugeaud Y. *Approximation by algebraic numbers*. Cambridge: Cambridge University Press; 2004. 290 p. (Cambridge tracts in mathematics; volume 160). DOI: 10.1017/CBO9780511542886.

16. Koksma JF. Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen. *Monatshefte für Mathematik.* 1939;48(1):176–189. DOI: 10.1007/bf01696176.

17. LeVeque WJ. Note on *S*-numbers. *Proceedings of the American Mathematical Society.* 1953;4:189–190. DOI: 10.1090/s0002-9939-1953-0054659-2.

18. Kasch F, Volkmann B. Zur Mahlerschen Vermutung über *S*-Zahlen. *Mathematische Annalen.* 1958;136(5):442–453. DOI: 10.1007/BF01347794.

19. Schmidt WM. Metrische Sätze über simultane Approximation abhängiger Größen. *Monatshefte für Mathematik.* 1964;68(2): 154–166. DOI: 10.1007/bf01307118.

20. Volkmann B. The real cubic case of Mahler's conjecture. *Mathematika.* 1961;8(1):55–57. DOI: 10.1112/s0025579300002126.

21. Davenport H. A note on binary cubic forms. *Mathematika.* 1961;8(1):58–62. DOI: 10.1112/s0025579300002138.

22. Bernik V, Götze F, Gusakova A. On points with algebraically conjugate coordinates close to smooth curves. *Zapiski nauchnykh seminarov POMI.* 2016;448:14–47.

23. Cassels JWS. Some metrical theorems in Diophantine approximation: v. on a conjecture of Mahler. *Mathematical Proceedings of the Cambridge Philosophical Society.* 1951;47(1):18–21. DOI: 10.1017/s0305004100026323.

24. Baker A, Schmidt WM. Diophantine approximation and Hausdorff dimension. *Proceedings of the London Mathematical Society.* 1970;s3-21(1):1–11. DOI: 10.1112/plms/s3-21.1.1.

25. Bernik V. [On the exact order of approximation of zero by values of integer polynomials]. *Acta Arithmetica.* 1989–1990;53(1): 17–28. Russian.

26. Beresnevich V. On approximation of real numbers by real algebraic numbers. *Acta Arithmetica.* 1999;90(2):97–112. DOI: 10.4064/aa-90-2-97-112.

27. Beresnevich V. On a theorem of V. Bernik in the metric theory of Diophantine approximation. *Acta Arithmetica.* 2005;117(1): 71–80. DOI: 10.4064/aa117-1-4.

28. Bernik VI, Vasilyev DV. [A Khintchine-type theorem for integer polynomials with a complex variable]. *Trudy Instituta matematiki NAN Belarusi*. 1999;3:10–20. Russian.

29. Beresnevich VV, Bernik VI, Kovalevskaya EI. On approximation of *p*-adic numbers by *p*-adic algebraic numbers. *Journal of Number Theory.* 2005;111(1):33–56. DOI: 10.1016/j.jnt.2004.09.007.

30. Mohammadi A, Golsefidy AS. *S*-arithmetic Khintchine-type theorem. *Geometric and Functional Analysis.* 2009;19(4):1147–1170. DOI: 10.1007/s00039-009-0029-z.

31. Adiceam F, Beresnevich V, Levesley J, Velani S, Zorin E. Diophantine approximation and applications in interference alignment. *Advances in Mathematics.* 2016;302:231–279. DOI: 10.1016/j.aim.2016.07.002.

32. Bernik VI, Shamukova NV. [Approximation of real numbers by integer algebraic numbers, and the Khintchine's theorem]. *Doklady of the National Academy of Sciences of Belarus.* 2006;50(3):30–32. Russian.

33. Bernik VI, Dodson MM. *Metric Diophantine approximation on manifolds*. Cambridge: Cambridge University Press; 1999. 172 p. (Cambridge tracts in mathematics; volume 137). DOI: 10.1017/CBO9780511565991.

34. Beresnevich V, Bernik V. On a metrical theorem of W. Schmidt. *Acta Arithmetica.* 1996;75(3):219–233. DOI: 10.4064/aa-75-3-219-233.

35. Kleinbock DY, Margulis GA. Flows on homogeneous spaces and Diophantine approximation on manifolds. *Annals of Mathematics.* 1998;148(1):339–360. DOI: 10.2307/120997.

36. Beresnevich V. A Groshev type theorem for convergence on manifolds. *Acta Mathematica Hungarica.* 2002;94(1–2):99–130. DOI: 10.1023/A:1015662722298.

37. Bernik V, Kleinbock D, Margulis G. Khintchine-type theorems on manifolds: the convergence case for standard and multiplicative versions. *International Mathematics Research Notices.* 2001;2001(9):453–486. DOI: 10.1155/S1073792801000241.

38. Beresnevich VV, Bernik VI, Kleinbock DYa, Margulis GA. Metric Diophantine approximation: the Khintchine – Groshev theorem for non-degenerate manifolds. *Moscow Mathematical Journal.* 2002;2(2):203–225. DOI: 10.17323/1609-4514-2002-2-2-203-225.

39. Baker A. On a theorem of Sprindžuk. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences.* 1966;292(1428):92–104. DOI: 10.1098/rspa.1966.0121.

40. Koksma JF. *Diophantische approximationen.* Berlin: Springer; 1974. 172 p. (Ergebnisse der Mathematik und ihrer Grenzgebiete; volume 4). DOI: 10.1007/978-3-642-65618-7.

41. Allen D, Beresnevich V. A mass transference principle for systems of linear forms and its applications. *Compositio Mathematica.* 2018;154(5):1014–1047. DOI: 10.1112/s0010437x18007121.

42. Bernik VI, Vasilyev DV, Zasimovich EV. Diophantine approximation with the constant right-hand side of inequalities on short intervals. *Doklady of the National Academy of Sciences of Belarus.* 2021;65(4):397–403. Russian. DOI: 10.29235/1561-8323-2021-65-4-397-403.

43. Jarnik V. Diophantische approximationen und Hausdorffsches mass. *Matematicheskii sbornik'.* 1929;36(3–4):371–382.

44. Besicovitch AS. Sets of fractional dimensions (IV): on rational approximation to real numbers. *Journal of the London Mathematical Society.* 1934;s1-9(2):126–131. DOI: 10.1112/jlms/s1-9.2.126.

45. Bernik VI. [Application of the Hausdorff dimension in the theory of Diophantine approximation]. *Acta Arithmetica.* 1983; 42:219–253. Russian. DOI: 10.4064/aa-42-3-219-253.

46. Melnichuk YuV. [Diophantine approximation on a circle and the Hausdorff dimension]. *Matematicheskie zametki.* 1979;26(3): 347–354. Russian.

47. Bernik VI, Morotskaya IL. [Diophantine approximation in $\mathbb{Q}_p$ and the Hausdorff dimension]. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series.* 1986;3:3–9. Russian.

48. Bernik VI, Kalosha NI. Approximation of zero by values of integer polynomials in the space $\mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p$. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2004;1:121–123. Russian.

49. Budarina NV. [Metric theory of simultaneous Diophantine approximation in $\mathbb{R}^k \times \mathbb{C}^l \times \mathbb{Q}_p^m$]. *Chebyshevskii sbornik. Posvyashchaetsya 65-i godovshchine so dnya rozhdeniya professora Sergeya Mikhailovicha Voronina.* 2011;12(1):17–50. Russian.

50. Badziahin D, Schleischitz J. An improved bound in Wirsing's problem. *Transactions of the American Mathematical Society.* 2021;374:1847–1861. DOI: 10.1090/tran/8245.

51. Bernik VI, Tishchenko KI. [Integral polynomials with an overfall of the coefficient values and Wirsing's theorem]. *Doklady of the National Academy of Belarus.* 1993;37(5):9–11. Russian.

52. Beresnevich V, Dickinson D, Velani S. Diophantine approximation on planar curves and the distribution of rational points (with an Appendix by R. C. Vaughan). *Annals of Mathematics.* 2007;166(2):367–426. DOI: 10.4007/annals.2007.166.367.

53. Dickinson H, Dodson MM. Extremal manifolds and Hausdorff dimension. *Duke Mathematical Journal.* 2000;101(2):271–281. DOI: 10.1215/S0012-7094-00-10126-3.

54. Rynne BP. Simultaneous Diophantine approximation on manifolds and Hausdorff dimension. *Journal of Number Theory.* 2003; 98(1):1–9. DOI: 10.1016/s0022-314x(02)00035-5.

55. Kudin AS, Lunevich AV. [An analogue of Khintchine's theorem in the case of divergence in the fields of real, complex and *p*-adic numbers]. *Trudy Instituta matematiki.* 2015;23(1):76–83. Russian.

56. Beresnevich V, Zorin E. Explicit bounds for rational points near planar curves and metric Diophantine approximation. *Advances in Mathematics.* 2010;225(6):3064–3087. DOI: 10.1016/j.aim.2010.05.021.

57. Beresnevich V, Vaughan RC, Velani S, Zorin E. Diophantine approximation on manifolds and the distribution of rational points: contributions to the convergence theory. *International Mathematics Research Notices.* 2017;2017(10):2885–2908. DOI: 10.1093/imrn/rnv389.

58. Huang J-J. The density of rational points near hypersurfaces. *Duke Mathematical Journal.* 2020;169(11):2045–2077. DOI: 10.1215/00127094-2020-0004.

59. Simmons D. Some manifolds of Khinchin type for convergence. *Journal de Théorie des Nombres de Bordeaux.* 2018;30(1): 175–193. DOI: 10.5802/jtnb.1021.

60. Beresnevich V, Velani S. An inhomogeneous transference principle and Diophantine approximation. *Proceedings of the London Mathematical Society.* 2010;101(3):821–851. DOI: 10.1112/plms/pdq002.

61. Yavid KYu. [An estimate for the Hausdorff dimension of sets of singular vectors]. *Doklady Akademii nauk BSSR.* 1987;31(9): 777–780. Russian.

62. Beresnevich V, Levesley J, Ward B. A lower bound for the Hausdorff dimension of the set of weighted simultaneously approximable points over manifolds. *International Journal of Number Theory.* 2021;17(8):1795–1814. DOI: 10.1142/S1793042121500639.

63. Bernik VI. Applications of measure theory and Hausdorff dimension to the theory of Diophantine approximation. *New advances in transcendence theory.* 1988:25–36. DOI: 10.1017/CBO9780511897184.003.

64. Bernik VI. [Application of Hausdorff dimension in the theory of Diophantine approximations]. *Acta Arithmetica*. 1983;42: 219–253. Russian.

65. Beresnevich V, Lee L, Vaughan RC, Velani S. Diophantine approximation on manifolds and lower bounds for Hausdorff dimension. *Mathematika.* 2017;63(3):762–779. DOI: 10.1112/s0025579317000171.

66. Bernik VI, Pereverseva NA. The method of trigonometric sums and lower estimates of Hausdorff dimension. *Analytic and Probabilistic Methods in Number Theory.* 1992;2:75–81. DOI: 10.1515/9783112314234-011.

67. Bugeaud Y. Approximation by algebraic integers and Hausdorff dimension. *Journal of the London Mathematical Society.* 2002; 65(3):547–559. DOI: 10.1112/S0024610702003137.

68. Beresnevich VV, Velani SL. A note on simultaneous Diophantine approximation on planar curves. *Mathematische Annalen.* 2007;337(4):769–796. DOI: 10.1007/s00208-006-0055-1.

69. Beresnevich VV. Application of the consept of regular systems in the Metric theory of numbers. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2000;1:35–39. Russian.

70. Beresnevich VV. [On construction of regular systems of points with real, complex and *p*-adic algebraic coordinates]. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 2003;1:22–27. Russian.

71. Kovalevskaya EI, Bernik V. Simultaneous inhomogeneous Diophantine approximation of the values of integral polynomials with respect to Archimedean and non-Archimedean valuations. *Acta Mathematica Universitatis Ostraviensis.* 2006;14(1):37–42.

72. Bernik VI, Marozava IM. Baker's conjecture and regular sets of algebraic numbers with a restriction on the value of the derivative. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*. 1996;3:109–113. Belarusian.

73. Kleinbock D, Tomanov G. Flows on *S*-arithmetic homogeneous spaces and applications to metric Diophantine approximation. *Commentarii Mathematici Helvetici.* 2007;82(3):519–581. DOI: 10.4171/cmh/102.

74. Bernik VI, Sakovich NV. Regular systems of complex algebraic numbers. *Doklady Akademii nauk Belarusi.* 1994;38(5):10–13. Russian.

75. Beresnevich VV, Kovalevskaya EI. [On Diophantine approximation of dependent variables in the *p*-adic case]. *Matematicheskie zametki.* 2003;25(1):22–37. Russian. DOI: 10.4213/mzm165.

76. Bernik VI. [A metric theorem on the simultaneous approximation of a zero by the values of integral polynomials]. *Izvestiya Akademii nauk SSSR. Seriya matematicheskaya.* 1980;44(1):24–45. Russian.

77. Želudevič F. Simultane diophantische Approximationen abhängiger Größen in mehreren Metriken. *Acta Arithmetica.* 1986; 46(3):285–296. DOI: 10.4064/aa-46-3-285-296.

78. Bernik V, Budarina N, Dickinson D. A divergent Khintchine theorem in the real, complex, and *p*-adic fields. *Lithuanian Mathematical Journal.* 2008;48(2):158–173. DOI: 10.1007/s10986-008-9005-9.

79. Budarina N, Dickinson D, Bernik V. Simultaneous Diophantine approximation in the real, complex and *p*-adic fields. *Mathematical Proceedings of the Cambridge Philosophical Society.* 2010;149(2):193–216. DOI: 10.1017/s0305004110000162.

80. Dombrovskii IR. [Simultaneous approximation of real numbers by algebraic numbers of bounded degree]. *Doklady Akademii nauk BSSR.* 1989;33(3):205–208. Russian.

81. Beresnevich V. Rational points near manifolds and metric Diophantine approximation. *Annals of Mathematics.* 2012;175(1): 187–235. DOI: 10.4007/annals.2012.175.1.5.

82. Beresnevich VV, Velani SL. Simultaneous inhomogeneous Diophantine approximation on manifolds. *Journal of Mathematical Sciences*. 2012;180(5):531–541. DOI: 10.1007/s10958-012-0651-4.

83. Budarina N, Dickinson D, Levesley J. Simultaneous Diophantine approximation on polynomial curves. *Mathematika.* 2010; 56(1):77–85. DOI: 10.1112/s0025579309000382.

84. Budarina N. On a problem of Bernik, Kleinbock and Margulis. *Glasgow Mathematical Journal.* 2011;53(3):669–681. DOI: 10.1017/s0017089511000255.

85. Budarina N, Dickinson D. Simultaneous Diophantine approximation in two metrics and the distance between conjugate algebraic numbers in $\mathbb{R} \times \mathbb{Q}_p$. *Indagationes Mathematicae.* 2012;23(1–2):32–41. DOI: 10.1016/j.indag.2011.09.012.

86. Bernik VI, Borbat VN. [Joint approximation of zero by values of integer-valued polynomials]. *Trudy Matematicheskogo instituta imeni V. A. Steklova.* 1997;218:58–73. Russian.

87. Bernik VI, Budarina N, O'Donnell H. On regular systems of real algebraic numbers of third degree in short intervals. *Sovremennye problemy matematiki.* 2013;17:61–75. DOI: 10.4213/spm43.

88. Bugeaud Y, Mignotte M. Polynômes à coefficients entiers prenant des valeurs positives aux points réels. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie.* 2010;53(3):219–224.

89. Bernik V, Götze F. A new connection between metric theory of Diophantine approximations and distribution of algebraic numbers. *Contemporary Mathematics.* 2015;631:33–45. DOI: 10.1090/conm/631/12594.

90. Budarina NV. [Simultaneous Diophantine approximation with non-monotonic right-hand sides]. *Doklady Akademii nauk.* 2011; 437(4):441–443. Russian.

91. Bernik V, Mc Guire S. How small can polynomials be in an interval of given length? *Glasgow Mathematical Journal.* 2020; 62(2):261–280. DOI: 10.1017/S0017089519000077.

92. Bugeaud Y, Mignotte M. Polynomial root separation. *International Journal of Number Theory.* 2010;6(3):587–602. DOI: 10.1142/ s1793042110003083.

93. Beresnevich V, Bernik V, Götze F. The distribution of close conjugate algebraic numbers. *Compositio Mathematica.* 2010;146(5): 1165–1179. DOI: 10.1112/S0010437X10004860.

94. Bernik V, Budarina N, O'Donnell H. Discriminants of polynomials in the Archimedean and non-Archimedean metrics. *Acta Mathematica Hungarica.* 2018;154(2):265–278. DOI: https://doi.org/10.1007/s10474-018-0794-y.

95. Huxley MN. The rational points close to a curve. *Annali della Scuola Normale Superiore di Pisa. Classe di Scienze. Sérіe 4.* 1994;21(3):357–375.

96. Koleda DV. On the asymptotic distribution of algebraic numbers with growing naive height. *Chebyshevskii sbornik.* 2015; 16(1):191–204. Russian. DOI: 10.22405/2226-8383-2015-16-1-191-204.

97. Götze F, Koleda D, Zaporozhets D. Joint distribution of conjugate algebraic numbers: a random polynomial approach. *Advances in Mathematics.* 2020;359:106849. DOI: 10.1016/j.aim.2019.106849.

98. Lebed VV, Bernik VI. Algebraic points on a plane. *Fundamental'naya i prikladnaya matematika.* 2005;11(6):73–80. Russian.

99. Koleda DU. Distribution of the real algebraic numbers of second degree. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series.* 2013;3:54–63. Russian.

100. Koleda D. On the density function of the distribution of real algebraic numbers. *Journal de Théorie des Nombres de Bordeaux.* 2017;29(1):179–200. DOI: 10.5802/jtnb.975.

101. Bernik VI, Götze F, Kalosha NI. Counting algebraic numbers in short intervals with rational points. *Journal of the Belarusian State University. Mathematics and Informatics.* 2019;1:4–11. Russian. DOI: 10.33581/2520-6508-2019-1-4-11.

102. Budarina NV, Dickinson D, Bernik VI. Lower bounds for the number of vectors with algebraic coordinates near smooth surfaces. *Doklady of the National Academy of Sciences of Belarus.* 2020;64(1):7–12. Russian. DOI: 10.29235/1561-8323-2020-64-1-7-12.

103. Bernik VI, Götze F. Distribution of real algebraic numbers of arbitrary degree in short intervals. *Izvestiya: Mathematics.* 2015; 79(1):18–39. DOI: 10.1070/im2015v079n01abeh002732.

104. Budarina N, Dickinson D. Diophantine approximation on non-degenerate curves with non-monotonic error function. *Bulletin of the London Mathematical Society.* 2009;41(1):137–146. DOI: 10.1112/blms/bdn116.

105. Budarina N. Diophantine approximation on the curves with non-monotonic error function in the p-adic case. *Chebyshevskii sbornik.* 2010;11(1):74–80.

106. Badziahin D, Beresnevich V, Velani S. Inhomogeneous theory of dual Diophantine approximation on manifolds. *Advances in Mathematics.* 2013;232(1):1–35. DOI: 10.1016/j.aim.2012.09.022.

107. Badziahin D. Inhomogeneous Diophantine approximation on curves and Hausdorff dimension. *Advances in Mathematics.* 2010;223(1):329–351. DOI: 10.1016/j.aim.2009.08.005.

108. Bernik V, Dickinson H, Yuan J. Inhomogeneous Diophantine approximation on polynomials in $\mathbb{Q}_p$. *Acta Arithmetica.* 1999; 90(1):37–48. DOI: 10.4064/aa-90-1-37-48.

109. Beresnevich V, Ganguly A, Ghosh A, Velani S. Inhomogeneous dual Diophantine approximation on affine subspaces. *International Mathematics Research Notices.* 2020;12:3582–3613. DOI: 10.1093/imrn/rny124.

110. Beresnevich VV, Vaughan RC, Velani SL. Inhomogeneous Diophantine approximation on planar curves. *Mathematische Annalen.* 2011;349(4):929–942. DOI: 10.1007/s00208-010-0548-9.

111. Arnold VI. [Small denominators and problem of stability of motion in classical and celestial mechanics]. *Uspekhi matematicheskikh nauk.* 1963;18(6):91–192. Russian.

112. Ptashnik BI. *Nekorrektnye granichnye zadachi dlya differentsial'nykh uravnenii s chastnymi proizvodnymi* [Incorrectly defined boundary problems for partial differential equations]. Kyiv: Naukova dumka; 1984. 264 p. Russian.

113. Cadambe VR, Jafar SA. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Transactions on Information Theory.* 2008;54(8):3425–3441. DOI: 10.1109/TIT.2008.926344.

114. Jafar SA. Interference alignment: a new look at signal dimensions in a communication network*. Foundations and Trends in Communications and Information Theory.* 2011;7(1):1–134. DOI: 10.1561/0100000047.

115. Jafar SA, Shamai Sh. Degrees of freedom region of the MIMO X channel. *IEEE Transactions on Information Theory.* 2008; 54(1):151–170. DOI: 10.1109/tit.2007.911262.

116. Beresnevich V, Velani S. Number theory meets wireless communications: an introduction for dummies like us. In: Beresnevich V, Burr A, Nazer B, Velani S, editors. *Number theory meets wireless communications.* [S. l.]: Springer International Publishing; 2020. p. 1–67. DOI: 10.1007/978-3-030-61303-7_1.

117. Budarina N, O'Donnell H. On a problem of Nesterenko: when is the closest root of a polynomial a real number? *International Journal of Number Theory.* 2012;8(3):801–811. DOI: 10.1142/s1793042112500455.

118. Motahari AS, Oveis-Gharan S, Maddah-Ali MA, Khandani AK. Real interference alignment: exploiting the potential of single antenna systems. *IEEE Transactions on Information Theory.* 2014;60(8):4799–4810. DOI: 10.1109/tit.2014.2329865.

119. Sliesoraitienė R. Malerio – Sprindžiuko teoremos analogas trečio laipsnio dviejų kintamųjų polinomams. (II). *Lietuvos matematikos rinkinys.* 1970;10:791–814. Russian.

120. Manstavičius E. Jonas Kubilius 1921–2011. *Lithuanian Mathematical Journal.* 2021;61:285–288. DOI: 10.1007/s10986-021-09522-z.

Received 14.09.2021 / revised 21.10.2021 / accepted 09.11.2021.

УДК 519.217.2

О СЛУЧАЙНЫХ БЛУЖДАНИЯХ НА ГРАФАХ КЭЛИ ГРУПП КОМПЛЕКСНЫХ ОТРАЖЕНИЙ

М. М. ВАСЬКОВСКИЙ[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Исследуются асимптотические свойства случайных блужданий на минимальных графах Кэли групп комплексных отражений. Основным результатом является теорема о быстром перемешивании для случайных блужданий на графах Кэли групп комплексных отражений. В частности, ключевую роль играют оценки диаметров и изопериметрических постоянных таких графов, а также известный результат о быстром перемешивании для случайных блужданий на экспандерах. Приводится конструктивный способ доказательства частного случая гипотезы Бабаи о логарифмическом порядке диаметров для графов групп комплексных отражений. На основании оценки диаметров и неравенства Чигера получена нетривиальная оценка снизу для спектральных пробелов минимальных графов Кэли групп комплексных отражений.

Ключевые слова: группы комплексных отражений; графы Кэли; случайные блуждания; экспандеры.

Образец цитирования:
Васьковский ММ. О случайных блужданиях на графах Кэли групп комплексных отражений. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:51–56.
https://doi.org/10.33581/2520-6508-2021-3-51-56

For citation:
Vaskouski MM. Random walks on Cayley graphs of complex reflection groups. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:51–56. Russian.
https://doi.org/10.33581/2520-6508-2021-3-51-56

Автор:
Максим Михайлович Васьковский – доктор физико-математических наук, доцент; заведующий кафедрой высшей математики факультета прикладной математики и информатики.

Author:
Maksim M. Vaskouski, doctor of science (physics and mathematics), docent; head of the department of higher mathematics, faculty of applied mathematics and computer science.
vaskovskii@bsu.by
https://orcid.org/0000-0001-5769-3678

RANDOM WALKS ON CAYLEY GRAPHS OF COMPLEX REFLECTION GROUPS

M. M. VASKOUSKI [a]

[a] *Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

Asymptotic properties of random walks on minimal Cayley graphs of complex reflection groups are investigated. The main result of the paper is theorem on fast mixing for random walks on Cayley graphs of complex reflection groups. Particularly, bounds of diameters and isoperimetric constants, a known result on fast fixing property for expander graphs play a crucial role to obtain the main result. A constructive way to prove a special case of Babai's conjecture on logarithmic order of diameters for complex reflection groups is proposed. Basing on estimates of diameters and Cheeger inequality, there is obtained a non-trivial lower bound for spectral gaps of minimal Cayley graphs on complex reflection groups.

Keywords: complex reflection groups; Cayley graphs; random walks; expander graphs.

Введение

В последние десятилетия разработаны глубокие и оригинальные приложения графов-экспандеров в теории алгоритмов и, в частности, в криптографии и теории кодирования [1–3]. В настоящее время нет строгого и общепринятого математического определения экспандера. Под экспандером, как правило, понимают большой разреженный граф или последовательность таких графов, имеющие достаточно хорошие параметры спектрального расширения (в случае последовательностей графов требуется отделенность снизу от нуля изопериметрических постоянных). Графы Кэли на конечных неабелевых группах обычно обладают худшими параметрами спектрального расширения, но имеют несложную комбинаторную структуру и позволяют строить простые алгоритмы маршрутизации, что делает их удобным инструментом при реализации алгоритмов [4]. В настоящей статье исследуется вопрос о времени перемешивания случайных блужданий на графах Кэли групп комплексных отражений. Отметим, что группы комплексных отражений являются естественными обобщениями групп Коксетера [5] и имеют значительные применения, в частности, в дифференциальной геометрии [6]. Свойства случайных блужданий на графах групп Коксетера глубоко исследовались во многих работах, в том числе в публикациях [7; 8]. Однако случайные блуждания на графах групп комплексных отражений до сих пор остаются малоизученными. Поскольку изопериметрические постоянные таких графов не отделены снизу от нуля, то для получения необходимых оценок времени перемешивания случайных блужданий в настоящей статье исследуются диаметры и спектральные пробелы упомянутых графов.

Основные результаты

Рассмотрим семейство неприводимых групп комплексных отражений $G(m, p, n)$, $m, p, n \in \mathbb{N}$, $n > 2$, $p \mid m$. Каждая из групп $G(m, 1, n)$ является полупрямым произведением абелевой группы порядка m^n и симметрической группы S_n. В частности, $G(1, 1, n) = S_n$. При $p > 1$ группа $G(m, p, n)$ – это подгруппа индекса p группы $G(m, 1, n)$. Элементами группы $G(m, p, n)$ являются матрицы $w \in \mathbb{C}^{n \times n}$, у которых на позициях $(k, \tau(k))$, $k \in \{1, \ldots, n\}$, стоят элементы ξ^{a_k}, где $\tau \in S_n$; $(a_1, \ldots, a_n) \in \mathbb{Z}_m^n$; $\sum_{k=1}^{n} a_k = 0 \pmod p$; ξ – некоторый первообразный комплексный корень из единицы степени m, а на остальных позициях стоят нули. Будем обозначать такую матрицу w символом $\xi^{(a_1, \ldots, a_n)} \otimes \tau$. Поскольку существует взаимно однозначное соответствие между матрицами $w = \xi^{(a_1, \ldots, a_n)} \otimes \tau$ и перестановками $(w_1, \ldots, w_n)$, где $w_k = \tau(k)\xi^{a_k}$, $k \in \{1, \ldots, n\}$, то в дальнейшем элементы группы $G(m, p, n)$ будем кодировать перестановками указанного вида. Порядок группы $G(m, p, n)$ равен $\dfrac{m^n n!}{p}$.

Определение. Пусть Γ – конечная группа, T – система образующих группы Γ, удовлетворяющая условиям $\mathrm{id} \notin T$ и $T = T^{-1}$, т. е. $s^{-1} \in T$ для любого $s \in T$. *Граф Кэли* $\mathrm{Cay}(\Gamma, T)$ – это неориентированный граф со множеством вершин $V = \Gamma$ и множеством ребер $E = \{(x, y) \mid x, y \in \Gamma,\ yx^{-1} \in T\}$. Граф Кэли $\mathrm{Cay}(\Gamma, T)$ называется *минимальным*, если порождающее множество T минимально, т. е. для любого $s \in T$ множество $T' = T \setminus \{s, s^{-1}\}$ не является системой образующих группы Γ.

Определим следующие элементы группы $G(m, p, n)$: $s_i = \xi^{(0, \ldots, 0)} \otimes (i, i+1)$, $i \in \{1, \ldots, n-1\}$, $t_1 = \xi^{(m-1, 1, 0, \ldots, 0)} \otimes (1, 2)$, $t = \xi^{(p, 0, \ldots, 0)} \otimes \mathrm{id}$. Рассмотрим семейство минимальных графов Кэли $A(m, p, n)$ на группах $G(m, p, n)$ с порождающими множествами $T(m, p, n)$, где $T(m, p, n) = \{s_1, \ldots, s_{n-1}\}$ при $p = m = 1$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t, t^{-1}\}$ при $p = 1, m > 1$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t_1, t, t^{-1}\}$ при $1 < p < m$; $T(m, p, n) = \{s_1, \ldots, s_{n-1}, t_1\}$ при $p = m > 1$ [9]. Отметим, что каждый граф $A(m, p, n)$ является связным, регулярным и вершинно-транзитивным. Обозначим через $d_{m, p, n}$ степень вершины данного графа.

Пусть $G = (V, E)$ – конечный связный k-регулярный граф. Определим на этом графе стандартное вероятностное пространство $(\Omega, \mathcal{F}, \mathbb{P})$ и рассмотрим случайное блуждание X_t, $t = 0, 1, 2, \ldots$, на графе G такое, что $\mathbb{P}(X_t = w | X_{t-1} = w_0) = \frac{1}{k}$ при $w \in N(w_0)$, где $N(w_0)$ – множество смежных вершин с вершиной w_0 в графе G; $\mathbb{P}(X_t = w | X_{t-1} = w_0) = 0$ при $w \in V \setminus N(w_0)$.

В дальнейшем будем опираться на следующий известный результат о времени перемешивания случайных блужданий на экспандерах.

Предложение 1 [1]. *Пусть $G = (V, E)$ – конечный связный k-регулярный граф, для которого нетривиальные собственные значения λ матрицы смежности удовлетворяют неравенству $|\lambda| \le c$ при некотором $c < k$, а S – произвольное подмножество вершин графа G, $v \in V$. Тогда для любого* $t \ge t_0 := \ln\left(\frac{2|V|}{|S|^{1/2}}\right)\left(\ln\frac{k}{c}\right)^{-1}$ *выполняется двойное неравенство*

$$\frac{|S|}{2|V|} \le \mathbb{P}(X_t \in S | X_0 = v) \le \frac{3|S|}{2|V|}.$$

Пусть $G = (V, E)$ – конечный граф, S – непустое подмножество множества вершин V графа G. Подмножество ребер $\partial_E S = \{(u, v) \in E | u \in S, v \in V \setminus S\}$ называется *реберной границей* множества S, а подмножество вершин $\partial_V S = \{v \in V \setminus S | \exists u \in S : (u, v) \in E\}$ – *вершинной границей* множества S. *Постоянной Чигера* графа G именуется величина $h_E(G) = \min\limits_{0 < |S| \le |V|/2} \frac{|\partial_E S|}{S}$, *матрицей Лапласа* графа G – матрица $L = D - A$, где D – диагональная матрица, состоящая из степеней вершин графа G; A – матрица смежности графа G. *Спектральным пробелом* графа G называется наименьшее положительное собственное значение матрицы Лапласа графа G. Через $\mathrm{diam}(G)$ обозначим *диаметр* графа $G = (V, E)$, т. е. $\mathrm{diam}(G) = \max\limits_{u, v \in V}(\mathrm{dist}(u, v))$, где $\mathrm{dist}(u, v)$ – расстояние между вершинами u, v в графе G.

В дальнейших рассуждениях будем использовать следующее неравенство Чигера.

Предложение 2 [10, гл. 1]. *Пусть $G = (V, E)$ – конечный связный k-регулярный граф, σ – спектральный пробел графа G. Тогда выполняется двойное неравенство*

$$\frac{\sigma}{2} \le h_E(G) \le \sqrt{2\sigma k}.$$

Для любого связного вершинно-транзитивного графа имеет место следующий результат Бабаи.

Предложение 3 [11]. *Пусть $G = (V, E)$ – конечный связный вершинно-транзитивный граф. Тогда для любого $S \subset V$, $0 < |S| \le \frac{|V|}{2}$, справедливо неравенство*

$$|\partial_V S| \ge \frac{|S|}{4\mathrm{diam}(G)}.$$

Поскольку $|\partial_E S| \ge |\partial_V S|$ для любого $S \subset V$, $0 < |S| \le \frac{|V|}{2}$, то из предложения 3 получаем следующий результат.

Следствие 1. *Пусть $G = (V, E)$ – конечный связный вершинно-транзитивный граф. Тогда справедливо неравенство*

$$h_E(G) \ge \frac{1}{4\mathrm{diam}(G)}.$$

Получим оценку сверху для диаметров графов Кэли $A(m,\ p,\ n)$.

Предложение 4. *Для любых $m,\ p,\ n \in \mathbb{N},\ n > 2,\ p|m$, справедливо неравенство*

$$\operatorname{diam}\big(A(m,\ p,\ n)\big) \le 2n^2 m.$$

Доказательство. *Так как граф $A(m,\ p,\ n)$* вершинно-транзитивный, то достаточно доказать существование пути длиной не более $2n^2m$ из произвольной вершины $v \in G(m,\ p,\ n)$ в вершину $\mathrm{id} \in G(m,\ p,\ n)$.

Зафиксируем произвольный элемент $w = (w_1, \ldots, w_n) \in G(m,\ p,\ n)$, где $w_i = \xi^{a_i} c_i,\ a_i \in \mathbb{Z}_m,\ c_i = \sigma(i)$ для некоторого $\sigma \in S_n$. Пусть $w^0 = \left(w_1^0, \ldots, w_n^0\right)$ – единичный элемент группы $G(m,\ p,\ n)$, где $w_i^0 = i$. Так как диаметр графа $A(1, 1,\ n)$ равен $\frac{n(n-1)}{2}$ [8], то $\operatorname{dist}(w,\ w\tau) \le \frac{n(n-1)}{2}$ для любого $\tau \in S_n$. Таким образом, достаточно показать, что существует элемент $\tau \in S_n$ такой, что $\operatorname{dist}\left(w\tau,\ w^0\right) \le 2n^2(m-1)$.

Рассмотрим случай $p = m > 1$ и опишем соответствующий алгоритм получения элемента $w\tau$ из единичного элемента w^0 с применением образующих $s_1, \ldots, s_{n-1}, t_1$. Существует целое неотрицательное число $k \le n$ такое, что

$$\sum_{i=1}^{n} a_i = kp. \tag{1}$$

Пусть $A_- = \{1, \ldots, k\},\ A_+ = \{k+1, \ldots, n\}$. Используем следующий алгоритм для получения элемента $w\tau$ из элемента w^0.

Шаг A1. Взять некоторые символы $w_i^0,\ i \in A_+$, и $w_j^0,\ j \in A_-$, и перемещать их на первую и вторую позиции соответственно, применяя транспозиции $s_1, \ldots, s_{n-1}$.

Шаг A2. Умножить перемещенные символы $w_i^0,\ w_j^0$ на $\xi,\ \xi^{-1}$ соответственно (эти действия эквивалентны применению образующего t_1).

Шаг A3. Повторять шаги A1 и A2 $\sum_{i \in A_+} a_i$ раз так, что каждый символ $w_i^0,\ i \in A_+$, будет умножен на ξ a_i раз, а каждый символ $w_j^0,\ j \in A_-$, будет умножен на ξ^{-1} $p - a_j$ раз (это возможно в силу равенства (1)).

Очевидно, что описанный алгоритм построит элемент $w\tau$ для некоторого $\tau \in S_n$. Так как $\left|A_+\right| \le n$ и $0 \le a_i < p$ для любого $i \in A_+$, то имеют место неравенства

$$\operatorname{dist}\left(w\tau,\ w^0\right) \le (2n-1)n(p-1) < 2n^2(p-1).$$

Таким образом, $\operatorname{diam}\big(A(m,\ p,\ n)\big) \le 2n^2 p = 2n^2 m$.

Теперь рассмотрим случай $m > p$. Для получения единичного элемента w^0 из элемента w используем следующие шаги.

Шаг B1. Получить элемент $\tilde{w} = (\tilde{w}_1, \ldots, \tilde{w}_n)$ из элемента $w = (w_1, \ldots, w_n)$, где $\tilde{w}_i = \xi^{k_i p} i,\ k_i = \left[\frac{a_i}{p}\right]$.

Шаг B2. Получить элемент $\varsigma \in S_n$ из элемента $\tilde{w}$.

Шаг B3. Получить единичный элемент w^0 из элемента ς.

Если $p = 1$, то шаг B1 тривиальный: $\tilde{w} = w$. Предположим, что $p > 1$. Применяя шаги алгоритма A1– A3, можно получить элемент $w\tau$ из элемента $\tilde{w}$ для некоторого $\tau \in S_n$ (достаточно заменить w^0 на $\tilde{w}$ и a_i на $a_i (\operatorname{mod} p)$). После этого мы получим элемент w из $w\tau$, используя транспозиции $s_1, \ldots, s_{n-1}$. Длина построенного пути из $\tilde{w}$ в w не превосходит $(2n-1)n(p-1) + \frac{n(n-1)}{2}$.

Для получения элемента $\varsigma \in S_n$ из элемента $\tilde{w}$ достаточно переместить каждый символ $\tilde{w}_i = \xi^{k_i p} i$, для которого $k_i \ne 0$, на первую позицию с помощью транспозиций $s_1, \ldots, s_{n-1}$ и затем применить $\frac{m}{p} - k_i$ раз образующий t. Длина построенного пути из $\tilde{w}$ в ς не превосходит $n\left(n - 2 + \frac{m}{p}\right)$.

Для получения единичного элемента w^0 из элемента ς достаточно применить не более $\frac{n(n-1)}{2}$ транспозиций $s_1, \ldots, s_{n-1}$.

Таким образом, $\operatorname{dist}\left(w,\ w^0\right) \le 2n^2 m$. Предложение доказано.

Основным результатом настоящей статьи является следующая теорема.

Теорема. *Пусть* $\frac{m}{p}$ *нечетно,* $p < m$. *Тогда существует постоянная* $C = C(m, p)$ *такая, что для любых натурального* $n > 2$, *подмножества S вершин графа* $A(m, p, n)$, $v \in G(m, p, n)$ *и* $t \geq Cn^7 \ln n$ *выполняется двойное неравенство*

$$\frac{|S|}{2|G(m, p, n)|} \leq \mathbb{P}(X_t \in S \mid X_0 = v) \leq \frac{3|S|}{2|G(m, p, n)|}.$$

Д о к а з а т е л ь с т в о. Так как $\frac{m}{p}$ нечетно и больше единицы, то в графе $A(m, p, n)$ существуют циклы нечетной длины, и, следовательно, граф $A(m, p, n)$ не является двудольным. Отсюда вытекает, что нетривиальные собственные значения λ матрицы смежности графа $A(m, p, n)$ удовлетворяют неравенству $|\lambda| < d_{m, p, n}$. Таким образом, можем воспользоваться предложением 1. В качестве постоянной c из предложения 1 можно взять величину $d_{m, p, n} - \sigma_{m, p, n}$, где $\sigma_{m, p, n}$ – спектральный пробел графа $A(m, p, n)$. Получим оценку снизу для $\sigma_{m, p, n}$. Используя предложения 2, 4 и следствие 1, имеем

$$\sigma_{m, p, n} \geq \frac{h_E^2(A(m, p, n))}{2d_{m, p, n}} \geq \frac{1}{32(n+2)(\mathrm{diam}(A(m, p, n)))^2} \geq \frac{1}{128n^4(n+2)m^2}. \quad (2)$$

Используя неравенство (2), получаем оценки, справедливые для всех m, p, n:

$$\ln\left(\frac{d_{m, p, n}}{d_{m, p, n} - \sigma_{m, p, n}}\right) = -\ln\left(1 - \frac{\sigma_{m, p, n}}{d_{m, p, n}}\right) = \frac{\sigma_{m, p, n}}{d_{m, p, n}} + \frac{1}{2}\left(\frac{\sigma_{m, p, n}}{d_{m, p, n}}\right)^2 \geq \frac{\sigma_{m, p, n}}{d_{m, p, n}} \geq \frac{C(m, p)}{n^6},$$

где постоянная $C(m, p) > 0$ не зависит от n.

Таким образом, получаем оценку для параметра t_0 из предложения 1:

$$t_0 = \ln\left(\frac{2|G(m, p, n)|}{|S|^{1/2}}\right)\left(\ln\left(\frac{d_{m, p, n}}{d_{m, p, n} - \sigma_{m, p, n}}\right)\right)^{-1} \leq \frac{\ln(|G(m, p, n)|) + \ln 2}{\frac{C(m, p)}{n^6}} \leq C_1(m, p)n^7 \ln n := \tilde{t}_0,$$

где постоянная $C_1(m, p)$ не зависит от n.

Следовательно, согласно предложению 1 для любого $t \geq \tilde{t}_0$ выполнено двойное неравенство

$$\frac{|S|}{2|G(m, p, n)|} \leq \mathbb{P}(X_t \in S \mid X_0 = v) \leq \frac{3|S|}{2|G(m, p, n)|},$$

что и требовалось доказать.

Замечание 1. Условие теоремы, обеспечивающее недвудольность графа $A(m, p, n)$, является существенным, так как в противном случае при четных значениях времени t вероятность оказаться в доле, не содержащей начальную вершину v, равна нулю. Отмеченный факт демонстрирует существенное отличие групп $G(m, p, n)$ от группы S_n, граф $A(1, 1, n)$ которой является двудольным.

Замечание 2. Выбирая в качестве множеств S одноэлементные подмножества $G(m, p, n)$, получаем, что $\mathbb{P}(X_t \in S \mid X_0 = v) = \Theta\left(\frac{1}{|G(m, p, n)|}\right)$, это свидетельствует о близости распределения X_t к равномерному распределению для достаточно больших t.

Библиографические ссылки / References

1. Jao D, Miller SD, Venkatesan R. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*. 2009;129(6):1491–1504. DOI: 10.1016/j.jnt.2008.11.006.
2. Charles DX, Lauter KE, Goren EZ. Cryptographic hash functions from expander graphs. *Journal of Cryptology.* 2009;22(1): 93–113. DOI: 10.1007/s00145-007-9002-x.
3. Spielman DA. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory.* 1996; 42(6):1723–1731. DOI: 10.1109/18.556668.

4. Sauerwald T. *Randomized protocols for information dissemination.* Padeborn: University of Padeborn; 2008. 146 p.
5. Shephard GC, Todd JA. Finite unitary reflection groups. *Canadian Journal of Mathematics.* 1954;6:274–304. DOI: 10.4153/CJM-1954-028-3.
6. Boalch P. Painleve equations and complex reflections. *Annales de l'Institut Fourier.* 2003;53(4):1009–1022. DOI: 10.5802/aif.1972.
7. Aldous DJ. Random walks on finite groups and rapidly mixing Markov chains. In: Azéma J, Yor M, editors. *Séminaire de probabilités de Strasbourg. Volume 17.* Berlin: Springer; 1983. p. 243–297 (Lecture notes in mathematics; 986).
8. Vaskouski M, Zadorozhnyuk A. Resistance distances in Cayley graphs on symmetric groups. *Discrete Applied Mathematics.* 2017;227:121–135. DOI: 10.1016/j.dam.2017.04.044.
9. Jian-yi Shi. Formula for the reflection length of elements in the group $G(m, p, n)$. *Journal of Algebra.* 2007;316(1):284–296. DOI: 10.1016/j.jalgebra.2007.06.031.
10. Krebs M, Shaheen A. *Expander families and Cayley graphs: a beginner's guide.* New York: Oxford University Press; 2011. 258 p.
11. Babai L. Local expansion of vertex-transitive graphs and random generation in finite groups. In: *Proceedings of the 23rd annual ACM symposium on theory of computing; 1991 May 5–8; New Orleans, Louisiana, USA.* New York: ACM Press; 1991. p. 164–174. DOI: 10.1145/103418.103440.

Получена 29.08.2021 / исправлена 20.09.2021 / принята 30.10.2021.
Received 29.08.2021 / revised 20.09.2021 / accepted 30.10.2021.

УДК 519.676

ДЕТЕРМИНИРОВАННЫЕ И СТОХАСТИЧЕСКИЕ МОДЕЛИ РАСПРОСТРАНЕНИЯ ИНФЕКЦИИ И ТЕСТИРОВАНИЕ В ИЗОЛИРОВАННОМ КОНТИНГЕНТЕ

А. В. ЧИГАРЕВ[1]***, М. А. ЖУРАВКОВ***[1]***, В. А. ЧИГАРЕВ***[2]

[1]*Белорусский государственный университет,*
пр. Независимости, 4, 220030, г. Минск, Беларусь
[2]*Белорусский национальный технический университет,*
пр. Независимости, 65, 220013, г. Минск, Беларусь

Представлено обобщение математической модели SIR динамики развития инфекционного процесса путем добавления модели тестирования, что требует расширения размерности пространства состояний за счет переменных, которые не могут быть измерены непосредственно, но позволяют более адекватно описать процессы, имеющие место в реальных ситуациях. Дальнейшее обобщение модели SIR рассматривается на основе учета случайности в оценках состояния, прогнозировании, что достигается благодаря использованию методов стохастических дифференциальных уравнений, связанных с применением уравнений Фоккера – Планка – Колмогорова для апостериорных вероятностей. Как показала практика COVID-19, широкое использование современных средств идентификации, диагностики и мониторинга не гарантирует получение адекватной информации о состоянии индивидуумов в популяции. При моделировании реальных эпидемических процессов на начальных стадиях целесообразно

Образец цитирования:
Чигарев АВ, Журавков МА, Чигарев ВА. Детерминированные и стохастические модели распространения инфекции и тестирование в изолированном контингенте. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:57–67.
https://doi.org/10.33581/2520-6508-2021-3-57-67

For citation:
Chigarev AV, Zhuravkov MA, Chigarev VA. Deterministic and stochastic models of infection spread and testing in an isolated contingent. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:57–67. Russian.
https://doi.org/10.33581/2520-6508-2021-3-57-67

Авторы:
Анатолий Власович Чигарев – доктор физико-математических наук, профессор; профессор кафедры био- и наномеханики механико-математического факультета.
Михаил Анатольевич Журавков – доктор физико-математических наук, профессор; заведующий кафедрой теоретической и прикладной механики механико-математического факультета.
Виталий Анатольевич Чигарев – кандидат физико-математических наук; доцент кафедры теоретической механики и механики материалов машиностроительного факультета.

Authors:
Anatoliy V. Chigarev, doctor of science (physics and mathematics), full professor; professor at the department of bio- and nanomechanics, faculty of mechanics and mathematics.
chigarevanatoli@yandex.ru
Michael A. Zhuravkov, doctor of science (physics and mathematics), full professor; head of the department of theoretical and applied mechanics, faculty of mechanics and mathematics.
zhuravkov@bsu.by
Vitaliy A. Chigarev, PhD (physics and mathematics); associate professor at the department of theoretical and structural mechanics, faculty of engineering.

применять методы эвристического моделирования, а затем уточнять модель с помощью методов математического моделирования, используя стохастические и неопределенно-нечеткие методы, позволяющие учитывать то, что протекание процессов, принятие решений и управление происходят в системах с неполной информацией. Для разработки более реалистичных моделей необходим учет пространственной кинетики, что, в свою очередь, требует использования моделей систем с распределенными параметрами (например, моделей механики сплошных сред). Очевидно, что реалистичные модели эпидемий и борьбы с ними должны включать экономические модели, а также модели социодинамики. Задачи прогнозирования эпидемий и их развития окажутся не менее сложны, чем задачи прогнозирования изменения климата, предсказания землетрясений, прогноза погоды.

Ключевые слова: математическая модель; эпидемия; оценивание; апостериорная вероятность; модель SIR.

DETERMINISTIC AND STOCHASTIC MODELS OF INFECTION SPREAD AND TESTING IN AN ISOLATED CONTINGENT

A. V. CHIGAREV[a]***, M. A. ZHURAVKOV***[a]***, V. A. CHIGAREV***[b]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
[b]*Belarusian National Technical University, 65 Niezaliežnasci Avenue, Minsk 220013, Belarus*
Corresponding author: A. V. Chigarev (chigarevanatoli@yandex.ru)

The mathematical SIR model generalisation for description of the infectious process dynamics development by adding a testing model is considered. The proposed procedure requires the expansion of states' space dimension due to variables that cannot be measured directly, but allow you to more adequately describe the processes that occur in real situations. Further generalisation of the SIR model is considered by taking into account randomness in state estimates, forecasting, which is achieved by applying the stochastic differential equations methods associated with the application of the Fokker – Planck – Kolmogorov equations for posterior probabilities. As COVID-19 practice has shown, the widespread use of modern means of identification, diagnosis and monitoring does not guarantee the receipt of adequate information about the individual's condition in the population. When modelling real epidemic processes in the initial stages, it is advisable to use heuristic modelling methods, and then refine the model using mathematical modelling methods using stochastic, uncertain-fuzzy methods that allow you to take into account the fact that flow, decision-making and control occurs in systems with incomplete information. To develop more realistic models, spatial kinetics must be taken into account, which, in turn, requires the use of systems models with distributed parameters (for example, models of continua mechanics). Obviously, realistic models of epidemics and their control should include models of economic, sociodynamics. The problems of forecasting epidemics and their development will be no less difficult than the problems of climate change forecasting, weather forecast and earthquake prediction.

Keywords: mathematical model; epidemic; estimation; posterior probability; SIR model.

Введение

Модель SIR (*susceptible*, *infectious*, *recovered*), описывающая распространение эпидемии, является базовой при применении подходов математического моделирования, так как в простейшем варианте включает в себя основные фазы эпидемии и в то же время допускает их уточнение с помощью корректирующих членов в уравнениях, а также добавления в систему исходных разрешающих уравнений новых уравнений. Модель SIR удобно использовать для модификации детерминированного подхода в вероятностный, поскольку она учитывает тот факт, что эпидемиологические процессы протекают в условиях наличия неполной информации и погрешностей наблюдения.

Базовая модель SIR и рандомизация модели

Введем следующие обозначения: $N = \text{const}$ – постоянная численность популяции; S – группа членов популяции, которые потенциально могут быть инфицированы; I – количество инфицированных; R – количество выздоровевших, привитых и умерших.

Достаточно обоснованным является принятие предположения

$$S(t) + I(t) + R(t) = N = \text{const}. \qquad (1)$$

Из (1) следует, что существуют три основные группы членов в рассматриваемой популяции, численность в каждой из них является переменной, причем изменения направлены в одну сторону: $S \to I \to R$.

Между группами S и I скорость изменения плотности подверженных инфицированию $s = \frac{S}{N}$ предполагается равной

$$\frac{ds}{dt} = -\beta \cdot s \cdot i, \tag{2}$$

где β – среднее количество контактов на одного человека во времени; $i = \frac{I}{N}$ – плотность инфицированных.

Отметим, что величина $s \cdot i$ представляет собой плотность контактов между членами групп S и I (за счет чего главным образом и происходит инфицирование).

Скорость передачи между членами групп S и R предполагается пропорциональной величине $\gamma \cdot i$, где $\gamma = \frac{1}{D}$, а D – средний период времени индивидуального инфицирования.

На основании изложенного компоненты математической модели инфицирования $S \to I$ могут быть представлены подобно закону взаимодействия реагирующих масс в химии [1], согласно которому скорость фракционирования пропорциональна концентрациям реагентов. Соответственно, часть модели инфицирования $I \to R$ подобна известному в теории массового обслуживания экспоненциальному распределению времени ожидания [2; 3].

Отметим, что описанная простейшая модель не содержит демографических факторов (рождение, смертность от других причин). Таким образом, она пригодна для краткосрочного прогноза, когда количество новорожденных и умерших за рассматриваемый период сравнительно мало (т. е. $N \approx \text{const}$).

Замкнутая система уравнений, описывающая кинетику модели SIR, имеет вид[1] [4; 5]

$$\begin{gathered}
\frac{ds}{dt} = -\beta \cdot s \cdot i, \\
\frac{di}{dt} = \beta \cdot s \cdot i - \gamma \cdot i, \\
\frac{dr}{dt} = \gamma \cdot i,\ r = \frac{R}{N}, \\
\frac{ds}{dt} + \frac{di}{dt} + \frac{dr}{dt} = 0.
\end{gathered} \tag{3}$$

Система дифференциальных уравнений (3) нелинейная.

Выполним обобщение модели (3) за счет рандомизации. Данную операцию можно осуществить, перейдя в (3) к стохастическим дифференциальным уравнениям путем введения случайных погрешностей в измерения скоростей в правой части (3). Тогда

$$\begin{gathered}
\frac{ds}{dt} = -\beta \cdot s \cdot i + G_1 \nu_1(t), \\
\frac{di}{dt} = \beta \cdot s \cdot i - \gamma \cdot i + G_2 \nu_2(t), \\
\frac{dr}{dt} = \gamma \cdot i + G_3 \nu_3(t), \\
G_1 \nu_1(t) + G_2 \nu_2(t) + G_3 \nu_3(t) = 0, \\
G = \begin{pmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{pmatrix}, \\
\langle \nu_i(t) \rangle = 0,\ \langle \nu_i(t_1) \nu_i(t_2) \rangle = G_i \delta(t_1 - t_2),\ i = 1, 2, 3.
\end{gathered} \tag{4}$$

Здесь $\nu_i(t)$ – случайные ошибки в оценивании скоростей процессов (по повторяющимся индексам нет суммирования).

[1]Compartmental models in epidemiology // Wikipedia [Electronic resource]. URL: https://en.wikipedia.org/wiki/compartmental_models_in_epidemiology (date of access: 14.03.2021).

Пандемия вируса COVID-19 показала, что мониторинг является неотъемлемой частью управления инфекционными процессами. Поэтому в качестве вероятностных характеристик величин $s(t)$, $i(t)$, $r(t)$ целесообразно использовать апостериорные вероятности [6]. Обозначим переменные состояния величин $s(t)$, $i(t)$, $r(t)$ как

$$x_1 = s,\ x_2 = i,\ x_3 = r. \tag{5}$$

С учетом (5) систему (4) можно записать в общем виде:

$$\dot{\overline{x}}(t) = f\left[t;\ \overline{x}(t)\right] + G_i(t)\overline{\nu}(t),\ \overline{x}(t_0) = \overline{x}_0, \tag{6}$$

$$\left\langle \overline{\nu}(t) \right\rangle = 0,\ \left\langle \overline{\nu}(t_1)\overline{\nu}^{\mathrm{T}}(t_2) \right\rangle = G_i \delta(t_1 - t_2).$$

В (6) вектор $\overline{x}(t)$ характеризует состояние системы, при этом в общем случае не все компоненты $\overline{x}(t)$ являются измеряемыми. Поэтому введем вектор непосредственных наблюдений (тестирования) $\overline{z}(t)$, связанный с вектором $\overline{x}(t)$ моделью измерения, которая в общем случае имеет вид

$$\overline{z}(t) = \overline{h}\left[t;\ \overline{x}(t)\right] + G_z \overline{n}(t),\ t \ge t_0, \tag{7}$$

где G_z – матрица; $\overline{n}(t)$ – вектор ошибок (измерения).

Введем дополнительно следующее обозначение апостериорной плотности вероятности:

$$P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right),$$

где $\overline{z}_{t_0,\, t}$ – измерения (тестирование) на интервале $\left[t_0,\ t\right]$.

Модель SIR в виде уравнений (6), (7) может использоваться для получения алгоритмов оценивания состояния системы и определения погрешности оценивания.

Считаем, что процесс $\overline{z}(t)$ можно измерять с момента t_0 до текущего момента времени t, т. е. известно $\overline{z}_{t_0,\, t}$. Проблема нахождения оценки $\tilde{\overline{x}}(t)$ заключается в получении оценки состояния марковского процесса $\tilde{\overline{x}}(t)$ на основании имеющихся в наличии измерений процесса $\overline{z}_{t_0,\, t}$ (в частности, $\overline{z}(t) = \overline{x}(t) + G_z \overline{n}(t)$).

Полагаем, что на протяжении времени наблюдения увеличивается количество обработанной информации, но использованная информация по мере поступления новой не корректируется.

Обозначим $\tilde{\overline{x}}(t)$ вектор оценивания состояния, который минимизирует среднеквадратичную ошибку оценки, т. е.

$$E_{\min} = \left\langle \left(\overline{x}(t) - \tilde{\overline{x}}(t)\right)^2 \right\rangle.$$

Как известно, искомая оценка является условным математическим ожиданием, вычисляемым по следующей формуле [6]:

$$\tilde{\overline{x}}(t) = \int_{-\infty}^{+\infty} \ldots \int_{-\infty}^{+\infty} \overline{x}(t) P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right) d\overline{x}(t).$$

Согласно теории фильтрации Калмана – Бьюси апостериорная плотность вероятности $P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right)$ удовлетворяет уравнению [6; 7]

$$\frac{\partial}{\partial t} P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right) = L^{+} P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right) + P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right)\left[\overline{h}(t;\ \overline{x}) - \left\langle \overline{h}(t;\ \overline{x}) \right\rangle\right]^{\mathrm{T}} G_z^{-1}\left[\overline{z}(t) - \left\langle \overline{h}(t;\ \overline{x}) \right\rangle\right]. \tag{8}$$

В (8) оператор L^{+} имеет форму [6; 7]

$$L^{+} = -\sum_{i=1}^{m} \frac{\partial}{\partial x_i} f_i(t;\ \overline{x})(*) + \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{m}\left[G(t)\overline{X}G^{\mathrm{T}}(t)\right]_{ij} \frac{\partial^2}{\partial x_i \partial x_j}(*), \tag{9}$$

где $\overline{X} = \begin{bmatrix} \overline{x} \\ \overline{y} \end{bmatrix};\ \overline{X}_0 = \begin{bmatrix} \overline{x}_0 \\ \overline{y}_0 \end{bmatrix};\ \overline{f} = \begin{bmatrix} \overline{f} \\ \overline{h} \end{bmatrix};\ \dot{\overline{y}} = \overline{z}.$

Как известно, $P\left(\overline{x};\ t \middle| \overline{z}_{t_0,\, t}\right)$ содержит наиболее полную информацию о процессе $\overline{x}(t)$. Но решение уравнений (8), (9) возможно в сравнительно небольшом числе случаев. Поэтому, как правило, ограничиваются информацией, полученной на основе уравнений или алгоритмов, выводимых из (8), (9) [6].

Обозначим ковариационную матрицу процесса $\bar{x}(t)$ следующим образом:

$$V = \left\langle \left(\bar{x}(t) - \tilde{\bar{x}}(t)\right)\left(\bar{x}(t) - \tilde{\bar{x}}(t)\right)^{\mathrm{T}} \right\rangle.$$

Очевидно, что матрица V характеризует среднеквадратичную погрешность оценивания процесса $\bar{x}(t)$. Согласно теории фильтрации для приближенных оценок $\tilde{\bar{x}}(t)$ и $V(t)$ на основе уравнений (8), (9) получаются уравнения вида

$$\dot{\tilde{\bar{x}}}(t) = \bar{f}\left(t;\, \tilde{\bar{x}}(t)\right) + VD\left[\bar{h}\left(t;\, \tilde{\bar{x}}(t)\right)\right]N^{-1}\left[\bar{z}(t) - \bar{h}\left(t;\, \tilde{\bar{x}}(t)\right)\right],\ \tilde{\bar{x}}(t_0) = \tilde{\bar{x}}_0. \tag{10}$$

Здесь $D\left[\bar{h}\left(t;\, \tilde{\bar{x}}(t)\right)\right]$ – матрица Якоби размером $m \times m$ с элементом $\dfrac{\partial h_j\left(t;\, \tilde{\bar{x}}(t)\right)}{\partial x_i}$.

$$\begin{gathered}\dot{V}(t) = D^{\mathrm{T}}\left[f\left(t;\, \tilde{\bar{x}}\right)\right]V(t) + V(t)D\left[\bar{f}\left(t;\, \tilde{\bar{x}}\right)\right] + G(t)\bar{X}G^{\mathrm{T}}(t) + \\ + V(t)D\left[D\left[\bar{h}\left(t;\, \tilde{\bar{x}}\right)\right]N^{-1}\left\{\bar{z}(t) - \bar{h}\left(t;\, \tilde{\bar{x}}\right)\right\}\right],\ V(t_0) = V_0.\end{gathered} \tag{11}$$

Замкнутая система уравнений (10), (11) позволяет в принципе получить решения задач оценивания и прогнозирования процессов $\bar{x}(t)$ и определить погрешность такой оценки.

В общем случае система (10), (11) нелинейная, что значительно усложняет получение решений как в общем, так и в конкретных случаях.

Эталонные стохастические модели оценки эпидемиологической ситуации в условиях неполной информации и самоорганизации

Как известно [3], естественный ход эпидемии обладает свойствами самоорганизации [7], что происходит при уменьшении числа степеней свободы системы.

Следуя [7; 8], принимаем, что $\dfrac{dr}{dt} = 0$. Тогда, как вытекает из (4), $\gamma = 0$, $G_3 = 0$.

Модель, которую в результате получаем, называется математической моделью SI. Она описывается уравнениями состояния

$$\begin{gathered}\frac{ds}{dt} = -\beta \cdot s \cdot i + G_1 \nu_1(t), \\ \frac{di}{dt} = \beta \cdot s \cdot i - \gamma \cdot i + G_2 \nu_2(t)\end{gathered} \tag{12}$$

и обобщает модель Лотки – Вольтерры [9].

Модель измерения (тестирования) выбираем в форме

$$z(t) = i(t) + n(t), \tag{13}$$

$$\langle n(t) \rangle = 0,\ \langle n(t_1) n(t_2) \rangle = G_z \delta(t_1 - t_2).$$

Преобразуем второе уравнение системы (12) с учетом $s + i = 1$ к виду

$$\frac{di}{dt} = \beta i \left[\frac{1}{N} + (1 - i)\right] + G_2 \nu_2(t). \tag{14}$$

Здесь β – среднее число контактов человека в единицу времени, т. е. число контактов, которые могут привести к инфицированию; i – вероятность (числовая плотность) принадлежности группе инфицированных.

Уравнения (13) и (14) представляют собой математическую основу для получения уравнения типа (10) для оценки и уравнения типа (11) для определения погрешности оценки числовой плотности инфицированных в рассматриваемом примере.

Рассмотрим задачу об оценивании числа инфицированных в случае, когда в некоторый момент времени t_0 в контингенте имеется лишь один инфицированный человек.

Замечание. Предполагаем, что вследствие каких-то причин (например, вакцинации) все члены популяции обладают иммунитетом.

Так как инфицированным остается только один человек, то $I(t) = I(0) = 1$.

Принимаем, что измерения (тестирование) в начальный момент времени $t = t_0$ проводятся с ошибкой $V_0 = 10$. Вследствие этого для периода $t > t_0$ оценка числа инфицированных тоже осуществляется с ошибкой. Исходя из этого, необходимо, чтобы предлагаемые алгоритмы оценки состояния инфицирования популяции были самокорректирующимися.

Уравнения (10) для данной задачи имеют вид

$$\dot{\tilde{i}} = \beta\tilde{i}\left[1 + \frac{1}{N} - \tilde{i}\right] + V(t)\left[Z(t) - \tilde{i}(t)\right],\ \tilde{i}(0) = 0. \tag{15}$$

Погрешность V оценки $\tilde{i}$ удовлетворяет уравнению

$$\dot{V}(t) = -\left[V(t)\right]^2,\ V(0) = 10. \tag{16}$$

Решение (16) имеет вид

$$V(t) = \frac{10}{10t + 1}. \tag{17}$$

Из (17) следует, что погрешность в начальном тесте уменьшается со временем за счет последующего тестирования.

Уравнение (15) типа Риккати преобразуем в линейное, используя замену

$$\tilde{i}(t) = \frac{1}{u(t)}. \tag{18}$$

Уравнение для $u(t)$ имеет вид

$$\dot{u} + \beta a(t)u = f(t), \tag{19}$$

$$a(t) = \beta\left[1 + \frac{1}{N} - \frac{V}{\beta}\right],\ f(t) = \beta - V(t)z(t),\ \tilde{i}_0^2(t) \approx \tilde{i}^2(0) \approx 1.$$

Решение (19) имеет вид [2; 3]

$$u(t) = \frac{1}{\mu(t)}\left[\int f(t)\mu(t)dt + C\right],\ \mu(t) = \exp\left(\int a(t)dt\right). \tag{20}$$

Модель наблюдений $z(t)$ выбираем в виде линейной зависимости от времени (результаты тестирования):

$$z(t) = t + \frac{n}{10}. \tag{21}$$

Подставляя (21) в (19), (20) с учетом (18), получаем

$$\tilde{i}(t) = \frac{\exp\left(\beta\left(1 + \frac{1}{10}\right)t\right)}{t + 1}\left[\frac{\beta - 1}{10}\exp(-ab)\left(Ei(ab + at) - Ei(ab) + 1\right)\right]^{-1},$$

$$Ei(x) = \int \frac{\exp(ax)}{x}dx. \tag{22}$$

Здесь $Ei(x)$ – интегральная показательная функция [8; 10].

Рассмотрим модель псевдоэпидемии, являющейся результатом ошибок измерения (тестирования).

Пусть в начальный момент времени в изолированный контингент попадает один инфицированный человек и при этом система остается в стационарном состоянии, т. е.

$$\frac{di}{dt} = \frac{ds}{dt} = \frac{dr}{dt} = 0.$$

Предполагаем, что в контингенте проводятся замеры (выборки), которые в реальности содержат ошибки.

Математическая модель инфицирования и измерения в рассматриваемом случае имеет вид

$$\frac{di}{dt} = 0,\ i(0) = 1, \tag{23}$$

$$z(t) = i(t) + n(t),$$

$$\langle \nu(t) \rangle = 0, \langle \nu(t_1) \nu(t_2) \rangle = \delta(t_1 - t_2).$$

Уравнения для оценки плотности инфицирования $i(t)$ и определения погрешности оценки $V(t)$ в данном случае получаются из (2), (13) и с учетом (23) имеют вид

$$\frac{d\tilde{i}}{dt} = \frac{10}{10t+1}\left[z(t) - \tilde{i}(t)\right], \ \tilde{i}(0) = 10^{-3}. \tag{24}$$

Выбираем модель наблюдения (21), уравнения которой подставляем в (24). В результате получаем

$$\tilde{i} = \frac{5t^2 + t + 10^{-3}}{10t+1}.$$

Таким образом, ошибка в начальном измерении $V(0) \neq 0$ приводит к возможности появления ошибок при $t > 0$. При этом оценка $\tilde{i}(t)$ в определении состояния растет, что создает эффект псевдоэпидемии при отсутствии таковой.

Оценка скорости инфицирования $\frac{d\tilde{i}}{dt}$ сначала растет, а потом убывает.

Краткий сравнительный анализ моделей

Уравнения классической модели SIR (3) описывают кинетику детерминированной системы, типичный график которой изображен на рис. 1.

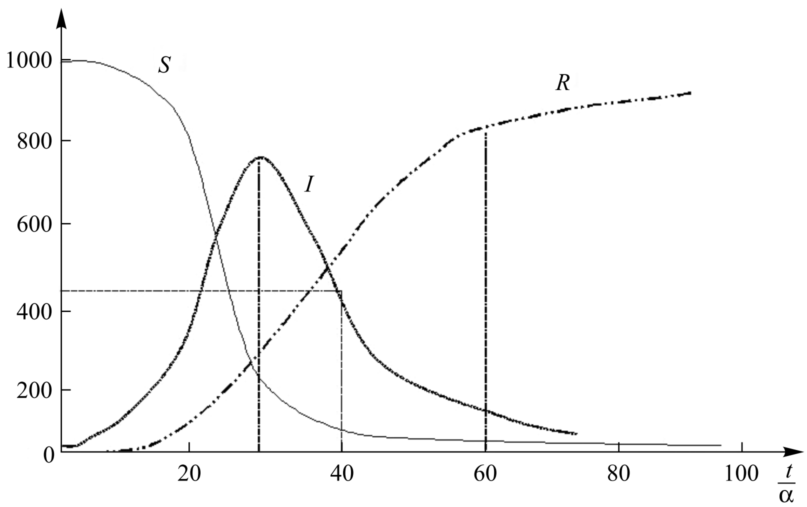


Рис. 1. Зависимость *S*, *I*, *R* от времени при начальных условиях $S(0) = 997$, $I(0) = 3$, $R(0) = 0$, скорости инфицирования $\beta = 0{,}4$ и скорости перехода из *I* в *R* $\gamma = 0{,}04$

Fig. 1. Dependence of *S*, *I*, *R* on time under initial conditions $S(0) = 997$, $I(0) = 3$, $R(0) = 0$, infection rate $\beta = 0.4$ and transition rate from *I* to *R* $\gamma = 0.04$

Обобщение модели на стохастический случай (4) или (6) и дополнение моделью измерения (7) меняют вид и характер системы (рис. 2).

Простейшая (эталонная) модель инфицирования с учетом случайности и измерений описывается уравнениями (12), (13), обобщающими модель *хищник – жертва* с чистым заражением контингента потенциально инфицируемых людей.

Модели оценивания числа людей в группах *S*, *I*, *R* построены на основе уравнений Фоккера – Планка – Колмогорова для априорных или апостериорных плотностей вероятностей. При включении модели измерений (тестирования) оптимальная оценка плотности инфицированных удовлетворяет уравнению (15), а оценка дисперсии (ошибки) – уравнению (16).

Из структурной схемы системы видно, что в стохастической модели наблюдения появляются обратные связи. В соответствии с теорией систем это обеспечивает большую устойчивость к возможности прогнозирования.

Рандомизация модели SIR (3) превращает ее из модели процесса естественного распространения инфекции в модель (4), (14), управляемую белым шумом.

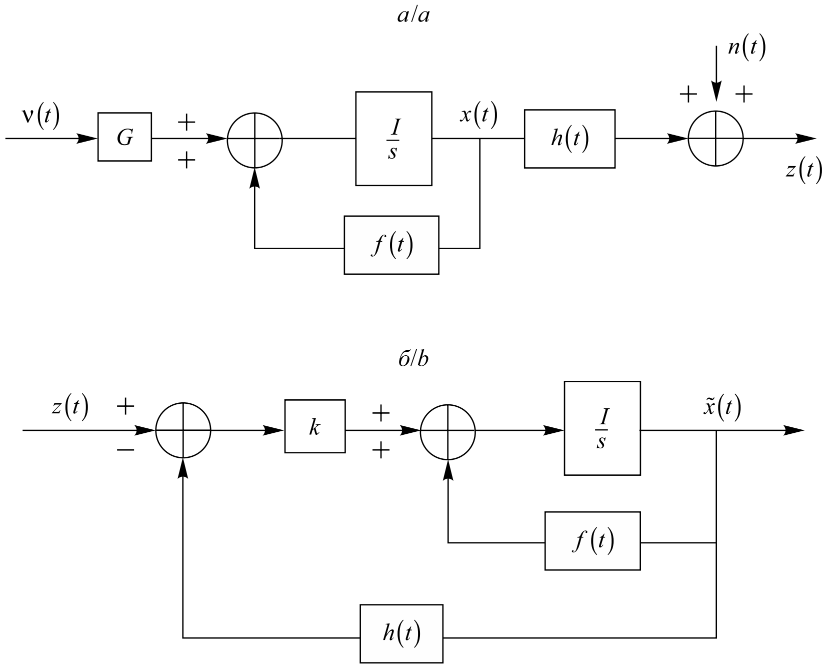


Рис. 2. Структурная схема моделей наблюдения (*а*) и оценивания (*б*)

Fig. 2. Block diagram of observation (*a*) and assessment (*b*) models

В некоторых странах мира хаотический характер управляющих воздействий наблюдался в начале эпидемии. Математическая модель оценивания (15), общий случай (10), вследствие рандомизации описывается неоднородными дифференциальными уравнениями, содержащими управляющие члены с нулевым трендом. При этом коэффициенты усиления управляющих воздействий, зависящие от дисперсий $V(t)$, удовлетворяющих уравнениям (16), в общем случае (11) изменяются во времени, что характерно для адаптивных систем с обратными связями.

Рассмотрим устойчивость в большом (нечувствительность к неопределенности начального состояния) для простейшей модели естественного распространения инфекции на фоне управляющего белого шума, который моделирует хаотический режим воздействий в начале эпидемии.

В рассматриваемых примерах начального распространения инфекции допустимо считать $i \ll 1 \ll N$. Тогда уравнение (14) принимает вид

$$\frac{di}{dt} = \beta \cdot i + G_2 \nu_2(t), \tag{25}$$

а уравнение (15) для оценки апостериорного состояния, соответственно,

$$\frac{d\tilde{i}}{dt} = \beta \tilde{i} + V(t)\left[Z(t) - \tilde{i}(t)\right],\ \tilde{i}(0) = 0.$$

Дискретизируем модель по времени [6; 7]. Тогда (25) запишется следующим образом:

$$\tilde{i}(k+1) = \alpha \tilde{i}(k) + \gamma(k+1)\left[Z(k+1) - \alpha \tilde{i}(k)\right],$$

$$\gamma(k+1) = \frac{Q(k+1)}{Q(k+1) + G_2},\ \tilde{i}(0) = \tilde{i}_0,\ \alpha \approx \beta.$$

Для дисперсии оценивания $V(k)$ получаем

$$V(k+1) = \frac{Q(k+1)G_i}{Q(k+1) + G_i},$$

$$Q(k+1) = a^2 V(k) + G_i,\ V(0) = V_0.$$

Условие стабилизации погрешности оценивания V имеет вид

$$V(k) = V(k-1) = V_{\text{ст}}. \tag{26}$$

Подставляя в общем случае $V(t)$ в дискретные моменты времени в (26), получаем квадратное уравнение относительно $V_{\text{ст}}$, положительный корень которого $V_{\text{ст}}(k) = 0{,}56W$ при $k = 3$.

На рис. 3 изображено поведение $V(k)$ в зависимости от V_0. Такое поведение $V(k)$ указывает на возможность существования апостериорной неопределенности оценки при определенных значениях параметров, т. е. устойчивость в большом.

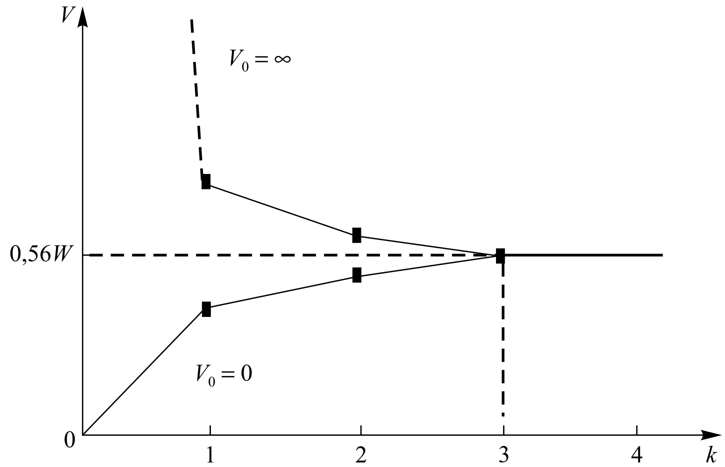


Рис. 3. Поведение $V(k)$ в зависимости от V_0
Fig. 3. $V(k)$ depending on V_0 behaviour

Замечание. Следует отметить работу [10], в которой используются дискретная модель SIR и ее модификации для генерации членов временного ряда.

Адекватность предложенной модели реальным процессам характеризует функция (матрица) чувствительности [6; 11], анализ которой является составной частью создания достоверной модели. Параметры (коэффициенты) модели b_i ($i = 1, \ldots, n$) точно неизвестны и определяются невязками $\Delta b_i = b_i - \bar{b}_i$, где b_i – истинное (неизвестное), а $\bar{b}_i$ – приближенное значение параметров, используемых в уравнениях оценивания [6].

Чувствительность модели характеризуется отношением вида

$$\Gamma_{i,\,j}(t) = \frac{V(t) - \bar{V}}{\Delta b_i}.$$

Здесь $V(t)$ – матрица дисперсии оценки, которая находится из (11) при истинном значении параметров задачи (теоретически).

Рассмотрим вопрос, связанный с оценкой чувствительности для стационарного состояния, описываемого уравнениями состояния и измерения

$$\frac{di}{dt} = 0,\ z(t) = hi(t) + n(t),\ h = \beta.$$

Выражение для дисперсии в этом случае имеет вид (16), (17).

Чувствительность параметра h в большом находится по формуле

$$\Gamma_h(t) = \frac{h^2 \Delta h \bar{V}^3(0)t^2 - 2\bar{V}^2(0)h\bar{r}t}{\left(h^2\bar{V}(0)t + \bar{r}\right)^2}.$$

График зависимости $\Gamma_h(t)$ от времени при заданных значениях входных параметров изображен на рис. 4.

Чувствительность в малом определяется формулой

$$\gamma_{i,\,j}(t) = \left.\frac{\partial V(t)}{\partial b_i}\right|_{b_i = \bar{b}}.$$

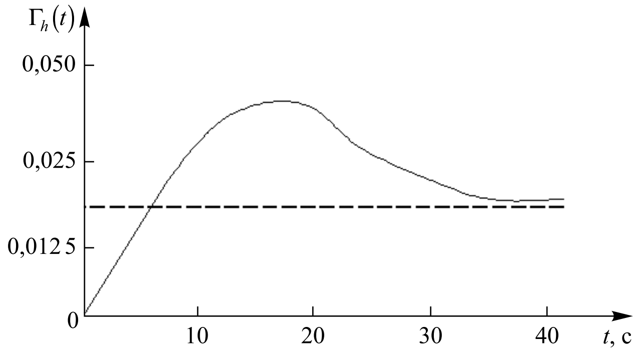


Рис. 4. Пример зависимости $\Gamma_h(t)$ от времени при $\bar{h}=1$, $\bar{r}=20$, $\bar{V}(0)=2$

Fig. 4. An example of the $\Gamma_h(t)$ time dependence for $\bar{h}=1$, $\bar{r}=20$, $\bar{V}(0)=2$

Введем следующее представление:

$$V(t)-\bar{V}(t)=\sum_{i=1}^{3}\gamma_{i,\,j}(t)d\bar{b}_i.$$

Тогда получаем

$$\gamma_h(t)=\frac{-2h\bar{V}^2(0)\bar{r}t}{\left(h^2V(0)t\bar{r}\right)^2}.$$

На рис. 5 изображена зависимость $\gamma_h(t)$ от времени при заданных значениях входных параметров.

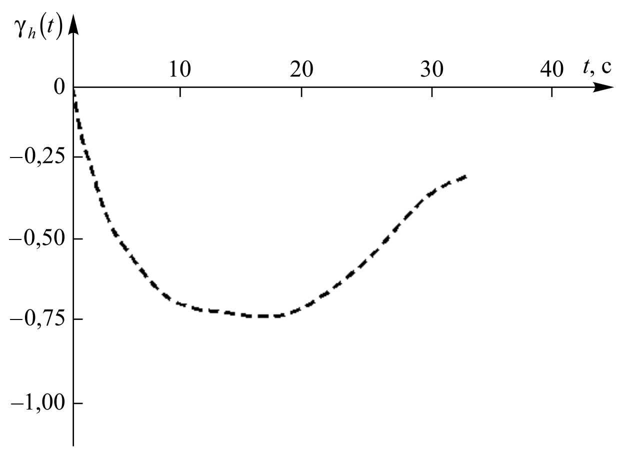


Рис. 5. Пример зависимости $\gamma_h(t)$ от времени при $\Delta h = 0{,}5$, $h = 1$, $r = 20$, $\bar{V}(0)=2$

Fig. 5. An example of the $\gamma_h(t)$ time dependence for $\Delta h = 0.5$, $h = 1$, $r = 20$, $\bar{V}(0)=2$

Заключение

1. В качестве математической модели процесса инфицирования предложена классическая модель SIR, управляемая процессами типа белого шума, что может быть адекватно начальной хаотической фазе эпидемии.

Таким образом, модельный процесс естественного распространения эпидемии развивается в среде управляющих белых шумов, моделирующих несистемный характер мер в начале эпидемии.

2. Модель наблюдения в общем случае учитывает существующие в реальности ошибки тестирования, что более адекватно реальности, так как решает проблему опосредствованного получения информации.

3. Грубость модели (устойчивость в большом и малом) позволяет выделить начальный и последующий периоды распространения инфекции с точки зрения регулирования и управления на начальном этапе.

Отмечено влияние начальных условий на длительность переходного режима эпидемии, в течение которого стохастический режим может возникать как следствие нелинейности системы.

4. Чувствительность (в большом и малом) позволяет оценить влияние параметров модели на ее свойства и структурировать процесс распространения инфекции в зависимости от времени. Оценка параметров должна состоять из совместного решения задач идентификации и управления.

Библиографические ссылки

1. Варфоломеев СД, Гуревич КГ. *Биокинетика.* Москва: Гранд; 1999. 716 с.

2. Ахмеров РР. Очерки по теории обыкновенных дифференциальных уравнений. § 37. Дифференциальные уравнения в биологии, химии, медицине [Интернет]. В: Ахмеров РР, Садовский БН. *Основы теории обыкновенных дифференциальных уравнений.* Новосибирск: Институт вычислительных технологий Сибирского отделения РАН; 2002 [процитировано 14 марта 2021 г.]. Доступно по: http://w.ict.nsc.ru/books/textbooks/akhmerov/ode_unicode/s-37/s-37.html.

3. Марри Дж. *Нелинейные дифференциальные уравнения в биологии. Лекции о моделях.* Бабский ВГ, переводчик; Мышкис АД, редактор. Москва: Мир; 1983. 397 с.

4. Eastman B, Meaner C, Przedborski M, Kohandel M. Mathematical modeling of COVID-19 containment strategies with consideration for limited medical resources. *medRxiv* [Preprint]. 2020 [cited 2021 March 14]. Available from: https://doi.org/10.1101/2020.04.17.20068585.

5. Dong E, Du H, Gardner L. An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases.* 2020;20(5):533–534. DOI: 10.1016/S1473-3099(20)30120-1.

6. Сейдж Э, Мелс Д. *Теория оценивания и ее применение в связи и управлении.* Москва: Связь; 1976. 496 с. (Статистическая теория связи; выпуск 6).

7. Snyder DL. *The state-variable approach to continuous estimation with applications to analog communication theory.* Cambridge: MIT Press; 1969. 114 p.

8. Хакен Г. *Синергетика. Иерархии неустойчивостей в самоорганизующихся системах и устройствах.* Москва: Мир; 1985. 424 с.

9. Фунтов АА. О приближенном аналитическом решении уравнений Лотки – Вольтерры. *Известия высших учебных заведений. Прикладная нелинейная динамика.* 2011;19(2):89–92. DOI: 10.18500/0869-6632-2011-19-2-89-92.

10. Харин ЮС, Волошко ВА, Дернакова ОВ, Малюгин ВИ, Харин АЮ. Статистическое прогнозирование динамики эпидемиологических показателей заболеваемости COVID-19 в Республике Беларусь. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;3:36–50. DOI: 10.33581/2520-6508-2020-3-36-50.

11. Оморов РО. Метод топологической грубости динамических систем: приложения к синергетическим системам. *Научно-технический вестник информационных технологий, механики, оптики.* 2020;20(2):257–262. DOI: 10.17586/2226-1494-2020-20-2-257-262.

References

1. Varfolomeev SD, Gurevich KG. *Biokinetika* [Biokinetics]. Moscow: Grand; 1999. 716 p. Russian.

2. Akhmerov RR. [Essays on the theory of ordinary differential equations. § 37. Differential equations in biology, chemistry, medicine] [Internet]. In: Akhmerov RR, Sadovsky BN. *Osnovy teorii obyknovennykh differentsial'nykh uravnenii* [Fundamentals of the theory of ordinary differential equations]. Novosibirsk: Institute of Computational Technologies, Siberian Branch of the Russian Academy of Sciences; 2002 [cited 2021 March 14]. Available from: http://w.ict.nsc.ru/books/textbooks/akhmerov/ode_unicode/s-37/s-37.html. Russian.

3. Murray JD. *Lectures on nonlinear-differential-equations. Models in biology.* Oxford: Clarendon Press; 1977. 397 p.

Russian edition: Murray J. *Nelineinye differentsial'nye uravneniya v biologii. Lektsii o modelyakh.* Babskii VG, translator; Myshkis AD, editor. Moscow: Mir; 1983. 397 p.

4. Eastman B, Meaner C, Przedborski M, Kohandel M. Mathematical modeling of COVID-19 containment strategies with consideration for limited medical resources. *medRxiv* [Preprint]. 2020 [cited 2021 March 14]. Available from: https://doi.org/10.1101/2020.04.17.20068585.

5. Dong E, Du H, Gardner L. An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases.* 2020;20(5):533–534. DOI: 10.1016/S1473-3099(20)30120-1.

6. Sage AP, Melse JL. *Estimation theory with application to communication and control.* New York: McGraw-Hill; 1971. 752 p.

Russian edition: Sage A, Melse J. *Teoriya otsenivaniya i ee primenenie v svyazi i upravlenii.* Moscow: Svyaz'; 1976. 496 p. (Statisticheskaya teoriya svyazi; vypusk 6).

7. Snyder DL. *The state-variable approach to continuous estimation with applications to analog communication theory.* Cambridge: MIT Press; 1969. 114 p.

8. Haken H. *Sinergetika. Ierarkhii neustoichivostei v samoorganizuyushchikhsya sistemakh i ustroistvakh* [Synergetics. Hierarchies of instabilities in self-organising systems and devices]. Moscow: Mir; 1985. 424 p. Russian.

9. Funtov AA. About approximate analytical solutions of Lotka – Volterra equations. *Izvestiya vysshikh uchebnykh zavedenii. Prikladnaya nelineinaya dinamika.* 2011;19(2):89–92. Russian. DOI: 10.18500/0869-6632-2011-19-2-89-92.

10. Kharin YuS, Valoshka VA, Dernakova OV, Malugin VI, Kharin AYu. Statistical forecasting of the dynamics of epidemiological indicators for COVID-19 incidence in the Republic of Belarus. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;3:36–50. Russian. DOI: 10.33581/2520-6508-2020-3-36-50.

11. Omorov RO. Method of topological roughness of dynamic systems: applications to synergetic systems. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki, optiki.* 2020;20(2):257–262. Russian. DOI: 10.17586/2226-1494-2020-20-2-257-262.

Получена 14.04.2021 / исправлена 26.04.2021 / принята 29.09.2021.
Received 14.04.2021 / revised 26.04.2021 / accepted 29.09.2021.

УДК 004.056:004.42

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД НА ОСНОВЕ ВСТРАИВАНИЯ СКРЫТЫХ СООБЩЕНИЙ В КРИВЫЕ БЕЗЬЕ ИЗОБРАЖЕНИЙ ФОРМАТА SVG

Е. А. БЛИНОВА[1], ***П. П. УРБАНОВИЧ***[1), 2)]

[1)]*Белорусский государственный технологический университет, ул. Свердлова, 13а, 220006, г. Минск, Беларусь*
[2)]*Люблинский католический университет им. Иоанна Павла II, ал. Рацлавицке, 14, 20-950, г. Люблин, Польша*

Приведено описание стеганографического метода встраивания цифрового водяного знака в файлы векторных изображений формата SVG. Векторные изображения формата SVG могут включать в себя элементы на основе кривых Безье. Предлагаемый стеганографический метод базируется на разбиении кубических кривых Безье. Встраивание скрытой информации предусматривает разбиение кубических кривых Безье в соответствии со значениями последовательности, формирующей цифровую метку. Рассмотрены алгоритмы прямого и обратного

Образец цитирования:
Блинова ЕА, Урбанович ПП. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021; 3:68–83 (на англ.).
https://doi.org/10.33581/2520-6508-2021-3-68-83

For citation:
Blinova EA, Urbanovich PP. Steganographic method based on hidden messages embedding into Bezier curves of SVG images. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:68–83.
https://doi.org/10.33581/2520-6508-2021-3-68-83

Авторы:
Евгения Александровна Блинова – старший преподаватель кафедры информационных систем и технологий факультета информационных технологий.
Павел Павлович Урбанович – доктор технических наук, профессор; профессор кафедры информационных систем и технологий факультета информационных технологий[1)], профессор[2)].

Authors:
Evgeniya A. Blinova, senior lecturer at the department of information systems and technology, faculty of information technology.
evgenia.blinova@belstu.by
https://orcid.org/0000-0001-7245-8721
Pavel P. Urbanovich, doctor of science (engineering), full professor; professor at the department of information systems and technology, faculty of information technology[a] and professor[b].
p.urbanovich@belstu.by
https://orcid.org/0000-0003-2825-4777

стеганографического преобразования для доказательства подлинности и целостности цифрового векторного изображения. Создана библиотека StegoSVG для выполнения прямого и обратного стеганографического преобразования. Кратко охарактеризовано разработанное настольное приложение, реализующее метод.

Ключевые слова: стеганография; авторское право; цифровой водяной знак; векторная графика; формат SVG.

STEGANOGRAPHIC METHOD BASED ON HIDDEN MESSAGES EMBEDDING INTO BEZIER CURVES OF SVG IMAGES

E. A. BLINOVA[a]***, P. P. URBANOVICH***[a, b]

[a]*Belarusian State Technological University, 13a Sviardlova Street, Minsk 220006, Belarus*
[b]*John Paul II Catholic University of Lublin, 14 Racławickie Alley, Lublin 20-950, Poland*
Corresponding author: E. A. Blinova (evgenia.blinova@belstu.by)

The description of the steganographic method for embedding the digital watermark into image vector files of the SVG format is given. Vector images in SVG format can include elements based on Bezier curves. The proposed steganographic method is based on the splitting of cubic Bezier curves. Embedding hidden information involves splitting cubic Bezier curves according to the digital watermark given as numerical sequence. Algorithms of direct and reverse steganographic transformation are considered for proving the authenticity and integrity of a digital vector image. The StegoSVG library has been developed to implement forward and reverse steganographic transformations. The developed desktop application that implements the method is briefly described.

Keywords: steganography; copyright; digital watermark; vector graphics; SVG format.

Introduction

Technologies make it possible to easily create, store and transmit various types of data, such as images, texts and sounds, but these advantages allow other actions to be done easily as well: illegal copying, distribution, use, intentional distortion or destruction of information. Nowadays, the protection of digital content is gaining popularity. In this regard, the problem of developing and using methods and tools for protection of intellectual property rights, one of the areas of which is digital watermark technologies based on steganographic methods, is becoming more and more acute [1].

Due to the specific features and properties of digital document formats that are protected by a copyright, specific protection methods are developed for various formats to achieve specific goals. This is how two main directions in the subject area were formed: text steganography [1–8] and image steganography [1; 9; 10]. However, at present, for some types of containers, methods can be considered that are a combination of different approaches. For example, an electronic text document can be considered as a text or as a graphic image or as a set of fields containing meta-information and as a container with a specific structure [5–8], which allows to combine the classical approaches of both text and image steganography.

Regardless of the type of a container, using steganographic methods solves two main classes of problems: data hiding and copyright protection. The first implies the inconspicuous transmission of information through open channels, as well as undeclared and hidden storage of information. The second is implemented using digital watermarks and digital fingerprints. Digital fingerprints, sometimes referred to as digital tags, imply different steganographic message tags that are unique to each copy of the media. Digital watermarking usually means having the same watermark for every copy of a container. Digital prints and watermarks can be used to protect copyright on each copy of content, and to confirm the accuracy and integrity of the information transmitted. The main requirements for digital marks or watermarks are reliability and resistance to distortion or conversions [1; 3; 9; 10].

Research usually focuses on raster image formats. A feature of such files is their ubiquitous distribution, a relatively large volume, and, as a result, ample opportunities for watermark embedding. The most popular are image formats like BMP and JPG, for which many methods for embedding labels have been developed, including steganographic ones. Typically, images use the classical least significant bit (LSB) method or its modification [1; 3; 9; 10]. In connection with the growing popularity of vector images, it is of interest to develop and study steganographic methods for images of this type.

Theoretical justification of the steganographic method

This paper proposes a new steganographic method for vector image files in scalable vector graphics (SVG) format and describes an algorithm for its implementation. The method is based on the functional features of the main graphic primitives, based on which two-dimensional images are formed. Modification of some of the parameters of these primitives allows to embed secret information into an SVG file used as a container.

SVG vector image format and usage of its features in steganography. SVG files are vector graphics files used to describe two-dimensional vector and mixed vector and raster graphics in XML format. The SVG image format is the main vector graphics format on the Internet. Such files are used as pictures on buttons and other elements of a web application, for representation of graphs, maps, diagrams in speeches, reports, presentations. This is justified because the SVG file is scalable and looks the same at all screen resolutions. Features of this format are small file size, scalability, integration with HTML documents, the ability to embed bitmap graphics, the ability to edit in text editors and support by most modern browsers such as Google Chrome, Internet Explorer, Mozilla Firefox and Safari. In addition, the popular office suite Microsoft Office 2016 supports direct import of such files.

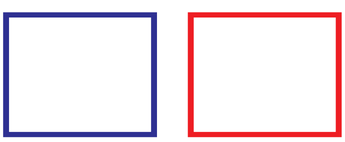
An SVG graphic file is a collection of XML tags that describe graphic elements. The first line is a standard XML header indicating the XML version and character encoding. Then the DOCTYPE header comes, that defines the SVG document type. Further is the root tag of the document <SVG> indicating the namespace, and it contains graphic and text elements. The document ends by closing the root tag </SVG>. An SVG file includes three types of objects: shapes, images, and text. All elements are described with XML subset tags. Text elements can be described as text or converted into curves.

An SVG file is a text, has a structure corresponding to markup files, geometric elements are described with appropriate tags. Tags have attributes whose values are enclosed in quotes. Shapes are described using RGB colour space, although CMYK is also supported.

Classical methods of text steganography, such as the insertion of trailing spaces and tabs method, as well as methods typical for markup files: the method of replacing the tags case, methods of substituting and rearranging of attributes [4] can be applied to files in the SVG format. Using the RGB colour model allows you to hide information in changing colour parameters by analogy with the methods of LSB.

The authors of [11; 12] substantiate the possibility of using additional vertices in the description of geometric shapes in an SVG file to embed a unique digital watermark to confirm copyright for images or for transfer a hidden message, and also propose a steganographic method that allows to embed a hidden message in placing additional vertices. Geometric shapes are specified by the coordinates of the vertices, and additional vertices can be placed on the line connecting these coordinates. Moreover, when viewing the image, these additional points are not displayed. Additional points in geometric shapes are set in a certain relation from the starting point of some file element, and a message is hidden in the value of this relation. This method allows to control the integrity of the image or to embed a hidden message to solve the problem of protecting the intellectual copyright to the image.

Figure 1 shows examples of rendering of the SVG file elements in the browser, as well as their description.



```
<polygon style = "stroke:blue; stroke-width:2; fill:none;"
points = "10,10  10,50  50,50  50,10"/>
<polygon style = "stroke:red; stroke-width:2; fill:none;"
points = "60,10  60,30  60,50  100,50  100,10"/>
```

Fig. 1. A rendering of the SVG file in the browser and its description

An additional vertex (60, 30) has been added in the second square, and since this element is in line with vertices (60, 10) and (60, 50), the vertex is not displayed.

Features of displaying Bezier curves in SVG files. SVG files support Bezier elements. To understand the essence of the proposed method, it is advisable to give a brief description of the parameters of the Bezier curves that form the basis of the method.

It is known that Bezier curves are a special case of polynomial plane curves with one parameter. They are often used in computer graphics to produce smooth curves, including fonts, vector images and CSS animations [13].

Bezier curves are generally defined by the expression

$$B(t) = \sum_{t}^{n} P_i b_{i,\,n}(t),\ 0 \le t \le 1, \tag{1}$$

where P_i is a function of the components of the vectors of the anchor points; $b_{i,n}(t)$ are the basic functions of the Bezier curve given by the expression

$$b_{i,n}(t) = \frac{n}{i} t^i (1-t)^{n-i}, \qquad (2)$$

where $\frac{n}{i} = \frac{n!}{i!(n-i)!}$ is a number of combinations from n to i, where n is the degree of the polynomial and i is the degree of the anchor point.

In the context of the method under consideration, two types of Bezier curves are of interest: a quadratic and cubic curve. From relations (1) and (2) we can obtain parametric equation of a quadratic Bezier curve in the following form:

$$Q = (1-t)^2 P_1 + 2(1-t)tP_2 + t^2 P_3,\ t \in [0, 1].$$

It can be seen that three points are required to uniquely determine the quadratic curve: P_1, P_2 and P_3. The starting point P_1 and the ending point P_3 are called the anchor point of the curve, and the point P_2 is the control point. The curve starts at point P_1, ends at point P_3, and point P_2 defines the direction and magnitude of the curve bend.

The parametric equation of cubic Bezier curve is as follows:

$$C = (1-t)^3 P_1 + 3(1-t)^2 tP_2 + 3(1-t)t^2 P_3 + t^3 P_4,\ t \in [0, 1]. \qquad (3)$$

To uniquely define this curve, four points are required: P_1, P_2, P_3 and P_4. The starting point P_1 and the ending point P_4 are the anchor points, and the points P_2 and P_3 are the control points. The curve starts at point P_1, ends at point P_4, and points P_2 and P_3 define the direction and magnitude of the curve bend.

To describe curves in SVG format, is used a special tag *path*. The SVG file parser parses the contents of the *path* tag and displays the corresponding shape. The *path* tag allows to sequentially set the coordinates of the vertices of a line, polygon and other geometric shapes. The *path* tag has one attribute *d*, which can contain a series of commands and parameters used by those commands. Each command is identified with a special letter. All commands come in two variants: a command with a uppercase letter indicates absolute coordinates on the page and a command with a lowercase letter indicates relative coordinates. Coordinates in the *d* attribute are always specified without units and in a custom coordinate system. Typically, custom coordinates are specified in pixels. For example, *M* is a command that tells the SVG parser to move to the specified point and to start the next command from there, and the *L* command draws a straight line from the current point to the specified one.

SVG files use quadratic and cubic Bezier curves. Commands *Q* and *T* are used to display quadratic curves, commands *C* and *S* are used to display curves of the third order. In this case, the commands *T* and *S* allow to set an additional segment of the curve without specifying a control point and are parts of the commands *Q* and *C*. These commands can be found in one element and used multiple times. If the parser cannot execute the statement due to an invalid command, the element is displayed as long as possible, and the rest is not displayed.

To reduce the number of elements of the SVG file, and, accordingly, the size of the image file, the combination of several curves in one geometric element can be used. The Bezier curve in this case consists of several segments. Adding segments can be achieved in two ways: either by mirroring the control point relatively to the ending anchor point, or by adding additional segments after the existing curve segment.

Figure 2 shows the cubic Bezier curve. The curve consists of three segments, the first of which is marked with additional red lines, the second segment is marked with orange lines, and the third is marked with green lines. Lines are drawn to the control points for clarity, to demonstrate how the location of the control points affects the appearance of the curve.

Figure 3 shows the part of the SVG file that is responsible for displaying such a curve.

The listing (see fig. 3) shows four blocks of *path* commands, at that the execution of the first one displays the entire quadratic curve, and the rest are needed only to demonstrate the location of the control points.

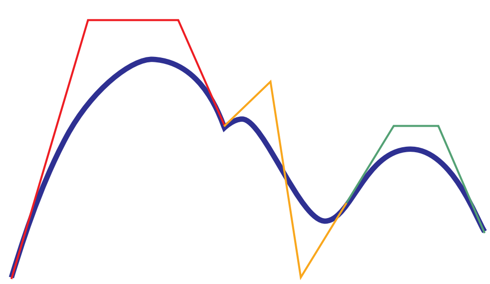


Fig. 2. A cubic Bezier curve consisting of three segments

```
<path d = "M 10,200 C 60,30 120,30 150,100 180,70 200,200 230,150
S 290,100 320,170" style = "stroke:blue; stroke-width:4; fill:none;"/>

<path d = "M 10,200 L 60,30" style = "stroke:red; stroke-width:1; fill:none;"/>
<path d = "M 60,30 L 120,30" style = "stroke:red; stroke-width:1; fill:none;"/>
<path d = "M 120,30 L 150,100" style = "stroke:red; stroke-width:1; fill:none;"/>

<path d = "M 150,100 L 180,70" style = "stroke:orange; stroke-width:1; fill:none;"/>
<path d = "M 180,70 L 200,200" style = "stroke:orange; stroke-width:1; fill:none;"/>
<path d = "M 200,200 L 230,150" style = "stroke:orange; stroke-width:1; fill:none;"/>

<path d = "M 230,150 L 260,100" style = "stroke:green; stroke-width:1; fill:none;"/>
<path d = "M 260,100 L 290,100" style = "stroke:green; stroke-width:1; fill:none;"/>
<path d = "M 290,100 L 320,170" style = "stroke:green; stroke-width:1; fill:none;"/>
```

Fig. 3. Description of a cubic Bezier curve, consisting of three segments, in SVG format

Let's consider the first path command. The curve starts at point (10, 200), the *M* command indicates to start displaying from this point. The *C* command then tells the SVG parser to display a third-order Bezier curve. Thus, point (60, 30) is perceived by parser as the first control point, point (120, 30) is perceived as the second control point, and point (150, 100) is perceived as the end point of the curve. If we look at the second, third and fourth commands of the listing, we will see that straight lines of red colour were drawn from the start and end points to the control points of the first segment using the *L* command. Since the command is not finished at point (150, 100), this point is perceived by the SVG parser as the starting point of the next segment. Thus, point (180, 70) is perceived as the first control point of the second curve segment, point (200, 200) is perceived as the second control point of the second curve segment, and point (230, 150) is perceived as the end point of the second curve segment. The next three lines of the listing draw additional orange lines to these points from the ends of the current segment of the curve. Since point (230, 150) is followed by an *S* operator, the SVG parser must display another segment of the curve starting at point (230, 150). Usually three points are required to display a segment which are two control points and an end anchor point, but in this case the first control point is calculated as a mirroring of the second control point of the previous segment at coordinates (200, 200) relative to the start point of the current segment at coordinates (230, 150). The coordinates of the new control point are calculated as follows: abscissa is calculated as

$$(230 - 200) + 230 = 260,$$

ordinate is calculated as

$$150 - (200 - 150) = 100.$$

So the operator displaying curves of the second and third order can be presented as follows:

```
path d = "M x1, y1 Q x2, y2 … T xi, yi … C xi, yi … S xk, yk …".
```

Some commands can be omitted here. If the command *Q* is omitted, then the command *T* is not used; if the command *C* is omitted, then the command *S* is not used. Any command can be followed by any number of points, but the command will be executed correctly provided that for command *Q* and *S* the number of points is $2k$, and for command *C* is respectively $3k$, where *k* is any non-negative integer.

Applying the de Casteljau dividing method to embed a hidden message. According to the method of dividing Bezier curves proposed by de Casteljau [13], any curve can be divided into two parts at some ratio. The result curves (which are segments of the original curve) will also be Bezier curves. Dividing the curve into segments can be used to embed a hidden message. If we divide the Bezier curve into segments at some ratio, then the value of this ratio can hide an element of the secret sequence, which is a digital watermark or digital fingerprint. Since in the general case one additional segment of the Bezier curve is required to embed one element of the sequence, it is rational to use a combined approach: dividing the Bezier curves into segments at a certain ratio and an additional method that will on the one hand increase the number of possible hidden characters of the sequence, and on the other hand it will control the integrity of the hidden data.

Let us show how de Casteljau's method works for a cubic Bezier curve, since for other orders the method is used in a similar way.

Let the cubic Bezier curve ***B*** (fig. 4) be described by four points: $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $P_3(x_3, y_3)$, $P_4(x_4, y_4)$, at that $P_1(x_1, y_1)$ is the starting point of the curve ***B***, $P_4(x_4, y_4)$ is the ending point, and $P_2(x_2, y_2)$ and $P_3(x_3, y_3)$ are control ones, point $P(x, y)$ divides this curve at some ratio *t*.

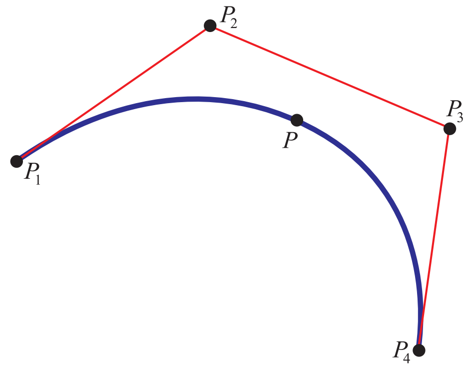


Fig. 4. An original Bezier curve ***B*** and intended dividing point *P*

Red (auxiliary) lines show the location of the original control points P_2 and P_3.

It is necessary to find the location of the anchor and control points of the two resulting Bezier curve segments. These segments, each of which is a cubic Bezier curve, will be denoted as $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$.

Let segment $\boldsymbol{B}_1$ be defined by points $P_{11}(x_{11}, y_{11})$, $P_{12}(x_{12}, y_{12})$, $P_{13}(x_{13}, y_{13})$, $P_{14}(x_{14}, y_{14})$, and segment $\boldsymbol{B}_2$ be defined by points $P_{21}(x_{21}, y_{21})$, $P_{22}(x_{22}, y_{22})$, $P_{23}(x_{23}, y_{23})$, $P_{24}(x_{24}, y_{24})$. Obviously, the starting point of the first curve segment $P_{11}(x_{11}, y_{11})$, is the same as the starting point of the entire curve $P_1(x_1, y_1)$, the ending point of the first curve segment $P_{14}(x_{14}, y_{14})$, and the starting point of the second curve segment $P_{21}(x_{21}, y_{21})$, coincide with the dividing point of the curve $P(x, y)$. The ending point of the second curve segment $P_{24}(x_{24}, y_{24})$, coincides with the ending point of the original curve $P_4(x_4, y_4)$.

The split ratio (t) of the Bezier curve is preserved for the lines connecting the anchor and control points. De Casteljau's method is to recursively divide such segments in the original ratio. The segment P_1P_2 is divided at the ratio *t*, just like segments P_3P_4 and P_2P_3. Figure 5, *a*, shows points separating the segments P_1P_2, P_3P_4 and P_2P_3 at the *t* ratio. Then the obtained segments are divided recursively in the same ratio, and the resulting line passes through the separation point *P*, as shown at fig. 5, *b*.

The intersection points of the line segments become new control points. Thus, we get two Bezier curves: $\boldsymbol{B}_1$ и $\boldsymbol{B}_2$, as indicated at fig. 6.

The coordinates of the starting, ending, and anchor points of the two curve segments can be calculated from the ratio (3). Let us denote as follows:

$$t_0 = 1 - t,\ t_1 = t_0^3,\ t_2 = 3t_0^2 t,\ t_3 = 3t_0 t^2,\ t_4 = t^3.$$

From the ratio (3) we obtain the coordinates of the point $P(x, y)$:

$$x = x_1t_1 + x_2t_2 + x_3t_3 + x_4t_4,\ y = y_1t_1 + y_2t_2 + y_3t_3 + y_4t_4. \quad (4)$$

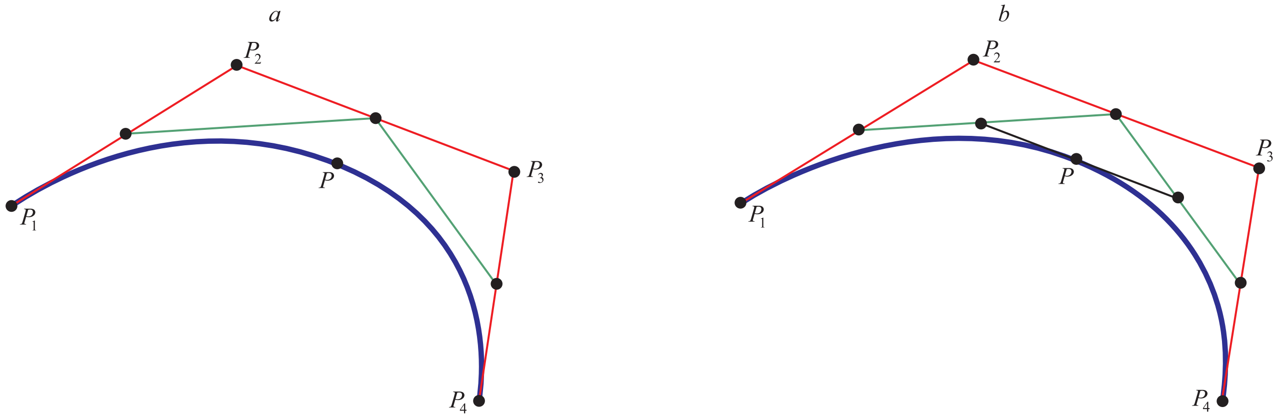


Fig. 5. A subdividing of a cubic Bezier curve using the de Casteljau's method

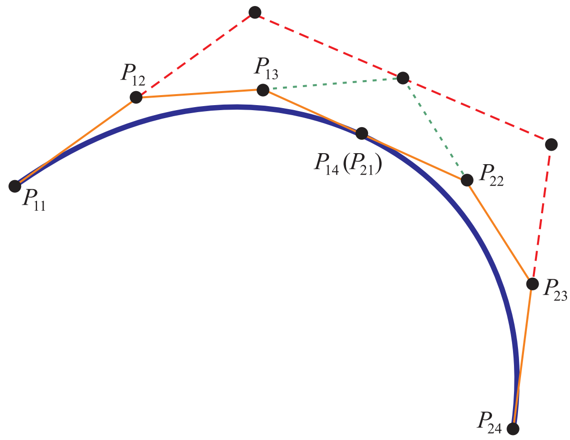


Fig. 6. Bezier curves $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$

Then the coordinates of points $P_{11}(x_{11}, y_{11})$, $P_{12}(x_{12}, y_{12})$, $P_{13}(x_{13}, y_{13})$, $P_{14}(x_{14}, y_{14})$ of the curve $\boldsymbol{B}_1$ can be calculated using the following formulas:

$$x_{11} = x_1,\ y_{11} = y_1;\ x_{12} = x_1 t_0 + x_2 t,\ y_{12} = y_1 t_0 + y_2 t;$$

$$x_{13} = x_{12} t_0 + (x_2 t_0 + x_3 t)t,\ y_{13} = y_{12} t_0 + (y_2 t_0 + y_3 t)t;\ x_{14} = x,\ y_{14} = y. \qquad (5)$$

The coordinates of the points $P_{21}(x_{21}, y_{21})$, $P_{22}(x_{22}, y_{22})$, $P_{23}(x_{23}, y_{23})$, $P_{24}(x_{24}, y_{24})$ of the segment $\boldsymbol{B}_2$ we calculate in a similar way:

$$x_{21} = x_{14},\ y_{21} = y_{14};\ x_{23} = x_3 t_0 + x_4 t,\ y_{23} = y_3 t_0 + y_4 t;$$

$$x_{22} = x_{23} t + (x_2 t_0 + x_3 t)t_0,\ y_{22} = y_{23} t + (y_2 t_0 + y_3 t)t_0;\ x_{24} = x_4,\ y_{24} = y_4. \qquad (6)$$

Thus, the original cubic Bezier curve $\boldsymbol{B}$ can be represented as two segments: $\boldsymbol{B}_1$ и $\boldsymbol{B}_2$, and for the display by the SVG parser it is written in one attribute *d* of the element *path* in general as follows:

$$\texttt{path d = "M } x_{11}, y_{12} \texttt{ C } x_{12}, y_{12}\ \ x_{13}, y_{13}\ \ x_{14}, y_{14}\ \ x_{22}, y_{22}\ \ x_{23}, y_{23}\ \ x_{24}, y_{24}\texttt{".}$$

Both curve segments are exactly the same as the original Bezier curve, and the presence of a dividing point is not displayed. Such a divided curve can be written both as separate geometric elements and as a curve of several segments. Further on we will call a curve of several segments a *polycurve.*

Steganographic algorithms for embedding and extracting the hidden message

The summary of the proposed steganographic method is that hidden information is located at the point of dividing the curve into segments.

Let us suppose the hidden message is a binary sequence. In case of dividing the Bezier curve into two segments in half, one symbol of the message can be hidden (the curve is not divided – 0, the curve is divided – 1; can be vice versa). If we choose a division ratio, then we can thereby hide a symbol of a message in a natural language, setting, for example, its own division ratio for each letter. The message will be extracted as follows: we check two successive curves, and if they form a single curve, then we calculate the division ratio, and so we find the hidden symbol.

It is assumed that in general the user of the application will be able to generate values for division on his own, which will be the part of his own steganographic key. Depending on the division ratio, the division point of the curve into segments is calculated and the control points of both new curves are found.

However, firstly, dividing the curve entails the creation of new anchor and control points which increases the file size, and secondly, it is not always possible to accurately calculate the division ratio from coordinates, which leads to the loss of a hidden message. Therefore, we propose to hide only a part of the hidden message in division ratio and to use the emerging anchor and control points for the rest, similar to the LSB method. When receiving new anchor and control points we will change the minor digits in them so that on the one hand this change was visually invisible, but a hidden message was deposited in them, and on the other hand so that during extraction it was possible to check whether the division ratio was extracted correctly.

The hidden message is converted into a binary form, after which it is divided into binary pairs, i. e. the message 01111000 is divided into pairs: 01, 11, 10, 00. For each Bezier curve and each two binary pairs, two actions are performed: the division of the curve at a certain ratio into two segments and embedding of data of two binary pairs into anchor points of segments. Thus, two binary pairs are embedded in one curve.

The method is designed for cubic Bezier curves. For additional embedding of the message, the second anchor point of the first segment (indicated at fig. 6 as P_{13}) and the first control point of the second segment of the curve (indicated at fig. 6 as P_{22}) are used. These points are chosen to embed the message because their coordinates do not affect the restoration of the original curve (which follows from the ratio (5) and (6) and will be demonstrated below with the example). To embed the message, LSB of the anchor point coordinate is used, in this case the sixth (0.00000x). This bit is chosen because of the visual invisibility of changes in coordinates in a vector drawing.

The following two parameters are suggested to be used as key information:

1) division ratio t;

2) values, that correspond the binary pairs V_i, $i = \{1, 2, 3, 4\}$.

Description of the steganographic method algorithm for hidden message embedding. Let us describe an algorithm for the steganographic method of embedding a hidden message in an SVG file, based on the division of cubic Bezier curves at a certain ratio.

The key information is the one of the division ratio t, as well as the values corresponding to the binary pairs V_i, $i = \{1, 2, 3, 4\}$.

The principle of random selection is used to obtain the value of t. It is assumed that this value will be generated on a case-by-case basis and is similar to key generation in symmetric cryptography. The value of t can range from 0.01 to 0.99, assuming that numbers with two decimal places are used.

The principle of random selection is also used to obtain integer values corresponding to binary pairs. For example, you can set the limits shown in table 1, assuming that the limits are numbers from 1 to 99.

Table 1

Correspondence of limits of values written in coordinates to binary pairs

Binary pair value	Limits
00	From 75 to 99
01	From 50 to 74
10	From 25 to 49
11	From 1 to 24

No effect was found for selected values corresponding to binary pairs on the display of a Bezier curve with an embedded message.

First, the SVG file is analysed and the number of cubic Bezier curves N is calculated. The length of the hidden message L is calculated. The maximum length of the hidden message must be less than one half the number of Bezier curves, because one message character is written in two curves, and one more character is needed to indicate the end of the message.

The hidden message is converted into a binary form, after which it is divided into binary pairs Q_k, $k = \{1, \ldots, 4L\}$. Each cubic Bezier curve $\boldsymbol{B}_j$, $j \in [1, N]$, will be successively associated with two binary pairs Q_k. If the length of the embedded message M is less than the number of curves N, then the curves which are not associated with binary pairs remain unchanged.

For each cubic curve $\boldsymbol{B}_j$ and each odd binary pair Q_k, we will perform as long as necessary the division at ratio t if the first symbol of the binary pair is 0, and $1 - t$ if the first symbol of the current binary pair is 1, in accordance with ratio (5) and (6). Thus we obtain a cubic Bezier curve $\boldsymbol{B}'_j$, $j \in [1, N]$, consisting of two segments.

Now, for each segment of the obtained curve $\boldsymbol{B}'_j$ we will embed the data of two binary pairs Q_k into the control points of the segments. The first binary pair is written to the second control point of the first segment of the obtained curve $P_{j13}\left(x_{j13}, y_{j13}\right)$: the first digit of the value is written to LSB of the x_{j13} coordinate, the second digit of the value is written to LSB of the y_{j13} coordinate. Similarly, the second binary pair is written to the coordinates of the first control point of the second segment of the resulting curve $P_{j22}\left(x_{j22}, y_{j22}\right)$. Thus, two binary pairs of the hidden message are written into one original Bezier curve.

The algorithm continues until all binary pairs have been embedded. After that, a new SVG file is generated, consisting of cubic Bezier curves divided into segments, and the original elements. The block diagram of the embedding algorithm is shown in fig. 7.

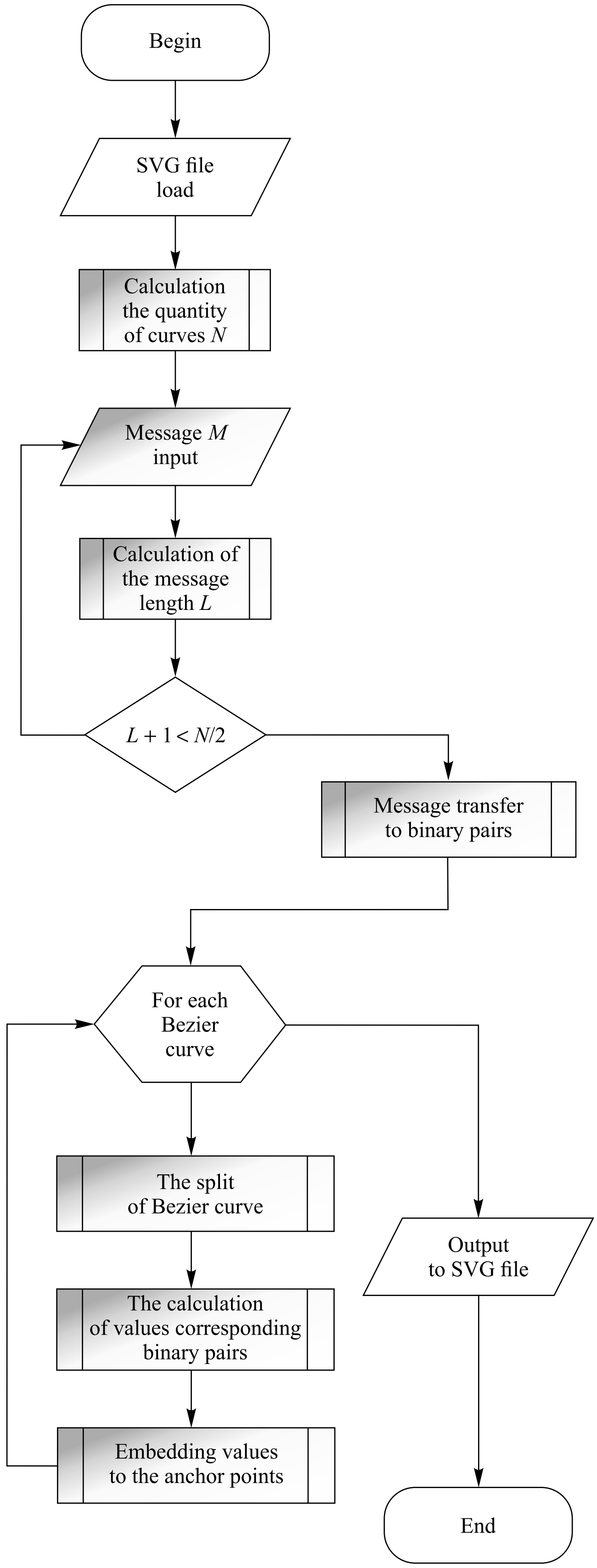


Fig. 7. Block diagram of the algorithm of hidden message embedding

Let us consider an example of how the method works. First we will describe the custom key. Let us take the division ratio as $t = 0.25$. The division of the curve into segments at the ratio is as follows: if the first character of a binary pair is 1, then the division ratio is taken as 0.25, if the first character of a binary pair is 0, then the division ratio is taken as 0.75.

Let us take a bijective mapping of a binary pair into the value V_i, $i = \{1, 2, 3, 4\}$, as given in table 2.

Table 2

Correspondence of values of binary pairs to values written in coordinates

Binary pairs value	Value for embedding
00	87
01	64
10	37
11	12

Figure 8 shows the part of the SVG file that is displaying two cubic Bezier curves without an embedded message.

```
<path d = "M 10,200 C 120,30 170,70 220,100"
style = "stroke:blue; stroke-width:2; fill:none;"/>
<path d = "M 10,200 C 180,70 200,200 230,150"
style = "stroke:red; stroke-width:2; fill:none;"/>
```

Fig. 8. Description of two cubic Bezier curves without hidden message

Assume the message to be embedded in this SVG file is 11000110. Let us divide the message into binary pairs: 11, 00, 01, 10. To embed such a message, we need two curves. The first binary pair 11 starts with 1, so the division ratio of the first curve will be 0.25. Let us divide the first curve at the ratio 0.25 and find the coordinates of the anchor and control points according to ratio (5) and (6). The coordinates of the original curve and two new curves are presented in table 3.

Table 3

Coordinates of the Bezier anchor and control points of the original first curve and curves obtained by its division

Curve	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
Original	10	200	120	30	170	70	220	100
1st segment	10	200	37.5	157.5	61.25	128.125	82.1875	108.4375
2nd segment	82.1875	108.4375	145	49.375	182.5	77.5	220	100

Thus, we can rewrite the display of the first curve as

path d = ″M 10,200 C 37.5,157.5 61.25,128.125
82.1875,108.4375 145,49.375 182.5,77.5 220,100″.

Now it is necessary to add hidden information to the control points. The first two binary pairs are 11 and 00. They correspond to the values 12 and 87. Therefore, in LSB (0.00000x) of the second control point of the first segment we write **1** and **2**, and in LSB of the first control point of the second segment we write **8** and **7**. Thus, we can rewrite the display of the first curve as

path d = ″M 10,200 C 37.5,157.5 61.25000**1**,128.12500**2**
82.1875,108.4375 145.00000**8**,49.37500**7** 182.5,77.5 220,100″.

Let us do the same for the second curve. The third binary pair 01 starts with 0, so the division ratio of the first curve will be 0.75. Let us divide the first Bezier curve at the ratio 0.75 and find the coordinates of the anchor and control points according to ratio (5) and (6). The coordinates of the original curve and two new curves are presented in table 4.

Table 4

Coordinates of the anchor and control points of the original second curve and curves obtained by its division

Curve	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
Original	10	200	180	70	200	200	230	150
1st segment	10	200	137.5	102.5	180.625	151.25	206.875	160.625
2nd segment	206.875	160.625	215.625	163.75	222.5	162.5	230	150

Thus, we can rewrite the display of the second curve as

path d = "M 10, 200 C 137.5, 102.5 180.625, 151.25
206.875, 160.625 215.625, 163.75 222.5, 162.5 230, 150".

Now it is necessary to add hidden information to the control points. The second two binary pairs are 01 and 10. They correspond to the values **64** and **37**. Therefore, in LSB (0.00000x) of the second control point of the first segment we write 6 and 4, and in LSB of the first control point of the second segment we write 3 and 7. Thus, we can rewrite the display of the first curve as

path d = "M 10, 200 C 137.5, 102.5 180.62500**6**, 151.25000**4**
206.875, 160.625 215.62500**3**, 163.75000**7** 222.5, 162.5 230, 150".

The description of the SVG file containing the hidden message is shown in fig. 9.

```
<path d = "M 10, 200 C 37.5, 157.5 61.250001, 128.125002 82.1875, 108.4375
145.000008, 49.375007 182.5, 77.5 220, 100"
style = "stroke:blue; stroke-width:1; fill:none;"/>
<path d = "M 10,200 C 137.5, 102.5 180.625006, 151.250004 206.875, 160.625
215.625003, 163.750007 222.5, 162.5 230, 150"
style = "stroke:red; stroke-width:1; fill:none;"/>
```

Fig. 9. Description of the SVG file of two cubic Bezier curves containing a hidden message

The description of the algorithm for extracting hidden messages. Next we will analyse the algorithm for extracting a hidden message from an SVG file (stego container), based on the division of third-order Bezier curves at a certain ratio. The key information is the one about the division ratio t and the values corresponding to binary pairs V_i, $i = \{1, 2, 3, 4\}$.

When extracting information, the file is analysed and the number of cubic Bezier curves N in the used container file is calculated. Then a sequential analysis of the curves $\boldsymbol{B}'_j$, $j \in [1, N]$, is performed. If the curve consists of two segments ($\boldsymbol{B}'_{j1}$ и $\boldsymbol{B}'_{j2}$), a check is performed: whether these segments form a single curve $\boldsymbol{B}_j$, and what is the division ratio t. The check is carried out in two stages: at the first stage, an assumption is made that the segments form a single Bezier curve, the coordinates of the control points of this curve are calculated; at the second stage it is checked whether the division point of the segments belongs to the assumed curve. If the division point belongs to a curve, then we can conclude that these curves are a single Bezier curve.

Let the segment $\boldsymbol{B}_{j1}$ be defined by the points $P_{j11}(x_{j11}, y_{j11})$, $P_{j12}(x_{j12}, y_{j12})$, $P_{j13}(x_{j13}, y_{j13})$, $P_{j14}(x_{j14}, y_{j14})$, and the segment $\boldsymbol{B}_{j2}$ by the points $P_{j21}(x_{j21}, y_{j21})$, $P_{j22}(x_{j22}, y_{j22})$, $P_{j23}(x_{j23}, y_{j23})$, $P_{j24}(x_{j24}, y_{j24})$. Let find the control and anchor points of the assumed Bezier curve $\boldsymbol{B}_j$. The starting point of the first segment of the curve $P_{j11}(x_{j11}, y_{j11})$ coincides with the starting point of the assumed curve $P_{j1}(x_{j1}, y_{j1})$, the ending point of the second segment of the curve $P_{j24}(x_{j24}, y_{j24})$ coincides with the ending point of the original curve $P_{j4}(x_{j4}, y_{j4})$.

From formula (5) and (6) find the coordinates of the control points of the assumed curve:

$$x_{j2} = \frac{x_{j12} - x_{j1}t_0}{t},\quad y_{j2} = \frac{y_{j12} - y_{j1}t_0}{t},\quad x_{j3} = \frac{x_{j23} - x_{j4}t}{t_0},\quad y_{j3} = \frac{y_{j23} - y_{j4}t}{t_0}.$$

Having determined the parameters of all points of the assumed curve, we check whether the division point of this curve corresponds to the parameter t. If this is the case, then the next step of the algorithm is performed;

otherwise, the division ratio $1 - t$ is additionally checked. If in this ratio the curve is divided by a point, then the next step of the algorithm is performed; otherwise, it is assumed that the message is not hidden in this curve.

At the next step of the algorithm, for each segment of the curve $\boldsymbol{B}_j'$ the data of two binary pairs Q_k is extracted from the control points of the segments. From the second control point of the first segment of the original curve $P_{j13}\left(x_{j13}, y_{j13}\right)$ the value corresponding to the first binary pair is extracted: the first digit of the value is extracted from LSB of the coordinate x_{j13}, and the second digit of the value is extracted from LSB of the coordinate y_{j13}. Similarly, the value corresponding to the second binary pair is extracted from the coordinates of the first control point of the second segment of the obtained curve $P_{j22}\left(x_{j22}, y_{j22}\right)$.

From the obtained values according to table 1 the binary pairs are formed, which are combined into a single message. The binary message is converted to text and analysed. If an end-of-message character is found in the recovered string, the message has been recovered.

The block diagram of the extraction algorithm is shown in fig. 10.

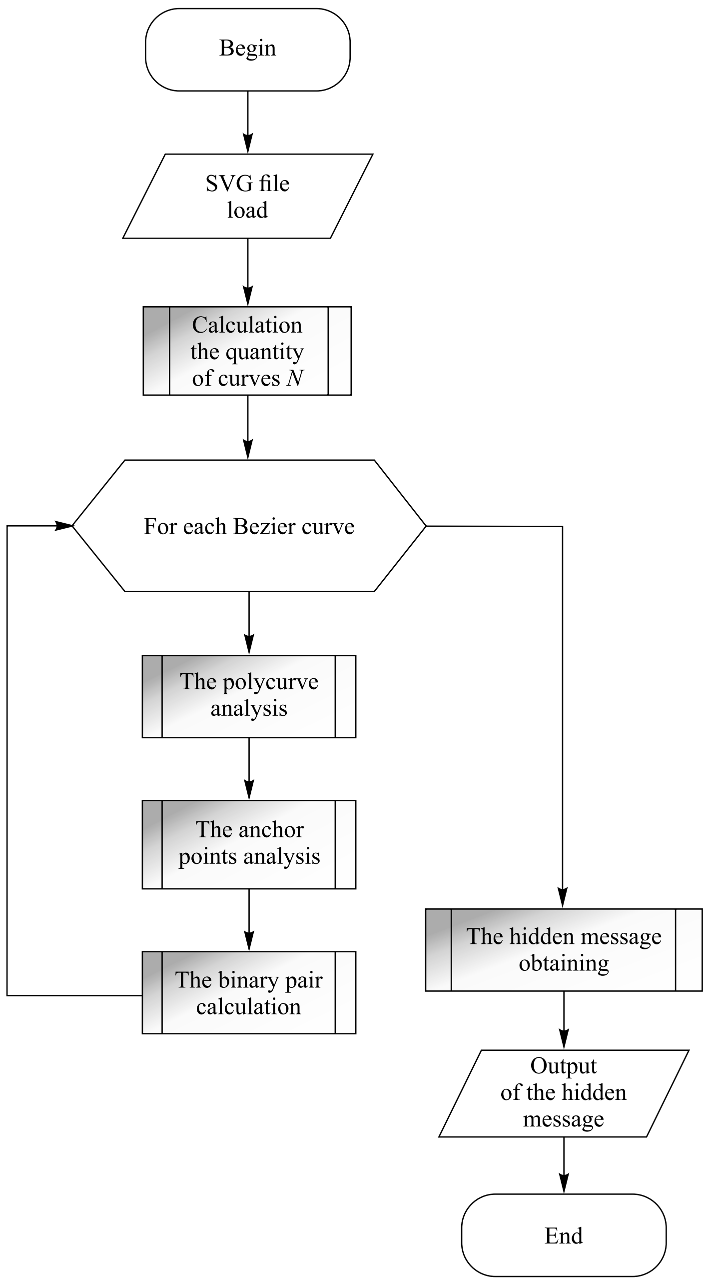


Fig. 10. Block diagram of the algorithm of a message extraction from the stego container

Let's continue with an example of how the method works. Assume we have a drawing in SVG format, the description of which is shown in fig. 9.

There are two of third-order Bezier curves in this image. Consider the first curve. It consists of two segments. We will check two stages: at the first stage we assume that the segments form a single Bezier curve and calculate the coordinates of the control points of this curve; at the second stage we check whether the division point of the segments belongs to the assumed curve. If the division point belongs to a curve, then we can conclude that this curve is a single Bezier curve.

From formulas (5) and (6), knowing x_1, x_{12}, t and t_0, it is possible to obtain x_2. Similarly, knowing y_1, y_{12}, t and t_0, it is possible to obtain y_2. Just the same, knowing x_4, x_{23}, t and t_0, it is possible to obtain x_3, and knowing y_4, y_{23}, t and t_0, it is possible to obtain y_3. We know that the division ratio t can be either 0.25 or 0.75, depending on the first symbol of the binary pair, if the binary pair is hidden in this curve. Assume that $t = 0.25$. Based on this, we calculate the coordinates of the assumed Bezier curve: $P_1(10, 200)$, $P_2(120, 30)$, $P_3(170, 70)$, $P_4(220, 100)$. Let's make sure that the point $(82.1875, 108.4375)$ belongs to the assumed curve. From formula (4) we obtain the coordinates of the division point of the assumed curve at the ratio 0.25, this is the point $(82.1875, 108.4375)$, therefore, the point $(82.1875, 108.4375)$ belongs to the curve, so the curve is a single Bezier curve. Consider points $P_{13}(61.250001, 128.125002)$ and $P_{22}(145.000008, 49.375007)$. At these points we expect to find an embedded message. Let's extract the values from the least significant digit of the coordinates: from the first coordinate 61.250001 we extract the last significant digit, i. e. 1, from the second coordinate 128.125002 we extract the last significant digit, i. e. 2, we get the first value 12. Similarly, we get 87 from the second control point. According to the table 2 we get binary pairs 11 and 00.

Let us do the same for the second curve. It also has two segments. It is necessary to check if these segments are a single Bezier curve and what is the division ratio. Suppose that the division ratio is $t = 0.25$, and from formulas (5) and (6) we calculate the coordinates of the assumed curve. We obtain the coordinates of the assumed Bezier curve: $P_1(10, 200)$, $P_2(520, -190)$, $P_3(220, 166.6667)$, $P_4(230, 150)$. Let us check if the point $(206.875, 160.625)$ belongs to the obtained curve. From formula (4) we obtain the coordinates of the division point of the assumed curve at the ratio 0.25, this is the point $(258.125, 30)$, therefore, the division ratio is not 0.25. Assume that the division ratio is $t = 0.75$, and from formulas (5) and (6) we calculate the coordinates of the assumed curve. We obtain the coordinates of the assumed Bezier curve: $P_1(10, 200)$, $P_2(180, 70)$, $P_3(200, 200)$, $P_4(230, 150)$. Let us check if the point $(206.875, 160.625)$ belongs to the obtained curve. From formula (5) we obtain the coordinates of the division point of the assumed curve at the ratio of 0.25, this is the point $(206.875, 160.625)$. Therefore, the point $(206.875, 160.625)$ belongs to the curve, this curve is a single Bezier curve. Consider points $P_{13}(180.625006, 151.250004)$ and $P_{22}(215.625003, 163.750007)$. At these point, we expect to find an embedded message. Let's extract the values from the least significant digits of the coordinates: 64 and 37, respectively. According to the table 1 we get binary pairs 01 and 10.

Thus, the extracted message will look like 11000110. The message has been recovered correctly.

Results and discussion

To implement the described steganographic method, the DLL StegoSVG library was developed. The library contains classes that implement the analysis of a file in SVG format, counting the number of cubic Bezier curves, dividing a message into binary pairs, dividing cubic Bezier curves into segments, both algorithms for embedding and extracting messages.

A desktop application StegoSVG Demo has been created to demonstrate the method. The application interface can be roughly divided into three areas: the configuration area, the analysis area, and the working area. The analysis area contains information obtained during the analysis of the file, such as the time of the beginning and the end of the analysis, the number of third-order Bezier curves found in the file, the maximum possible message length, errors that occur when the library or application is running. The working area, depending on the operating mode, provides the ability to add or extract a message. Figure 11 shows a general view of the application in the hidden message embedding mode. This is a small SVG file of 100 kilobytes.

To test the operation of the program SVG images were taken from the site *www.freesvg.org.* The results of the program are presented in table 5.

Not all images were suitable for analysis as they did not contain cubic Bezier curves. Ten SVG files containing cubic Bezier curves and suitable for the implementation of the watermark were analysed. The hidden message consisted of 25 characters (Stegano Message 21/07/2021), with the exception of file No. 5 where a hidden message of 10 characters was embedded (21/07/2021).

Table 5

Results of hidden message embedding into SVG files

No.	Source file size (V_1), bytes	The number of curves	The size of stego container (V_2), bytes	The difference ($V_1 - V_2$), bytes
1	5 115 022	17 882	5 126 306	11 284
2	5 028 074	17 878	5 042 548	14 474
3	429 566	472	435 923	6357
4	1 426 801	13 048	1 432 974	6173
5	45 826	40	48 340	2514
6	136 111	52	140 410	4299
7	117 750	297	122 281	4531
8	108 998	144	113 419	4421
9	83 261	219	87 666	4405
10	122 579	229	127 187	4608

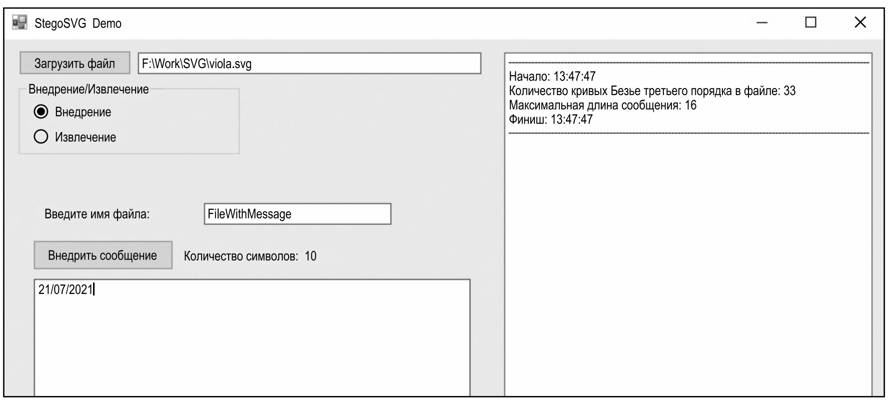


Fig. 11. StegoSVG Demo application interface

File sizes are in bytes. We also note that the difference in size between the original and the file and the corresponding steganographic file is not constant. The increase in the size of the latter, of course, depends on the length of the message, but also depends on the original image. Since the hidden message is embedded in the new control points, and the calculation accuracy is no less than 0.000001, then, depending on the initial coordinates of the anchor and control points of the Bezier curve, the number of characters in the file description can increase when fractional coordinates appear.

Visually, the original file and the steganographic file look the same. When viewed in specialised software (Corel DRAW v.20), the number of objects and curves is the same, but the number of points and file size are different.

When changing a file with a watermark with specialised software, the sign can either be preserved or destroyed, depending on the type of changes. When converting a steganographic file using Corel DRAW v.20 to PNG and TIFF raster formats and vice versa, the mark is completely lost, because from raster formats the file is restored close to the original, but not exactly the same. When converting a steganographic file to EPS vector format and vice versa, the mark is also lost. In this case the file also does not return to its original state, all coordinates change. When archiving a file with an embedded message using ZIP and RAR archivers, the watermark remains after unpacking.

Conclusion

A new steganographic method is considered for embedding and extracting hidden messages when using SVG files as stego containers. The method is based on modifying the parameters of cubic Bezier curves. In particular, a combined approach is used to embed digital watermarks or digital labels in additional points of Bezier curves, as well as in additional lower digits of control points. The combined use of several methods of introducing a secret message allows to increase the length of the hidden sequence, as well as to control the integrity of the message being embedded.

To implement the method, the StegoSVG library was developed, which was used in the development of the author's desktop application (StegoSVG Demo). Several files of the SVG format taken from open sources have been analysed for the possibility of placing steganographic DWMs in them.

The method can be used to apply digital watermarks or digital labels on graphic images in SVG format, in which cubic Bezier curves are present. With some modifications the method can be applied to SVG images with quadratic Bezier curves. Two Bezier curves are required to embed one message symbol, so this method is also suitable for relatively small images. Two parameters are the steganographic key: the ratio of dividing the original curve into segments and the correspondence of the values of binary pairs to the values written in LSB of coordinates.

Due to the specificity of the path tag used to embed hidden information into an image, the method cannot be directly used in other kinds of XML containers such as electronic documents and electronic maps, however, an approach that connects the separation of an object in some way and a record of hidden information in LSB of emerging points seems to be quite promising.

Since the SVG format provides web designers with tremendous opportunities in the implementation of static and interactive animated images for sites, the proposed method can be used to protect sites from fakes. Phishing protection can also be developed on this basis.

Further research in this direction is of interest from the point of view of ensuring a given level of steganographic resistance of the method, for example, based on the development and use of the corresponding key information.

Библиографические ссылки

1. Грибунин ВГ, Оков ИН, Туринцев ИВ. *Цифровая стеганография.* Москва: Солон-пресс; 2009. 264 с.

2. Urbanovich P, Chourikov K, Rimorev A, Urbanovich N. Text steganography application for protection and transfer of the information. *Przeglad elektrotechniczny.* 2010;7:95–97.

3. Agarwal M. Text steganographic approaches: a comparison. *International Journal of Network Security & Its Applications.* 2013; 1(5):91–106. DOI: 10.5121/ijnsa.2013.5107.

4. Blinova E, Shutko N. The use of steganographic methods in SVG format graphic files. In: *New electrical and electronic technologies and their industrial implementation. Proceedings of the 10th International conference; 2017 June 23–26; Zakopane, Poland.* Lublin: Lublin University of Technology; 2017. p. 45.

5. Шутько НП. Защита и передача текстовой информации на основе изменения кернинга. *Труды БГТУ. Серия 3. Физико-математические науки и информатика.* 2017;2:92–95.

6. Shutko N, Urbanovich P, Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd elektrotechniczny.* 2018;6:82–85. DOI: 10.15199/48.2018.06.15.

7. Блинова ЕА, Сущеня АА. Применение нескольких стеганографических методов для осаждения скрытых данных в электронных текстовых документах. *Системный анализ и прикладная информатика.* 2019;2:32–38. DOI: 10.21122/2309-4923- 2019-2-32-38.

8. Урбанович ПП, Юрашевич ДЭ. Использование системных свойств и параметров текстовых файлов в стеганографических приложениях. В: Харин ЮС, Чернявский АФ, Берник ВИ, Кучинский ПВ, Курбацкий АН, Агиевич СВ, редакторы. *Теоретическая и прикладная криптография. Материалы Международной научной конференции; 20–21 октября 2020 г.; Минск, Беларусь.* Минск: БГУ; 2020. с. 68–73.

9. Kaur D, Verma HK, Singh RK. Image steganography: hiding secrets in random LSB pixels. In: Pant M, Sharma TK, Verma OP, Singla R, Sikander A, editors. *Soft computing: theories and applications.* Singapore: Springer; 2020. p. 331–341 (AISC; volume 1053). DOI: 10.1007/978-981-15-0751-9_31.

10. Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: a review of the recent advances. *IEEE Access.* 2021;9:23409–23423. DOI: 10.1109/access.2021.3053998.

11. Блинова ЕА, Урбанович ПП. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG. *Труды БГТУ. Серия 3. Физико-математические науки и информатика.* 2018;2:104–109.

12. Блинова ЕА, Голик АА. Модификация стеганографического метода на основе встраивания дополнительных значений координат в изображения формата SVG. В: Тузиков АВ, Григянец РБ, Венгеров ВН, редакторы. *Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2018). Доклады XVII Международной конференции; 20 сентября 2018 г.; Минск, Беларусь.* Минск: ОИПИ НАН Беларуси; 2018. с. 130–133.

13. Farin GE, Hansford D. *The essentials of CAGD.* 1st edition. Natick: A. K. Peters Ltd.; 2000. 242 p.

References

1. Gribunin VG, Okov IN, Turintsev IV. *Tsifrovaya steganografiya* [Digital steganography]. Moscow: Solon-press; 2009. 264 p. Russian.

2. Urbanovich P, Chourikov K, Rimorev A, Urbanovich N. Text steganography application for protection and transfer of the information. *Przeglad elektrotechniczny.* 2010;7:95–97.

3. Agarwal M. Text steganographic approaches: a comparison. *International Journal of Network Security & Its Applications.* 2013; 1(5):91–106. DOI: 10.5121/ijnsa.2013.5107.

4. Blinova E, Shutko N. The use of steganographic methods in SVG format graphic files. In: *New electrical and electronic technologies and their industrial implementation. Proceedings of the 10th International conference; 2017 June 23–26; Zakopane, Poland.* Lublin: Lublin University of Technology; 2017. p. 45.
5. Shutko NP. Protection and transfer of text information on the basis of kerning changing. *Trudy BGTU. Seriya 3. Fiziko-matematicheskie nauki i informatika.* 2017;2:92–95. Russian.
6. Shutko N, Urbanovich P, Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd elektrotechniczny.* 2018;6:82–85. DOI: 10.15199/48.2018.06.15.
7. Blinova EA, Sushchenia AA. Several steganographic methods using for embedding of hidden data in electronic text documents. *Sistemnyi analiz i prikladnaya informatika.* 2019;2:32–38. Russian. DOI: 10.21122/2309-4923-2019-2-32-38.
8. Urbanovich PP, Yurashevich DE. [Using system properties and text file settings in steganographic applications]. In: Kharin YuS, Chernyavskii AF, Bernik VI, Kuchinskii PV, Kurbatskii AN, Agievich SV, editors. *Teoreticheskaya i prikladnaya kriptografiya. Materialy Mezhdunarodnoi nauchnoi konferentsii; 20–21 oktyabrya 2020 g.; Minsk, Belarus'* [Theoretical and applied cryptography. Materials of an International scientific conference; 2020 October 20–21; Minsk, Belarus]. Minsk: Belarusian State University; 2020. p. 68–73. Russian.
9. Kaur D, Verma HK, Singh RK. Image steganography: hiding secrets in random LSB pixels. In: Pant M, Sharma TK, Verma OP, Singla R, Sikander A, editors. *Soft computing: theories and applications.* Singapore: Springer; 2020. p. 331–341 (AISC; volume 1053). DOI: 10.1007/978-981-15-0751-9_31.
10. Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: a review of the recent advances. *IEEE Access.* 2021;9:23409–23423. DOI: 10.1109/access.2021.3053998.
11. Blinova EA, Urbanovich PP. A steganographic method based on the embedding of additional coordinates into images of SVG format. *Trudy BGTU. Seriya 3. Fiziko-matematicheskie nauki i informatika.* 2018;2:104–109. Russian.
12. Blinova EA, Golik AA. [The modification of the steganographic method based on the embedding of additional coordinates into images in SVG format]. In: Tuzikov AV, Grigyanets RB, Vengerov VN, editors. *Razvitie informatizatsii i gosudarstvennoi sistemy nauchno-tekhnicheskoi informatsii (RINTI-2018). Doklady XVII Mezhdunarodnoi konferentsii; 20 sentyabrya 2018 g.; Minsk, Belarus'* [Development of informatisation and the state system of scientific and technical information (RINTI-2018). Reports of the 17th International conference; 2018 September 20; Minsk, Belarus]. Minsk: Joint Institute for Informatics Problems of the National Academy of Sciences of Belarus; 2018. p. 130–133. Russian.
13. Farin GE, Hansford D. *The essentials of CAGD.* 1st edition. Natick: A. K. Peters Ltd.; 2000. 242 p.

Received 02.09.2021 / revised 12.10.2021 / accepted 09.11.2021.

УДК 519.714:004.3

СИНТЕЗ КВАНТОВЫХ СХЕМ НА ОСНОВЕ НЕ ПОЛНОСТЬЮ ОПРЕДЕЛЕННЫХ ФУНКЦИЙ И *if*-ДИАГРАММ РЕШЕНИЙ

А. А. ПРИХОЖИЙ[1)]

[1)]*Белорусский национальный технический университет, пр. Независимости, 65, 220013, г. Минск, Беларусь*

Рассматривается задача синтеза и оптимизации логических обратимых и квантовых схем по функциональным описаниям, представленным диаграммами решений. Задача относится к ключевым проблемам, решаемым в целях создания квантовых компьютеров и технологий квантовых вычислений. Предлагается новый метод последовательной трансформации исходной функциональной спецификации в квантовую схему, предусматривающий следующие состояния проекта: сокращенную упорядоченную диаграмму двоичных решений, *if*-диаграмму решений, функциональную *if*-диаграмму решений, обратимую схему, квантовую схему. Новизна метода состоит в расширении разложений Шеннона и Давио булевой функции по отдельной переменной до разложений этой же функции по другой булевой функции с получением продуктов разложения, представленных не полностью определенными функциями. Неопределенность в продуктах разложения расширяет возможности по минимизации графового представления заданной функции. Вместо двух исходящих ветвей вершины двоичной диаграммы генерируются три исходящие ветви вершины *if*-диаграммы, что увеличивает уровень параллелизма в обратимых и квантовых схемах. Для каждого шага трансформации предложены свои правила отображения, сокращающие число линий и вентилей и глубину схемы. Сравнение новых результатов с результатами, полученными известным методом отображения вершин двоичных диаграмм решений на каскады обратимых и квантовых вентилей, показало, что использование предложенного метода позволит существенно улучшить параметры синтезируемых квантовых схем.

Ключевые слова: обратимое вычисление; квантовая логическая схема; синтез; не полностью определенная функция; разложение функции; диаграмма решений; размер схемы; глубина схемы; минимизация.

SYNTHESIS OF QUANTUM CIRCUITS BASED ON INCOMPLETELY SPECIFIED FUNCTIONS AND *if*-DECISION DIAGRAMS

A. A. PRIHOZHY[a]

[a]*Belarusian National Technical University, 65 Niezaliežnasci Avenue, Minsk 220013, Belarus*

The problem of synthesis and optimisation of logical reversible and quantum circuits from functional descriptions represented as decision diagrams is considered. It is one of the key problems being solved with the aim of creating quantum computing technology and quantum computers. A new method of stepwise transformation of the initial functional

Образец цитирования:
Прихожий АА. Синтез квантовых схем на основе не полностью определенных функций и *if*-диаграмм решений. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:84–97 (на англ.).
https://doi.org/10.33581/2520-6508-2021-3-84-97

For citation:
Prihozhy AA. Synthesis of quantum circuits based on incompletely specified functions and *if*-decision diagrams. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:84–97.
https://doi.org/10.33581/2520-6508-2021-3-84-97

Автор:
Анатолий Алексеевич Прихожий – доктор технических наук, профессор; профессор кафедры программного обеспечения информационных систем и технологий факультета информационных технологий и робототехники.

Author:
Anatoly A. Prihozhy, doctor of science (engineering), full professor; professor at the department of information system and technology software, faculty of information technologies and robotics.
prihozhy@yahoo.com

specification to a quantum circuit is proposed, which provides for the following project states: reduced ordered binary decision diagram, *if*-decision diagram, functional *if*-decision diagram, reversible circuit and quantum circuit. The novelty of the method consists in extending the Shannon and Davio expansions of a Boolean function on a single variable to the expansions of the same Boolean function on another function with obtaining decomposition products that are represented by incompletely defined Boolean functions. Uncertainty in the decomposition products gives remarkable opportunities for minimising the graph representation of the specified function. Instead of two outgoing branches of the binary diagram vertex, three outgoing branches of the *if*-diagram vertex are generated, which increase the level of parallelism in reversible and quantum circuits. For each transformation step, appropriate mapping rules are proposed that reduce the number of lines, gates and the depth of the reversible and quantum circuit. The comparison of new results with the results given by the known method of mapping the vertices of binary decision diagram into cascades of reversible and quantum gates shows a significant improvement in the quality of quantum circuits that are synthesised by the proposed method.

Keywords: reversible computation; quantum logic circuit; synthesis; incompletely specified function; expansion of function; decision diagram; circuit size; circuit depth; minimisation.

Introduction

Nowadays, the synthesis of reversible and quantum logic circuits is an intensely investigated scientific direction [1–4]. The circuits have the same number of inputs and outputs, consist of reversible gates and implement permutation functions, therefore carry out information-lossless computations and have the dramatically reduced power consumption. The application domains of reversible computations are optical and DNA computing, nanotechnologies, cryptography and quantum computers [5]. The reversible and quantum design flow is mostly similar to the design automation flow of electronic circuits. It considers a design at abstraction levels from technology independent behavioural (high-level) descriptions to technology dependent quantum-level descriptions. Methods of synthesis of reversible and quantum logic circuits has been developed in [6–9]. Firstly, a reversible quantum compiler maps an input functional or algorithmic specification to a technology independent logic description that is composed of reversible gates from a reversible gate library. Its goal is the minimisation of the number of gates and the number of lines (qubits). Different intermediate representations and formats, including truth tables, binary decision diagrams (BDD), reduced ordered binary decision diagrams (ROBDD), functional decision diagrams (FDD), reduced ordered functional diagrams (ROFDD), Reed – Muller forms, etc., have been proposed in the literature [10–14]. At this level, exact and heuristic synthesis methods are used. The method based on Boolean satisfiability [15] gives exact solutions for only small circuit sizes. To synthesise larger functional specifications, heuristic methods as follows are proposed [6; 9; 10; 16]: transformation-based approach, evolutionary algorithms, decision diagram based methods, etc. Secondly, the obtained reversible logic circuit is mapped to a quantum circuit composed of technology dependent quantum gates from a quantum elementary gate library.

The approach proposed in [12] immediately maps a ROBDD to a reversible and then a quantum circuit. A new class of *if*-decision diagrams (IFD) and functional *if*-decision diagrams (FIFD) that is based on incompletely specified Boolean functions is proposed in [17–19]. The main contribution of this paper is as follows: 1) novel expansions of incompletely and completely specified Boolean functions, which use a minimisation operation, perform efficient transition from ROBDD to IFD, support the synthesis of three-branch-node diagrams with higher parallelism; 2) new step-wise method of transforming ROBDD to IFD and further transforming IFD to FIFD of reduced size and (or) depth; 3) efficient rules of mapping FIFD nodes to cascades of reversible gates and mapping FIFD to a reversible circuit; 4) new techniques for synthesis, minimisation and parallelisation of quantum circuits from the reversible circuits.

Reversible logic circuits

A reversible circuit [1; 3] realises a reversible logic function by means of lines and reversible gates. The function is bijective since it has equal number of inputs and outputs, maps each input to a unique output, and is capable of reconstructing the input from the output. The circuit has no fan-out and feedback connections. The lines are labeled by Boolean variables of a set X. The reversible gate has the form of $G(T, C)$, where $T \subset X$ is a set of target lines, and $C \subset X$ is a set of control lines ($C \cap T = \varnothing$). The gate operation is applied to the target line if the control lines meet a true condition. The target line is represented by $\oplus$, and its control line is represented by $\bullet$. Nowadays, some reversible gate libraries are available. The NCT library [1] includes (fig. 1, *a*) the NOT gate, the CNOT gate with one control line, and the Toffoli gate with two control lines. The GT library [6] includes generalised multiple-control Toffoli gates. The Toffoli gate maps three inputs to three outputs: $G(L, C_0, C_1) = (L \oplus (C_0 \wedge C_1), C_0, C_1)$, where $\oplus$ is exclusive-or; $\wedge$ is Boolean conjunction;

L is input at target line; C_0, C_1 are conditions at control lines. The CNOT gate maps two inputs to two outputs: $G(L, C_0) = (L \oplus C_0, C_0)$. The NOT gate realises Boolean inversion: $G(L) = (\neg L)$. Therefore, the reversible circuit describes a behaviour with a superposition of three Boolean operations: $\neg$, $\wedge$ and $\oplus$.

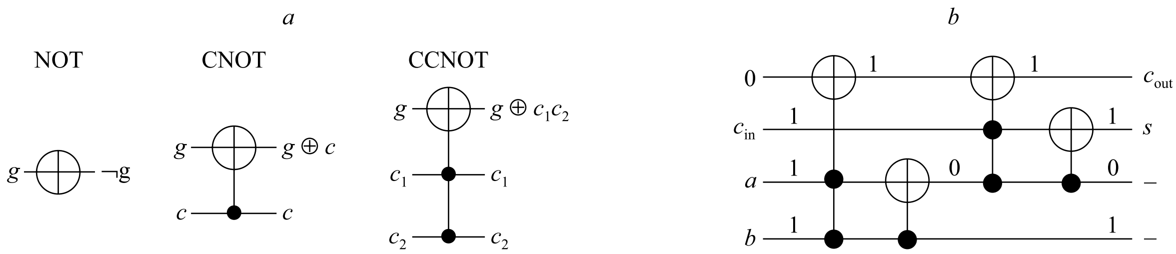


Fig. 1. Reversible gates of NCT library:
a – reversible gates NOT, CNOT and CCNOT (Toffoli);
b – realisation of 1-bit full adder by cascade of gates

Quantum logic circuits

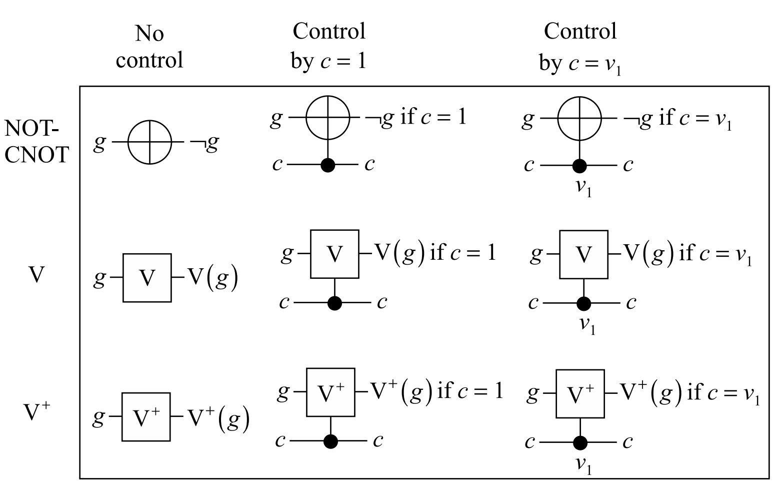
Quantum circuits carry out computations by changing states of qubits [1; 3]. The qubit state is $|\Psi\rangle = \alpha|0\rangle +$ $+ \beta|1\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Quantum gates perform operations on qubits. A cascade of quantum gates applied to qubits is a quantum circuit. Quantum logic gates and circuits are reversible. Competitive quantum gate libraries are developed. The NCV library [1] is the most commonly used for synthesis of quantum circuits. Its gates require Boolean control lines. To the NOT and CNOT gates, the NCV adds V, CV, V^+ and CV^+ gates, which are known as square-root of the NOT gate:

$$\text{V} = \frac{1+i}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, \quad \text{V}^+ = \frac{1-i}{2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

The NCV-$|v_1\rangle$ [3] library considers a 4-level (0, v_0, 1 and v_1) quantum system and uses qudits instead of qubits. Its gates use v_1 as control value. Figure 2, *a*, depicts the key NCV and NCV-$|v_1\rangle$ quantum gates. The NOT gate without control, and CNOT gate controlled by 1 are similar to the corresponding gates of NCT. NCV-$|v_1\rangle$ introduces a CNOT gate controlled by v_1. The gate keeps the value unchanged if $c \neq v_1$. There are V and V^+ gates without control and with control by v_1. Figure 2, *b*, describes the gates' mapping functions.

Since the quantum libraries have no gate that immediately implements the Toffoli gate, they replace the gate by a cascade of quantum gates from the NCV (fig. 3, *a*) or NCV-$|v_1\rangle$ (fig. 3, *b*) library. A n-control Toffoli gate can be replaced by $2n + 1$ quantum gates from NCV-$|v_1\rangle$. After the replacement, minimisation techniques can reduce the quantum circuit size. Figure 3, *c*, depicts a minimised quantum circuit of 1-bit full adder.

a



b

g	NOT(g)	V(g)	$\text{V}^+(g)$
0	1	v_0	v_1
v_0	v_1	1	0
1	0	v_1	v_0
v_1	v_0	0	1

Fig. 2. Quantum gates of NCV and NCV-$|v_1\rangle$ libraries:
a – quantum gates NOT, CNOT, V and V^+; *b* – operation of quantum gates in 4-level quantum system

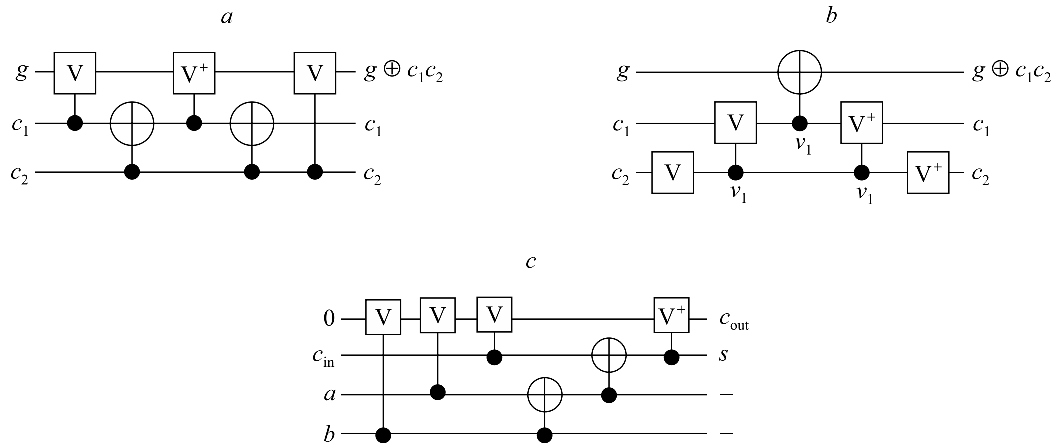


Fig. 3. Realisation of Toffoli two-control gate by cascades of quantum gates:
a – cascade of NCV library gates; *b* – cascade of NCV-$|v_1\rangle$ library gates;
c – quantum circuit for 1-bit full adder

Approaches for modelling, synthesis and optimisation of reversible and quantum circuits

Various models and methods are used for synthesis and optimisation of reversible and quantum logic circuits.

Reed – Muller expansions (Zhegalkin polynomials). The forms are based on two-level AND/EXOR and directly mapped into reversible circuits using the multi-control Toffoli gates.

Optimisation based on exclusive-sum-of-products (ESOP). Described in the literature [11] approaches for minimising the exclusive-or of Boolean cubes are applicable to reversible and quantum circuits.

Quantum operator form. It is a quantum extension [14] to the Reed – Muller form, which represents quantum circuits based on the CNOT, CV and CV^+ quantum gates, and permits minimisation of circuits by using properties of quantum gates in addition to Toffoli gates.

Binary decision diagram. It is a graph representation of a Boolean function [12; 13] based on the Shannon expansion (1) of Boolean function $f(x)$, $x = (x_1, \ldots, x_n)$ on variable x_i:

$$f = \neg x_i \wedge f_{x_i = 0} \vee x_i \wedge f_{x_i = 1}, \tag{1}$$

where $\vee$ is Boolean disjunction. Residual functions $f_{x_i=0}$ and $f_{x_i=1}$ are called negative and positive cofactors. Syntactically, BDD is a rooted acyclic directed graph consisting of terminal nodes labeled by 0 and 1 and non-terminal nodes (fig. 4, *a*) labeled by Boolean variables $x_i \in X$ and having outgoing edges *low* and *high*. Term $bdd(x_i, n, p)$ denotes a non-terminal node. In a reduced ordered ROBDD, the variable order is the same along all paths from root to leaves. Rules *S* and *I* perform the reduction: rule *S* deletes non-terminal node $v = bdd(x_i, n, n)$ and redirects the incoming edges from *v* to *n*; rule *I* removes one of two identical nodes and redirects its incoming edges to the remaining node. Figure 4, *b*, depicts an example ROBDD.

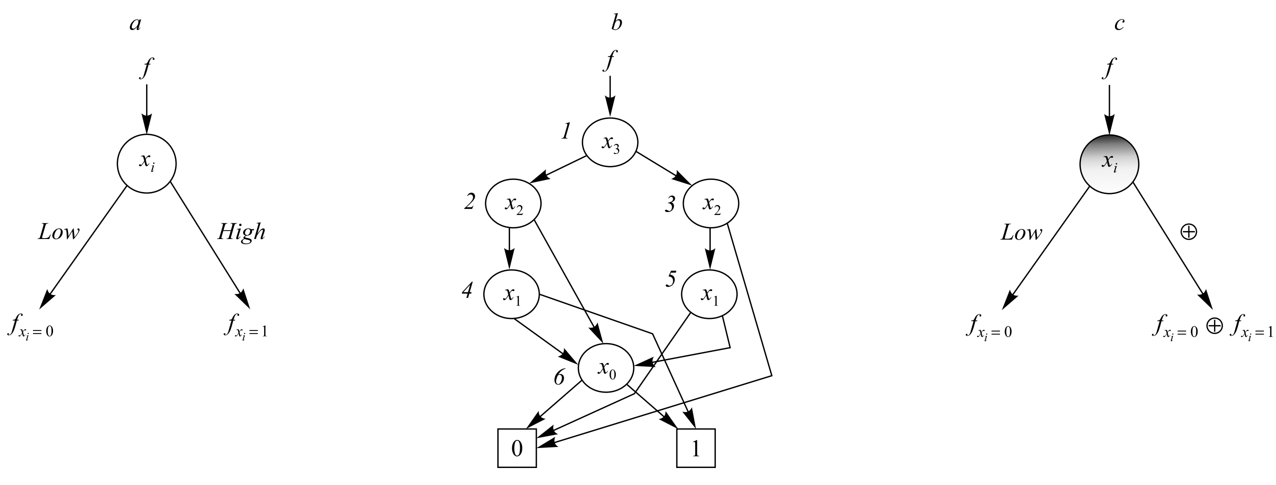


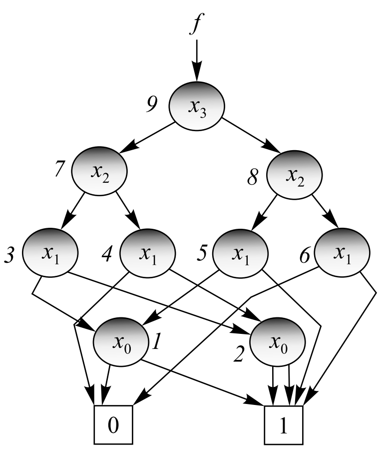
Fig. 4. Binary and functional decision diagrams: *a* – non-terminal node of BDD;
b – example ROBDD (*1–6* denote the diagram node numbers); *c* – non-terminal node of FDD

Functional decision diagrams. The positive and negative Davio expansions (2) and (3) of Boolean function $f(x)$ was a basic idea for creating the FDD:

$$f = f_{x_i=0} \oplus x_i \wedge \left(f_{x_i=0} \oplus f_{x_i=1}\right), \tag{2}$$

$$f = f_{x_i=1} \oplus \neg x_i \wedge \left(f_{x_i=0} \oplus f_{x_i=1}\right). \tag{3}$$

Constructively FDD is similar to BDD. The non-terminal node (fig. 4, *c*) is labeled by $x_i \in X$, and has two outgoing edges *low* and ⊕, which point two sub-diagrams representing cofactors $n = f_{x_i=0}$ and $b = f_{x_i=0} \oplus f_{x_i=1}$ respectively for (2). Term $fdd(x_i, n, b)$ denotes the FDD. A ROFDD orders the variables and has exactly two terminal nodes labeled by 0 and 1. Two rules *D* and *I* reduce the diagram: rule *D* deletes non-terminal node $v = fdd(x_i, n, 0)$ and redirects the incoming edges from *v* to *n*; rule *I* is the same as for ROBDD. Figure 5, *a*, depicts an example ROFDD derived from the example ROBDD. The ROFDD's nodes match well reversible gates.



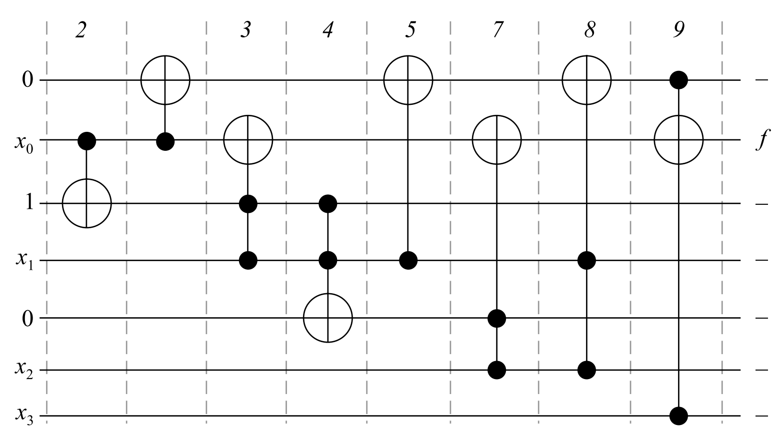


Fig. 5. Mapping BDD to reversible circuit:
a – example ROFDD that is functionally equivalent
to example ROBDD (*1–9* denote the diagram node numbers);
b – realisation of ROFDD by reversible circuit (diagram node numbers are above columns)

Works [11; 12] propose a technique of synthesising a reversible circuit from ROBDD, which substitutes all diagram nodes with cascades of reversible gates. The size of reversible circuit directly depends on the ROBDD size. Since the ROBDD size can grow exponentially over the number of input variables, the reversible circuit size can grow exponentially too. An alternative technique first transforms ROBDD to ROFDD, and then maps the ROFDD to a reversible circuit. Figure 5, *b*, depicts a reversible circuit synthesised from the example ROFDD.

Quantum gates controlled by various quantum levels. The gates controlled by value v_1 that are introduced in the NCV-$|v_1\rangle$ library reduce the overall size of cascades that realise the multiple-control Toffoli gates [3; 6].

Template matching. It is a common approach to reversible and quantum circuit simplification [6]. Each template that is a cascade of gates in a circuit is replaced by a functionally equivalent smaller cascade.

Using additional ancillaries. Sometimes extra ancillary lines leads to reducing the quantum circuit size and depth [16].

Parallelisation of gates. In a reversible or quantum circuit, two adjacent gates $G(T1, C1)$ and $G(T2, C2)$ can be parallelised [16] and decrease the circuit depth if $(T1 \cup C1) \cap (T2 \cup C2) = \varnothing$.

Expansions of incompletely specified functions

Let $B = \{0, 1\}$ be the set of Boolean values. Set $M = \{0, 1, dc\}$ extends *B* with a don't care value *dc*. A partial variable y_i assumes values from *M*. A partial function $\Phi(y)$ (also known as Kleene function) of variable $y = (y_1, \dots, y_n)$ is a mapping $\Phi\colon M^n \to M$. From functions $\Phi(y)$ and $\Psi(y)$, a superposition $\Phi(y_1, \dots, y_{i-1}, \Psi(y), y_{i+1}, \dots, y_n)$ can be created describing a new partial function. Key unary and binary partial operations are analogues of Boolean unary and binary operations. A partial negation $\sim y_i$ (analogue of Boolean negation ¬) produces 1, 0 and *dc* if y_i is 0, 1 and *dc* respectively. Table 1 defines key partial binary operations: conjunction (&), disjunction (+), implication (⇒) and exclusive disjunction (⊗). These are analogues of the Boolean operations $\wedge$, $\vee$, $\to$ and $\oplus$. For partial operations ~, & and +, the following laws hold: associativity, commutativity, distributivity, identity, annihilator, idempotence, double negation, De Morgan's laws and others.

Table 1

Binary partial logic operations

Variable y_1	0	0	0	1	1	1	*dc*	*dc*	*dc*	Notation
Variable y_2	0	1	*dc*	0	1	*dc*	0	1	*dc*	
Conjunction	0	0	0	0	1	*dc*	0	*dc*	*dc*	$y_1 \,\&\, y_2$
Disjunction	0	1	*dc*	1	1	1	*dc*	1	*dc*	$y_1 + y_2$
Implication	1	1	1	0	1	*dc*	*dc*	1	*dc*	$y_1 \Rightarrow y_2$
Exclusive disjunction	0	1	*dc*	1	0	*dc*	*dc*	*dc*	*dc*	$y_1 \otimes y_2$

An incompletely specified function $\varphi(x)$ of vector Boolean variable $x = (x_1, \ldots, x_n)$ is a mapping φ: $B^n \to M$. Three sets represent $\varphi(x)$: on-set ON^φ; off-set OFF^φ and don't care set DC^φ. Three Boolean characteristic functions describe the sets: $\varphi^{\mathrm{on}}(x)$, $\varphi^{\mathrm{off}}(x)$ and $\varphi^{\mathrm{dc}}(x)$. Function $\varepsilon(x)$ is an extension of $\varphi(x)$ if $\mathrm{ON}^\varepsilon \supseteq \mathrm{ON}^\varphi$ and $\mathrm{OFF}^\varepsilon \supseteq \mathrm{OFF}^\varphi$.

Definition 1. A pair $(f(x)|d(x))$ of Boolean functions is called a value/domain representation of an incompletely specified function $\varphi(x)$ if $f^{\mathrm{on}}(x) \subseteq \varphi^{\mathrm{on}}(x) \cup \varphi^{\mathrm{dc}}(x)$ denotes a value Boolean function and $d(x) = \neg\varphi^{\mathrm{dc}}(x)$ denotes a certainty domain Boolean function (or simply domain function). The pair specifies that $\varphi(x) = 1$ in the area described by Boolean characteristic function $\varphi^{\mathrm{on}}(x) = f(x) \wedge d(x)$, $\varphi(x) = 0$ in the area described by Boolean characteristic function $\varphi^{\mathrm{off}}(x) = \neg f(x) \wedge d(x)$, and $\varphi(x) = dc$ in the area described by Boolean characteristic function $\varphi^{\mathrm{dc}}(x) = \neg d(x)$.

Function $\varphi(x)$ specifies constant 0, constant 1 and constant *dc* by terms $(0|1)$, $(1|1)$ and $(v|0)$ respectively where v is an arbitrary Boolean function. Since the partial logic operations can be applied to pairs $(f(x)|d(x))$, it becomes possible to construct expressions for describing various incompletely specified functions. It also appears to be possible to reduce such expressions to a pair of Boolean functions that are described by Boolean expressions.

Theorem 1. *Following equalities hold for any incompletely specified functions* $(v_1|d_1)$ *and* $(v_2|d_2)$.

$$\sim(v_1|d_1) = (\neg v_1|d_1), \tag{4}$$

$$(v_1|d_1) \,\&\, (v_2|d_2) = (v_1 \wedge v_2 | d_1 \wedge d_2 \vee \neg v_1 \wedge d_1 \vee \neg v_2 \wedge d_2), \tag{5}$$

$$(v_1|d_1) + (v_2|d_2) = (v_1 \vee v_2 | d_1 \wedge d_2 \vee v_1 \wedge d_1 \vee v_2 \wedge d_2), \tag{6}$$

$$(v_1|d_1) \Rightarrow (v_2|d_2) = (v_1 \to v_2 | d_1 \wedge d_2 \vee \neg v_1 \wedge d_1 \vee v_2 \wedge d_2), \tag{7}$$

$$(v_1|d_1) \otimes (v_2|d_2) = (v_1 \oplus v_2 | d_1 \wedge d_2). \tag{8}$$

P r o o f. The equalities are proved in work [18, p. 65–71].

An advantage of equalities (4)–(8) is that the value function of each right part is a Boolean operation that corresponds to the partial operation of the left part. The domain function of the right part is a Boolean function of four essential variables v_1, d_1, v_2, d_2. Equalities (4)–(8) allow the development of expansions of incompletely specified functions on partial logic operations. Let construct expansions on operations &, + and ~.

Theorem 2. *The following equality holds for any incompletely specified function* $(f|d)$ *and any Boolean function c.*

$$(f|d) = (c|1) \,\&\, (f|d \wedge c) + \sim(c|1) \,\&\, (f|d \wedge \neg c). \tag{9}$$

P r o o f. Using (4)–(6), the right part of (9) is equivalently transformed to its left part:

$$(c|1) \,\&\, (f|d \wedge c) + \sim(c|1) \,\&\, (f|d \wedge \neg c) =$$

$$= (c \wedge f | d \wedge c \vee \neg c \wedge 1 \vee \neg f \wedge d \wedge c) + (\neg c \wedge f | d \wedge \neg c \vee c \wedge 1 \vee \neg f \wedge d \wedge \neg c) =$$

$$=(c \wedge f | d \vee \neg c)+(\neg c \wedge f | d \vee c)=$$
$$=(c \wedge f \vee \neg c \wedge f | (d \vee \neg c) \wedge (d \vee c) \vee c \wedge f \wedge (d \vee \neg c) \vee \neg c \wedge f \wedge (d \vee c))=$$
$$=(f | d \vee f \wedge d \wedge c \vee f \wedge d \wedge \neg c)=(f | d).$$

The theorem is proved.

Expansion (9) generalises the well-known Shannon expansion for incompletely specified functions. It replaces a Boolean variable with an arbitrary Boolean function, and replaces cofactors on one Boolean variable with cofactors that are incompletely specified functions.

Corollary 1. *If function d is constant* 1 *and* $(f|1)$ *is a completely specified function, (9) is reduced to (10):*

$$(f|1)=(c|1) \,\&\, (f|c)+\sim(c|1) \,\&\, (f|\neg c). \tag{10}$$

Expansion (10) of the completely specified function introduces terms that describe incompletely specified functions with the same Boolean value function *f* and domain functions *c* and ¬*c* reducing the area of certainty. It is a strength of the expansion. Note that (8) does not support the development of similar expansions for exclusive disjunction.

The following theorem and its corollaries allow to obtain novel expansions of an incompletely specified function whose domain function is represented by a complex Boolean expression. The expression is constructed of such operations as Boolean negation, conjunction, disjunction, implication and exclusive disjunction. The key expansion decomposes an incompletely specified function with the if-then-else Boolean function in the domain part.

Theorem 3. *The following equality holds for any Boolean functions f, e, g and h:*

$$(f | e \wedge g \vee \neg e \wedge h)=(e|1) \,\&\, (f | e \wedge g)+\sim(e|1) \,\&\, (f | \neg e \wedge h). \tag{11}$$

P r o o f. The right part of (11) is equivalently transformed to its left part using (4)–(6):

$$(e|1) \,\&\, (f | e \wedge g)+\sim(e|1) \,\&\, (f | \neg e \wedge h)=$$
$$=(e \wedge f | e \wedge g \vee \neg e \wedge 1 \vee e \wedge \neg f \wedge g)+(\neg e \wedge f | \neg e \wedge h \vee e \wedge 1 \vee \neg e \wedge \neg f \wedge h)=$$
$$=(e \wedge f | \neg e \vee g)+(\neg e \wedge f | e \vee h)=$$
$$=(e \wedge f \vee \neg e \wedge f | (\neg e \vee g) \wedge (e \vee h) \vee e \wedge f \wedge (\neg e \vee g) \vee \neg e \wedge f \wedge (e \vee h))=$$
$$=(f | g \wedge h \vee e \wedge g \vee \neg e \wedge h \vee e \wedge f \wedge g \vee \neg e \wedge f \wedge h)=(f | e \wedge g \vee \neg e \wedge h).$$

The theorem is proved.

Corollary 2. *If function g is Boolean constant* 1 *and the domain function is Boolean disjunction* $e \vee h$ *then (11) is reduced to (12):*

$$(f | e \vee h)=(e|1) \,\&\, (f|e)+\sim(e|1) \,\&\, (f | \neg e \wedge h). \tag{12}$$

Corollary 3. *If function h is Boolean constant* 1 *and the domain function is Boolean implication* $e \to g = \neg e \vee g$ *then (11) is reduced to (13):*

$$(f | e \to g)=(e|1) \,\&\, (f | e \wedge g)+\sim(e|1) \,\&\, (f|\neg e). \tag{13}$$

Corollary 4. *If function* $g = \neg h$ *and the domain function is Boolean exclusive disjunction* $e \oplus h = e \wedge \neg h \vee \neg e \wedge h$ *then (11) is reduced to (14):*

$$(f | e \oplus h)=(e|1) \,\&\, (f | e \wedge \neg h)+\sim(e|1) \,\&\, (f | \neg e \wedge h). \tag{14}$$

Corollary 5. *Incompletely specified function* $(f|c),\ c = e \wedge g \vee \neg e \wedge h$ *that is described by (11) can be considered as a positive cofactor of completely specified function* $(f|1)$ *in (10). Since* $\neg c = e \wedge \neg g \vee \neg e \wedge \neg h$*, a negative cofactor* $(f|\neg c)$ *is inferred from (11) by substituting ¬g instead of g and substituting ¬h instead of h. As a result, equality (10) can be transformed to (15):*

$$(f|1)=(c|1) \,\&\, \left[(e|1) \,\&\, (f | e \wedge g)+\sim(e|1) \,\&\, (f | \neg e \wedge h)\right]+$$
$$+\sim(c|1) \,\&\, \left[(e|1) \,\&\, (f | e \wedge \neg g)+\sim(e|1) \,\&\, (f | \neg e \wedge \neg h)\right]. \tag{15}$$

Equalities (9)–(15) have a wonderful property: all domain functions in right part terms are conjunctions of positive and negative literals. The property simplifies the construction of cofactors of completely and incompletely specified functions.

Expansions based on minimisation of incompletely specified functions

In an incompletely specified function $\varphi = (f \mid c)$, Boolean function *f* may be replaced with any extension *v* from slice (16) without changing φ:

$$(f \wedge c)^{\text{on}} \subseteq v^{\text{on}} \subseteq (f \vee c)^{\text{on}}. \tag{16}$$

Since the functions of slice (16) may obtain different features, in particular they can produce quantum circuits of smaller time delay and (or) occupied area, the author of works [17; 18] introduced an operation $v = \min(f \mid c)$ to select a best function of the slice. In (9)–(15), all incompletely specified functions represented by a pair $(f \mid c)$ of Boolean functions may be replaced with the Boolean function $\min(f \mid c)$, and $(f \mid 1)$ may be replaced with *f* in case all partial logical operations are replaced by corresponding Boolean operations. It should be noted, in a single expression, several *min* operations can be considered as mutually dependent. It can improve the result of incompletely specified function minimisation.

Thus, expansion (10) is transformed to the following expansion:

$$f = c \wedge \min(f \mid c) \vee \neg c \wedge \min(f \mid \neg c). \tag{17}$$

Expansion (17) generalises the Shannon expansion (2) by replacing a Boolean variable x_i with a Boolean function *c*, and replacing the cofactors on x_i with the cofactors on *c* and *min*. Expansion (15) with $c = e \wedge g \vee \neg e \wedge h$ from corollary 5 can be rewritten as follows:

$$\begin{aligned} f = c \wedge \left[e \wedge \min(f \mid e \wedge g) \vee \neg e \wedge \min(f \mid \neg e \wedge h)\right] \vee \\ \vee \neg c \wedge \left[e \wedge \min(f \mid e \wedge \neg g) \vee \neg e \wedge \min(f \mid \neg e \wedge \neg h)\right]. \end{aligned} \tag{18}$$

Expansion (18) has no analogue in the literature. Its special cases are expansion (19) for $c = e \wedge g$:

$$f = c \wedge \left[\min(f \mid e \wedge g)\right] \vee \neg c \wedge \left[e \wedge \min(f \mid e \wedge \neg g) \vee \neg e \wedge \min(f \mid \neg e)\right] \tag{19}$$

and expansion (20) for $c = e \oplus h$:

$$\begin{aligned} f = c \wedge \left[e \wedge \min(f \mid e \wedge \neg h) \vee \neg e \wedge \min(f \mid \neg e \wedge h)\right] \vee \\ \vee \neg c \wedge \left[e \wedge \min(f \mid e \wedge h) \vee \neg e \wedge \min(f \mid \neg e \wedge \neg h)\right]. \end{aligned} \tag{20}$$

Equalities (17)–(20) not only select a particular value function from slice (16) for each *min* operation, they rather prove to be held for any value function from slice (16) that corresponds to every incompletely specified term. The positive and negative Davio expansions are also generalised by means of using incompletely specified functions and the *min* operation:

$$f = \min(f \mid \neg c) \oplus c \wedge \left(\min(f \mid \neg c) \oplus \min(f \mid c)\right), \tag{21}$$

$$f = \min(f \mid c) \oplus \neg c \wedge \left(\min(f \mid \neg c) \oplus \min(f \mid c)\right). \tag{22}$$

In expansions (17)–(22), the value function of all incompletely specified terms is *f*. Contrary, the domain functions are different as well as the level of uncertainty they describe.

Most important realisations of the *min* operation are those reducing the number of essential variables in cofactors. For this reason, we consider the replacement of functions *e*, *g* and *h* with Boolean variables: $e = x_i$, $g = x_j$ and $h = x_k$. Moreover, we introduce new cofactors: $f_{x_i = 0,\, x_j = 0}$, $f_{x_i = 0,\, x_k = 1}$, $f_{x_i = 1,\, x_k = 0}$, $f_{x_i = 1,\, x_j = 1}$, $f_{x_k = x_i}$ and $f_{x_k = \neg x_i}$ of function *f*. The first four cofactors are constructed on Boolean conjunction and are given by residual functions of two variables less. Cofactors $f_{x_k = x_i}$ and $f_{x_k = \neg x_i}$ being introduced by the authors of works [18; 20] replace variable x_k with variable x_i and its negation $\neg x_i$ respectively, and reduce by one the number of essential variables in function *f*. If $c = x_i \wedge x_j \vee \neg x_i \wedge x_k$, expansion (18) is transformed to expansion (23):

$$f = c \wedge \left(x_i \wedge f_{x_i = 1,\, x_j = 1} \vee \neg x_i \wedge f_{x_i = 0,\, x_k = 1}\right) \vee \neg c \wedge \left(x_i \wedge f_{x_i = 1,\, x_j = 0} \vee \neg x_i \wedge f_{x_i = 0,\, x_k = 0}\right). \tag{23}$$

If $c = x_i \wedge x_j$, expansion (19) is transformed to expansion (24):

$$f = c \wedge f_{x_i = 1,\, x_j = 1} \vee \neg c \wedge \left(x_i \wedge f_{x_i = 1,\, x_j = 0} \vee \neg x_i \wedge f_{x_i = 0}\right). \tag{24}$$

If $c = x_i \oplus x_k$, expansion (20) is transformed to expansion (25):

$$f = c \wedge f_{x_k = \neg x_i} \vee \neg c \wedge f_{x_k = x_i}. \tag{25}$$

Expansions (17)–(25) are capable of efficiently solving the problems of reversible and quantum circuit modelling, synthesis and optimisation.

If-decision diagrams

The author of works [17–19] proposed the concept of IFD and FIFD that are derived from expansions of incompletely specified functions. IFD is a rooted directed acyclic labeled graph consisting of non-terminal and terminal nodes. Semantically a non-terminal node of the graph is interpreted as a representation of Boolean function using (17). Figure 6, *a*, depicts a non-terminal node of IFD, which is not labeled and has three outgoing edges *if*, *high* and *low*. Edge *if* points a sub-graph representing function c. Edge *high* points a sub-graph representing function $g = \min(f|c)$. Edge *low* points a sub-graph representing function $h = \min(f|\neg c)$. A term $ifd(c, g, h)$ denotes the node. A labeled terminal node represents a Boolean constant 0, constant 1, variable x_i or its negation $\neg x_i$. IFD can be with or without complement edges. Many reduction rules can be applied to IFD. The *S* and *I* rules of reducing ROBDD are also applicable to IFD. The rules as follows being inapplicable to BDD are new for reducing IFD: $ifd(c, c, h) = ifd(c, 1, h)$, $ifd(c, \neg c, h) = ifd(c, 0, h)$, $ifd(c, g, c) = ifd(c, g, 0)$, $ifd(c, g, \neg c) = ifd(c, g, 1)$ and others. A biconditional binary decision diagram that is proposed in works [18; 20] is a special case of IFD at $c = x_i \oplus x_{i+1}$ and is efficiently applicable to the synthesis of reversible and quantum circuits.

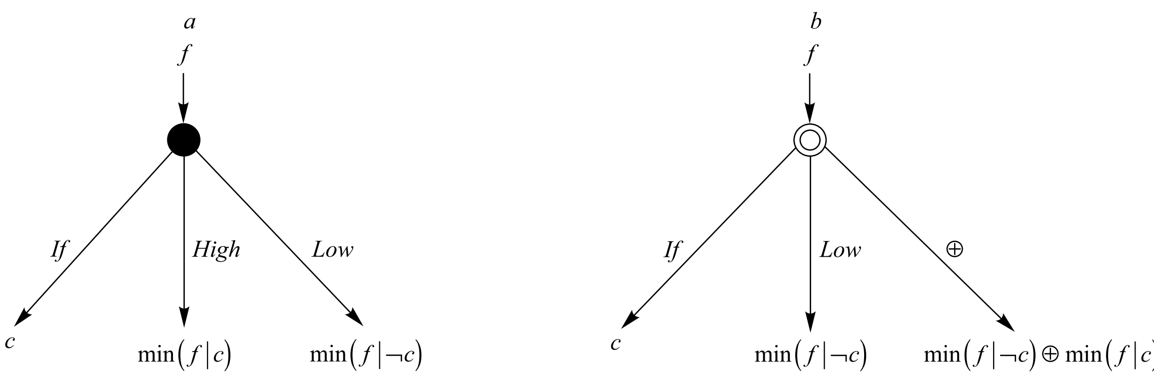


Fig. 6. Non-terminal node of IFD (*a*) and positive FIFD (*b*)

Figure 6, *b*, depicts a non-terminal node of positive FIFD constructed using expansion (21). The node has three outgoing edges *if*, *low* and ⊕, which point sub-graphs representing functions c, $\min(f|\neg c)$ and $\min(f|\neg c) \oplus \min(f|c)$ respectively. Slightly different negative FIFD is constructed using expansion (22). The non-terminal nodes of IFD and FIFD have different views. IFD and FIFD are a promising generalisation of BDD and FDD. All BDDs and FDDs including ROBDDs and ROFDDs can be directly modelled by IFDs and FIFDs. At the same time, tremendous number of IFD and FIFD configurations exist that are not modelled by BDD and FDD. The configurations may allow producing quantum circuit solutions, which overcome those provided by BDD and FDD regarding time and cost parameters. IFD and FIFD have three outgoing edges instead of two in BDD and FBDD, therefore their capabilities for parallelisation are much larger [19].

Synthesis of *if*-decision diagrams from binary decision diagrams

Starting from BDD or ROBDD, we ask the question, what could be a method of generating a functionally equivalent IFD, which has better parameters? To synthesise an IFD of a smaller size and (or) depth, we have developed a method, which intensively exploits the expansions of logic functions proposed in previous sections. Key points of the method are as follows:

1) the transition from ROBDD to IFD which reduces the diagram size and (or) depth is accomplished by the step-wise replacement of nodes with two outgoing edges by nodes with three outgoing edges; the transition is carried out by applying the proposed expansions of incompletely and completely specified functions, minimisation operation and reduction rules;

2) the construction of a new non-terminal *ifd*-node is based on the selection of two or three variables x_i, x_j and x_k, and a Boolean function c from the set $\{x_i \wedge x_j \vee \neg x_i \wedge x_k,\ x_i \wedge x_j,\ x_i \oplus x_k, \ldots\}$ including numerous modifications of the set's functions obtained by replacing positive literals with negative literals in various combinations;

3) the selection of a preferable expansion and one or more sub-diagrams is carried out for the chosen c function. The selection depends on the expansion properties and sub-diagram features associated with their ability of further diagram reduction;

4) the introduction of new *ifd*-nodes and applying the selected expansion to selected sub-diagrams give a new intermediate IFD;

5) the application of reduction rules to the current IFD gives a next-step IFD of decreased size and depth;

6) the diagram step-wise transformation is over if no expansion and sub-diagram have been found improving the IFD parameters.

Let demonstrate how the technique works on the example ROBDD depicted in fig. 4, *b*, which is immediately transformed to a non-reduced initial IFD depicted in fig. 7, *a*.

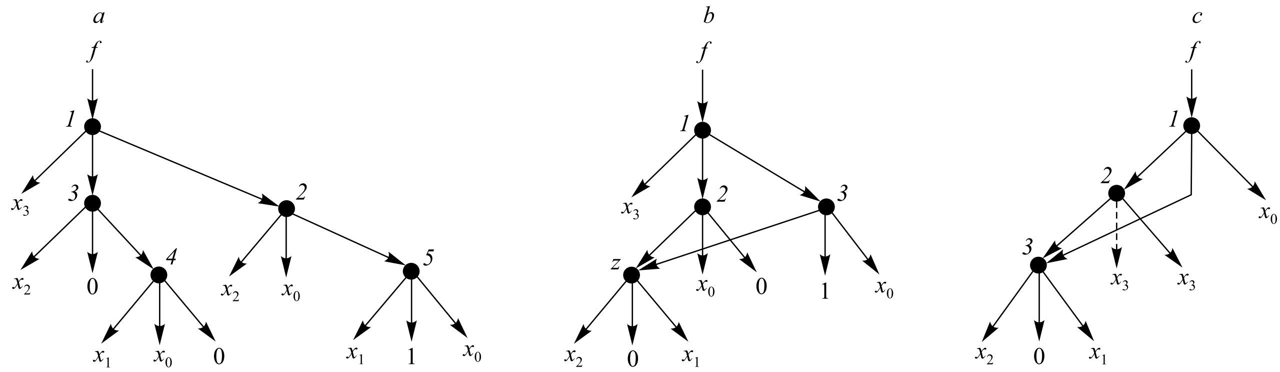


Fig. 7. Transforming example ROBDD to IFD:
a – initial IFD (*1–5* denote the diagram node numbers);
b – intermediate IFD (*1–3* denote the diagram node numbers; *z* is a function associated with the node);
c – minimised IFD (*1–3* denote the diagram node numbers; dash line denotes complement edge)

First observe that the sub-diagram consisting of non-terminal nodes *2* and *4* (node numbering in fig. 4, *b*) can be represented by a term $t_2 = ifd\big(x_2,\ ifd(x_1, t_6, t_6),\ ifd(x_1, 1, t_6)\big)$, where t_2 and t_6 are sub-diagrams on nodes *2* and *6* respectively. Let construct function $c = \neg x_2 \wedge x_1$ that selects constant 1 in the term and rewrites (24) to (26):

$$f = c \wedge f_{x_2=0,\, x_1=1} \vee \neg c \wedge \left(\neg x_2 \wedge f_{x_2=0,\, x_1=0} \vee x_2 \wedge f_{x_2=1}\right). \tag{26}$$

Expansion (26) allows grouping identical nodes in such a way that the IFD is reduced significantly. Its application to t_2 gives $ifd\big(ifd(x_2, 0, x_1), 1, ifd\big(x_2, ifd(x_1, t_6, t_6), t_6\big)\big)$, which can be reduced to $\mathrm{IFD}_2 = ifd\big(ifd(x_2, 0, x_1), 1, t_6\big)$ using the S reduction rule twice. Similarly, the sub-diagram consisting of non-terminal nodes *3* and *5* is represented as $t_3 = ifd\big(x_2, 0, ifd(x_1, t_6, 0)\big)$. Applying expansion (26) to t_3 gives $ifd\big(ifd(x_2, 0, x_1), t_6, ifd\big(x_2, ifd(x_1, 0, 0), 0\big)\big)$, which is reduced by the S reduction rule to $\mathrm{IFD}_3 = ifd\big(ifd(x_2, 0, x_1), t_6, 0\big)$.

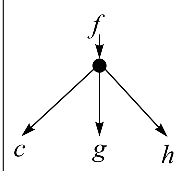
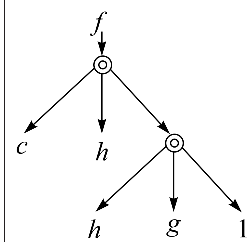
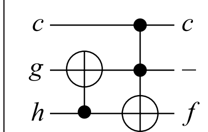
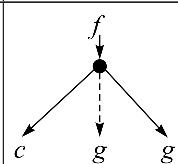
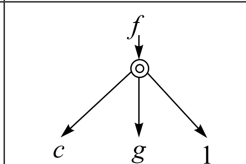
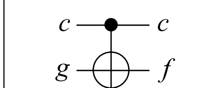
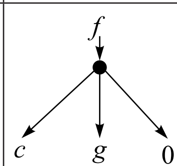
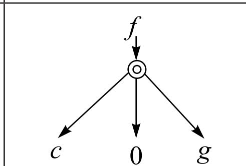
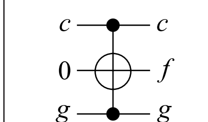
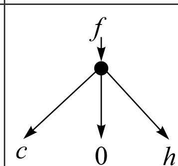
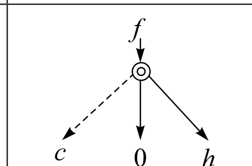
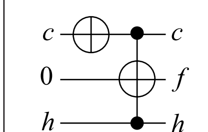
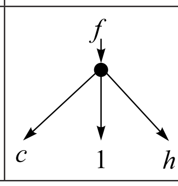
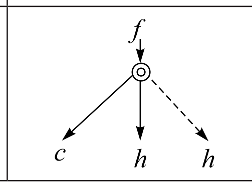
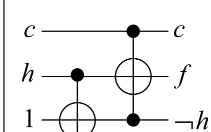
Merging the initial IFD root with IFD_2 and IFD_3 yields an intermediate IFD depicted in fig. 7, *b*. Its size is 4 non-terminal nodes, one less against the IFD shown in fig. 7, *a*. Since the outgoing *if*-edges of nodes *1*, *2* and *3* point two variables x_3 and z, and the *high*-edge of node *2* and the *low*-edge of node *3* point the same variable x_0, it is reasonable to apply expansion (25) to the IFD using $c = z \oplus x_3$. Term $ifd\big(\neg z, ifd(z, x_0, 0), ifd(z, 1, x_0)\big)$ describes the cofactor $f_{x_3=\neg z}$. It can be reduced to $ifd(\neg z, 0, 1) = z$. Term $ifd\big(z, ifd(z, x_0, 0), ifd(z, 1, x_0)\big)$ describes the cofactor $f_{x_3=z}$. It can be reduced to $ifd(z, x_0, x_0) = x_0$. Merging the diagrams that represent function $c = z \oplus x_3$, cofactor $f_{x_3=\neg z}$ and cofactor $f_{x_3=z}$ gives the final optimised IFD depicted in fig. 7, *c*. The diagram size is 3 non-terminal nodes, 2 nodes less than the size of the initial IFD shown in fig. 7, *a*.

Mapping *if*-decision diagrams to reversible circuits

The technique of mapping IFD to a reversible circuit works in two steps: 1) mapping the IFD to a FIFD; 2) mapping FIFD to a reversible circuit. Observing the IFDs depicted in fig. 7, we recognise five types of node. Table 2 presents rules of mapping each node of IFD to corresponding one or two nodes of FIFD.

Table 2

Rules of mapping IFD nodes to FIFD nodes and further to reversible gates

No.	Function	Term	IFD node	Equivalent FIFD nodes	Reversible gates
1	$f = c \wedge g \vee \neg c \wedge h$	$ifd(c,\ g,\ h)$			
2	$f = c \oplus g$	$ifd(c,\ \neg g,\ g)$			
3	$f = c \wedge g$	$ifd(c,\ g,\ 0)$			
4	$f = \neg c \wedge h$	$ifd(c,\ 0,\ h)$			
5	$f = c \vee h$	$ifd(c,\ 1,\ h)$			

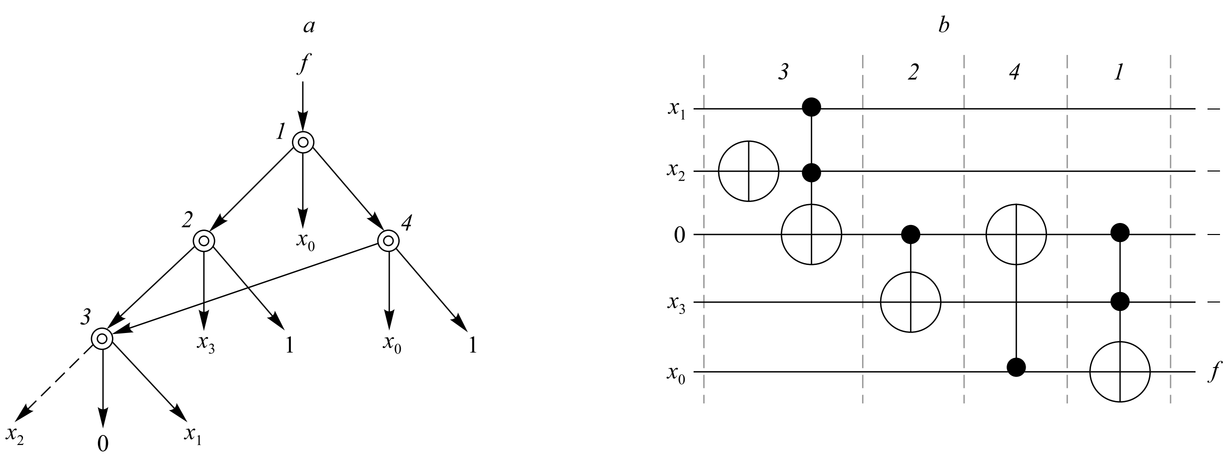


Fig. 8. Transforming optimised IFD to FIFD and then to reversible circuit:
a – FIFD functionally equivalent to optimised IFD (*1–4* denote the diagram node numbers);
b – reversible circuit realising the FIFD (diagram node numbers are above columns)

For each IFD-node type, table 2 describes the corresponding Boolean function, term, graphical view of the node, corresponding FIFD nodes, and reversible gates, which implement the nodes. The IFD nodes realise the functions as follows: $c \wedge g \vee \neg c \wedge h$, $c \oplus g$, $c \wedge g$, $\neg c \wedge h$ and $c \vee h$. Let apply the rules to the optimised IFD shown in fig. 7, *c*. Figure 8, *a*, depicts the functionally equivalent FIFD. To estimate the efficiency of the proposed transformation technique, we apply the rules to the IFD from fig. 7, *a*, and obtain the immediate FIFD (fig. 9, *a*). While the FIFD has the size of 7 non-terminal nodes and the depth of 4 nodes, the optimised FIFD has the size of 4 non-terminal nodes and the depth of 3 nodes. Mapping the FIFD nodes to reversible gates yields for optimised and immediate FIFDs the reversible circuits depicted in fig. 8, *b*, and 9, *b*, respectively.

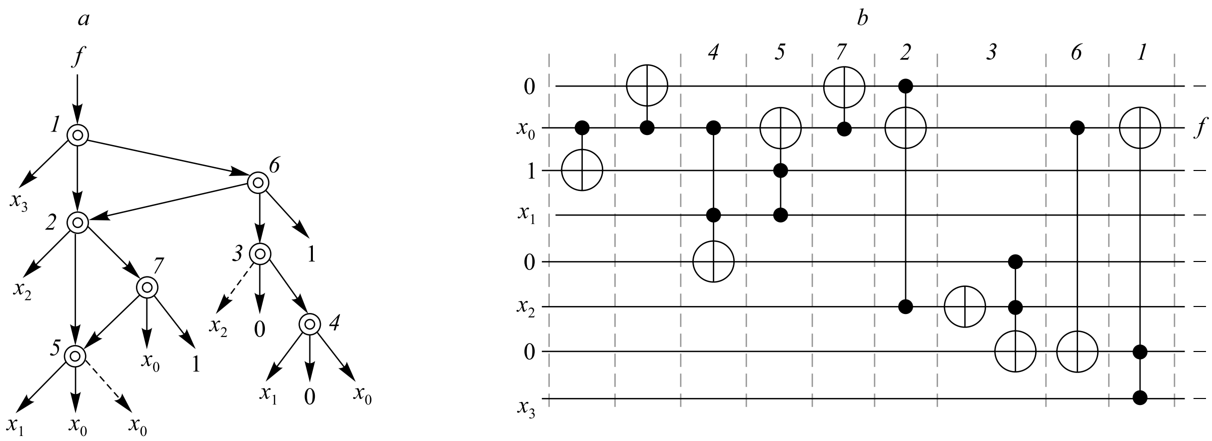


Fig. 9. Transforming immediate IFD to FIFD and then to reversible circuit:
a – FIFD that is functionally equivalent to immediate IFD (*1–7* denote the diagram node numbers);
b – reversible circuit realising the FIFD (diagram node numbers are above columns)

The comparison of three reversible circuits shows the efficiency of the proposed synthesis – transformation – optimisation technique. The circuit from fig. 5, *b*, synthesised from the ROFDD (see fig. 5, *a*) consists of 8 reversible gates, has the depth of 8 and uses 3 ancillary lines. The circuit from fig. 9, *b*, synthesised from the direct FIFD (see fig. 9, *a*) has the worsen parameters since it consists of 10 reversible gates, has the depth of 10 and uses 4 ancillary lines. The optimised circuit (see fig. 8, *b*) derived from FIFD has much better parameters since it consists of 5 reversible gates, has the depth of 5 gates and uses only 1 ancillary line.

Synthesis of quantum logic circuits from reversible circuits

The synthesis technique and parameters of quantum logic circuits essentially depend on the quantum library. Since NCV-$|v_1\rangle$ is a library that allows the generation of good quality quantum circuits [3], we have developed a technique of mapping the reversible gates of NCT library to quantum gates of NCV-$|v_1\rangle$ library, which consists of the following steps:

1) replacing all two-control Toffoli reversible gates with the cascade of quantum gates that is depicted in fig. 3, *b*; the procedure reduces the critical path of quantum circuit;

2) reducing the obtained circuit size by annihilating consequent V^+ and V gates and deleting gates for unessential line outputs;

3) parallelising the execution of quantum gates and reducing the circuit depth.

The procedure searches for such assignment of the V and V^+ gates to lines, which gives the lowest size and depth of resulting circuit. It has been applied to three reversible circuits shown in fig. 8, *b*, fig. 5, *b*, and fig. 9, *b*. Table 3 and fig. 10 show that the quantum circuit that is synthesised from the optimised IFD (see fig. 8, *b*) has the lowest size of 9 gates and the lowest depth of 8. The circuit synthesised from the ROBDD has a higher size of 16 gates and a higher depth of 11. The circuit synthesised from the direct IFD has a worst size of 21 gates and a worst depth of 17. The final and initial figures for the size and depth (see table 3) show that the size reduction of 4, 12 and 9 gates and the depth reduction of 1, 5 and 4 are obtained by the technique when applied to the optimised IFD, ROBDD and immediate IFD respectively.

Table 3

Comparison of synthesised reduced parallelised quantum circuits

Circuit	NOT gates	CNOT gates	V gates	CV gates	V^+ gates	CV^+ gates	Size (initial)	Depth (initial)	Ancillary lines
Optimised IFD	1	4	2	2	–	–	9 (13)	8 (9)	1
ROBDD	0	8	3	4	0	1	16 (28)	11 (16)	3
Immediate IFD	1	9	4	5	1	1	21 (30)	17 (21)	4

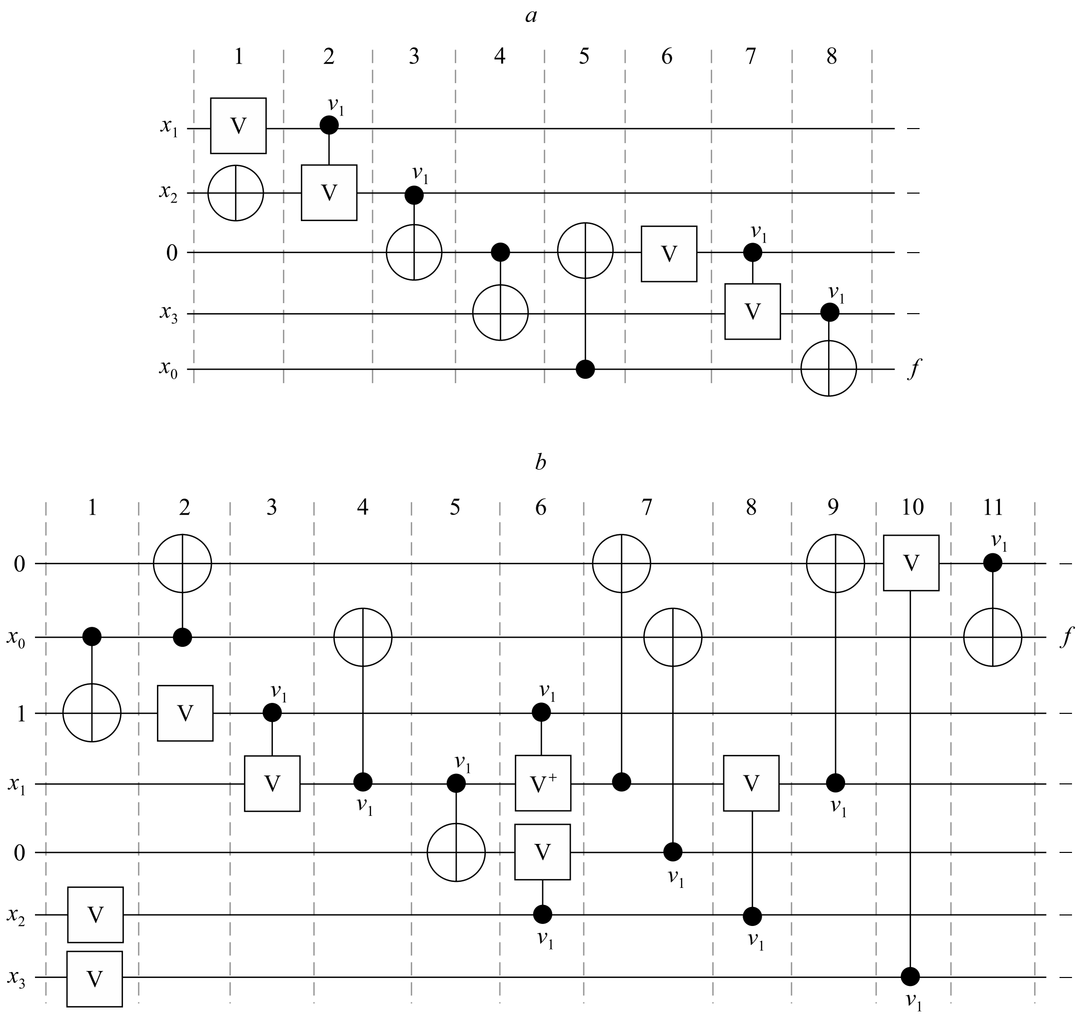


Fig. 10. Quantum circuits synthesised from optimised IFD (*a*) and ROBDD (*b*).
Numbers of columns indicate parallelisation steps

Conclusion

The problem of modelling, synthesis and optimisation of digital reversible and quantum circuits has been considered. All quantum circuits are reversible, therefore the first step in the quantum circuit synthesis process is the optimisation of reversible circuits with further mapping to quantum circuits. Although several models and methods have been developed for synthesis of reversible and quantum circuits (Reed – Muller forms or Zhegalkin polynomials, quantum operator forms, BDD, FDD and others), the problem of minimising the circuit size and depth is still open and requires further scientific research.

It is assumed in the literature that the ROBDD that is derived from the Shannon expansion with applying reduction rules is a most compact representation of Boolean functions. The promising extension of ROBDD is IFD, which is based on decomposition of incompletely specified functions and is capable of increasing the parallelisation potential of diagrams. This paper has obtained theoretical results which show that the IFD can provide graph representations that have lower size and depth against ROBDD. To synthesise IFDs with such properties, novel expansions of completely and incompletely specified Boolean functions that are based on the minimisation operation have been proposed in the paper. They allow for a particular diagram to find reconstructions that lead to reduction of the resulting diagram size and depth.

To synthesise a reversible circuit, the rules of transforming IFD to FIFD, which intensively use exclusive-or operations and extend the known functional binary decision diagrams have been proposed. New expansions of incompletely specified functions that extend the positive and negative Davio expansions of Boolean functions lie in the basis of constructing and generating FIFD. The FIFD is a source of generating a reversible circuit of smaller size by means of mapping diagram nodes to cascades of reversible gates. The technique of synthesising and optimising a quantum circuit from the generated reversible circuit has been developed in the paper. The optimisation aims at the reduction of quantum gate count after replacing Toffoli gates with cascades of quantum gates. It takes into account unessential output variables and carries out the reduction of the quantum circuit depth due to parallelisation. All stages of transforming ROBDD through IFD to a quantum circuit are illustrated by an example, which has shown the advantages of the obtained theoretical results.

References

1. Barenco A, Bennett CH, Cleve R, Di Vincenzo DP, Margolus N, Shor P, et al. Elementary gates for quantum computation. *Physical Review A.* 1995;52(5):3457–3467. DOI: 10.1103/PhysRevA.52.3457.

2. Nielsen M, Chuang IL. *Quantum computation and quantum information.* Cambridge: Cambridge University Press; 2000. 700 p.

3. Sasanian Z, Wille R, Miller DM. Realizing reversible circuits using a new class of quantum gates. In: Groeneveld P, editor. *The 49th Annual design automation conference 2012; 2012 June 3–7; San Francisco, USA*. New York: Association for Computing Machinery; 2012. p. 36–41.

4. Handique M, Sonka A. An extended approach for mapping reversible circuits to quantum circuits using NCV-$|v_1\rangle$ library. *Procedia Computer Science.* 2018;125:832–839. DOI: 10.1016/j.procs.2017.12.106.

5. Wille R, Chattopadhyay A, Drechsler R. From reversible logic to quantum circuits: logic design for an emerging technology. In: Najjar WA, Gerstlauer A, editors. *Proceedings of the 2016 International conference on embedded computer systems: architectures, modeling and simulation; 2016 July 17–21; Samos, Greece.* New York: IEEE; 2016. p. 268–274. DOI: 10.1109/SAMOS.2016.7818357.

6. Sasanian Z. Technology mapping and optimization for reversible and quantum circuits [dissertation]. Victoria: University of Victoria; 2012. 145 p.

7. Smith K. Technology-dependent quantum logic synthesis and compilation [dissertation] [Internet]. Dallas: Southern Methodist University; 2019 [cited 2021 September 9]. 133 p. Available from: https://scholar.smu.edu/engineering_electrical_etds/30.

8. Burgholzer L, Raymond R, Sengupta I, Wille R. Efficient construction of functional representations for quantum algorithms. In: Yamashita S, Yokoyama T, editors. *Reversible Computation. Proceedings of 13th International conference; virtual event; 2021 July 7–8.* Cham: Springer; 2021. p. 227–241. (Lecture Notes in Computer Science; volume 12805). DOI: 10.1007/978-3-030-79837-6_14.

9. Sasamala TN, Singh AK, Mohan A. Reversible logic circuit synthesis and optimization using adaptive genetic algorithm. *Procedia Computer Science.* 2015;70:407–413. DOI: 10.1016/j.procs.2015.10.054.

10. Bhattacharjee A, Bandyopadhyay C, Mukherjee A, Wille R, Drechsler R, Rahaman H. Efficient implementation of nearest neighbor quantum circuits using clustering with genetic algorithm. In: *2020 IEEE 50th International Symposium on Multiple-Valued Logic (ISMVL); 2020 November 9–11; Miyazaki, Japan.* Los Alamitos: IEEE; 2020. p. 40–45. DOI: 10.1109/ISMVL49045.2020.00-32.

11. Meuli G, Schmitt B, Ehlers R, Riener H, De Micheli G. Evaluating ESOP optimization methods in quantum compilation flows. In: Thomsen M, Soeken M, editors. *Reversible Computation. Proceedings of the 11th International conference; 2019 June 24–25; Lausanne, Switzerland.* Cham: Springer; 2019. p. 191–208. (Lecture Notes in Computer Science; volume 11497). DOI: 10.1007/978-3-030-21500-2_12.

12. Wille R, Drechsler R. Effect of BDD optimization on synthesis of reversible and quantum logic. *Electronic Notes in Theoretical Computer Science.* 2010;253(6):57–70. DOI: 10.1016/j.entcs.2010.02.006.

13. Zulehner A, Niemann P, Drechsler R. Accuracy and compactness in decision diagrams for quantum computation. In: *2019 Design, automation and test in Europe Conference and Exhibition (DATE); 2019 March 25–29; Florence, Italy.* [S. l.]: IEEE; 2019. p. 280–283. DOI: 10.23919/DATE.2019.8715040.

14. Lukac M, Kameyama M, Perkowski M, Kerntopf P. Minimization of quantum circuits using quantum operator forms. arXib:1701.01999. 2017 [cited 2021 September 9]: [11 p.]. Available from: https://arxiv.org/abs/1701.01999.

15. Große D, Wille R, Dueck GW, Drechsler R. Exact multiple-control Toffoli network synthesis with SAT techniques. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.* 2009;28(5):703–715. DOI: 10.1109/TCAD.2009.2017215.

16. Abdessaied N, Wille R, Soeken M, Drechsler R. Reducing the depth of quantum circuits using additional circuit lines. In: Dueck GW, Miller DM, editors. *Reversible Computation. Proceedings of the 5th International Conference; 2013 July 4–5; Victoria, BC, Canada*. Berlin: Springer; 2013. p. 221–233 (Lecture Notes in Computer Science; volume 7948). DOI: 10.1007/978-3-642-38986-3_18.

17. Prihozhy AA. *If*-diagrams: theory and application. In: *Proceedings of the 7th International workshop PATMOS'97; 1997 September 8–10; Louvain-la-Neuve, Belgium.* [S. l.]: UCL; 1997. p. 369–378.

18. Prihozhy AA. *Chastichno opredelennye logicheskie sistemy i algoritmy* [Incompletely specified logical systems and algorithms]. Minsk: Belarusian National Technical University; 2013. 343 p. Russian.

19. Prihozhy AA. Synthesis of parallel adders from *if*-decision diagrams. *System Analysis and Applied Information Science.* 2020; 2:61–70. DOI: 10.21122/2309-4923-2020-2-61-70.

20. Amarú L, Gaillardon P-E, De Micheli G. Biconditional BDD: a novel canonical BDD for logic synthesis targeting XOR-rich circuits. In: *2013. Design, Automation & Test in Europe Conference & Exhibition; 2013 March 18–22; Grenoble, France.* [S. l.]: IEEE; 2013. p. 1014–1017. DOI: 10.7873/DATE.2013.211.

Received 19.10.2021 / revised 21.10.2021 / accepted 29.10.2021.

Краткие сообщения

Short communications

УДК 517.968.73

ЧИСЛЕННОЕ РЕШЕНИЕ ОДНОГО СЛАБОСИНГУЛЯРНОГО ИНТЕГРАЛЬНОГО УРАВНЕНИЯ МЕТОДОМ ОРТОГОНАЛЬНЫХ МНОГОЧЛЕНОВ

С. М. ШЕШКО[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Построена схема численного решения сингулярного интегрального уравнения с логарифмическим ядром методом ортогональных многочленов. Предлагаемая схема приближенного решения задачи основана на представлении искомой функции в виде линейной комбинации ортогональных многочленов Чебышева и спектральных соотношениях, позволяющих получить простые аналитические выражения для сингулярной составляющей уравнения. Коэффициенты разложения решения по базису полиномов Чебышева вычисляются как решение системы линейных алгебраических уравнений. Результаты численных экспериментов показывают, что на сетке из 20–30 узлов погрешность приближенного решения достигает минимального предела, обусловленного погрешностью представления действительных чисел с плавающей запятой.

Ключевые слова: интегро-дифференциальное уравнение; численное решение; метод ортогональных многочленов.

Благодарность. Автор выражает благодарность научному руководителю Г. А. Расолько за постановку задачи и полезные замечания.

Образец цитирования:
Шешко СМ. Численное решение одного слабосингулярного интегрального уравнения методом ортогональных многочленов. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:98–103.
https://doi.org/10.33581/2520-6508-2021-3-98-103

For citation:
Sheshko SM. Numerical solution of a weakly singular integral equation by the method of orthogonal polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:98–103. Russian.
https://doi.org/10.33581/2520-6508-2021-3-98-103

Автор:
Сергей Михайлович Шешко – старший преподаватель кафедры цифровой экономики экономического факультета.

Author:
Sergei M. Sheshko, senior lecturer at the department of digital economy, faculty of economics.
sheshkasm@bsu.by
https://orcid.org/0000-0001-6366-4961

NUMERICAL SOLUTION OF A WEAKLY SINGULAR INTEGRAL EQUATION BY THE METHOD OF ORTHOGONAL POLYNOMIALS

S. M. SHESHKO[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

A scheme is constructed for the numerical solution of a singular integral equation with a logarithmic kernel by the method of orthogonal polynomials. The proposed schemes for an approximate solution of the problem are based on the representation of the solution function in the form of a linear combination of the Chebyshev orthogonal polynomials and spectral relations that allows to obtain simple analytical expressions for the singular component of the equation. The expansion coefficients of the solution in terms of the Chebyshev polynomial basis are calculated by solving a system of linear algebraic equations. The results of numerical experiments show that on a grid of 20–30 points, the error of the approximate solution reaches the minimum limit due to the error in representing real floating-point numbers.

Keywords: integro-differential equation; numerical solution; method of orthogonal polynomials.

Acknowledgements. The author would like to thank to the scientific advisor G. A. Rasolko for setting the problem and valuable comments.

Введение

Аппарат сингулярных интегральных уравнений широко используется в задачах аэродинамики, дифракции и других областях естествознания [1]. Точность приближенного численного решения интегральных уравнений во многом определяется способом их дискретизации, т. е. выбором квадратурных формул, базисных функций и узлов аппроксимации, позволяющих свести исходную задачу к системе линейных алгебраических уравнений приемлемой размерности и обусловленности. При наличии особенностей в подынтегральных функциях (что характерно для сингулярных интегральных уравнений) требуется максимально учитывать специфику задачи.

В работе [1, с. 58–59] рассматривается квадратурный метод приближенного решения разрешимого сингулярного интегрального уравнения с логарифмическим ядром

$$\varphi(x)+\frac{1}{\pi}\int_{-1}^{1}\varphi(t)\ln|t-x|\,dt+\frac{1}{\pi}\int_{-1}^{1}\varphi(t)K(x,t)\,dt=f(x),\ -1<x<1, \tag{1}$$

где $\varphi(x)$ – искомая функция; $K(x, t)$ и $f(x)$ – известные функции из класса Гёльдера H.

В настоящей работе предлагается алгоритм численного решения уравнения (1) методом ортогональных многочленов, основной идеей которого является использование спектральных или квазиспектральных соотношений для входящих в уравнение интегралов.

Данная статья продолжает серию работ по приближенному решению сингулярных интегро-дифференциальных уравнений, в том числе со слабой особенностью, методом ортогональных многочленов [2–5].

Предварительные сведения

Прежде чем переходить к конструированию вычислительной схемы приближенного решения уравнения (1) в классе функций $h(-1, 1)$ по Мусхелишвили [6, с. 31], приведем некоторые предварительные сведения. Класс функций $h(-1, 1)$ составляют ограниченные в окрестности точек $x=\pm1$ функции.

Известны спектральные соотношения для слабосингулярного интеграла

$$\frac{1}{\pi}\int_{-1}^{1}\frac{T_k(t)}{\sqrt{1-t^2}}\ln|t-x|\,dt=\alpha_k T_k(x),\ \alpha_0=-\ln 2,\ \alpha_k=-\frac{1}{k},\ k>0,$$
$$T_k(x)=\cos(k\arccos x), \tag{2}$$

которым воспользуемся далее.

При построении вычислительной схемы используем интерполяционный многочлен для функции $f(x)$ по узлам Чебышева первого рода [7]:

$$f(x)\approx f_n(x)=\sum_{j=0}^{n} f_j^n T_j(x). \tag{3}$$

Здесь

$$f_0^n = \frac{1}{n+1}\sum_{k=0}^{n} f(x_k),\ \ f_j^n = \frac{2}{n+1}\sum_{k=0}^{n} f(x_k)T_j(x_k),\ \ j = 1, \ldots, n,$$

$$x_k = \cos\frac{2k+1}{2n+2}\pi,\ \ k = 0, 1, \ldots, n.$$

Чтобы получить разложение функции $f(x)$ по многочленам Чебышева второго рода, применим в (3) тождества [7, с. 23]

$$T_0(x) = U_0(x),\ 2T_1(x) = U_1(x),\ 2T_j(x) = U_j(x) - U_{j-2}(x),\ \ j \ge 2,$$

что дает следующее:

$$f_n(x) = \sum_{j=0}^{n} f_j U_j(x),$$

где

$$f_j = G_j - G_{j+2},\ j = 0, 1, \ldots, n-2,\ f_{n-1} = G_{n-1},\ \ f_n = G_n,$$

$$G_j = \frac{1}{n+1}\sum_{k=0}^{n} f(x_k)T_j(x_k),\ j = 0, 1, \ldots, n,$$

$$x_k = \cos\frac{2k+1}{2n+2}\pi,\ k = 0, 1, \ldots, n.$$

Для получения интерполяционного многочлена $K_{n,n}(x, t)$ функции двух переменных $K(x, t)$ в виде разложения по многочленам Чебышева первого рода используем (3), в результате чего имеем

$$K_{n,n}(x, t) = \sum_{m=0}^{n} T_m(x)\sum_{j=0}^{n} T_j(t)k_{m,j}^{*},$$

$$k_{m,j}^{*} = \frac{\delta_m\delta_j}{(n+1)^2}\sum_{l=0}^{n} T_m(x_l)\sum_{r=0}^{n} K(x_l, x_r)T_j(x_r),$$

$$\delta_q = \begin{cases} 1, & q = 0, \\ 2, & q \ne 0, \end{cases}\ \ x_k = \cos\frac{2k+1}{2n+2}\pi,\ k = \overline{0, n}.$$

На основании предыдущих результатов получим интерполяционный многочлен $K_{n,n}(x, t)$ функции двух переменных $K(x, t)$ в виде разложения по многочленам Чебышева первого и второго рода:

$$K_{n,n}(x, t) = \sum_{m=0}^{n} T_m(x)\sum_{j=0}^{n} k_{m,j}U_j(t), \tag{4}$$

где

$$k_{m,j} = \frac{\delta_m}{(n+1)^2}\sum_{l=0}^{n} T_m(x_l)\sum_{r=0}^{n} K(x_l, x_r)\left(T_j(x_r) - \theta_j T_{j+2}(x_r)\right),$$

$$\theta_j = \begin{cases} 1, & j = 0, 1, \ldots, n-2, \\ 0, & j = n-1, n, \end{cases}\ \ \delta_m = \begin{cases} 1, & m = 0, \\ 2, & m \ne 0, \end{cases}\ \ x_k = \cos\frac{2k+1}{2n+2}\pi,\ k = \overline{0, n}.$$

Приближенное решение уравнения (1)

Приближенное решение данного уравнения в классе функций $h(-1, 1)$ будем искать как решение следующего уравнения относительно новой неизвестной функции $v_n(x)$:

$$\varphi_n(x) + \frac{1}{\pi}\int_{-1}^{1}\varphi_n(t)\ln|t-x|\,dt + \frac{1}{\pi}\int_{-1}^{1}\varphi_n(t)K_{n,n}(x, t)\,dt = F_n(x),\ -1 < x < 1, \tag{5}$$

где $\varphi_n(x) = \sqrt{1-x^2}\,v_n(x)$; $K_{n,n}(x, t)$ – интерполяционный многочлен (4) функции $K(x, t)$ степени n по обеим переменным; $F_n(x)$ – некоторая функция из класса $C[-1, 1]$ такая, что $F_n(x_j) = f(x_j)$, $x_j = \cos\frac{2j+1}{2n+2}$, $j = 0, 1, \ldots, n$.

Отметим, что уравнение (5) в заданном классе также разрешимо.

Рассмотрим следующие утверждения.

Утверждение 1. Для $|x| < 1$ имеет место равенство

$$J_k(x) = \frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,U_k(t)\ln|t-x|\,dt = \begin{cases} -\frac{\ln 2}{2}T_0(x) + \frac{1}{4}T_2(x), \; k = 0, \\ -\frac{1}{2k}T_k(x) + \frac{1}{2k+4}T_{k+2}(x), \; k \ge 1. \end{cases} \tag{6}$$

Доказательство. С учетом соотношения [7] $2(1-x^2)U_k(x) = T_k(x) - T_{k+2}(x)$ подынтегральная функция в (6) сводится к виду (2), откуда следует истинность утверждения.

Утверждение 2. Для $|x| < 1$ имеет место равенство

$$I_k(x) = \frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,T_k(t)\ln|t-x|\,dt =$$

$$= \begin{cases} -\left(\frac{\ln 2}{2} + \frac{1}{8}\right)U_0(x) + \frac{1}{8}U_2(x), \; k = 0, \\ -\frac{1}{6}U_1(x) + \frac{1}{24}U_3(x), \; k = 1, \\ \left(\frac{\ln 2}{4} + \frac{1}{8}\right)U_0(x) - \frac{5}{32}U_2(x) + \frac{1}{32}U_4(x), \; k = 2, \\ -\frac{1}{8(k-2)}U_{k-4}(x) + \frac{3k-4}{8k(k-2)}U_{k-2}(x) - \frac{3k+4}{8k(k+2)}U_k(x) + \frac{1}{8(k+2)}U_{k+2}(x), \; k \ge 3. \end{cases} \tag{7}$$

Доказательство. С учетом соотношений $2T_k(x) = U_k(x) - U_{k-2}(x)$, $k \ge 1$, $U_{-1}(x) = 0$, $T_0 = U_0$ левая часть (7) сводится к вычислению интегралов вида (6), и тождества (7) проверяются непосредственными вычислениями.

Положим далее

$$\varphi_n(x) = \sqrt{1-x^2}\,v_n(x) = \sqrt{1-x^2}\sum_{k=0}^{n} c_k T_k(x), \tag{8}$$

где c_k, $k = 0, 1, \ldots, n$, – пока неизвестные постоянные.

Рассмотрим первый интеграл в (5) с учетом представления (8):

$$\frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,v_n(t)\ln|t-x|\,dt = \sum_{k=0}^{n} c_k \frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,T_k(t)\ln|t-x|\,dt = \sum_{k=0}^{n} c_k I_k(t).$$

Рассмотрим второй интеграл в (5) и воспользуемся интерполяционным многочленом (4). Отсюда

$$\frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,v_n(t)K_{n,n}(x, t)\,dt = \sum_{k=0}^{n} c_k \sum_{m=0}^{n} T_m(x)\sum_{j=0}^{n} k_{m,j}\frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\,T_k(t)U_j(t)\,dt =$$

$$= \sum_{k=0}^{n} c_k \sum_{m=0}^{n} T_m(x)\sum_{j=0}^{n} k_{m,j}\frac{1}{2}\left(\frac{1}{\pi}\int_{-1}^{1}\sqrt{1-t^2}\left(U_{j+k}(t) + U_{j-k}(t)\right)dt\right) = \sum_{k=0}^{n} c_k \sum_{m=0}^{n} T_m(x)\,\omega_{m,k},$$

$$\omega_{m,k} = \begin{cases} 0{,}5\,k_{m,k}, \; k = 0, \\ 0{,}25\,k_{m,k}, \; k > 0. \end{cases}$$

Уравнение (5) в заданном классе переходит в уравнение

$$\sqrt{1-x^2}\sum_{k=0}^{n} c_k T_k(x) + \sum_{k=0}^{n} c_k I_k(x) + \sum_{k=0}^{n} c_k \sum_{m=0}^{n} T_m(x)\omega_{m,\,k} = F_n(x). \quad (9)$$

В качестве внешних узлов x в (9) выберем узлы Чебышева первого рода, а именно $x_j = \cos\frac{2j+1}{2n+2}$, $j = 0, \ldots, n$. Из (9) получим систему линейных алгебраических уравнений

$$\sum_{k=0}^{n} c_k A_{j,\,k} = f\left(x_j\right),\ j = 0, \ldots, n, \quad (10)$$

$$A_{j,\,k} = \sqrt{1-x_j^2}\,T_k\left(x_j\right) + I_k\left(x_j\right) + \sum_{m=0}^{n} T_m\left(x_j\right)\omega_{m,\,k}.$$

Уравнения (5) и (9) равносильны, так как, выполняя действия, приводящие (5) в (9), в обратном порядке, из (9) получим (5) (см., например, [8, с. 535]). Следовательно, система (10), полученная из уравнения (9), разрешима и имеет единственное решение.

Решив систему (10) относительно неизвестных c_k, $k = 0, 1, \ldots, n$, приближенное решение уравнения (1) получим по формуле

$$\varphi_n(x) = \sqrt{1-x^2}\sum_{k=0}^{n} c_k T_k(x). \quad (11)$$

Предложенная схема протестирована на примере решения модельной задачи для уравнения (1) при $k(x,\,t) = \frac{4t}{(x+2)(t+2)}$, $f(x) = 2x\sqrt{1-x^2} + \frac{2}{3}x^3 - x + \left(56 - 32\sqrt{3}\right)\frac{1}{x+2}$.

Известно, что решением уравнения (1) в данном случае является функция

$$\varphi(x) = 2x\sqrt{1-x^2}.$$

Как показывают расчеты, проведенные в среде компьютерной алгебры *Mathcad*, уже при сравнительно небольших значениях n достигается достаточно высокая точность вычисления приближенного решения.

Решая систему (10) при n, равных 7, 14 и 29, видим, что точное решение $\varphi(x)$ отличается от приближенного $\varphi_n(x)$, вычисленного по формуле (11), в системе точек $x = -0{,}99, -0{,}98, \ldots, 0{,}99$ не более чем на $4{,}6 \cdot 10^{-4}$, $1{,}8 \cdot 10^{-7}$ и $1{,}7 \cdot 10^{-13}$ соответственно.

Библиографические ссылки

1. Панасюк ВВ, Саврук МП, Назарчук ЗТ. *Метод сингулярных интегральных уравнений в двумерных задачах дифракции.* Киев: Наукова думка; 1984. 344 с.

2. Расолько ГА. Численное решение сингулярного интегро-дифференциального уравнения Прандтля методом ортогональных многочленов. *Журнал Белорусского государственного университета. Математика. Информатика.* 2018;3:68–74.

3. Расолько ГА. К численному решению сингулярного интегро-дифференциального уравнения Прандтля методом ортогональных многочленов. *Журнал Белорусского государственного университета. Математика. Информатика.* 2019;1:58–68.

4. Расолько ГА, Шешко СМ, Шешко МА. Об одном методе численного решения некоторых сингулярных интегро-дифференциальных уравнений. *Дифференциальные уравнения.* 2019;55(9):1285–1292.

5. Расолько ГА, Шешко СМ. Приближенное решение одного сингулярного интегро-дифференциального уравнения методом ортогональных многочленов. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020; 2:86–96.

6. Мусхелишвили НИ. *Сингулярные интегральные уравнения.* 3-е издание. Москва: Наука; 1968. 513 с.

7. Пашковский С. *Вычислительные применения многочленов и рядов Чебышева.* Москва: Наука; 1983. 384 с.

8. Колмогоров АН, Фомин СВ. *Элементы теории функций и функционального анализа.* 6-е издание. Москва: Наука; 1989. 624 с.

References

1. Panasyuk VV, Savruk MP, Nazarchuk ZT. *Metod singulyarnykh integral'nykh uravnenii v dvumernykh zadachakh difraktsii* [The method of singular integral equations in two-dimensional diffraction problems]. Kyiv: Naukova dumka; 1984. 344 p. Russian.

2. Rasolko GA. Numerical solution of singular integro-differential Prandtl equation by the method of orthogonal polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2018;3:68–74. Russian.

3. Rasolko GA. To the numerical solution of singular integro-differential Prandtl equation by the method of orthogonal polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2019;1:58–68. Russian.

4. Rasolko GA, Sheshko SM, Sheshko MA. [Numerical method for some singular integro-differential equations]. *Differentsial'nye uravneniya.* 2019;55(9):1285–1292. Russian.

5. Rasolko GA, Sheshko SM. An approximate solution of one singular integro-differential equation using the method of orthogonal polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;2:86–96. Russian.

6. Muskhelishvili NI. *Singulyarnye integral'nye uravneniya* [Singular integral equations]. 3rd edition. Moscow: Nauka; 1968. 513 p. Russian.

7. Pashkovskii S. *Vychislitel'nye primeneniya mnogochlenov i ryadov Chebysheva* [Computational applications of polynomials and Chebyshev series]. Moscow: Nauka; 1983. 384 p. Russian.

8. Kolmogorov AN, Fomin SV. *Elementy teorii funktsii i funktsional'nogo analiza* [Elements of the theory of functions and functional analysis]. 6th edition. Moscow: Nauka; 1989. 624 p. Russian.

Получена 03.06.2021 / исправлена 11.06.2021 / принята 29.09.2021.
Received 03.06.2021 / revised 11.06.2021 / accepted 29.09.2021.

УДК 002.6;004.7;004.722

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОГО ОТКАЗОУСТОЙЧИВОГО ОБЛАЧНОГО РЕПОЗИТОРИЯ ПИСЬМЕННЫХ РАБОТ ОБУЧАЮЩИХСЯ И СОТРУДНИКОВ УЧРЕЖДЕНИЙ ОБРАЗОВАНИЯ

В. П. КОЧИН[1]***, А. В. ЖЕРЕЛО***[1]

[1]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Показаны основные подходы к проектированию и разработке автоматизированной информационной системы защищенного облачного репозитория письменных работ обучающихся и работников учреждений образования и научных организаций (рефераты, эссе, курсовые и дипломные работы, магистерские диссертации, депонированные статьи). Описаны исследования и отработка архитектурных решений для обеспечения надежного и безопасного хранения данных с использованием облачных технологий. Рассмотрены ключевые проблемы проектирования защищенного репозитория и пути их решения. Облачный репозиторий письменных работ построен на базе распределенной файловой системы Ceph. В качестве платформы для создания облачного интерфейса использована система NextCloud, в качестве вычислительной платформы – виртуальные вычислительные ресурсы виртуальной сетевой инфраструктуры БГУ.

Ключевые слова: облачные вычисления; проектирование информационных систем; образовательные технологии; защищенное облачное хранилище; виртуализация; сетевая инфраструктура.

DESIGNING A SECURE FAIL-SAFE CLOUD REPOSITORY OF PAPERWORKS OF STUDENTS AND EMPLOYEES OF EDUCATIONAL INSTITUTIONS

V. P. KOCHYN[a]***, A. V. ZHERELO***[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
Corresponding author: V. P. Kochyn (kochyn@bsu.by)

The article discusses the main approaches to the design and development of an automated information system for a secure cloud repository of paperworks of students and employees of educational and research organisations (abstracts, essays, term papers and theses, master's theses, deposited articles), providing secure storage and secure mobile access to stored data. The research and development of architectural solutions to ensure reliable and secure data storage using cloud technologies are described. The main problems of designing a secure repository and ways to solve them are considered. The cloud repository of written works is built on the basis of the Ceph distributed file system, which uses the NextCloud system and the virtual computing resources of the virtual network infrastructure of the Belarusian State University as a platform for building a cloud interface.

Keywords: cloud computing; information systems design; educational technologies; secure cloud storage; virtualisation; network infrastructure.

Образец цитирования:
Кочин ВП, Жерело АВ. Проектирование защищенного отказоустойчивого облачного репозитория письменных работ обучающихся и сотрудников учреждений образования. *Журнал Белорусского государственного университета. Математика. Информатика.* 2021;3:104–108 (на англ.).
https://doi.org/10.33581/2520-6508-2021-3-104-108

For citation:
Kochyn VP, Zherelo AV. Designing a secure fail-safe cloud repository of paperworks of students and employees of educational institutions. *Journal of the Belarusian State University. Mathematics and Informatics.* 2021;3:104–108.
https://doi.org/10.33581/2520-6508-2021-3-104-108

Авторы:
Виктор Павлович Кочин – кандидат технических наук, доцент; начальник Центра информационных технологий.
Анатолий Владимирович Жерело – кандидат физико-математических наук, доцент; заместитель начальника Центра информационных технологий.

Authors:
Viktor P. Kochyn, PhD (engineering), docent; head of the Center for Information Technologies.
kochyn@bsu.by
Anatolii V. Zherelo, PhD (physics and mathematics), docent; deputy head of the Center for Information Technologies.
zherelo@bsu.by

Introduction

In the era of formation and development of the knowledge economy based on the production, distribution, and use of information, the education system is being transformed, responding to the challenges of the present and the future. The request for education from society, the family, and the student himself is changing. Education becomes continuous, mobile, open. At the same time, the design, development, and use of information and communication technologies are not an end in themselves but should provide a software and technical platform for the creation and application of pedagogical innovations [1; 2].

One of the characteristic features of the digital transformation of the education system is a significant increase in the generated digital data. The issue of reliable storage of a sufficiently large amount of data is very acute. Traditional data storage devices (flash drives, hard drives, optical media) do not meet modern requirements for a number of reasons. Firstly, such devices do not provide a sufficient level of data storage reliability. Secondly, it is currently necessary to have access to data from any device: home computer, work computer, phone, laptop. Thirdly, to increase the volume of stored data, the purchase of additional devices is always required. In this regard, recently there has been an increase in the popularity of using cloud data storage.

In 2018, the Belarusian State University was the first among the Belarusian universities to develop a digital transformation strategy, including updating the content, forms, and methods of teaching, changing the processes of scientific research and management by improving its information, and communication infrastructure. One of the objectives of the given strategy is to create conditions for the transition to paperless technologies which allow creating and storing paperworks of students and employees of educational institutions (abstracts, essays, term papers, theses, master's theses, deposited articles) based on cloud technologies [1; 2].

Cloud storage significantly facilitates the work of modern users by virtualising the location of the data [3; 4]. Another advantage is the ability to process data on the storage side, in which the user does not face the tasks of ensuring the reliability and fault-tolerance of the storage, as well as managing the resources that process the data [5]. Due to these advantages, network storage (OneDrive, GoogleDrive, iCloud, Yandex.Disk, DropBox, etc.) is widely used for data storage and processing. On the one hand, these services provide reliable, fault-tolerant storage, on the other hand, they have a number of disadvantages:

• these resources are commercial, which are provide only a service, hiding the details of implementation;

• data is stored on servers located outside the Republic of Belarus, which contradicts the Decree of the President of the Republic of Belarus No. 60 «On measures to improve the use of the national segment of the Internet» dated 1 February 2010;

• they are inable to integrate with existing automated systems of universities, which makes it impossible to integrate these services into the educational process.

In this regard, there is a need to create your own cloud storage. When designing a secure fault-tolerant cloud repository of students' paperworks, the following criteria must be taken into account:

• providing multiple user access to resources;
• ensuring reliability and fault-tolerance;
• hardware independence and ability to quickly scale computing resources and storage systems;
• ability to generate analytical reports and various search queries;
• integration possibility with corporate information systems;
• ability to check for anti-plagiarism on stored data.

Providing multiple user access to resources. The bottleneck of traditional storage systems is the performance of a particular disk. When multiple users access the disk at the same time, its performance is divided by all.

Ensuring reliability and fault-tolerance. The designed storage should ensure the operability of the system even in case of failure of individual hardware nodes.

Hardware independence and ability to quickly scale computing resources and storage systems. At the system designing, it is necessary to ensure the possibility of creating and scaling the system on servers of various manufacturers. This approach will allow, firstly, to use existing equipment, and, secondly, to gradually increase computing and storage resources without reference to existing solutions.

Ability to generate analytical reports and various search queries. When designing a secure fault-tolerant cloud repository, it is necessary to provide for the possibility of generating reports according to various criteria. It is also necessary to develop of a search module for stored data.

Integration possibility with corporate information systems. When designing a secure fault-tolerant cloud repository, it is necessary to provide for the possibility of integration with corporate information systems [3–5]. This is due to the following main factors:

• access to the storage must be provided based on user data from active directory;

• the ability to store and process documents and files from various information systems and services must be provided;

• access to the repository must be personalised and confirmed by the appropriate authority. For example, a user with the student role should have access to their own repository, a user with the teacher role should have access to the works of their students. The corresponding user role should be assigned automatically based on data from automated personnel and student management systems.

Ability to check for anti-plagiarism on stored data. To check uploaded students' paperworks, it is necessary to provide an interface for integration with anti-plagiarism testing systems. It will be improve the quality of term papers and theses.

Results and discussion

The information system of a secure cloud repository of students' paperworks and employees of educational and research organisations is a set of architectural solutions and software designed to ensure reliable storage of information using cloud technologies and cloud services that provide secure access to resources stored in the cloud to mobile users, regardless of the hardware and software platform used.

By organising cloud storage at the Belarusian State University, the emphasis was placed on the use of a distributed file system.

This was done due to the following disadvantages of hardware storage systems:

• the limitation of the total bandwidth of interaction with the storage system, as noted above. For example, according to the technical documentation, for the Lenovo DE6000H system, the data reading bandwidth reaches 21 Gbit/s. Obviously, with the growing number of clients, especially connecting from the outside, this bandwidth will not be enough. Using distributed file systems, the independence of requests sent to the storage is essential. Although the performance of each individual connection will be lower than in the system mentioned above, the cumulative data flow to (from) the system can be practically unlimited. This is achieved due to the possibility of increasing access points to a distributed file system resource and organising alternative access paths to data storage. The bandwidth of which is practically unlimited and in total can be significantly exceed the limit of several tens, hundreds or even thousands of gigabits per second;

• the need to localise the storage system and the systems using it within the same geographic location. Traditional data storage systems, as usual, require placement in the same data center where the consumer of their data is located. In addition, even in this case, the distance from the consumer of information to the storage system is limited. The organisation of distributed storage requires additional resources both software and hardware solutions (as an example is the idea of metro-cluster). Due to the reasons mentioned in point one, namely the separation of information transmission flows, as well as, due to some typical structure of services used in distributed file systems and virtualisation of the data access point. The proposed structure allows us to form a storage cluster more dependent on the quality of communication channels, but loosely related to management and maintenance tasks, and also allows us to increase storage space almost indefinitely.

As the basis of such a repository, it is advisable to choose one of the free distributed open-source systems.

The automatic identification system is built from the following components:

• hardware and software platform for the organisation of a fault-tolerant data storage with distributed management and data networks;

• a system for managing and monitoring the state of a fault-tolerant storage;

• IaaS platform based on data center resources for deploying microservices of the cloud storage system;

• a set of microservices images that provide a cloud storage user interface.

By choosing technologies and solutions, one of the main requirements was the use of solutions based on publicly available technologies and protocols and presented in the form of freely distributed source code.

The overall architecture of the system is shown in figure.

Fault-safe distributed storage module. The fault-safe distributed storage module was developed on the base of the Ceph distributed file system[1], as it has the following main implementation features:

• the system combines the resources of several servers by merging them into a single cluster with a single management system;

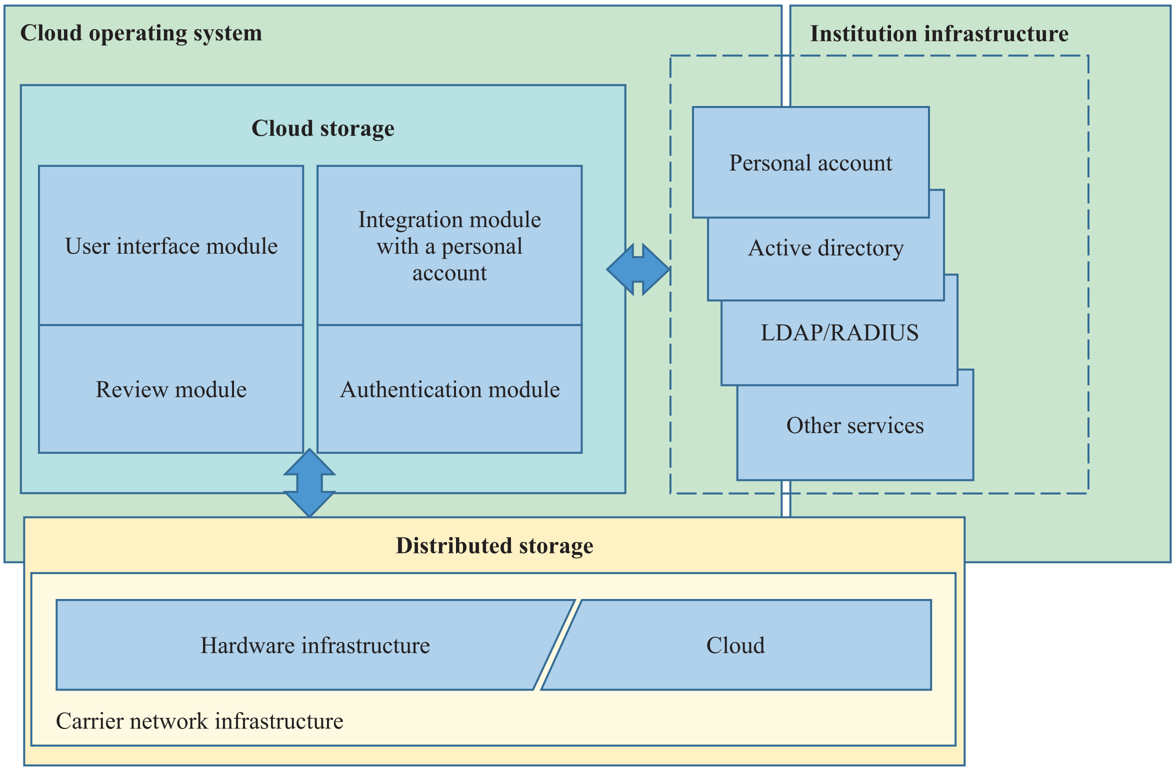
• data is stored as blocks (similar to a traditional file system), and the system continuously check the status of these blocks by monitoring and replicating these blocks on the fly, if it is necessary;

• Ceph provides a variety of interfaces for accessing stored data, which is also the subject of research to identify more productive and (or) more resilient to failures mechanisms;

• Ceph implements a web-based cluster management interface with status monitoring elements.

During the installation of Ceph cluster servers, CentOS Linux release 7.7.1908 was selected as the base operating system, kernel version 3.10.0-1062-el7.x86_64. Using the SSH service, the trust relationships necessary for Ceph deployment were set up between the cluster servers.

[1]Официальный сайт Ceph [Электронный ресурс]. URL: https://ceph.io/ (дата обращения: 10.03.2021).



General system architecture

By creating the storage module, the DHCP and NIS services were additionally deployed. The use of these services makes it possible to reduce the costs of configuring and subsequent maintenance of a fault-tolerant storage system due to the mechanism of centralised distribution of information necessary for the functioning of the system. Maintaining such as services allows, for example, to reduce the time for adding a new server to an existing storage system. Since a set of standard software is installed on the new server, and the necessary settings for integrating the server into the general system are transmitted by these services.

The DHCP server is used to distribute the network interface settings of the cluster servers. In the current configuration, two subnets are declared, corresponding to the segments described in the previous section.

In contrast, the NIS server is used to distribute configuration files which are necessary for the functioning of the cluster, in particular information about some accounts required for automated maintenance of the storage system, server names, etc.

Virtual platform for building a cloud interface. Based on the analysis of existing open solutions, the NextCloud system was chosen as the basis for the created platform that provides a cloud interface for accessing fault-tolerant storage[2]. The choice in favour of NextCloud was made based on the requirements specified in the introduction. At the moment also it is the only opensource solution in terms of functionality comparable to proprietary cloud storage. There are other cloud storages, for example, SeaFile[3], but it is not yet possible to consider them, and even to compare them, because they are in the initial phase of their development [6]. Additional complexity by choosing a platform is associated with the need to install not only the selected solution on some server, but to create an image of a virtual machine independent of the cloud platform on which such a virtual machine can be deployed in the future. In this regard, CentOS Linux GenericCloud 1907 OS was chosen as the main operating system for the virtual machine, which in turn is a cloud implementation of CentOS Linux release 7.6.1810 (Core) OS with Linux kernel version 3.10.0-957.27.2.el7.x86_64. The choice of the Linux dialect is not critical, since the system being deployed can work with any modern Linux implementation.

To ensure free migration between different cloud environments, the original image was converted to VHD format, which allows it to be run on most of the virtual environments, in particular, OpenStack and Windows Hyper-V, using which cloud solutions currently operate at the Belarusian State University.

Note that the module being created provides only interface interaction between the user and the secure storage and does not require large amounts of disk space. As a result, the time for deploying and launching a new virtual machine image is reduced, if it is necessary.

[2]Официальный сайт NextCloud [Электронный ресурс]. URL: https://nextcloud.com/ (дата обращения: 01.10.2021).
[3]Официальный сайт SeaFile [Электронный ресурс]. URL: https://seafile.com (дата обращения: 01.10.2021).

Conclusion

The developed solutions for creating a cloud repository include various levels of service provision and allow using the results obtained both in the construction of cloud repositories for educational institutions and in the design of individual modules of fault-tolerant systems. The developed secure fail-safe cloud repository of students' paperworks allows to provide the mass user access to the system and reliable storage, create a single cloud, while it can be geographically distributed.

Accordingly, the applied approaches can be used in various sectors of the economy for safe and reliable storage as well as for processing of various documents under the legislation of the Republic of Belarus.

Библиографические ссылки

1. Король АД, Воротницкий ЮИ, Кочин ВП. Дистанция в образовании: от методологии к практике. *Наука и инновации.* 2020;6:22–29.

2. Король АД, Воротницкий ЮИ, Кочин ВП. Информационно-коммуникационные технологии дистанционного и онлайн-обучения. В: Тузиков АВ, Григянец РБ, Венгеров ВН, редакторы. *Развитие информатизации и государственной системы научно-технической информации (РИНТИ-2020). Материалы XIX Международной конференции; 19 ноября 2020 г.; Минск, Беларусь.* Минск: ОИПИ НАН Беларуси; 2020. с. 22–29.

3. Кочин ВП, Воротницкий ЮИ, Жерело АВ. Виртуализация сетевой инфраструктуры учреждений образования. *Цифровая трансформация*. 2020;1:51–56.

4. Кочин ВП, Жерело АВ. Виртуализация сетевой инфраструктуры Белорусского государственного университета. *Вестник компьютерных и информационных технологий.* 2020;17(8):45–51. DOI: 10.14489/vkit.2020.08.pp.045-051.

5. Курбацкий АН, Кочин ВП, Слесаренко ОВ. Проектирование и автоматизация работы облачной кластерной системы с учетом интеграции с внешними информационными системами. *Веснік сувязі.* 2021;2:56–61.

6. Кочин ВП. *Разработать технологии аутентификации и авторизации пользователей в образовательных сетях на базе смарт-карт (отчет о научно-исследовательской работе (заключительный)).* Минск: БГУ; 2020. 68 с. № государственной регистрации 20163472.

References

1. Korol' AD, Vorotnitskii YuI, Kochyn VP. [Distance in education: from methodology to practice]. *Nauka i innovatsii.* 2020;6: 22–29. Russian.

2. Korol' AD, Vorotnitskii YuI, Kochyn VP. [Information and communication technologies of distance and online learning]. In: Tuzikov AV, Grigyanets RB, Vengerov VN, editors. *Razvitie informatizatsii i gosudarstvennoi sistemy nauchno-tekhnicheskoi informatsii (RINTI-2020). Materialy XIX Mezhdunarodnoi konferentsii; 19 noyabrya 2020 g.; Minsk, Belarus'* [Development of informatisation and the state system of scientific and technical information (RINTI-2020). Materials of the 19th International conference; 2020 November 19; Minsk, Belarus]. Minsk: Joint Institute for Informatics Problems of the National Academy of Sciences of Belarus; 2020. p. 22–29. Russian.

3. Kochyn VP, Vorotnitsky YuI, Zherelo AV. Virtualization of the network infrastructure in educational institutions. *Tsifrovaya transformatsiya.* 2020;1:51–56. Russian.

4. Kochyn VP, Zherelo AV. Virtualization of the network infrastructure of the Belarusian State University. *Vestnik komp'yuternykh i informatsionnykh tekhnologii.* 2020;17(8):45–51. Russian. DOI: 10.14489/vkit.2020.08.pp.045-051.

5. Kurbatskii AN, Kochyn VP, Slesarenko OV. Design and automation of the cloud cluster system taking into account the integration with external information systems. *Vesnik suvjazi.* 2021;2:56–61. Russian.

6. Kochyn VP. *Develop technologies for user authentication and authorization in educational networks based on smart cards (research report (final)).* Minsk: Belarusian State University; 2020. 68 p. State registration No. 20163472. Russian.

Received 15.10.2021 / revised 19.10.2021 / accepted 26.10.2021.

АННОТАЦИИ ДЕПОНИРОВАННЫХ В БГУ РАБОТ
INDICATIVE ABSTRACTS OF THE PAPERS DEPOSITED IN BSU

УДК 519.633(075.8)

Егоров А. А. **Метод Фурье решения смешанных задач для неоднородных гиперболических уравнений с постоянными коэффициентами** [Электронный ресурс] : учеб.-метод. разработка для студентов физ. фак. и фак. радиофизики и компьютер. технологий / А. А. Егоров, И. В. Рыбаченко ; БГУ. Электрон. текстовые дан. Минск : БГУ, 2021. 58 с. Библиогр.: с. 58. Режим доступа: https://elib.bsu.by/handle/123456789/268377. Загл. с экрана. Деп. в БГУ 16.09.2021, № 009316092021.

Учебно-методическая разработка посвящена одному из важнейших разделов математической физики, связанному с применением метода разделения переменных для неоднородных уравнений в частных производных гиперболического типа. В работу включены темы «Смешанные задачи для неоднородного уравнения колебаний струн и стержней» и «Смешанные задачи о вынужденных колебаниях в общей постановке». В каждой из них даны краткие теоретические сведения и рассмотрены примеры решения задач различной степени сложности. Также приведены задачи для самостоятельного решения и индивидуальных заданий.

Представленная разработка адресована студентам, обучающимся на физическом факультете и факультете радиофизики и компьютерных технологий БГУ. Может оказаться полезной преподавателям при подготовке и проведении практических занятий по дисциплине «Методы математической физики».

СОДЕРЖАНИЕ

CONTENTS

REAL, COMPLEX AND FUNCTIONAL ANALYSIS

MATHEMATICAL LOGIC, ALGEBRA AND NUMBER THEORY

DISCRETE MATHEMATICS AND MATHEMATICAL CYBERNETICS

COMPUTATIONAL MATHEMATICS

THEORETICAL FOUNDATIONS OF COMPUTER SCIENCE

SHORT COMMUNICATIONS

Журнал включен Высшей аттестационной комиссией Республики Беларусь в Перечень научных изданий для опубликования результатов диссертационных исследований по физико-математическим наукам (в области математики и информатики), техническим наукам (в области информатики).

Журнал включен в наукометрические базы данных Scopus, Mathematical Reviews, Ulrichsweb, Google Scholar, zbMath, РИНЦ.

Журнал Белорусского государственного университета. Математика. Информатика. № 3. 2021

Учредитель:
Белорусский государственный университет

Юридический адрес: пр. Независимости, 4, 220030, г. Минск.
Почтовый адрес: пр. Независимости, 4, 220030, г. Минск.
Тел. (017) 259-70-74, (017) 259-70-75.
E-mail: jmathinf@bsu.by
URL: https://journals.bsu.by/index.php/mathematics

«Журнал Белорусского государственного университета. Математика. Информатика» издается с января 1969 г.
До 2017 г. выходил под названием «Вестник БГУ. Серия 1, Физика. Математика. Информатика» (ISSN 1561-834X).

Редакторы *О. А. Семенец, М. А. Подголина*
Технический редактор *В. В. Пишкова*
Корректор *Л. А. Меркуль*

Подписано в печать 30.11.2021.
Тираж 100 экз. Заказ 548.

Республиканское унитарное предприятие «Информационно-вычислительный центр Министерства финансов Республики Беларусь».
ЛП № 02330/89 от 03.03.2014.
Ул. Кальварийская, 17, 220004, г. Минск.

Journal of the Belarusian State University. Mathematics and Informatics. No. 3. 2021

Founder:
Belarusian State University

Registered address: 4 Niezaliežnasci Ave., Minsk 220030.
Correspondence address: 4 Niezaliežnasci Ave., Minsk 220030.
Tel. (017) 259-70-74, (017) 259-70-75.
E-mail: jmathinf@bsu.by
URL: https://journals.bsu.by/index.php/mathematics

«Journal of the Belarusian State University. Mathematics and Informatics» published since January, 1969.
Until 2017 named «Vestnik BGU. Seriya 1, Fizika. Matematika. Informatika» (ISSN 1561-834X).

Editors *O. A. Semenets, M. A. Podgolina*
Technical editor *V. V. Pishkova*
Proofreader *L. A. Merkul'*

Signed print 30.11.2021.
Edition 100 copies. Order number 548.

Republican Unitary Enterprise «Informatsionno-vychislitel'nyi tsentr Ministerstva finansov Respubliki Belarus'».
License for publishing No. 02330/89, 3 March 2014.
17 Kal'varyjskaja Str., Minsk 220004.