ISSN 1684-8853 (print); ISSN 2541-8610 (online)

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

6(109)/2020

doi:10.31799/1684-8853-2020-6

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

SCIENTIFIC JOURNAL

6(109)/2020

PEER REVIEWED JOURNAL

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

Founder
«Information and Control Systems», Ltd.
Publisher
Saint-Petersburg State University
of Aerospace Instrumentation
Editor-in-Chief
M. Sergeev
Dr. Sc., Professor, Saint-Petersburg, Russia
Deputy Editor-in-Chief
E. Krouk
Dr. Sc., Professor, Moscow, Russia
Executive secretary
O. Muravtsova

Editor: A. Larionova
Proofreader: T. Zvertanovskaia
Design: M. Chernenko, Y. Umnitsina
Layout and composition: Y. Umnitsina

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, e-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press,
Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom,
Information Technologies and Mass Communications (ROSKOMNADZOR)
due to change of the founder: «Information and Control Systems», Ltd.,
JD № FS77-49181 from March, 30, 2012.

Submitted for publication 02.11.20. Passed for printing 17.12.20. Format $60\times84_{1/8}$.
Phototype SchoolBookC. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

The journal is indexed in Scopus.

doi:10.31799/1684-8853-2020-6 **ISSN 1684-8853 (print); ISSN 2541-8610 (online)**

НАУЧНЫЙ ЖУРНАЛ

6(109)/2020

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
ООО «Информационно-управляющие системы»
Издатель
Санкт-Петербургский государственный университет
аэрокосмического приборостроения
Главный редактор
М. Б. Сергеев,
д-р техн. наук, проф., Санкт-Петербург, РФ
Зам. главного редактора
Е. А. Крук,
д-р техн. наук, проф., Москва, РФ
Ответственный секретарь
О. В. Муравцова

Редактор: А. Г. Ларионова
Корректор: Т. В. Звертановская
Дизайн: М. Л. Черненко, Ю. В. Умницына
Компьютерная верстка: Ю. В. Умницына

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, эл. адрес: ius.spb@gmail.com,
сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в БД SCOPUS и в Перечень рецензируемых научных изданий,
в которых должны быть опубликованы основные научные результаты диссертаций
на соискание ученой степени кандидата наук,
на соискание ученой степени доктора наук.

Сдано в набор 02.11.20. Подписано в печать 17.12.20. Формат 60×84 1/8.
Гарнитура SchoolBookC. Печать цифровая.
Усл. печ. л. 9,2. Уч.-изд. л. 12,7. Тираж 1000 экз (1-й завод 50 экз.). Заказ № 393.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 519.614
doi:10.31799/1684-8853-2020-6-2-11

Окружности на решетках и матрицы максимума детерминанта

Н. А. Балонин[а]**,** *доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
М. Б. Сергеев[а]**,** *доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277*
Дж. Себерри[б]**,** *доктор наук, профессор, orcid.org/0000-0002-9558-4293*
О. И. Синицына[а]**,** *аспирант, orcid.org/0000-0002-2819-4682*
*[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*
[б]Университет Вуллонгонг, Вуллонгонг, Новый Южный Уэльс 2522, Австралия

Введение: *гипотеза Адамара о существовании матриц максимума детерминанта порядков, кратных четырем, тесно связана с проблемой Гаусса о числе точек с целыми координатами (точек на решетке Z3) на сфероиде, конусе, параболоиде или параболе. Расположение точек Гаусса диктует количество и виды экстремальных матриц.* ***Цель:*** *выявить связь точек Гаусса на сечениях тел вращения с количеством и видами матриц максимума детерминанта с фиксированной структурой для нечетных порядков. Определить точную верхнюю границу значений максимумов детерминанта для бициклических матриц с каймой и порядки их превалирования над более простыми циклическими структурами.* ***Результаты:*** *приведена формула, уточняющая излишне оптимистическую границу Элича — Войтаса на случай матриц фиксированной структуры. Показана особая роль чисел Ферма для порядков 4t + 1. Показано влияние чисел Барбы на формирование классов матриц максимального детерминанта, занимающих последовательно сменяющие друг друга области порядков 4t + 3. Для бициклической структуры с каймой приведена оценка 67 для максимального порядка, на котором наблюдается оптимальное симметричное решение, и доказано превосходство детерминанта блочных матриц с каймой над детерминантами циклических матриц везде, за исключением особого 39-го порядка.* ***Практическая значимость:*** *связанные с точками решетки матрицы максимального для фиксированной структуры детерминанта имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

Ключевые слова *— точки Гаусса, проблема Гаусса, параболоид на решетке, ортогональные матрицы, матрицы Адамара, матрицы максимального детерминанта, бициклические матрицы с каймой.*

Для цитирования: Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И. Окружности на решетках и матрицы максимума детерминанта. *Информационно-управляющие системы*, 2020, № 6, с. 2–11. doi:10.31799/1684-8853-2020-6-2-11
For citation: Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices, and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2020-6-2-11

Введение

Настоящая статья является продолжением работы [1], посвященной связи классических задач о поиске точек Гаусса (точек с целочисленными координатами) на окружностях, образованных сечениями тел вращения, и матриц большого или наибольшего детерминанта [2], в частности, матриц Адамара [3, 4]. Экстремальные по детерминанту ортогональные (и неортогональные) матрицы представляют большой научный и практический интерес [5, 6] ввиду сложности их поиска, отражающего нетривиальность объекта, являющегося источником уникальных кодов в прикладных задачах обработки цифровой информации и помехоустойчивого кодирования [7, 8].

Адамар [3], который более столетия назад занимался оцениванием детерминанта матрицы с ограниченными единицей (по модулю) элементами, установил, что его верхняя граница не превосходит $n^{n/2}$. Серией последующих основополагающих работ эта граница была уточнена для матриц порядков, не кратных четырем [2] (на которых недостижима оптимистическая оценка) и нечетных порядков [9–11].

Первые компьютерные [12, 13] и теоретические исследования [14–19] привели к представлению о том, что широкий диапазон четных порядков разрешим относительно простыми оптимальными матрицами, состоящими из двух и более циклических блоков, чей размер пропорционален порядку [20, 21]. Матрицы нечетного порядка оказались структурно сложными даже при невысокой размерности задачи [22–24].

Эти исследования свелись постепенно к соревновательному процессу, в ходе которого находились преимущественно оптимальные матрицы все более высоких четных порядков [25, 26]. Опыт показал, что рекорд можно наращивать привлечением алгоритмов теории полей и групп [27, 28].

Постепенно это привело к диспропорции в размерах известных матриц четных и нечетных порядков, вследствие чего последовательности значений детерминантов в OEIS [29] и размеры матриц каталога [30] весьма ограничены. Для того чтобы изменить положение, необходимо предлагать новые подходы и методы оценивания детерминантов и матриц, на которых оптимум достигается.

Орнаменты экстремальных матриц

Впервые вопрос о существовании экстремальных матриц, отличных от сильвестровых и существующих на порядках, кратных четырем, поставил Адамар [3]. Содержание так называемой *гипотезы Адамара* [31, 32] состоит в том, что ортогональные матрицы с элементами ±1 существуют на всех порядках $4t$, где t — натуральное число. Заметим, что если экстремальная по детерминанту матрица не ортогональна, это не означает, что ее нельзя ортогонализовать вариацией значений элементов [33], не меняя узора матрицы (орнамента) — порядка расположения элементов в ней. Таким образом, при поиске параметров узоров различие между двумя названными видами матриц несущественно и не препятствует построению общей теории, сходной с изложенной в работе [1].

Различают одноблочную, двухблочную и четырехблочную конструкции ортогональных матриц порядка n:

$$\mathbf{A};\ \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix};$$

$$\begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ \mathbf{CR} & \mathbf{RD} & -\mathbf{A} & -\mathbf{RB} \\ \mathbf{BR} & -\mathbf{A} & -\mathbf{RD} & \mathbf{RC} \\ \mathbf{DR} & -\mathbf{RC} & \mathbf{RB} & -\mathbf{A} \end{pmatrix}, \qquad (1)$$

где **A**, **B**, **C** и **D** — моноблоки размера v. Блоки характеризуются k_1, k_2, k_3, k_4 — количествами элементов со значением –1 в каждой строке, и количеством пар отрицательных элементов λ для каждых двух строк матрицы в целом; **R** — реверсная единичная матрица, содержащая (в отличие от **I**) ненулевые элементы на другой ее диагонали.

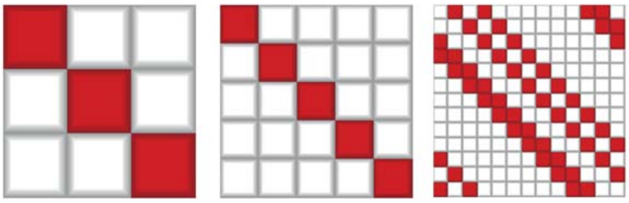
Третья конструкция в (1) с симметричным блоком **A** удобна для симметрирования ее в целом путем приравнивания блоков **B** и **C**. Это отличает ее от массива Вильямсона [4] с симметричными блоками, но несимметричного в целом. Если блоки конструкций (1) циклические, то двухблочная конструкция называется бициклической, а последняя при **B** = **C** — трициклической, или Пропусом [1] с тремя блоками **A**, **B** и **D** и параметрами, которые нумеруются k_1, k_2 и k_3.

Известно, что циклическая симметричная матрица Адамара порядка, отличного от 1, согласно гипотезе Райзера [34] всего одна. Три циклические версии матриц порядков 3, 5 и 13 приведены на рис. 1 [35]. Здесь светлая клетка соответствует элементу матрицы со значением 1, а темная — со значением –1. Заметим, что последняя из трех матриц является несимметричной.

Детерминант остается высок и у матрицы порядка 19, но не является максимальным. Этот порядок у бициклических матриц с каймой выделяется аномально большим значением детерминанта, превышающим некоторую общую для всех таких матриц границу.

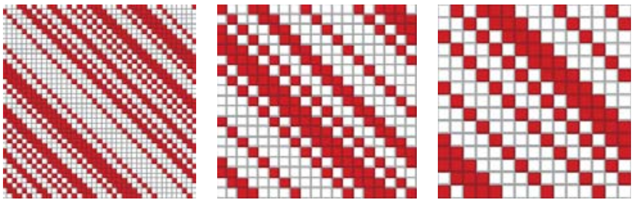
Известны и мультипликативные порядки 15 (3 × 5), 27 (3 × 3 × 3) и 39 (3 × 13) циклических матриц с большим детерминантом, портреты которых приведены на рис. 2. Последний из указанных порядков примечателен тем, что на нем бициклическая матрица с каймой уступает по детерминанту несимметричной циклической матрице.

На этом преимущества моноциклических матриц заканчиваются. Перейдем к конструкциям из большего числа блоков. Нечетные порядки отличаются от четных тем, что на них структура матриц максимального детерминанта неограниченно усложняется — нет универсальной основы. Задача обрастает большим количеством субоптимальных решений в виде матриц большого (не наибольшего) детерминанта (МБД).



■ *Рис. 1.* Циклические матрицы максимума детерминанта порядков 3, 5, 13 [35]

■ *Fig. 1.* Maximum determinant circulant matrices of orders 3, 5, 13 [35]



■ *Рис. 2.* Циклические матрицы большого детерминанта порядков 19, 15 и 39

■ *Fig. 2.* Large determinant circulant matrices of orders 19, 15 and 39

Для практических приложений все равно, какую именно из них мы используем. Поэтому выделим в отдельный класс матрицы с экстремумом на заданной бициклической структуре, понимая в дальнейшем под МБД именно такие матрицы. Как общее, объединяющее все решения правило, отметим, что для симметричных матриц есть пороговый порядок, который отодвигается с увеличением числа используемых блоков, однако адамаровы трициклы существуют для всех порядков, кратных четырем [1].

Уравнения орнаментов

Уравнения, связывающие структурные (орнаментальные) инварианты v, k_1, k_2, k_3 и λ, возникают вследствие того, что квадратная бинарная матрица ограничена в возможности содержать описываемый параметрами узор. Наиболее известно уравнение $k(k-1)=\lambda(v-1)$. Если блоков в матрице несколько, то слева будет сумма $k_1(k_1-1)+k_2(k_2-1)$ или взвешенная сумма $k_1(k_1-1)+2k_2(k_2-1)+k_3(k_3-1)$. Это является переходом к канонической форме, описывающей сфероид $x^2+2y^2+z^2=n$ [1] или параболоид, представленные на рис. 3.

Правая часть канонического уравнения у матриц Адамара равна порядку n, при обобщении она усложняется до $f(v)=n+\delta(v-1)$, где δ — невязка матрицы наименьших квадратов (МНК) вида $\mathbf{H}^{\mathrm{T}}\mathbf{H}$, размещенная за пределами ее диагонали и вне нулей внедиагональных блоков. Она равна нулю для ортогональных матриц порядков, кратным четырем, и различается знаком $\delta=2$ или $\delta=-2$ для случаев сильного и слабого экстремумов матриц четных порядков $n=4t+2$.

Теорема 1. Орнаментальные инварианты k_1, k_2, k_3 ортогональных и экстремальных по детерминанту матриц (1) определяются линейными функциями

$$k_1=(v-x)/2,\ k_2=(v-y)/2,\ k_3=(v-z)/2 \qquad (2)$$

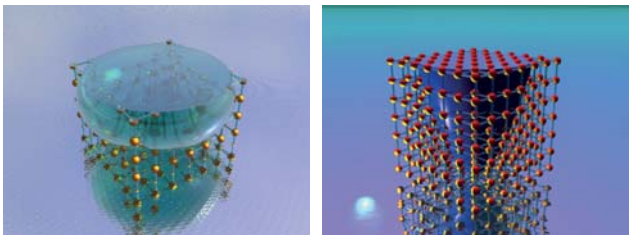
от переменных канонического уравнения $x^2+2y^2+z^2=f(v)$ или, при уменьшении числа блоков, его усечений $x^2+y^2=f(v)$, $x^2=f(v)$. Здесь $\lambda=k+(\delta-v)/4$ и k — параметры матрицы в целом, т. е. $k=k_1+2k_2+k_3$ или сумма $k=k_1+k_2$ для бициклической матрицы.

Доказательство восходит к квадратичному уравнению совместности, известному со времен разработки теории графов. Это нашло свое отражение в наименованиях с упоминанием абстрактного блочного дизайна [4].

Для ортогонального моноцикла при $\delta=0$ имеем $\lambda=k-v/4$. Тогда $k(k-1)=(k-v/4)(v-1)$ или $4(k^2-kv)+v^2=v$. С учетом $k=(v-x)/2$ это дает $(v-x)^2-2(v-x)v+v^2=v$, которое немедленно приводит к нужному нам результату: $x^2=n$. Экстремальные задачи для порядков $n=4t+2$ связаны с делением матриц на парные блоки. Матриц Адамара ввиду ненулевого смещения $\delta=\pm2$ среди них нет. Изменение количества блоков ничего не меняет в приведенной схеме доказательства, регулируя лишь количество связываемых каноническим уравнением базовых переменных, входящих в определение k_1, k_2, k_3.

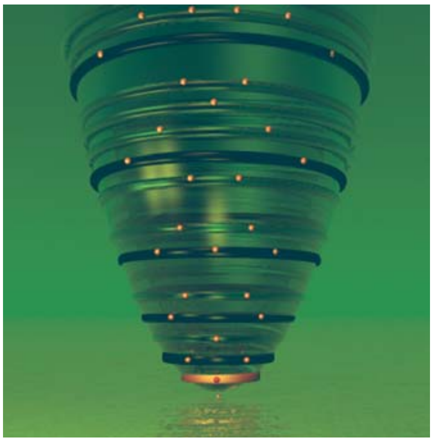
Классификация точек параболоида

В расчетах орнаментальных инвариантов $k_1=(v-x)/2$ и $k_2=(v-y)/2$ может фигурировать любая точка Гаусса квадратичной поверхности, охватывая всю совокупность глобальных и локальных экстремумов (рис. 4). Например, в отличие от матриц Адамара с их наибольшим значением детерминанта, для дихотомичных по своей структуре экстремальных матриц порядков $n=2v$ с блоками $\mathbf{A}$ и $\mathbf{B}$ правая часть канонического уравнения $x^2+y^2=n+\delta(v-1)$ при $\delta=-2$ сводится к константе $x^2+y^2=2$. Это дает разнообразие значений k_1 и k_2 при смене размера v при одной на все решения точке Гаусса ($x=1$, $y=1$),



■ ***Рис. 3.*** Срезы сфероида и параболоида на решетке

■ ***Fig. 3.*** Sections of a spheroid and paraboloid on a lattice



■ ***Рис. 4.*** Параболоид $x^2+y^2=f(v)$ с точками Гаусса

■ ***Fig. 4.*** Paraboloid $x^2+y^2=f(v)$ with Gauss points расположенной на постоянной минимальной высоте 2.

Этот слабый экстремум был замечен при поисках матриц Адамара бициклической конструкции с двойной каймой, т. е. при добавлении парной каймы решение переходит в строгий максимум. Кроме того, эта бициклическая матрица ортогонализуется понижением значения одного из двух возможных элементов матрицы, переходя в матрицу Эйлера [31, 32]. Это делает ее аналогом матриц Адамара на четных порядках, не кратных четырем.

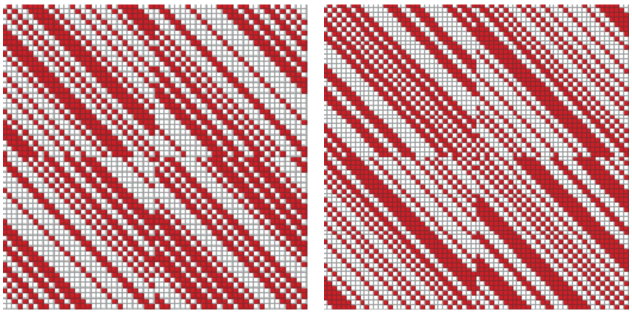
Такая бициклическая матрица существует всегда, поскольку платой за усложнение структуры является максимальный детерминант.

Эта характерная черта поясняет, почему при поиске бициклических матриц с одинарной каймой нет смысла искать строгие оптимумы их основ — бициклических матриц. Поскольку кайма одна, то точка Гаусса сходит с отмеченного на рис. 4 желтым цветом кольца матриц Эйлера, поднимаясь выше. Но, в отличие от строго оптимальных матриц, ведущая точка для расчетов орнаментальных инвариантов не следует за размером бициклической матрицы. Она, в отличие также от простейшего случая стабилизации на одном нижнем значении, отвечает не всем возможным четным порядкам, а их диапазону. Теория МБД позволяет вычислить эти диапазоны, указав, чем они различаются между собой.

Для начала перечислим видимые на рис. 4 координаты стартовых независимых точек Гаусса для порядков: 2 ($x = 1$, $y = 1$), 6 (1, 3), 10 (3, 3), 14 (1, 5), 18 (3, 5), 22 (неразрешим), 26 (1, 7) и (5, 5), 30 (3, 7), 34 (неразрешим) и т. д. Порядки матриц максимума детерминанта принято разбивать на два семейства, когда оценка максимума детерминанта проходит через целочисленную точку и, следовательно, становится достижимой.

Первое семейство порядков $n = 2v$, для которых $v = L + 1$, где $L = q(q + 1)$ и q — целое число, содержит порядки матриц Барбы [2] 2, 6, 14, 26, 42, 62, 86, 114, ..., отмеченные на рис. 4 синими кольцами. На них всегда имеются крайние точки с координатами $x = 1$ и (или) $y = 1$, нулевых значений не бывает. Именно к ним относится точка с кольца Эйлера с координатами (1, 1). Из канонического уравнения для орнамента оптимальной матрицы $x^2 + y^2 = 2n - 2$ следует, что если $x = 1$, то $y^2 = 4L + 1$.

Второе семейство порядков $n = 2v$, для которых $v = 2L + 1$, где $L = q(q + 1)$ и q — целое число, содержит порядки 2, 10, 26, 50, 82, 122, 170, ... Оно описывает кольца, содержащие средние точки Гаусса с $x = y$, $x^2 = y^2 = n - 1 = 2v - 1 = 4L + 1$. Эти множества точек на параболоиде, как видно из рис. 4, пересекаются, хотя численные значения показателя L для них не те же самые, поскольку L здесь иначе связан с размером блока.



■ ***Рис. 5.*** Портреты симметричных бициклических матриц порядков 58 и 66

■ ***Fig. 5.*** Symmetric two circulant matrices of orders 58 and 66

Наиболее интересно первое семейство колец Барбы, поскольку ведущая точка Гаусса для расчета матрицы с каймой может быть связана только с одним кольцом, но не с обоими сразу — компьютерный анализ показывает превалирование структур для первого семейства. Условимся, что q — номер кольца Барбы — начинает отсчет с нуля. Кроме того, отметим, что $L = q(q + 1)$ имеет смысл числа альтернансов: числа переключений знаков в диагональных блоках матриц МНК вида $\mathbf{H}^{\mathrm{T}}\mathbf{H}$ или $\mathbf{N} = \mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B}$. Матрицу $\mathbf{N}$ будем называть *орнаментальной* матрицей.

Найденные симметричные бициклические матрицы порядков 58 и 66, портреты которых представлены на рис. 5, продолжают сет симметричных матриц порядков 6, 10, 14, 18, 22, 26, 34, нет 42 (42/2 = 21 — не простое), 50 экстремальных матриц порядков $n = 4t + 2$, охваченных каймой.

На следующем ожидаемом порядке 74 (66 + 8) симметричная бициклическая матрица не найдена (74/2 = 37 — простое число), что позволяет предположить, что симметричные решения МБД ограничены порядком 66. Напомним, что у матриц Адамара эта граница почти вдвое меньше — 32 [34, 35].

Формулы для расчета детерминантов

Детерминант $\det(\mathbf{D}) = (1 + \sigma)\det(\mathbf{H})$ матрицы $\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$ с каймой $\mathbf{e}$ в виде вектора из единиц в $\mathbf{D} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{H} \end{pmatrix}$ зависит от эксцесса [36] $\sigma = \sigma(\mathbf{H}^{-1})$ — суммы элементов матрицы, обратной к $\mathbf{H}$.

Отступая при расчете орнаментальных инвариантов к точкам Гаусса не своего кольца, мы, безусловно, теряем в значении детерминанта бициклической матрицы основы det(**H**), но выигрываем в значении второго сомножителя с σ, что и объясняет стационарность точки Гаусса. Оценку детерминанта матрицы четного порядка, не делимого на 4, дает теорема, доказанная независимо в двух источниках, что отразилось в ее названии [9–11].

Теорема 2 (Элича — Войтаса). Оптимальная по детерминанту матрица **H** порядка $n = 4t + 2$ дихотомична, отвечает бициклической структуре, и ее детерминант det(**H**) $\le$ Е(v), где

$$\mathrm{E}(v) = 2^{v}(2v - 1)(v - 1)^{(v-1)}.$$

Теорема доказывается рассмотрением детерминанта *орнаментальной матрицы* $\mathbf{N} = \mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B}$, который по абсолютному значению равен детерминанту **H** и легко оценивается при монотонном характере заполнения внедиагональных элементов, повысить значения которых нельзя в силу ограничений на блоки **A** и **B**.

Граница Элича — Войтаса является острой в том смысле, что она достижима на порядках $n = 2v$, на которых невязка МНК для диагональных блоков матрицы $\mathbf{H}^{\mathrm{T}}\mathbf{H}$ строго равна $\delta = 2$ (за пределами диагонали). Компьютерное исследование показывает, что при нарушении монотонности в знаках орнаментальной матрицы **N** с сохранением только L элементов со значениями $\delta = 2$ в каждой строке оценка детерминанта падает на величину, оцениваемую множителем $h(v) = 1 - (v/(L + 1) - 1)/\mathrm{K}$.

При $L = v - 1$ множитель становится единичным. В диапазоне порядков блоков $L < v < (L + 1) \times (\mathrm{K} + 1)$ коэффициент K, регулирующий наклон этой линейной относительно размера v зависимости, стационарен и равен примерно 15.

Порядки колец Барбы $n^* = 2v^*$, $v^* = q(q + 1) + 1$, где q — номер кольца, задают точки надлома характеристик, описывающих переход с 1 при $L = v^* - 1$ на линейное уменьшение множителя детерминанта. Отсюда $L = q(q + 1) = 0,\ 2,\ 6,\ 12,\ 20, \ldots$.

Величина эксцесса $\sigma = \sigma\left(H^{-1}\right) = v\dfrac{\sqrt{4L+1}}{2L+1}$, где $\sqrt{4L+1} = 2q+1$, где q — номер кольца Барбы, линейно зависит от размера блока v при L альтернансах орнаментальной матрицы **N**. Напомним, что из канонического уравнения для орнамента оптимальной матрицы $x^2 + y^2 = 4v - 2$ следует, что если $x = 1$ и $v = L + 1$, то $y^2 = 4L + 1$, т. е. $\sigma = yv/(v^* + L)$, где $v^* = L + 1$ — размер оптимального для кольца Барбы блока, дополненный, как видно, числом альтернансов.

Теорема 3. Максимальное увеличение детерминанта матрицы **H** с L альтернансами det(**D**) $\cong d(v) \times \mathrm{E}(v)$ при охвате матрицы каймой описывается квадратичной функцией (относительным по отношению к границе Е(v) детерминантом)

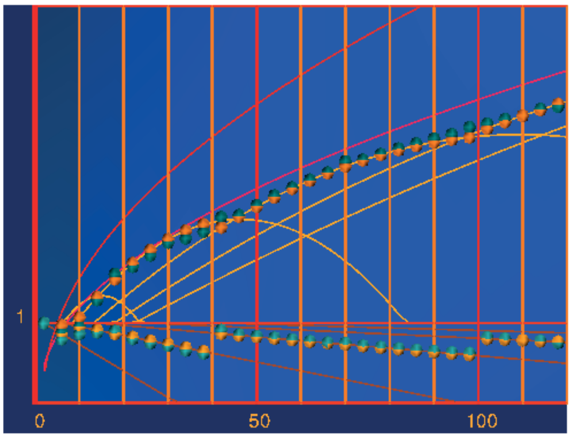
$$d(v) = \bigl(1+\sigma(v)\bigr)h(v) =$$
$$= \left(1+v\frac{\sqrt{4L+1}}{2L+1}\right)\Bigl(1-\bigl(v/(L+1)-1\bigr)/\mathrm{K}\Bigr)$$

с максимумом на порядке $n^{**} = 2v = L(\mathrm{K} + 1) + \mathrm{K}$. Это дает представление о тесной связи точки экстремума характеристики с наклоном K аппроксимирующей det(**H**) прямой.

Доказательство элементарно вытекает из аналитических выражений для сомножителей det(**D**) = (1 + σ)det(**H**), линейно зависящих от v, что позволяет найти максимум аналитически по точке равенства нулю производной этой функции.

Формула для эксцесса выведена нами и подтверждена в большом количестве компьютерных экспериментов с альтернирующими матрицами, она точно описывает коэффициент усиления det(**H**), зависящий от соотношения размеров текущего и ведущего блоков с учетом отмеченной поправки.

Графоаналитическое исследование аналитических значений оценок линейного $h(v)$ и квадратичного $d(v)$ относительных детерминантов при изменении количества альтернансов $L = q(q + 1) = 0,\ 2,\ 6,\ 12,\ 20$, вызванных сменой номера ведущего кольца Барбы $q = 0, 1, 2, 3, 4, 5$, представлено на рис. 6. Здесь пять линейных графиков $h(v)$, размещенных ниже 1, и пять ква-



■ ***Рис. 6.*** Результаты графоаналитического исследования детерминантов (масштаб графиков 1:3 выше 1 для сопоставимости результатов)

■ ***Fig. 6.*** The results of the graphic-analytical study of determinants (scale of graphs 1:3 is higher than 1 for comparability of results) дратичных графиков $d(v)$, описывающих последствия усиления бициклической основы каймой. Детерминант $\mathbf{H}$ оценивается по отношению к $\mathrm{E}(v)$ и не может превосходить теоретическую верхнюю границу.

На графики нанесены желтые точки, соответствующие аналитическим оценкам детерминантов, и зеленые — значениям относительных детерминантов реальных матриц, найденных в процессе оптимизации детерминанта при заранее не заданных количествах альтернансов L и параметров орнамента k_1, k_2 и λ. Проверка выполнена на матрицах до порядка 118.

Для упрощения общей качественной картины над квадратичными зависимостями можно разместить огибающую, описывающую границу детерминантов структурированных матриц бициклической конструкции с каймой, как

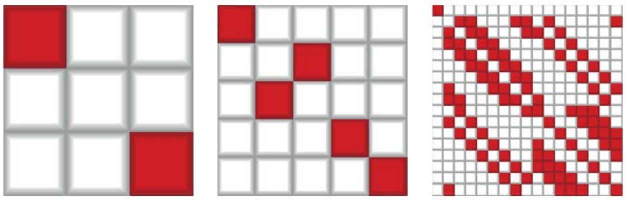
$$\det(\mathbf{D}) \le (2v)^{v+1/2}\mathrm{E}(v).$$

Она справедлива везде, кроме отмеченного $v = 9$, связанного с резонансом, когда две полоски равномерно распределяются между элементами орнаментальной матрицы. Выше этой зависимости, обозначенной на графике малиновым цветом, находится легко различимая оценка максимума детерминанта Барбы, не учитывающая структуру матрицы.

Для порядков матриц $n = 4t + 3$ известно приближение Элича. Оно на рис. 6 не отображено, поскольку размещается между двумя кривыми — общей и адаптированной под структуру МБД. По краям образовавшихся при сравнении квадратичных функций диапазонов порядков возникают отклонения от линейного закона, но значения этих краевых эффектов нивелируются малым значением второго параметра σ.

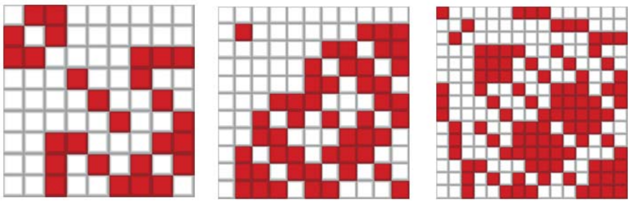
Отклонения объясняются, как и на порядке 18, повышением детерминанта матрицы $\mathbf{H}$ при равномерном делении $\mathbf{N}$ альтернансами. Эти отклонения не в состоянии изменить диапазоны стационарности L — метод устойчив для такой идентификации структур оптимальных матриц, когда сами матрицы не находятся. Для экспериментальной проверки результатов привлекались таблицы матриц большого детерминанта с фиксированной структурой [30, 37] наряду с найденными с использованием алгоритмов теории групп и полей образцами матриц более высоких порядков.

Отметим, что для альтернативных нечетных порядков $n = 4t + 1$ интерес представляют бициклические матрицы с каймой (рис. 7) [35] размеров, выделенных простыми числами Ферма: 3, 5, 17, 257, 65 537, ... [38].



■ *Рис. 7.* Матрицы максимума детерминанта порядков 3, 5, 17 [35]

■ *Fig. 7.* Maximum determinant matrices of orders 3, 5, 17 [35]



■ *Рис. 8.* Последовательное усложнение структур матриц порядков 9, 11, 15

■ *Fig. 8.* Sequential complication of structures of matrices of orders 9, 11, 15

Здесь можно провести параллель с достижением Гаусса, который, построив с помощью циркуля и линейки правильный семнадцатиугольник, вышел на понимание уникальности этих чисел для простых геометрических фигур. Ровно также и матрицы максимума детерминанта упрощаемы до простой структуры на указанных порядках, не достигая излишне оптимистичной границы Барбы. Это держало долгое время в тени решения на числах Ферма. Ранее отмечалось, что упрощенные структуры в форме циклических блоков наблюдаются только для стартовых порядков 3, 5 и 13.

Отсутствие исследований, описывающих матрицы максимального детерминанта нечетных порядков, объясняется большой сложностью этой задачи. Можно упомянуть такие известные антагонисты чисел Ферма, как числа Мерсенна $n = 2^k - 1 = 1$, 3, 7, 15 и 31 для подтверждения высказанного предположения об особой роли первых. Ведь экстремальная матрица на числах Мерсенна наблюдается для порядка, не превышающего 7. На всех остальных порядках матрицы максимума детерминанта не просто сложны, они существенно усложняются на каждом следующем порядке, что демонстрируется, например, портретами матриц порядков 9, 11, 15 (рис. 8).

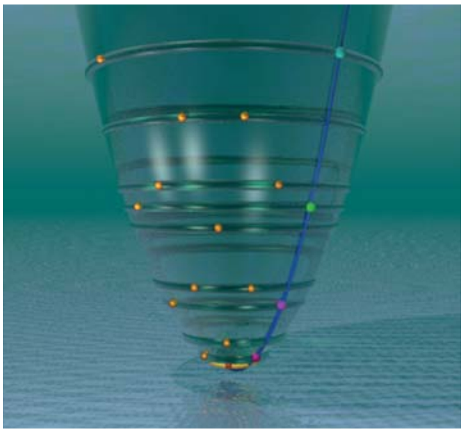
Классификация окружностей и точек Гаусса для матриц Адамара

Сферу и сфероид можно рассматривать как совокупность окружностей (или эллипсов) с варьируемым радиусом. Шанс получить на них точку Гаусса высок: согласно базовой теореме он не нулевой для любого характерного для матриц Адамара порядка. Для бициклической матрицы характерно количество основных орнаментальных инвариантов, меньшее трех. Это подразумевает отсутствие ряда решений для порядков, для которых разложение n на сумму двух квадратов невозможно.

Первое кольцо на рис. 9, отмеченное желтым цветом, встречается на стартовом для матриц Адамара порядке 2. Оно имеет одну точку Гаусса с координатами (1, 1). Следующее кольцо для порядка 4 имеет пару точек с координатами (0, 2) и (2, 0), соответствующими двум матрицам с взаимно переставленными блоками **A** и **B**. Как видно, это первая точка, которая сидит также на пересечении колец сечений параболоида и вертикальной плоскости с образованием точек Гаусса на отмеченной синим цветом параболе.

Соответственно, на этом порядке существует регулярная матрица Адамара в виде моноблока с параметрами $n = 4$, $k = (n - x)/2 = 1$, $\lambda = k - n/4 = 0$. Этим условиям удовлетворяет циклическая матрица с единственным отрицательным элементом в каждой строке на ее диагонали. Далее следует кольцо с точкой с координатами (2, 2) для порядка 8. Выше идут кольца адамаровых порядков 16 (0, 4), 20 (2, 4), 32 (4, 4), 36 (0, 6), 40 (2, 6), 52 (4, 6), 64 (6, 6).

Для порядка 12 точек Гаусса нет, и это первый порядок матрицы, неразрешимый с помощью бициклической структуры. Далее идут пропуски 24, 28, 44, 48, 56, 60 и т. п. Признак неразложимости хорошо известен благодаря работам Ферма и Эйлера. Во всех таких случаях в составе делителей порядка наблюдается число 3 mod 4 = 3, 7, 11, ... или любая его нечетная степень. Для четных степеней этих делителей точкам Гаусса даже тогда, когда они есть, могут отвечать моноблочные структуры матриц, отличные от циклических. Первый такой порядок матрицы 36 (4 × 9).



■ ***Рис. 9.*** Параболоид $x^2 + y^2 = n$ с точками Гаусса

■ ***Fig. 9.*** Paraboloid $x^2 + y^2 = n$ with Gauss points

Заключение

Бициклические матрицы большого детерминанта, являясь матрицами четного порядка, регулируют детерминанты матриц с каймой нечетного, на единицу большего, порядка. Это означает, что на порядках, равных числам Ферма, их анализ позволит проверить очень важное предположение [38] о том, что именно они и только на этих порядках являются матрицами абсолютного максимума детерминанта. Этот класс матриц, по всей видимости, очень важен и имеет относительно стабильную орнаментальную матрицу, позволяющую проверять субоптимальность матриц бициклической конструкции, и их теорию необходимо развивать. Теория матиц Адамара оперирует кольцами, лежащими между кольцами матриц большого детерминанта, что объединяет обе теории в одну, касающуюся соответствия экстремальных матриц точкам Гаусса для квадратичных поверхностей на решетках [1]. Нами проведен обзор и вычислительный эксперимент, дополненный найденными матрицами бициклической конструкции с каймой, обладающими экстремально большим детерминантом. Эти матрицы значительно расширяют результаты численных исследований [30, 37] новыми решениями.

Финансовая поддержка

Статья подготовлена при финансовой поддержке Министерства науки и высшего образования РФ, грант FSRF-2020-0004.

Литература

1. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi:10.31799/1684-8853-2019-3-2-9
2. **Barba G.** Intorno al teorema di Hadamard sui determinanti a valore massimo. *Giorn. Mat. Battaglini*, 1933, vol. 71, pp. 70–86.
3. **Hadamard J.** Resolution d’une question relative aux determinants. *Bulletin des Sciences Mathematiques*, 1893, no. 17, pp. 240–246.
4. **Seberry J., Yamada M.** Hadamard matrices, sequences, and block designs. In: *Contemporary Design Theory: A Collection of Surveys*. J. H. Dinitz and D. R. Stinson, eds. John Wiley and Sons, Inc., 1992. Pp. 431–560.

5. **Seberry J., Yamada M.** Hadamard matrices constructed using number theory and algebra. John Wiley (to appear).
6. **Horadam K. J.** Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
7. **Wang R.** Introduction to orthogonal transforms with applications in data processing and analysis. Cambridge University Press, 2010. 504 p.
8. **Ahmed N., Rao R.** Orthogonal transforms for digital signal processing. Springer-Verlag, Berlin-Heidelberg-New York, 1975. 263 p.
9. **Ehlich H.** Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, vol. 83, pp. 123–132.
10. **Ehlich H.** Determinantenabschätzungen für binäre Matrizen mit N≡3 mod 4. *Mathematische Zeitschrift*, 1964, vol. 84, pp. 438–447.
11. **Wojtas M.** On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloq. Math.*, 1964, vol. 12, pp. 73–83. doi:10.4064/cm-12-1-73-83
12. **Yang C. H.** On designs of maximal (+1, –1)-matrices of order n≡2 (mod 4). *Math. Comp.*, 1968, vol. 22, pp. 174–180.
13. **Yang C. H.** On designs of maximal (+1, –1)-matrices of order n≡2 (mod 4). II. *Math. Comp.*, 1969, vol. 23, pp. 201–205.
14. **Brenner J.** The Hadamard maximum determinant problem. *The American Mathematical Monthly*, 1972, vol. 79, no. 6, pp. 626–630.
15. **Yang C. H.** Maximal binary matrices and sum of two squares. *Math. Comp.*, 1976, vol. 30, pp. 148–153.
16. **Chadjipantelis Th., Kounias S.** Supplementary difference sets and D-optimal designs for n≡2 mod 4. *Discrete Math.*, 1985, vol. 57, pp. 211–216.
17. **Cohn J. H. E.** On determinants with elements ±1. II. *Bull. London Math. Soc.*, 1989, vol. 21, pp. 36–42. doi.org/10.1112/blms/21.1.36
18. **Djokovic D. Z.** On maximal (1, –1)-matrices of order 2n, n odd. *Radovi Matematicki*, 1991, vol. 7, pp. 371–378.
19. **Brent R. P., Osborn J. H.** On minors of maximal determinant matrices. arXiv preprint arXiv:1208.3819 [math.CO], 2012. http://arxiv.org/abs/1208.3819 (дата обращения: 09.04.2020).
20. **Chadjipantelis Th., Kounias S., Moyssiadis C.** Construction of D-optimal designs for n≡2 mod 4 using block-circulant matrices. *J. Combin. Theory Ser. A*, 1985, vol. 40, pp. 125–135.
21. **Kharaghani H.** A construction of D-optimal designs for N = 2 mod 4. *J. Combin. Theory Ser. A*, 1987, vol. 46, pp. 156–158.
22. **Chadjipantelis Th., Kounias S., Moyssiadis C.** The maximum determinant of 21 × 21 (+1, –1)-matrices and D-optimal designs. *J. Statist. Plann. Inference*, 1987, vol. 16, pp. 167–178.
23. **Brent R. P., Orrick W. P., Osborn J., Zimmermann P.** Maximal determinants and saturated D-optimal designs of orders 19 and 37. arXiv preprint arXiv:1112.4160 [math.CO], 2011. http://arxiv.org/abs/1112.4160 (дата обращения: 09.04.2020).
24. **Orrick W.** The maximal {–1, 1}-determinant of order 15. *Metrika*, 2005, vol. 62, pp. 195–219.
25. **Cohn J. H. E.** A D-optimal design of order 102. *Discrete Math.*, 1992, vol. 102, pp. 61–65.
26. **Fletcher R. J., Seberry J.** New D-optimal designs of order 110. *Australas. J. Combin.*, 2001, vol. 23, pp. 214–225.
27. **Djokovic D. Z.** Some new D-optimal designs. *Australas. J. Combin.*, 1997, vol. 15, pp. 221–231.
28. **Djokovic D. Z., Kotsireas I. S.** New results on D-optimal designs. *J. Combin. Designs*, 2012, vol. 20, pp. 278–289.
29. **Sloane N. J. A.** The on-line encyclopedia of integer sequences. Published electronically: Sequences A003432/M0720, A003433/M1291, A051752, A051753, and A188895. http://oeis.org/ (дата обращения: 19.03.2020).
30. **Orrick Will, and Solomon Bruce.** The Hadamard maximal determinant problem. http://www.indiana.edu/~maxdet/ (дата обращения: 10.03.2020).
31. **Балонин Н. А., Сергеев М. Б.** Как гипотезе Адамара помочь стать теоремой. Ч. 1. *Информационно-управляющие системы*, 2018, № 6, с. 2–13. doi:10.31799/1684-8853-2018-6-2-13
32. **Балонин Н. А., Сергеев М. Б.** Как гипотезе Адамара помочь стать теоремой. Ч. 2. *Информационно-управляющие системы*, 2019, № 1, с. 2–10. doi:10.31799/1684-8853-2019-1-2-10
33. **Balonin N., Sergeev M.** Quasi-orthogonal local maximum determinant matrices. *Applied Mathematical Sciences*, 2015, vol. 9, no. 8, pp. 285–293. doi:10.12988/ams.2015.4111000
34. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея. *Информационно-управляющие системы*, 2015, № 3, с. 2–17. doi:10.15217/issn1684-8853.2015.3.2
35. **Балонин Н. А., Сергеев М. Б.** Расширение гипотезы Райзера на двуциклические структуры и разрешимость матриц Адамара орнаментом в виде бицикла с двойной каймой. *Информационно-управляющие системы*, 2017, № 1, с. 2–10. doi:10.15217/issn1684-8853.2017.1.2
36. **Farmakis N., Kounias S.** The excess of Hadamard matrices and optimal designs. *Discrete Math.*, 1987, vol. 67, pp. 165–176.
37. **Rokicki T.** New records for maximal determinants, based on pairs of circulant matrices. http://tomas.rokicki.com/newrec.html (дата обращения: 10.03.2020).
38. **Балонин Н. А., Сергеев М. Б., Востриков А. А.** Простые числа Ферма и гипотеза о матрицах максимума детерминанта. *Информационно-управляющие системы*, 2020, № 2, с. 2–9. doi:10.31799/1684-8853-2020-2-2-9

UDC 519.614
doi:10.31799/1684-8853-2020-6-2-11

Circles on lattices, and maximum determinant matrices

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
M. B. Sergeev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277
J. Seberry[b], Dr. Sc., Tech., Honorary Professor, orcid.org/0000-0002-9558-4293
O. I. Sinitsyna[a], Post-Graduate Student, orcid.org/0000-0002-2819-4682
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[b]Department of Computing and Information Techology, University of Wollongong, NSW 2522, Australia

Introduction: The Hadamard conjecture about the existence of maximum determinant matrices in all orders multiple of 4 is closely related to Gauss's problem about the number of points with integer coordinates (Z3 lattice points) on a spheroid, cone, paraboloid or parabola. The location of these points dictates the number and types of extreme matrices. **Purpose:** Finding out how Gaussian points on sections of solids of revolution are related to the number and types of maximum determinant matrices with a fixed structure for odd orders. Specifying a precise upper bound of maximum determinant values for edged two-circulant matrices and the orders on which they prevail over simpler cyclic structures. **Results:** A newly proposed formula refines the overly optimistic Elich – Wojtas' upper bound for the case of matrices with a fixed structure. Fermat numbers have a special role for orders of $4t + 1$, and Barba numbers affect the formation of classes of maximum determinant matrices which occupy the areas of orders $4t + 3$, successively replacing each other. For a two-circulant structure with an edge, the maximum order of an optimal symmetric solution is estimated as 67. It is proved that the determinant of edged block matrices is superior to the determinants of circulant matrices everywhere except for a special order 39. **Practical relevance:** Maximum (for a fixed structure) determinant matrices related to lattice points have a direct practical significance for noise-resistant coding, compression and masking of video data.

Keywords — Gaussian points, Gaussian problem, paraboloid on a lattice, orthogonal matrices, Hadamard matrices, maximum determinant matrices, two-circulant edged matrices.

For citation: Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices, and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2020-6-2-11

References

1. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9
2. Barba G. Intorno al teorema di Hadamard sui determinanti a valore massimo. *Giorn. Mat. Battaglini*, 1933, vol. 71, pp. 70–86 (In Italian).
3. Hadamard J. Resolution d'une question relative aux determinants. *Bulletin des Sciences Mathematiques*, 1893, no. 17, pp. 240–246 (In French).
4. Seberry J., Yamada M. *Hadamard matrices, sequences, and block designs*. In: *Contemporary Design Theory: A Collection of Surveys*. J. H. Dinitz and D. R. Stinson, eds. John Wiley and Sons, Inc., 1992. Pp. 431–560.
5. Seberry J., Yamada M. *Hadamard matrices constructed using number theory and algebra*. John Wiley (to appear).
6. Horadam K. J. Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
7. Wang R. *Introduction to orthogonal transforms with applications in data processing and analysis*. Cambridge University Press, 2010. 504 p.
8. Ahmed N., Rao R. *Orthogonal transforms for digital signal processing*. Springer-Verlag, Berlin-Heidelberg-New York, 1975. 263 p.
9. Ehlich H. Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, vol. 83, pp. 123–132 (In German).
10. Ehlich H. Determinantenabschätzungen für binäre Matrizen mit N≡3 mod 4. *Mathematische Zeitschrift*, 1964, vol. 84, pp. 438–447 (In German).
11. Wojtas M. On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloquium Mathematicum*, 1964, vol. 12, pp. 73–83. doi:10.4064/cm-12-1-73-83
12. Yang C. H. On designs of maximal (+1, –1)-matrices of order n≡2 (mod 4). *Math. Comp.*, 1968, vol. 22, pp. 174–180.
13. Yang C. H. On designs of maximal (+1, –1)-matrices of order n≡2 (mod 4). II. *Math. Comp.*, 1969, vol. 23, pp. 201–205.
14. Brenner J. The Hadamard maximum determinant problem. *The American Mathematical Monthly*, 1972, vol. 79, no. 6, pp. 626–630.
15. Yang C. H. Maximal binary matrices and sum of two squares. *Math. Comp.*, 1976, vol. 30, pp. 148–153.
16. Chadjipantelis Th., Kounias S. Supplementary difference sets and D-optimal designs for n≡2 mod 4. *Discrete Math.*, 1985, vol. 57, pp. 211–216.
17. Cohn J. H. E. On determinants with elements ±1. II. *Bull. London Math. Soc.*, 1989, vol. 21, pp. 36–42. doi.org/10.1112/blms/21.1.36
18. Djokovic D. Z. On maximal (1, –1)-matrices of order 2n, n odd. *Radovi Matematicki*, 1991, vol. 7, pp. 371–378.
19. Brent R. P., Osborn J. H. On minors of maximal determinant matrices. arXiv preprint arXiv:1208.3819 [math.CO], 2012. Available at: http://arxiv.org/abs/1208.3819 (accessed 9 April 2020).
20. Chadjipantelis Th., Kounias S., Moyssiadis C. Construction of D-optimal designs for n≡2 mod 4 using block-circulant matrices. *J. Combin. Theory Ser. A*, 1985, vol. 40, pp. 125–135.
21. Kharaghani H. A construction of D-optimal designs for N = 2 mod 4. *J. Combin. Theory Ser. A*, 1987, vol. 46, pp. 156–158.
22. Chadjipantelis Th., Kounias S., Moyssiadis C. The maximum determinant of 21 × 21 (+1, –1)-matrices and D-optimal designs. *J. Statist. Plann. Inference*, 1987, vol. 16, pp. 167–178.
23. Brent R. P., Orrick W. P., Osborn J., Zimmermann P. Maximal determinants and saturated D-optimal designs of orders 19 and 37. arXiv preprint arXiv: 1112.4160 [math.CO], 2011. Available at: http://arxiv.org/abs/1112.4160 (accessed 9 April 2020).
24. Orrick W. The maximal {–1, 1}-determinant of order 15. *Metrika*, 2005, vol. 62, pp. 195–219.
25. Cohn J. H. E. A D-optimal design of order 102. *Discrete Math.*, 1992, vol. 102, pp. 61–65.
26. Fletcher R. J., Seberry J. New D-optimal designs of order 110. *Australas. J. Combin.*, 2001, vol. 23, pp. 214–225.
27. Djokovic D. Z. Some new D-optimal designs. *Australas. J. Combin.*, 1997, vol. 15, pp. 221–231.
28. Djokovic D. Z., Kotsireas I. S. New results on D-optimal designs. *J. Combin. Designs*, 2012, vol. 20, pp. 278–289.
29. Sloane N. J. A. *The on-line encyclopedia of integer sequences*. Published electronically: Sequences A003432/M0720,

A003433/M1291, A051752, A051753, and A188895. Available at: http://oeis.org/ (accessed 19 March 2020).

30. Orrick Will, and Solomon Bruce. *The Hadamard maximal determinant problem*. Available at: http://www.indiana.edu/~maxdet/ (accessed 10 March 2020).
31. Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 6, pp. 2–13 (In Russian). doi:10.31799/1684-8853-2018-6-2-13
32. Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 2. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 1, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2019-1-2-10
33. Balonin N., Sergeev M. Quasi-orthogonal local maximum determinant matrices. *Applied Mathematical Sciences*, 2015, vol. 9, no. 8, pp. 285–293. doi:10.12988/ams.2015.4111000
34. Balonin N. A., Djokovic D. Z. Symmetry of two-circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 2–17 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
35. Balonin N. A., Sergeev M. B. Ryser’s conjecture expansion for bicirculant structures and Hadamard matrix resolvability by double-border bicycle ornament. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 1, pp. 2–10 (In Russian). doi:10.15217/issn1684-8853.2017.1.2
36. Farmakis N., Kounias S. The excess of Hadamard matrices and optimal designs. *Discrete Math.*, 1987, vol. 67, pp. 165–176.
37. Rokicki T. *New records for maximal determinants, based on pairs of circulant matrices*. Available at: http://tomas.rokicki.com/newrec.html (accessed 10 March 2020).
38. Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 2, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2020-2-2-9

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org

UDC 004.89
doi:10.31799/1684-8853-2020-6-12-20

Interpretation of a trained neural network based on genetic algorithms

Pimenov V. I.[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0002-7228-3009, v_pim@mail.ru*
Pimenov I. V.[b], *PhD, Tech., Associate Professor, orcid.org/0000-0002-1954-6463*
[a]*Saint-Petersburg State University of Industrial Technologies and Design, 18, B. Morskaya St., 191186, Saint-Petersburg, Russian Federation*
[b]*Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya St., 198035, Saint-Petersburg, Russian Federation*

Introduction: *Artificial intelligence development strategy involves the use of deep machine learning algorithms in order to solve various problems. Neural network models trained on specific data sets are difficult to interpret, which is due to the "black box" approach when knowledge is formed as a set of interneuronal connection weights.* ***Purpose:*** *Development of a discrete knowledge model which explicitly represents information processing patterns encoded by connections between neurons.* ***Methods:*** *Adaptive quantization of a feature space using a genetic algorithm, and construction of a discrete model for a multidimensional OLAP cube with binary measures.* ***Results:*** *A genetic algorithm extracts a discrete knowledge carrier from a trained neural network. An individual's chromosome encodes a combination of values of all quantization levels for the measurable object properties. The head gene group defines the feature space structure, while the other genes are responsible for setting up the quantization of a multidimensional space, where each gene is responsible for one quantization threshold for a given variable. A discrete model of a multidimensional OLAP cube with binary measures explicitly represents the relationships between combinations of object feature values and classes.* ***Practical relevance:*** *For neural network prediction models based on a training sample, genetic algorithms make it possible to find the effective value of the feature space volume for the combinations of input feature values not represented in the training sample whose volume is usually limited. The proposed discrete model builds unique images of each class based on rectangular maps which use a mesh structure of gradations. The maps reflect the most significant integral indicators of classes that determine the location and size of a class in a multidimensional space. Based on a convolution of the constructed class images, a complete system of production decision rules is recorded for the preset feature gradations.*

Keywords *— classification, deep machine learning, neural network, genetic algorithm, multidimensional OLAP cube, decision rule, semantic interpretation, visualization of classes.*

For citation: Pimenov V. I., Pimenov I. V. Interpretation of a trained neural network based on genetic algorithms. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 12–20. doi:10.31799/1684-8853-2020-6-12-20

Introduction

It is known, that the up-to-date artificial intelligence research and technology uses deep machine learning algorithms, which improves quality of modern business processes in the areas of logistics management, optimize supply planning, financial operations, production processes, predict risks, increase customer satisfaction, diagnose diseases, selects dosages of drugs and solve other narrow classification problems, as well as the creation of a strong artificial intelligence, universal in application to various tasks [1–7].

But, the deep neural network models, which trained on specific data sets, are difficult to interpret for both human mind and machine algorithms. Also, the creation of a strong artificial intelligence, which capable of adapting and interacting with the external environment is an actual complex scientific challenge [8, 9].

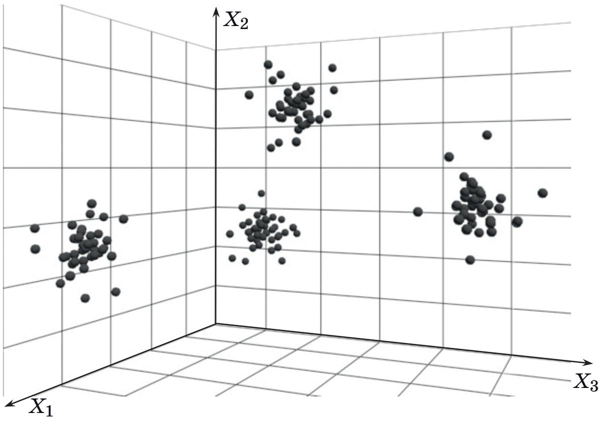
The difficulty of verbalizing the output of deep learning and clearly clarification of the obtained result (i. e. why the model made those or another decisions) is associated with the using of the "black box" model [10], in which in the process of training neural network, the "knowledge" is formed from the sets of links weight between the neighbor neurons. Herewith, visualization and synthesis of new solutions can be carried out using generative adversarial networks [11, 12]. In this case, one network generates artificially created examples of complex objects, and the other network evaluates their reality based on a training set, which allows performing creative tasks, generating variants and prototypes of multidimensional objects.

The creation of a universal algorithm for strong artificial intelligence can be based on the method of complex use of multidimensional data analysis, aimed at transforming a multidimensional feature space into a finite set of classes, and then building a basic discrete code that stores information in a compressed form about a set of features characteristic of a given class. This discrete form of knowledge, not only provides the ability to interpret themselves by the various methods, e. g., mathematical production rules, but also allows to made cognitive visualization of multidimensional classes using descriptive (explanatory) variables.

Neural network as a discretization model of the signs space

Classifying neural network uses object data at the training stage $\omega_i, i = \overline{1, n},$ which can be aggregated from different sources, e. g. the Internet, or can be inclusions of a variety of sensors in a process control loop or some technical object. The geometric paradigm of machine learning uses an attributive description of objects of the training sample and their representation by the points in a multidimensional coordinate system. Using conversion of nominal and ordinal variables to a binary type is applied we are providing a numerical representation of qualitative properties.

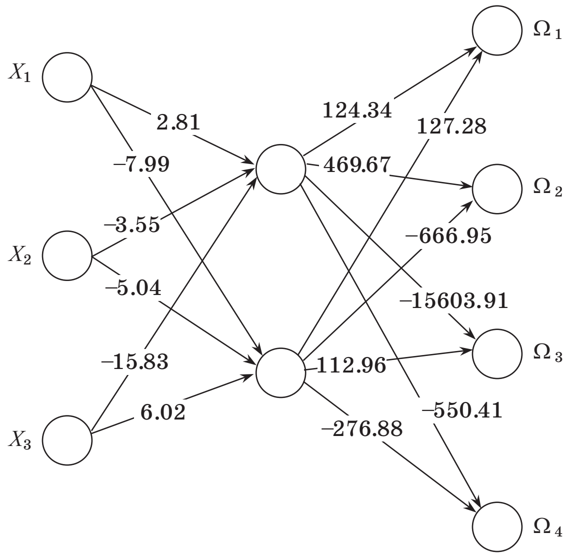
Descriptive signs $\{X_j | j = \overline{1, N}\},$ entered to the input layer of the neural network, characterize the properties of objects of the training sample. The classifying output attribute indicates the belonging of objects ω_i to the one of the class sets $\Omega_m,\ m = \overline{1, M}.$ Having an adequate set of signs **X**, it is possible to form an individual space, in which the objects of the training sample are separated by non-intersecting class hulls (Fig. 1).



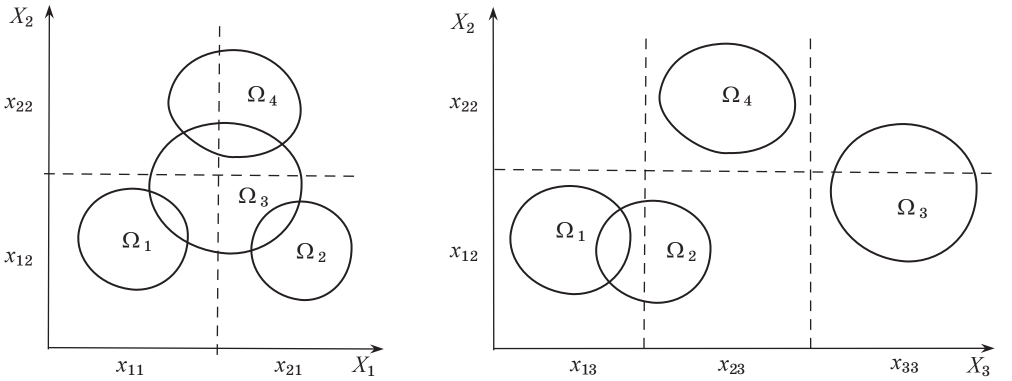
■ ***Fig. 1.*** Training set objects in a multidimensional space

By the classification process, the neural network transforms a continuous signs space into a discrete set of classes. So, trained on data corresponding to Fig. 1, a three-layer (one input and output layer, one middle layer) neural network transform a combination of the values of three signs into one of four specified classes. The model defined by a set of weighting coefficients shown in Fig. 2. This is uses the activation function likes $f(S) = \dfrac{1}{1+e^{-S}},$ where S is the signal on the input layer.

For the clearly interpret the constructed neural network, the information processing should be presented explicitly as connections between combinations of values of N signs X_j and classes Ω_m. Such a view can be attracted using a discrete model of a



■ ***Fig. 2.*** Structure and weight coefficients of the classifying neural network



■ ***Fig. 3.*** Separation of cluster shells in the X_1–X_2 and X_2–X_3 subspaces multidimensional OLAP (online analytical processing) cube with binary measures (cell values) [13].

The key step in this case, is the quantization of the multidimensional space into the minimum allowable number of cells that preserve the separating power of the original dictionary of signs **X**. Accordingly, for each signs X_j the minimum number of thresholds t_j, is set, at which the distinguishability of classes not violated (Fig. 3).

The number of thresholds t_j is determined by the number of class pairs separable by the X_j signs. If several pairs of classes have a common gap, then one threshold is used.

Method of neural network interpretation

A discrete carrier of knowledge should be built in the form of a binary decision matrix [14] or a multidimensional OLAP cube with binary measures and measurement labels, which are gradations of signs values.

The number of signs gradations and the location of the thresholds are determined in the process of adaptive quantization of the signs space using a genetic algorithm.

The creations of the intervals of changes in the initial signs X_j within the specified classes Ω_m, is performed by independently changing the value of X_j at the input of the neural network. Herewith, we using the set of average values for the remaining sign, when the m-th output neuron is triggered.

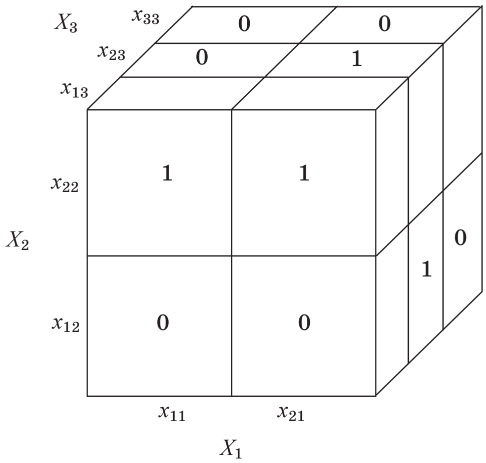
If an object of the m-th class has a binary signs (attribute) X_j, or the values of the quantitative signs X_j belong to the interval $(d_{(i-1)\,j},\, d_{ij})$, then the gradations of the signs value x_{ij} for the class Ω_m in the cells of the OLAP cube take single values

$$x_{ij}(m) = \\ = \begin{cases} 1,\ \exists\omega \in \Omega_m,\ x_j \in (d_{(i-1)j},\, d_{ij}),\ m = \overline{1,\, M},\ i = \overline{1,\, t_j}; \\ 0,\ \text{otherwise}, \end{cases}$$

where t_j — the number of gradations of the sign X_j (so-called, the nominal values).

The subcube of the discretized multidimensional space for class Ω_4 is shown in Fig. 4.

In such a discrete classifying space, the values of signs are set in the form of single elements of the OLAP cube and threshold levels. By this way, it is provided an easy semantic interpretation of the decision rule, based on the trained neural network.



■ ***Fig. 4.*** Subcube Ω_4 of a discretized multidimensional space

Interpreting an OLAP cube with binary measures, based on a system of mathematical production (decision) rules of the form

$$\text{“if } \bigwedge_{j=1}^{N} (x_j \in (d_{(i-1)j},\, d_{ij})_m), \text{ then } \omega \in \Omega_m\text{”},\ m = \overline{1,\, M},$$

which use gradations $(d_{(i-1)j},\, d_{ij})_m$ values of signs x_j, $j = \overline{1,\, N}$, for each class Ω_m.

The object signs values points to the cells in the OLAP cube. During the recognition process, occurs element-by-element conjunction (logical AND) of cells, resulting to distinguish the single cell, corresponding to the class code. The space of “own” gradations point out to the found object.

After the coding process in a discretized multidimensional signs space, the images of the classes are rendered using rectangular maps, that use a mesh structure of gradations. On the basis of the such constructed maps (with the gradations sets of signs) we can create a complete system of mathematical production rules.

Genetic model for optimizing discretized feature signs

To describe the discretization algorithm and the choice of the signs space, we use genetic methods concepts, used for the solving common optimization tasks [15–18].

Individual objects in a population represent a discretized multidimensional space $X_1 \times X_2 \times \ldots \times X_N$ using phenotype — a set of combinations of levels of signs of the working vocabulary $\mathbf{X}_w$, $\mathbf{X}_w = \{X_j \,|\, j = \overline{1,\, N_w}\}$, containing a list of measurable properties of objects.

The match function (so-called, fitness-function) of an individual objects determined by its separating ability — the proportion of combinations of levels of signs, indicating that the object ω belongs to the one of the pairwise disjoint classes Ω_m, $\Omega_m \subset \mathbf{\Omega}$, $\mathbf{\Omega} = \Omega_1 \cup \Omega_2 \cup \ldots \cup \Omega_M$.

At the level of the heritable structures, information about space is determined by the genotype —

a set of genes of a given individual objects, aggregated in a chromosome series. An individual objects in a population can be represented by a genotype or a single chromosome, when the genotype consists of one chromosome. The coding system for heritable information is a genetic code.

We use a kind of genetic-like algorithm that represents chromosomes using bit strings. Only one gene in a chromosome corresponds to each level of quantization of a signs in a phenotype. A gene is a fixed length bit string containing the value of this level. Thus, a combination of values of all quantization levels for measurable properties of an object is encrypted in the chromosome of an individual.

Improving the quality of the individual's matching function is associated with minimizing the volume of the signs space

$$V(N_w, t_j) = \prod_{j=1}^{N_w} t_j \to \min$$

providing $I(\mathbf{X}_w) = 1$, ensure error-free division of the sample into M classes in the discretized space of the working vocabulary, and natural limits $x_j \in [x_{j\,\min}, x_{j\,\max}]$, where $j = \overline{1, N_w}$, $N_w = |\mathbf{X}_w|$. Thus, for choosing the best individual, we should reduce both the number of object signs and the number of their gradations t_j, which makes it possible to increase the extrapolating power of the classifying rule [19].

For these conditions, the length of the chromosome depends on the unknown number of gradations of the signs.

Therefore, the size of the chromosome is fixed by specifying for each signs the minimum number of thresholds, which makes it possible to separate all completely separable classes for which the intervals of change in the values of the signs do not intersect.

Chromosome G consists of two gene groups: $G = \{g_x, g_d\}$.

Gene groups g_x contains single-bit genes bit(x_j), indicating the occurrence of a signs X_{ij} in optimizing space $\mathbf{X}_w$:

$$g_x = \{\mathrm{bit}(x_1), \ldots, \mathrm{bit}(x_j), \ldots, \mathrm{bit}(x_N)\}.$$

Gene groups g_d combines genes that in binary format represent quantization threshold values d_j sign X_j, $i = \overline{1, p_j}$, $p_j = t_j - 1$, where t_j — minimum number of sign quantization levels:

$$g_d = \{\mathrm{bin}(d_{11}), \ldots, \mathrm{bin}(d_{ij}), \ldots, \mathrm{bin}(d_{pN\,N})\}.$$

Number of bits to represent the threshold gene bit string

$$K_j = \log_2\left(\frac{x_{j\max} - x_{j\min}}{\delta_j} + 1\right),$$

where δ_j — accuracy of representation of sign X_j.

Structure of chromosomal thread **Ch**

$$\underbrace{1001101101}_{N\ positions}\ \underbrace{\underbrace{00101011}_{K_1\ positions}\ldots\underbrace{10100010}_{K_1\ positions}}_{p_1}\ldots\ \underbrace{\underbrace{0110}_{K_j\ positions}\ \ldots\ \underbrace{1011}_{K_j\ positions}}_{p_j}\ \ldots\underbrace{\underbrace{01100010}_{K_N\ positions}\ldots\underbrace{10001011}_{K_N\ positions}}_{p_N}.$$

The head gene group determines the structure of the signs space, the rest of the genes are responsible for setting the quantization of the multidimensional space, where each gene is responsible for one quantization threshold for a given variable.

The values of the quantization thresholds are determined by the genes of the found individual

$$d_{ij} = \frac{\mathrm{bin}(d_{ij})}{2^{K_j} - 1}(X_{j\max} - X_{j\min}) + X_{j\min}.$$

Therms "individual" means the value of the chromosome vector belonging to the range of permissible values, $Ch \in \mathbf{Ch}_{permissible}$:

$$\mathbf{Ch}_{permissible} = \{Ch | I(\mathbf{X}_w) = I(\mathbf{X})\},$$

where $I(\mathbf{X}_w)$ — separating power of the signs system $\mathbf{X}_w$, $\mathbf{X}_w \subset \mathbf{X}$, which is defined as the number of class pairs completely separable by a given system to the total number of class pairs $M(M-1)/2$.

The work of the genetic algorithm is generally described as follows [16, 18].

1. Initialization. An initial population is randomly generated from N_I binary chromosomes.
2. Computation of the match function and assessment of the fitness of chromosomes in the population.
3. Selection of parents for crossing (performed using a selection operator).
4. Execution of the operator of crossing.
5. Mutation of offspring (descendant) chromosomes.
6. Formation of a new population by selecting the best individuals in a generation.
7. Switch to the next generation of parents and descendants by repeating steps 2–6 until the stop rule is met.

This algorithm implements adaptive quantization of the signs space. The solution of this algorithm is the discrete neural chromosome code. It describes the space of signs of the minimum volume, while maintaining the separating power of the trained neural network.

Individuals of the initial population contain randomly filled threshold genes, they limited by the values of signs, and the chromosome vector Ch belongs to the range of permissible values.

The algorithm has the following parameters:

— size of population of individuals N_I;

— number of pairs selected for reproduction;

— mutation probability P_{mut};

— crossing probability P_{cross}.

For each population, we determine the number of mutating chromosomes, the number of pairs of crossing chromosomes, a given level of convergence of the algorithm ε.

Probability of selection of an individual for reproduction

$$P_i = \frac{f_i}{\sum_{i=1}^{N} f_i},$$

where i — individual number; $f_i = V(N) - V(N_w)$, $i = \overline{1,\, N_I}$ — individuals match function.

Probability of using the crossing operator $P_{cross} = 0.9...1$. We use some elite individuals in the crossing procedure with quantity $N_e = (1 - P_{cross})N_I$. In conditions when $P_{cross} < 1$ the best individuals of the current population moves into the population without any changes.

In relation to our task, the crossing operator must ensure the process of study of the set of signs for which the head gene group is responsible, and the set of thresholds, encoded by the corresponding genes. Parent-encodings transfer genetic material to new descendant-encodings. To reproduce them, we use a two-parent crossover, which exchanges parts of the bit string of genes at break points.

Reproduction of parent individuals with chromosomes Ch^l and Ch^k looks as follows

$$b^l_{N-1}\ldots b^l_r\ldots b^l_2 b^l_1 b^l_0 \;\; b^l_{K_1-1}\ldots b^l_r\ldots b^l_2 b^l_1 b^l_0 \;\ldots\; b^l_{K_j-1}\ldots b^l_r\ldots b^l_2 b^l_1 b^l_0 \;\ldots\; b^l_{K_N-1}\ldots b^l_r\ldots b^l_2 b^l_1 b^l_0$$

$$+$$

$$b^k_{N-1}\ldots b^k_r\ldots b^k_2 b^k_1 b^k_0 \;\; b^k_{K_1-1}\ldots b^k_r\ldots b^k_2 b^k_1 b^k_0 \;\ldots\; b^k_{K_j-1}\ldots b^k_r\ldots b^k_2 b^k_1 b^k_0 \;\ldots\; b^k_{K_N-1}\ldots b^k_r\ldots b^k_2 b^k_1 b^k_0$$

$$\downarrow$$

$$b^k_{N-1}\ldots b^k_{p+1} b^l_p\ldots b^l_1 b^l_0 \;\; b^k_{K_1-1}\ldots b^k_{p+1} b^l_p\ldots b^l_1 b^l_0 \;\ldots\; b^k_{K_j-1}\ldots b^k_{p+1} b^l_p\ldots b^l_1 b^l_0 \;\ldots\; b^k_{K_N-1}\ldots b^k_{p+1} b^l_p\ldots b^l_1 b^l_0$$

and

$$b^l_{N-1}\ldots b^l_{p+1} b^k_p\ldots b^k_1 b^k_0 \;\; b^l_{K_1-1}\ldots b^l_{p+1} b^k_p\ldots b^k_1 b^k_0 \;\ldots\; b^l_{K_j-1}\ldots b^l_{p+1} b^k_p\ldots b^k_1 b^k_0 \;\ldots\; b^l_{K_N-1}\ldots b^l_{p+1} b^k_p\ldots b^k_1 b^k_0,$$

where the p-th bits of genes act as the breaking point, $b_p = \text{random}(0, K-1)$, K — number of gene encoding bits.

When exchanging pieces of parental-encodings, the existing fragments of alleles will be redistributed among the genes of the descendant-encodings while preserving their loci.

To enforce the genetic variability of alleles, we use the mutation operator, which leads to the appearance of new alleles from fragments that were not previously contained in the parental genes.

Chromosomes descendants are exposed with random changes with probability P_{mut} (0.001...0.01). The number of changes made to the chromosome is defined as follows

$$K_{mut} = \beta \cdot \text{random}(1, K),$$

where K — size of the chromosomes, $K = N + \sum_{j=1}^{N} p_j K_j$; β — mutation power coefficient, $\beta \in [0; 1]$.

Mutation stands in inverting the binary sequence, which position in the chromosome determined strongly randomly:

$$b_{r_n} := \left| b_{r_n} - 1 \right|,$$

where $r_n = \text{random}(1, K)$, $n = \overline{1, K_{mut}}$.

During the simulation modeling we configure the power of mutation because this is one of the most important properties of the search algorithm.

The rule (decision) for stopping the genetic algorithm is to achieve a given level of convergence $f_{i\ \max} - f_{i\ \min} < \varepsilon$ — determining such power of match of individuals in the population, at which their further improvement does not occur.

The result of the genetic algorithm computation leads to the choice of an individual from a finite population that has the maximum value of the matching function f_i.

The genetic algorithm makes it possible to find the effective value of the volume of the signs space $V(\mathbf{X}_w)$, for neural network prediction models based on a "black box" type and trained on a samples. This type of space provides us with a prediction for those combinations of values of input signs that were not represented in the training sample, which is usually strongly limited by size.

Visualization and interpretation of classes

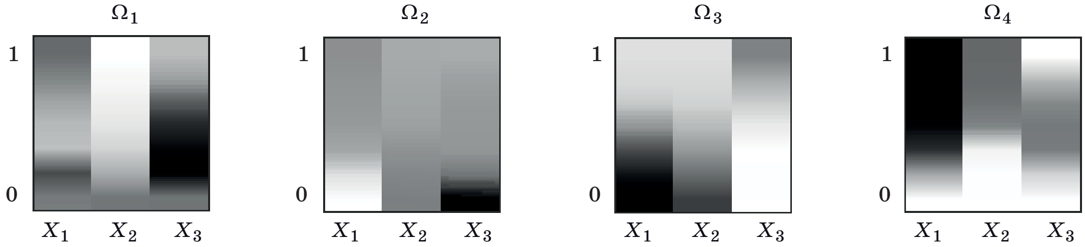
Strictly accurate mapping of characteristic and general signs of object classes is a challenged issue when visualizing solutions in multidimensional continuous spaces [20–27]. It is required to analyze $N_w(N_w - 1)/2$ slices to unambiguously identify a class based on an OLAP cube.

Since the information about the combinations of gradations of the initial features for any class is contained in a compressed form, in a trained discrete knowledge carrier with binary measures, we can use a rectangular map to form a unique image of each class, which use a mesh structure of gradations.

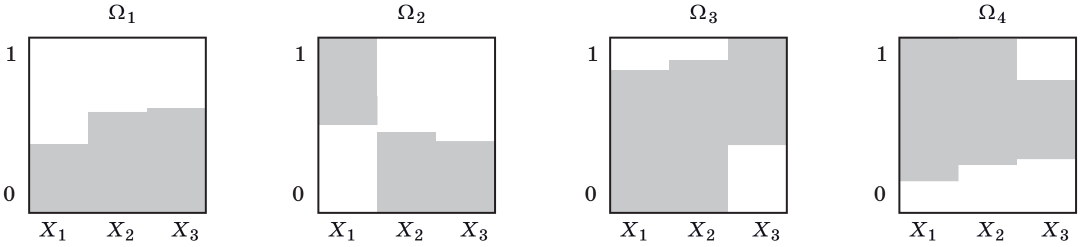
After coding in a discretized multidimensional space of signs, the images of classes reflects the most significant, integral indicators of classes and smooth out the insignificant signs, which observed on image maps, representing the ranges of changes in signs and signals at the input of the output neuron with varying signs.

The class image for each output neuron of the trained network can be mapped in grayscale (Fig. 5) or in 3D. We used the values of linear combinations of inputs coming to the output neurons and the values of the corresponding activation functions. This mappings introduce the proportion of the training sample, objects belonging to the given m-th class (also known as estimation of the "conditional probability" of the class), in which the j-th characteristic lands into the i-th interval.

We use a bar chart (Fig. 6) to assess the interval of changes in a signs within the considered m-th class. The columns formed by independently vary-



■ ***Fig. 5.*** Class images representing signals at the input of the output neuron when signs vary



■ ***Fig. 6.*** Class images representing ranges of signs variation in a normalized space ing the value of each initial signs at the input of the multilayer neural network (with the set average values of the remaining signs), when the m-th output neuron is triggered. Input indicators (showings) are normalized linearly to the interval 0...1.

Variation ranges of signs at the input of a trained neural network, at which triggered a neuron of the class Ω_1 is: $X_1 = 0...0.4$, $X_2 = 0...0.57$, $X_3 = 0.0...0.59$.

Triggered a neuron of the class Ω_2 is: $X_1 = 0.50...1.0$, $X_2 = 0...0.47$, $X_3 = 0.0...0.43$.

Triggered a neuron of the class Ω_3 is: $X_1 = 0...0.86$, $X_2 = 0...0.89$, $X_3 = 0.63...1.0$.

Triggered a neuron of the class Ω_4 is: $X_1 = 0.17...1.0$, $X_2 = 0.30...1.0$, $X_3 = 0.31...0.77$.

As it was disclaimed early, after the coding process, we get the images of the classes that rendered using rectangular maps with a mesh structure of gradations. Note, that as we says early, this algorithms use a discretized multidimensional signs space. The maximum number of gradations T set to according to the most featured (discrete) sign (Fig. 7). We set "free" gradations, if the signs values in the class correspond to the highest gradation — that's need for the maximum conformity of the images and a bar chart with continuous ranges of signs values.

With the using of the cognitive images, we can clearly determine the classes that have the minimum and maximum values of integral indicators (showings) — the sum of gradations for all binarized signs $Sg(\Omega_m)$ and the spread of signs values $R(\Omega_m)$

$$\Omega'_m = \arg \operatorname*{extr}_{\Omega_m \in \mathbf{\Omega}} Sg(\Omega_m);$$

$$\Omega''_m = \arg \operatorname*{extr}_{\Omega_m \in \mathbf{\Omega}} R(\Omega_m).$$

Small signs values have a class Ω_1, $Sg(\Omega_1) = 1 \cdot (1 + 1 + 1) = 3$. Classes with the highest characteristic values follows Ω_3 и Ω_4: $Sg(\Omega_3) = 1 \cdot (1 + 1) + 2 \cdot (1 + 1) + 3 \cdot (1 + 1 + 1) = 15$, $Sg(\Omega_4) = 1 \cdot 1 + 2 \cdot (1 + 1 + 1) + 3 \cdot (1 + 1) = 14$. Class Ω_1 has the smallest spread of signs values $R(\Omega_1) = \sqrt{1\cdot 1\cdot 1} = 1$. Class with the highest spread of values Ω_3, $R(\Omega_3) = \sqrt{3\cdot 3\cdot 1} = 3$.

Using the convolution of the constructed images (of classes) for the set gradations of signs, we can produce a complete system of mathematical production rules as follows:

$$\text{"if } (X_1 \in X_{12}) \text{ and } (X_2 \in X_{21}) \text{ and } (X_3 \in X_{32}),$$
$$\text{then } \omega \in \Omega_2\text{".}$$

Thus, by varying the values of the descriptive variables at the input of the trained neural network, we used the genetic algorithm to extract a discrete carrier of knowledge. This makes it possible to clearly interpret the classes using cognitive maps and produce a full system of mathematical production rules.

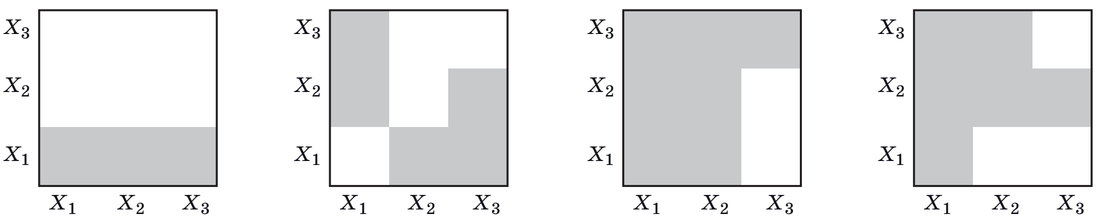
Conclusion

As it was noted before, the complex challenge of verbalizing the output of deep learning and clearly clarification of the obtained result (i. e. why the model made those or another decisions) related to the using of the common "black box" model — by the learning process, the "knowledge" organized in form of set of the weight coefficients of the links between neurons.

Neural network converts a continuous feature space into a discrete set of classes by the process of classification. For the interpretation of the trained neural network decision, the data can be represented in an obvious form as mappings between combinations of values N of signs of X_j and the classes Ω_m, using discrete model of a multidimensional OLAP cube with binary measures.

The discrete knowledge model is formed by the process of adaptive quantization of a signs space using a common genetic algorithm. Individual's chromosome encrypts a set of values of all quantization levels for measurable properties of an object. The head gene group define the structure of the signs space, the remaining genes responsible for configuring the quantization of the multidimensional space, where each gene in charge for one quantization threshold of a given variable.

The genetic algorithm makes it possible to find the effective value of the volume of the signs space $V(\mathbf{X}_w)$, for neural network prediction models based on a "black box" type and trained on a samples. This type of space provides us with a prediction for those



■ ***Fig. 7.*** Images of classes after encoding in a discretized multidimensional signs space combinations of values of input signs that were not represented in the training sample, which is usually strongly limited by size.

Using the proposed discrete model we can form a unique images of each class based on rectangular maps with cellular structure of gradations. Maps reflect the most significant, integral indicators (showings) of classes, which strongly determine the location and size of a class in multivariate space.

Thus, we can form a complete set of mathematical production decision rules, both in the process of directly interpreting a discrete model of a multidimensional OLAP cube, and on the convolution of class images for signs gradations.

References

1. Martin Prause, Jurgen Weigand. Market model benchmark suite for machine learning techniques. *IEEE Computational Intelligence Magazine*, 2018, vol. 13, iss. 4, pp. 14–24. doi:10.1109/MCI.2018.2866726
2. Mehdi Mohammadi, Ala Al-Fuqaha, Sameh Sorour, Mohsen Guizani. Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, iss. 4, pp. 2923–2960. doi:10.1109/COMST.2018.2844341
3. Sung-Yu Tsai, Jen-Yuan Changc. Parametric study and design of deep learning on leveling system for smart manufacturing. *IEEE International Conference on Smart Manufacturing, Industrial & Logistics Engineering (SMILE)*, February 8–9, 2018, pp. 48–52. doi:10.1109/SMILE.2018.8353980
4. Abdelrahman M. Shaker, Manal Tantawi, Howida A. Shedeed, Mohamed F. Tolba. Generalization of convolutional neural networks for ECG classification using generative adversarial networks. *IEEE Access*, 2020, vol. 8, pp. 35592–35605. doi:10.1109/ACCESS.2020.2974712
5. Gusev A. V. Prospects for neural networks and deep machine learning in creating health solutions. *Information Technologies for the Physician*, 2017, no. 3, pp. 92–105 (In Russian).
6. Sozykin A. V. An overview of methods for deep learning in neural networks. *Bulletin of the South Ural State University. Series: Computational Mathematics and Software Engineering*, 2017, vol. 6, no. 3. pp. 28–59 (In Russian). doi:10.14529/cmse170303
7. Guangxin Lou, Hongzhen Shi. Face image recognition based on convolutional neural network. *IEEE Transactions on Neural Networks and Learning Systems*, 2020, vol. 31, iss. 1, pp. 117–124. doi:10.23919/JCC.2020.02.010
8. Rex Martinez. Artificial intelligence: Distinguishing between types & definitions. *Nevada Law Journal*, 2019, vol. 19:3, pp. 1015–1042.
9. Lukyanova O. A., Nikitin O. Y. Selfish general intelligence. *Cloud of Science*, 2019, vol. 6, no. 3. Available at: http://cloudofscience.ru (accessed 10 May 2020) (In Russian).
10. Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson. Output reachable set estimation and verification for multilayer neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2018, vol. 25, iss. 11, pp. 5777–5783. doi:10.1109/TNNLS.2018.2808470
11. Na Li, Ziqiang Zheng, Shaoyong Zhang, Zhibin Yu, Haiyong Zheng, Bing Zheng. The Synthesis of unpaired underwater images using a multistyle generative adversarial network. *IEEE Access*, 2018, vol. 6, pp. 54241–54257. doi:10.1109/ACCESS.2018.2870854
12. Mu Zhou, Yixin Lin, Nan Zhao, Qing Jiang, Xiaolong Yang, Zengshan Tian. Indoor WLAN intelligent target intrusion sensing using ray-aided generative adversarial network. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2020, vol. 4, iss. 1, pp. 61–73. doi:10.1109/TETCI.2019.2892748
13. Davardoost F., Babazadeh Sangar A., Majidzadeh K. Extracting OLAP cubes from document-oriented NoSQL database based on parallel similarity algorithms. *Canadian Journal of Electrical and Computer Engineering*, 2020, vol. 43, no. 2, pp. 111–118. doi:10.1109/CJECE.2019.2953049
14. Pimenov V. I., Voronov M. V., Pimenov I. V. The cognitive visualization of classifying rules extracted from data based on binary solver matrix model. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2019-6-2-11
15. Andras Takacs, Manuel Toledano-Ayala, Aurelio Dominguez-Gonzalez, Alberto Pastrana-Palma, Dimas Talavera Velazquez, Juan Manuel Ramos, Edgar Alejandro Rivas-Araiza. Descriptor generation and optimization for a specific outdoor environment. *IEEE Access*, 2020, vol. 8, pp. 2169–3536. doi:10.1109/ACCESS.2020.2975474
16. Abinet Tesfaye Eseye, Matti Lehtonen, Toni Tukia, Semen Uimonen, R. John Millar. Machine learning based integrated feature selection approach for improved electricity demand forecasting in decentralized energy systems. *IEEE Access*, 2019, vol. 7, pp. 91463–91475. doi:10.1109/ACCESS.2019.2924685
17. Hossam M. J. Mustafa, Masri Ayob, Mohd Zakree Ahmad Nazri, Graham Kendall. An improved adaptive memetic differential evolution optimization algorithms for data clustering problems. *PLOS ONE*, 2019, May 28, pp. 1–28. doi:10.1371/journal.pone.0216906
18. Ryadchikov I. V., Gusev A. A., Sechenev S. I., Nikulchev E. V. Genetic algorithm for search PID-controllers parameters of a walking robot stabilization. *Transactions of NNSTU n.a. R. E. Alekseev*, 2019, no. 1(124), pp. 58–65 (In Russian).
19. Jochen L. Cremer, Ioannis Konstantelos, Goran Strbac. From optimization-based machine learning to interpretable security rules for operation. *IEEE*

Transactions on Power Systems, 2019, vol. 34, iss. 5, pp. 3826–3836. doi:10.1109/TPWRS.2019.2911598

20. Yunhai Wang, Kang Feng, Xiaowei Chu, Jian Zhang, Chi-Wing Fu, Michael Sedlmair, Xiaohui Yu, Baoquan Chen. A perception-driven approach to supervised dimensionality reduction for visualization. *IEEE Transactions on Visualization and Computer Graphics*, 2018, vol. 24, iss. 5, pp. 1828–1840. doi:10.1109/TVCG.2017.2701829
21. Yunhai Wang, Xin Chen, Tong Ge, Chen Bao, Michael Sedlmair, Chi-Wing Fu, Oliver Deussen, Baoquan Chen. Optimizing color assignment for perception of class separability in multiclass scatterplots. *IEEE Transactions on Visualization and Computer Graphics*, 2019, vol. 25, iss. 1, pp. 820–829. doi:10.1109/TVCG.2018.2864912
22. Ruizhen Hu, Tingkai Sha, Oliver Van Kaick, Oliver Deussen, Hui Huang. Data sampling in multi-view and multi-class scatterplots via set cover optimization. *IEEE Transactions on Visualization and Computer Graphics*, 2020, vol. 26, iss. 1, pp. 739–748. doi:10.1109/TVCG.2019.2934799
23. Zhe Wang, Nivan Ferreira, Youhao Wei, Aarthy Sankari Bhaskar, Carlos Scheidegger. Gaussian cubes: real-time modeling for visual exploration of large multidimensional datasets. *IEEE Transactions on Visualization and Computer Graphics*, 2017, vol. 23, iss. 1, pp. 681–690. doi:10.1109/TVCG.2016.2598694
24. Min Lu, Shuaiqi Wang, Joel Lanir, Noa Fish, Yang Yue, Daniel Cohen-Or, Hui Huang. Winglets: visualizing association with uncertainty in multi-class scatterplots. *IEEE Transactions on Visualization and Computer Graphics*, 2020, vol. 26, iss. 1, pp. 770–779. doi:10.1109/TVCG.2019.2934811
25. Ying Zhao, Feng Luo, Minghui Chen, Yingchao Wang, Jiazhi Xia, Fangfang Zhou, Yunhai Wang, Yi Chen, Wei Chen. Evaluating multi-dimensional visualizations for understanding fuzzy clusters. *IEEE Transactions on Visualization and Computer Graphics*, 2019, vol. 25, iss. 1, pp. 12–21. doi:10.1109/TVCG.2018.2865020
26. Lazutin O. G. Technique of communicating information about the technical state of space vehicles using data compression algorithms and cognitive graphical representation. *Proceedings of the Mozhaisky Military Space Academy*, 2016, vol. 650, pp. 11–17 (In Russian).
27. Emelyanova Ju. G., Fralenko V. P. Methods of cognitive-graphical representation of information for effective monitoring of complex technical systems. *Program Systems: Theory and Applications*, 2018, vol. 9, no. 4(39), pp. 117–158 (In Russian). doi:https://doi.org/10.25209/2079-3316-2018-9-4-117-158

УДК 004.89
doi:10.31799/1684-8853-2020-6-12-20

Интерпретация обученной нейронной сети на основе генетических алгоритмов

В. И. Пименов[а], доктор техн. наук, профессор, orcid.org/0000-0002-7228-3009, v_pim@mail.ru
И. В. Пименов[б], канд. техн. наук, доцент, orcid.org/0000-0002-1954-6463
[а]Санкт-Петербургский государственный университет промышленных технологий и дизайна, Б. Морская ул., 18, Санкт-Петербург, 191186, РФ
[б]Государственный университет морского и речного флота им. адмирала С. О. Макарова, Двинская ул., 5/7, Санкт-Петербург, 198035, РФ

Введение: стратегия развития искусственного интеллекта предполагает применение алгоритмов глубокого машинного обучения для решения задач различного класса. Обученные на конкретных наборах данных нейросетевые модели трудно интерпретировать, что связано с подходом «черного ящика», когда знания формируются как набор весовых коэффициентов связей между нейронами. **Цель:** разработка дискретной модели знаний, представляющей в явной форме закономерности обработки информации, закодированные связями между нейронами. **Методы:** адаптивное квантование признакового пространства с помощью генетического алгоритма и построение дискретной модели многомерного OLAP-куба с бинарными мерами. **Результаты:** генетический алгоритм выполняет извлечение из обученной нейронной сети дискретного носителя знаний. В хромосоме особи зашифровывается комбинация значений всех уровней квантования для измеримых свойств объекта. Головная генная группа определяет структуру признакового пространства, остальные гены отвечают за настройку квантования многомерного пространства, где каждый ген отвечает за один порог квантования заданной переменной. Дискретная модель многомерного OLAP-куба с бинарными мерами представляет в явной форме связи между комбинациями значений признаков объектов и классами. **Практическая значимость:** для нейросетевых моделей предсказания, построенных по обучающей выборке, генетический алгоритм дает возможность найти эффективное значение объема пространства признаков для тех комбинаций значений входных признаков, которые не были представлены в обучающей выборке, обычно ограниченной в объеме. С помощью предложенной дискретной модели формируются уникальные образы каждого класса на основе прямоугольных карт, в которых используется ячеистая структура градаций. Карты отражают наиболее существенные, интегральные показатели классов, которые определяют местоположение и размер класса в многомерном пространстве. На основе свертки построенных образов классов для установленных градаций признаков записывается полная система продукционных решающих правил.

Ключевые слова — классификация, глубокое машинное обучение, нейронная сеть, генетический алгоритм, многомерный OLAP-куб, решающее правило, семантическая интерпретация, визуализация классов.

Для цитирования: Pimenov V. I., Pimenov I. V. Interpretation of a trained neural network based on genetic algorithms. *Информационно-управляющие системы*, 2020, № 6, с. 12–20. doi:10.31799/1684-8853-2020-6-12-20

For citation: Pimenov V. I., Pimenov I. V. Interpretation of a trained neural network based on genetic algorithms. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 12–20. doi:10.31799/1684-8853-2020-6-12-20

UDC 003.26
doi:10.31799/1684-8853-2020-6-21-29

A novel method for development of post-quantum digital signature schemes

D. N. Moldovyan[a], *PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru*
A. A. Moldovyan[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-5480-6016*
N. A. Moldovyan[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0002-4483-5048*
[a]*Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation*

Introduction: *Development of post-quantum digital signature standards represents a current challenge in the area of cryptography. Recently, the signature schemes based on the hidden discrete logarithm problem had been proposed. Further development of this approach represents significant practical interest, since it provides possibility of designing practical signature schemes possessing small size of public key and signature.* ***Purpose:*** *Development of the method for designing post-quantum signature schemes and new forms of the hidden discrete logarithm problem, corresponding to the method.* ***Results:*** *A method for designing post-quantum signature schemes is proposed. The method consists in setting the dependence of the public-key elements on masking multipliers that eliminates the periodicity connected with the value of discrete logarithm of periodic functions constructed on the base of the public parameters of the cryptoscheme. Two novel forms for defining the hidden discrete logarithm problem in finite associative algebras are proposed. The first (second) form has allowed to use the finite commutative (non-commutative) algebra as algebraic support of the developed signature schemes.* ***Practical relevance:*** *Due to significantly smaller size of public key and signature and approximately equal performance in comparison with the known analogues, the developed signature algorithms represent interest as candidates for practical post-quantum cryptoschemes.*

Keywords *— post-quantum cryptoschemes, computer security, digital signature, discrete logarithm problem, finite commutative groups, non-commutative associative algebras.*

For citation: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29

Introduction

Since the mid-1990s, cryptographic algorithms and protocols have been widely used to solve information security problems [1, 2]. Public key cryptosystems are of particular importance in electronic document management technologies [3, 4]. The most widely used public-key algorithms and protocols are based on the computational complexity of the factorization problem (FP) [5, 6] and the discrete logarithm problem (DLP) [7, 8]. However, progress in the theory and technology of quantum computing suggests that in the fairly near future, a quantum computer will be available and can be used to solve FP and DLP.

Since polynomial algorithms for solving FP and DLP are known for a quantum computer [9, 10], the implementation of this forecast will make it insecure to use public-key cryptographic algorithms and protocols based on FP and DLP [11, 12]. This raises the problem of the development of post-quantum public-key cryptoschemes based on the computationally hard problems of other types

Over the past decade the global cryptographic community has been actively developing the post-quantum public-key cryptosystems [13, 14]. As a basic primitive, a number of studies consider the problem of searching for a conjugating element in non-commutative braid groups [15, 16]. This problem has been studied in numerous papers and fundamental difficulties associated with the development of practical post-quantum cryptosystems based on it have been identified [17].

At the end of 2016, the National Institute of Standards and Technology of the United States (NIST) announced a program on the developing a project for post-quantum standards for public key-agreement and electronic digital signature (EDS) schemes by 2024, within which a world competition was announced [18] for the development of cryptoschemes of the said type. Out of 69 proposed candidates for post-quantum cryptographic schemes 17 public key-agreement schemes and 9 EDS schemes were selected for participation in the second stage of the competition [19, 20].

The main drawback of the proposed post-quantum EDS schemes is the large total size of the public key and digital signature. A promising approach to the development of post-quantum EDS schemes, based on the use of the computational complexity of the hidden discrete logarithm problem (HDLP), remained out of the attention of the participants of the NIST competition.

The known forms of HDLP are given in finite non-commutative associative algebras (FNAA) given over a ground finite field $GF(p)$ [21]. The extention of the class of algebraic carriers of HDLP and the development of new forms of HDLP is of significant interest for the development of practical post-quantum cryptosystems [22, 23]. In this paper, we propose two new forms of setting the HDLP, which differ in that they use a commutative group with μ-dimensional cyclicity ($\mu \geq 2$) as a hidden group. One of the forms is set in a commutative group with multidimensional cyclicity [24, 25] (a finite group whose basis includes two or more group elements that have the same order is called group with multidimensional cyclicity). The second form of HDLP is set in the FNAAs, various types of which are considered in the works [22, 26, 27].

The hidden discrete logarithm problem as base primitive of post-qantum cryptoschemes

The well-known polynomial algorithms for solving DLP and FP on a quantum computer are based on reducing each of them to the problem of finding the period length of a periodic function constructed using public parameters of the cryptosystem. When solving DLP, a periodic function is constructed that contains a period that depends on the value of the logarithm. A sufficiently fast calculation of the period length is provided by the fact that for functions that take values in a finite cyclic group, a quantum computer effectively performs a discrete Fourier transform [28, 29].

The DLP is formulated as follows: given a public key Y', which is an element of a cyclic group of prime order and calculated by the formula $Y' = G^x$, where G is the group generator, x is the private key ($x < q$). You need to calculate the value of x from the known G and Y'. For a classical computer, polynomial algorithms for finding discrete logarithm are unknown in the multiplicative group of the field $GF(p)$ and in the groups of elliptic curve points.

Calculating the value of x on a quantum computer consists in constructing a periodic function $f(i, j) = (Y')^i G^j$ from two variables i and j, taking integer values, which contains periods of the following lengths: $(0, q)$, $(q, 0)$, (q, q) and $(-1, x)$. The first three values are related to the order value of the cyclic group, and the last one is related to the discrete logarithm:

$$(Y')^i G^j = (Y')^{i-1} G^{j+x} \Rightarrow f(i, j) = f(i-1, j+x).$$

For a function $f(i, j)$, that takes values in an explicitly defined cyclic group of any nature, the quantum algorithm finds the period of length $(-1, x)$ in polynomial time.

For the construction of HDLP-based EDS schemes, FNAAs of various dimensions m are used as algebraic carriers (usually $m = 4$ and $m = 6$), which contain a sufficiently large number of isomorphic cyclic groups [22, 26, 27]. A secret cyclic group of prime order is selected to generate the public key. Some group element $\mathbf{N}$ that is different from the unit element of the group is selected, and the element $\mathbf{N}^x$ is calculated, two secret masking operations ψ_1 and ψ_2 are formed, each of which is mutually commutative with the base exponentiation operation, and two elements of the algebra are calculated $\mathbf{Y}$ and $\mathbf{Z}$: $\mathbf{Y} = \psi_1(\mathbf{N}^x)$, $\mathbf{Z} = \psi_2(\mathbf{N})$, belonging to two other cyclic groups of algebra. To ensure the correct operation of the EDS scheme coordinated operations ψ_1 and ψ_2 are selected. Thanks to this feature the function $f(i, j) = \mathbf{Y}^i\mathbf{Z}^j$ is periodic and contains a period of length $(-1, x)$, however, it takes arbitrary values in the FNAA used as an algebraic carrier, i. e. the values are not restricted to some fixed finite group. This determines the security of the HDLP-based EDS schemes to attacks using known algorithms for finding the length of a period on a quantum computer.

The design criterion of the post-quantum signature schemes, described in [22, 26], this is the following: *setting periodic functions constructed on the base of public parameters of the EDS scheme should lead to the fact that these functions with a fairly low probability take values that belong to any one fixed group*.

However, quantum algorithms for finding the period length for a broader class of periodic functions may appear in the future. The possibility of maintaining high security of EDS schemes with the appearance of such quantum algorithms can potentially be provided by specifying the computational impossibility of constructing periodic functions with a period length that depends on the value of the discrete logarithm.

Thus, the wording of the strengthened criterion of providing resistance to quantum attacks can be shown as follows: *cryptoscheme should be constructed in such a way that the construction of periodic functions based on public parameters of the cryptoscheme should cause these functions will be free from period, depending on the value of discrete logarithm, although there will be periods whose lengths are set by prime order of hidden cyclic group*.

In this paper, finite associative algebras containing finite commutative groups with multidimensional cyclicity are used as the algebraic carrier of the cryptosystem to develop EDS schemes that satisfy the enhanced criterion. Groups of this type include groups whose basis includes two or more elements, the order of each of which is equal to the same value [24, 25].

Setting the finite commutative groups with multidimensional cyclicity

Suppose a finite m-dimensional vector space is set over the field $GF(p)$, where p is a prime. Usually, a vector is presented as an ordered set of coordinates $\mathbf{A} = (a_0, a_1, ..., a_{m-1})$ or as a sum of one-component vectors $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + ... + a_{m-1}\mathbf{e}_{m-1}$, where $\mathbf{e}_i$ ($i = 0, 1, ..., m - 1$) are basis vectors. Defining additionally the operation of vector multiplication ($\circ$) possessing the property of the two-sided distributivity relatively the addition operation of vectors, one gets the finite m-dimensional algebra.

The multiplication operation of the vectors $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is set with the following formula: $\mathbf{A} \circ \mathbf{B} = \sum_{j=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j$, where each pair of the basis vectors is replaced by the one-component vector indicated in the intersection of the i-th row and j-th column of the so called basis vector multiplication table.

Setting the hidden discrete logarithm problem in a finite commutative group with multi-dimensional cyclicity

In commutative groups, the method of masking the base cyclic group, in which it is supposed to perform the exponentiation operation, should be focused on the implementation of the mentioned earlier strengthened criterion of providing resistance to quantum attacks. Indeed, in commutative groups, it is not possible to perform the automorphic and homomorphic mapping operations used in FNAA [22, 26], therefore we need to offer a new method of masking.

The hidden logarithm problem is set at the stage of forming a public key, which includes the selection of a secret base cyclic group by generating a random vector $\mathbf{G}$, considered as the generator of this group. After performing the basic exponentiation operation (which makes the main contribution to the security of the cryptosystem), we get the vector $\mathbf{G}^x$, which together with the vector $\mathbf{G}$ is subject to masking, which will give two vectors that are elements of the public key. The proposed masking method uses the idea of multiplying vectors $\mathbf{G}$ and $\mathbf{G}^x$ by randomly selected vectors $\mathbf{U}$ and $\mathbf{D}$ of order q, which belong to different cyclic groups other than the base one, and such that the triple of vectors ($\mathbf{G}$, $\mathbf{U}$, $\mathbf{D}$) forms the basis of a primary subgroup of order q^3. Thus, one gets the public key as a pair of vectors $\mathbf{Y} = \mathbf{G}^x \circ \mathbf{U}$ and $\mathbf{Z} = \mathbf{G} \circ \mathbf{D}$.

It is easy to see that a pair of vectors ($\mathbf{Y}$, $\mathbf{Z}$) forms the basis of a primitive subgroup of order q^2, therefore, the periodic function $f_r(i, j) = \mathbf{Y}^i \circ \mathbf{Z}^j$ takes on all q^2 values of the specified primitive subgroup with a period of length (q, q). This function also contains length periods (q, 0) and (0, q) and is free of explicit periodicity, the length of which depends on the discrete logarithm. The latter is determined by the masking influence of multipliers $\mathbf{U}$ and $\mathbf{D}$.

The principal point is that these multipliers have the same order as the vectors $\mathbf{G}$ and $\mathbf{G}^x$. If this condition is violated, for example, if the multipliers are vectors $\mathbf{U}$ and $\mathbf{D}$ have a prime order $r \neq q$, then their masking influence can be completely eliminated by exponentiating the vectors $\mathbf{Y}$ and $\mathbf{Z}$ to the degree r and defining the periodic function $f_r(i, j) = \mathbf{Y}^{ri} \circ \mathbf{Z}^{rj}$, that contains a period of the length (–1, x): $\mathbf{Y}^{r(i-1)} \circ \mathbf{Z}^{r(j+x)} = \mathbf{Y}^{ri}\mathbf{Z}^{-rx} \circ \mathbf{Z}^{r(j+x)} = \mathbf{Y}^{ri} \circ \mathbf{Z}^{rj}$.

Masking multipliers contribute to the digital-signature verification equation. This effect must be compensated for ensuring the correct functioning of the EDS algorithm. The latter is supposed to be provided by calculating an additional element of the digital signature in the form of a vector $\mathbf{S}$, that is included as a multiplier in the verification equation.

If there is a multiplier that is a signature element, it is possible to easily forge the signature using the vector $\mathbf{S}$ as a fitting parameter, the random value of which is calculated as unknown in the EDS authentication equation. To prevent this method of the EDS forgery, the idea of doubling the verification equation can be used, i. e. instead of one verification equation, two similar equations will be used, which use different pairs of the values ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$) and the same signature in the form of triple of the values (e, s, $\mathbf{S}$). In this case forgery of the signature for the first and second verification equations will lead to different values of the fitting parameter $\mathbf{S}$, which makes the specified method of EDS forgery computationally infeasible.

The proposed mechanism for doubling the verification ratio assumes the calculation of the public key in the form of two pairs of vectors ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$), which ensure that the verification equation will be satisfied for the same signature value. This is ensured by the fact that the first and second elements in each of the pairs ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$) are connected by the same value of the discrete logarithm x and the same values of masking factors $\mathbf{U}$ and $\mathbf{D}$. Independence of the pairs ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$) is ensured by the fact that independent base cyclic groups are used for calculating the said pairs, and random multipliers $\mathbf{U}$ and $\mathbf{D}$ are chosen such that the four vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form the basis of a primary group of order q^4. The latter provides the implementation of the enhanced post-quantum resistance criterion (the computational infeasibility of constructing a periodic function with a period defined by the value x).

In the versions of the HDLP specified in the FNAAs and used for designing EDS schemes in [22, 26], the calculation of the value of the discrete logarithm x in the secret base cyclic group can be performed using the baby-step-giant-step algorithm. This is directly connected with the possibility of constructing a periodic function containing a period whose length depends on the x. This circumstance makes it necessary to use a hidden cyclic group of prime order, the size of which is 256 bits while providing 128-bit security.

The proposed version of the HDLP, set in finite commutative groups, implements the enhanced criterion for ensuring post-quantum resistance, i. e. periodic functions constructed on the base of public parameters of the EDS scheme are free from the periodicity associated with the value of the discrete logarithm x. The calculation of the value x by the baby-step-giant-step method and other known analogues can not be carried out due to the fact that the calculation of the value of x can not be separated from the calculation of at least one of the secret vectors **G**, **U**, and **D**. Thus, you can expect that a 128-bit value q is sufficient to provide 128-bit security. However, due to the fact that the new version of the HDLP is little studied, we will consider the implementation of the HDLP-based EDS algorithm for the case of using 256-bit values q.

Digital signature scheme using calculations in a finite group with four-dimensional cyclicity

As the algebraic carrier of the EDS scheme, we will use a four-dimensional finite commutative algebra defined over a field $GF(p)$, where $p = 2q + 1$ with the 256-bit prime q, when using BVMT shown as Table 1, where the structural coefficient $\lambda = 4$.

The unit of this associative algebra is the vector (0, 0, 1, 0), and its multiplicative group has a four-dimensional (two-dimensional) cyclicity at the value λ equal to the quadratic residue (non-residue) in the field $GF(p)$. In the case of forming a group with two-dimensional cyclicity, its basis includes two vectors, each of which has the order $p^2 - 1$, and the group order is equal to $(p^2 - 1)^2$. When developing the EDS scheme in this section, we will consider the case of four-dimensional cyclicity, when the basis of the multiplicative group includes four vectors, each of which has an order $p - 1$, and the group order is equal to $(p - 1)^4$.

■ ***Table 1.*** Setting the multiplication operation in finite algebra multiplicative group of which possesses multi-dimensional cyclicity

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$

The public key is generated as follows:

1. Generate random vectors **G**, **Q**, **U** and **D**, the order of each of which is equal to the same prime number q.

2. Generate random natural number $x < q$ and calculate vectors $\mathbf{Y}_1 = \mathbf{G}^x \circ \mathbf{U}$ and $\mathbf{Y}_2 = \mathbf{Q}^x \circ \mathbf{U}$.

3. Calculate vectors $\mathbf{Z}_1 = \mathbf{G} \circ \mathbf{D}$ and $\mathbf{Z}_2 = \mathbf{Q} \circ \mathbf{D}$.

The public key is two pairs of vectors $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$. The private key of the owner of this public key is a set of the following values x, **G**, **Q**, **U**, and **D**, knowledge of which is required for calculation of the signature. The probability that the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form the basis of a primary group of order q^4, practically is equal to 1. Indeed, the said four vectors are random because they depend on random vectors **G**, **Q**, **U** and **D**. The probability that the products of all possible degrees of the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ and $\mathbf{Z}_2$ form a primary subgroup of order q^3 or q^2 is negligible and equal to $\approx q^{-1}$ (if the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ are independent and form a primary group of order q^3, then the probability that a random vector $\mathbf{Z}_2$ is contained in this primary group is equal to the ratio of its order to the number of all vectors of order q, which are contained in the multiplicative group of the four-dimensional algebra under consideration (accounting for case when the vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ form a primary group of order q^2 makes a small adjustment to the value q^{-1}).

Let an electronic document M be given, to which a digital signature of owner of the public key $(\mathbf{Y}_1, \mathbf{Z}_1)$ and $(\mathbf{Y}_2, \mathbf{Z}_2)$ is to be created. To do this, the following procedure is performed, which uses some pre-defined secure 256-bit hash function f_h (the algorithm for calculating a hash value is part of the EDS scheme under consideration):

1. Generate three random natural numbers $k < q$, $t < q$ and $u < q$.

2. Calculate two vector fixators $\mathbf{V}_1$ and $\mathbf{V}_2$ using the following formulas:

$\mathbf{V}_1 = \mathbf{G}^k \circ \mathbf{D}^t \circ \mathbf{U}^u$ and $\mathbf{V}_2 = \mathbf{Q}^k \circ \mathbf{D}^t \circ \mathbf{U}^u$.

3. Calculate the value $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (the first signature element).

4. Calculate the value $s = k - ex \bmod q$ (the second signature element).

5. Calculate the vector $\mathbf{S} = \mathbf{D}^{t-e} \circ \mathbf{U}^{u-s}$ (the third signature element).

At the output of this algorithm we get the digital signature $(e, s, \mathbf{S})$. The main contribution to the computational complexity W of the algorithm is made by exponentiation operations in the four-dimensional algebra under consideration, i. e. one can accept the estimate $W = 8$ exponentiation operations.

Algorithm for verifying triples of values (e, s, $\mathbf{S}$) as a genuine signature to a document M includes the following steps:

1. Using the public key, namely, two pairs of the vectors ($\mathbf{Y}_1$, $\mathbf{Z}_1$) and ($\mathbf{Y}_2$, $\mathbf{Z}_2$), calculate the vectors $\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s$ and $\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s$.

2. Attaching vectors $\tilde{\mathbf{V}}_1$ and $\tilde{\mathbf{V}}_2$ to the document M, calculate the hash-function value $\tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right)$.

3. Check whether the equality is valid $\tilde{e} = e$. If it is true, the EDS (e, s, $\mathbf{S}$) is accepted as a genuine one. If $\tilde{e} \neq e$, the signature (e, s, $\mathbf{S}$) is rejected.

The computational complexity of the EDS authentication algorithm is equal to $W = 4$ exponentiation operations. Demonstration of the correctness of the considered EDS scheme involves performing a proof that the signature calculated by the owner of the public key successfully passes the signature authentication procedure. Let the signature (e, s, $\mathbf{S}$) be obtained in accordance with the signature generation procedure when using the correct signer's private key. Then, submitting the signature (e, s, $\mathbf{S}$) to the input of the verification procedure, we have the following proof of the correctness of the proposed signature scheme:

$$\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s = \left(\mathbf{G}^x \circ \mathbf{U}\right)^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ (\mathbf{G} \circ \mathbf{D})^s =$$
$$= \mathbf{G}^{xe} \circ \mathbf{U}^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ \mathbf{G}^s \circ \mathbf{D}^s = \mathbf{G}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{G}^s =$$
$$= \mathbf{G}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{G}^{k-xe} = \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{D}^u = \mathbf{V}_1;$$

$$\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s = \left(\mathbf{Q}^x \circ \mathbf{U}\right)^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ (\mathbf{Q} \circ \mathbf{D})^s =$$
$$= \mathbf{Q}^{xe} \circ \mathbf{U}^e \circ \mathbf{U}^{t-e} \circ \mathbf{D}^{u-s} \circ \mathbf{Q}^s \circ \mathbf{D}^s = \mathbf{Q}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{Q}^s =$$
$$= \mathbf{Q}^{xe} \circ \mathbf{U}^t \circ \mathbf{D}^u \circ \mathbf{Q}^{k-xe} = \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{D}^u = \mathbf{V}_2 \Rightarrow$$
$$\Rightarrow \tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = e.$$

The obtained equality $\tilde{e} = e$ means the signature (e, s, $\mathbf{S}$) passes the verification procedure as a genuine one.

Setting the HDLP in non-commutative algebra and the EDS scheme based on it

Used in the previous section mechanism of doubling the signature authentication equation can also be applied to develop the EDS algorithms based on the computational complexity of the HDLP set in FNAAs. Let's consider the implementation of an EDS scheme of this type as a doubling of the cryptosystem described earlier in the paper [26] and using the four-dimensional FNAA as its algebraic carrier, in which the vector multiplication operation is set by Table 2 over the field $GF(p)$. As in the previous signature scheme, we assume $p = 2q + 1$ for a 256-bit prime value q.

■ ***Table 2.*** Setting the multiplication operation in 4-dimensional non-commutative algebra [26] ($\lambda \neq 0$; $\lambda \neq 1$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$

The said four-dimensional FNAA contains a global two-sided unit $\mathbf{E} = ((1 - \lambda)^{-1}, (1 - \lambda)^{-1}, \lambda(\lambda - 1)^{-1}, (\lambda - 1)^{-1})$ and $p(p + 1)(p - 1)^2$ invertible vectors. A sign of the invertibility of a certain vector $\mathbf{A} = (a_0, a_1, a_2, a_3)$ is non-equality $a_0a_1 \neq a_2a_3$. Multiplying a certain vector $\mathbf{X} = (x_0, x_1, x_2, x_3)$ by vectors of the form $\mathbf{D} = (d(1 - \lambda)^{-1}, d(1 - \lambda)^{-1}, d\lambda(\lambda - 1)^{-1}, d(\lambda - 1)^{-1}) = d\mathbf{E}$ is actually a multiplication by a scalar d: $\mathbf{D} \circ \mathbf{X} = d\mathbf{X}$. The latter means that for any value $d \in GF(p)$ the vector $\mathbf{D}$ is permutable with each vector $\mathbf{X}$ in the considered FNAA: $\mathbf{D} \circ \mathbf{X} = \mathbf{X} \circ \mathbf{D}$. Obviously, the equation $\mathbf{D}^i = d^i\mathbf{E}$ holds true. When choosing an integer d, which is a primitive root modulo p, one gets the vector $\mathbf{D}$ that is a generator of a cyclic group $\Gamma_{\mathbf{D}}$ having order equal to $p - 1$.

The maximum order of invertible vectors of the multiplicative group of the considered FNAA is $p^2 - 1$. In this group you can find many different pairs of vectors $\mathbf{G} \notin \Gamma_{\mathbf{D}}$ and $\mathbf{Q} \notin \Gamma_{\mathbf{D}}$ of the order $p - 1$, for which the non-equality $\mathbf{G} \circ \mathbf{Q} \neq \mathbf{Q} \circ \mathbf{G}$ holds true. Each of the pairs of vectors $<\mathbf{G}, \mathbf{D}>$ and $<\mathbf{Q}, \mathbf{D}>$ forms a minimal system of generators (basis) of some commutative group $\Gamma_{<\mathbf{G},\mathbf{D}>}$ and $\Gamma_{<\mathbf{Q},\mathbf{D}>}$, correspondingly, of order $(p - 1)^2$. Intersection of the groups $\Gamma_{<\mathbf{G},\mathbf{D}>}$ and $\Gamma_{<\mathbf{Q},\mathbf{D}>}$ represents the cyclic group $\Gamma_{\mathbf{D}}$. Thus, the four-dimensional algebra under consideration contains a large number of different commutative groups with two-dimensional cyclicity, and the cyclic group $\Gamma_{\mathbf{D}}$ being a subgroup of each of them. This structure of the algebra allows for such modification of the EDS scheme [26], in which a new form of HDLP is specified, which implements an enhanced criterion for ensuring post-quantum security.

This modification is based on the idea of using a commutative group with two-dimensional cyclicity (instead of a cyclic group in the analog [26]) as a hidden group. The proposed version of the EDS scheme is described as follows.

Procedure of generating the public key includes the following steps:

1. Generate random vectors $\mathbf{G} \notin \Gamma_{\mathbf{D}}$ and $\mathbf{B} \in \Gamma_{\mathbf{D}}$, whose order is equal to a prime number q. (These two vectors form the basis $<\mathbf{G}, \mathbf{B}>$ of the group

$\Gamma_{<\mathbf{G},\mathbf{B}>}$ that is commutative, has two-dimensional cyclicity, and has order equal to q^2.)

2. Generate two random numbers r_1 ($r_1 < q$) and r_2 ($r_2 < q$) and calculate the vector $\mathbf{Q} = \mathbf{G}^{r_1} \circ \mathbf{B}^{r_2} \in \Gamma_{<\mathbf{G},\mathbf{B}>}$.

3. Generate two random numbers u_1 ($u_1 < q$) and u_2 ($u_2 < q$) and calculate the vector $\mathbf{U} = \mathbf{G}^{u_1} \circ \mathbf{B}^{u_2} \in \Gamma_{<\mathbf{G},\mathbf{B}>}$.

4. Generate a random natural number x ($x < q$) and two random vectors $\mathbf{J}$ and $\mathbf{H}$ of order $p^2 - 1$, which satisfy the conditions $\mathbf{G} \circ \mathbf{J} \neq \mathbf{J} \circ \mathbf{G}$, $\mathbf{G} \circ \mathbf{H} \neq \mathbf{H} \circ \mathbf{G}$, and $\mathbf{H} \circ \mathbf{J} \neq \mathbf{J} \circ \mathbf{H}$. Then calculate the vectors $\mathbf{Z}_1 = \mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}$, $\mathbf{Y}_1 = \mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}$, $\mathbf{Y}_2 = \mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}$, and $\mathbf{Z}_2 = \mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}$.

The public key is a set of four vectors $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, and $\mathbf{Z}_2$. All other parameters are secret. You can specify the integer number x and vectors $\mathbf{G}$, $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{H}$, $\mathbf{J}$ as private key of the owner of the public key. Calculation of the value x according to the public parameters of the EDS scheme, represents the HDLP, the specific form of which is determined by formulas describing the dependence of the public values $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, and $\mathbf{Z}_2$ on secret vectors $\mathbf{G}$, $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{H}$, $\mathbf{J}$.

Algorithm for creating EDS for an electronic document M:

1. Generate random integers k ($k < q$) and t ($t < q$) and calculate the vectors $\mathbf{V}_1 = \mathbf{J} \circ \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1}$ and $\mathbf{V}_2 = \mathbf{J} \circ \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1}$.

2. Calculate the value $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (the first signature element).

3. Calculate the value $s = k - ex \bmod q$ (the second signature element).

4. Calculate the vector $\mathbf{S} = \mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}$ (the third signature element).

The computational complexity of the signature generation algorithm is equal to $W = 5$ exponentiation operation.

Signature verification algorithm:

1. Calculate the vectors $\mathbf{V}_1' = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s$ and $\mathbf{V}_2' = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s$.

2. Calculate the hash-function value $e' = f_h(M, \mathbf{V}_1', \mathbf{V}_2')$.

3. If $e' = e$ and the vector $\mathbf{S}$ satisfies the invertibility condition, then the signature is accepted as genuine one. Otherwise the signature is rejected as false one.

The computational complexity of the signature verification algorithm is equal to $W = 4$ exponentiation operation.

Correctness proof of the signature scheme is as fallows:

$$\mathbf{V}_1' = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s =$$

$$= \left(\mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}\right)^e \circ \left(\mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}\right) \circ \left(\mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}\right)^s =$$

$$= \mathbf{J} \circ \mathbf{G}^{xe} \circ \mathbf{U}^{t-s} \mathbf{G}^s \circ \mathbf{U}^s \circ \mathbf{H}^{-1} = \mathbf{J} \circ \mathbf{G}^{xe} \circ \mathbf{U}^t \mathbf{G}^{k-ex} \circ \mathbf{H}^{-1} =$$

$$= \mathbf{J} \circ \mathbf{G}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1} = \mathbf{V}_1;$$

$$\mathbf{V}_2' = \mathbf{Z}_2^s \circ \mathbf{S} \circ \mathbf{Y}_2^e =$$

$$= \left(\mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}\right)^s \circ \left(\mathbf{J} \circ \mathbf{U}^{t-s} \circ \mathbf{H}^{-1}\right) \circ \left(\mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}\right)^e =$$

$$= \mathbf{J} \circ \mathbf{Q}^s \circ \mathbf{U}^s \circ \mathbf{U}^{t-s} \circ \mathbf{Q}^{xe} \circ \mathbf{H}^{-1} = \mathbf{J} \circ \mathbf{Q}^{k-xe} \circ \mathbf{U}^t \mathbf{Q}^{ex} \circ \mathbf{H}^{-1} =$$

$$= \mathbf{J} \circ \mathbf{Q}^k \circ \mathbf{U}^t \circ \mathbf{H}^{-1} = \mathbf{V}_2;$$

$$\left\{\mathbf{V}_1' = \mathbf{V}_1; \mathbf{V}_2' = \mathbf{V}_2\right\} \Rightarrow e' = e.$$

The last equality means the correctly computed signature passes the verification procedure as a genuine one.

Discussion

Within the framework of the NIST competition [18], 9 different digital signature schemes are currently being considered as a candidate for the post-quantum EDS standard [20]. The most attractive from the point of view of a compromise between the performance and size of the public key and signature are the following EDS schemes: Falcon [https://falcon-sign.info/], Dilithium [https://pq-crystals.org/dilithium/index.shtml], Rainbow [30], and qTESLA [https://qtesla.org/]. Table 3 shows a rough comparison of the developed EDS schemes with the listed candidates for the post-quantum EDS standard, namely with their versions Falcon-512, Dilithium-1024x768, Rainbow, and qTESLA-p-I, corresponding to the level of 128-bit security. (The relative performance of the proposed signature schemes is estimated under the assumption that multiplication operations in 4-dimensional algebras and in finite ground field $GF(p')$ with 1024-bit characteristic p' have approximately the same computational complexity, when using literature data on the comparative perfor-

■ ***Table 3.*** Comparison with candidates for the post-quantum standard of EDS

Signature scheme	Signature size, byte	Public key size, byte	Rate of signature generation, arb. un.	Rate of signature verification, arb. un.
Falcon-512	657	897	50	25
Dilithium	2044	1184	15	2
Rainbow	64	150 000	–	–
qTESLA-p-I	2592	15 000	20	40
Section 5	192	512	40	80
Section 6	192	512	64	80

mance evaluation of the specified candidates for the post-quantum EDS standard and of the 2048-bit RSA cryptosystem.)

Let's consider the construction of periodic functions based on the public parameters of the proposed EDS schemes. In the case of the signature scheme using computations in the finite commutative group with four-dimensional cyclicity we have the following public parameters $\mathbf{Y}_1 = \mathbf{G}^x \circ \mathbf{U}$, $\mathbf{Y}_2 = \mathbf{Q}^x \circ \mathbf{U}$, $\mathbf{Z}_1 = \mathbf{G} \circ \mathbf{D}$, and $\mathbf{Z}_2 = \mathbf{Q} \circ \mathbf{D}$, where each pair of public key elements depends on some three vectors from the basis <**Q**, **U**, **G**, **D**>, and where each triple of the elements depends on four vectors from the basis. Therefore, periodic functions constructed as products of natural powers of two and three public parameters can only contain periods whose lengths depend on the order of the basis elements, i. e. on the prime value q.

Consider the periodic function $F(i, j, k, h) = \mathbf{Y}_1^i \circ \mathbf{Z}_1^j \circ \mathbf{Y}_2^k \circ \mathbf{Z}_2^h$. Expressing this function from integer variables in terms of the basis of the multiplicative group of the four-dimensional algebra given in Table 3, we obtain: $F(i, j, k, h) = \mathbf{G}^{xi+k} \circ \mathbf{U}^{i+j} \circ \mathbf{Q}^{xj+h} \circ \mathbf{D}^{k+h}$. Let this function have a period $(\delta_i, \delta_j, \delta_k, \delta_h)$. Since all basis vectors are independent, we have the following system of linear congruencies with the unknowns $\delta_i, \delta_j, \delta_k, \delta_h$:

$$\begin{cases} x\delta_i + \delta_k \equiv 0 \bmod q \\ \delta_i + \delta_j \equiv 0 \bmod q \\ x\delta_j + \delta_h \equiv 0 \bmod q \\ \delta_k + \delta_h \equiv 0 \bmod q \end{cases}.$$

The main determinant of this system is different from zero, so there is the single solution $(\delta_i, \delta_j, \delta_k, \delta_h) = (0, 0, 0, 0)$, which means that the function in question contains only periods whose length depends only on the value q.

For the EDS scheme using computations in the four-dimensional FNAA we have the following public parameters $\mathbf{Z}_1 = \mathbf{H} \circ \mathbf{G} \circ \mathbf{U} \circ \mathbf{H}^{-1}$, $\mathbf{Y}_1 = \mathbf{J} \circ \mathbf{G}^x \circ \mathbf{J}^{-1}$, $\mathbf{Y}_2 = \mathbf{H} \circ \mathbf{Q}^x \circ \mathbf{H}^{-1}$, and $\mathbf{Z}_2 = \mathbf{J} \circ \mathbf{Q} \circ \mathbf{U} \circ \mathbf{J}^{-1}$. Consider the periodic function $F_1(i, j) = \mathbf{Y}_1^i \circ \mathbf{Z}_2^j = \mathbf{J} \circ \mathbf{G}^{xi} \circ (\mathbf{Q} \circ \mathbf{U})^j \circ \mathbf{J}^{-1}$. Since the vector **G** and the vector $\mathbf{Q} \circ \mathbf{U}$ are generators of different cyclic groups of the order q, the function F_1 can only contain periods associated with the value q.

The same situation holds for the function $F_2(i, j) = \mathbf{Y}_2^i \circ \mathbf{Z}_1^j = \mathbf{H} \circ \mathbf{Q}^{xi} \circ (\mathbf{G} \circ \mathbf{U})^j \circ \mathbf{H}^{-1}$. Setting other periodic functions based on the public parameters also does not result in functions containing a period that depends on the value x.

Conclusion

This is the first time that a HDLP-based signature using a finite commutative algebra has been constructed. Thus, the proposed signature scheme satisfies the enhanced criteria of post-quantum security. An EDS scheme is also proposed that meets the enhanced post-quantum security criterion and is based on the computational complexity of the HDLP set in the FNAA. The specified criterion is met by using a commutative finite group with two-dimensional cyclicity as a hidden group.

Financial support

This work was supported by the budget theme No. 0060-2019-010.

References

1. *Advances in Cryptology — CRYPT0'95. 15th Annual International Cryptology Conference*, Santa Barbara, California, USA, August 27–31, 1995, Proceedings. Lecture Notes in Computer Science series, Springer, 1995, vol. 963.
2. *Advances in Cryptology — CRYPTO 2019. 39th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings. Lecture Notes in Computer Science series, Springer, Cham, 2019, vol. 11692.
3. *Public Key Cryptography, PKC'98. The First International Workshop on Practice and Theory of Public-Key Cryptography*, Pacifico Yokohama, Japan, February 1998, Proceedings. Lecture Notes in Computer Science series, Springer, 1998, vol. 1431.
4. *Public-Key Cryptography — PKC 2019. 22nd IACR International* Conference *on Practice and Theory of Public-Key Cryptography*, Beijing, China, April 14–17, 2019, Proceedings. Lecture Notes in Computer Science series, Springer, 2019, vol. 11443.
5. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
6. Chiou S. Y. Novel digital signature schemes based on factoring and discrete logarithms. *International Journal of Security and its Applications*, 2016, vol. 10, no. 3, pp. 295–310.
7. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, vol. IT-31, no. 4, pp. 469–472.
8. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
9. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum com-

puter. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.

10. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
11. Yan S. Y. *Quantum Computational Number Theory*. Springer, 2015. 252 p.
12. Yan S. Y. *Quantum Attacks on Public-Key Cryptosystems*. Springer, 2014. 207 p.
13. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018*, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. Lecture Notes in Computer Science series, Springer, 2018, vol. 10786.
14. *Proceedings of the 10th International Workshop on Post-Quantum Cryptography, PQCrypto 2019*, Chongqing, China, May 8–10, 2019. Lecture Notes in Computer Science series, Springer, 2019, vol. 11505.
15. Verma G. K. A proxy blind signature scheme over braid groups. *International Journal of Network Security*, 2009. vol. 9, no. 3, pp. 214–217.
16. Hiranvanichakorn P. Provably authenticated group key agreement based on braid groups – the dynamic case. *International Journal of Network Security*, 2017, vol. 19, no. 4, pp. 517–527.
17. Myasnikov A., Shpilrain V., Ushakov A. *A Practical Attack on a Braid Group Based Cryptographic Protocol*. In: *Advances in Cryptology – CRYPTO'05*. Lecture Notes in Computer Science series, Springer-Verlag, 2005. Vol. 3621. Pp. 86–96.
18. *Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 03 September 2020).
19. *Post-Quantum Cryptography. Round 2 Submissions*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (accessed 03 September 2020).
20. Zimmer D. *NIST Round 2 and Post-Quantum Cryptography — The New Digital Signature Algorithms*. 2019. Available at: https://www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantum-cryptography-the-new-digital-signature-algorithms/ (accessed 03 September 2020).
21. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
22. Moldovyan N. A., Moldovyan A. A. Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS)*, 2019, vol. 12, no. 1, pp. 66–81. doi:10.14529/mmp190106
23. Moldovyan N. A., Moldovyan A. A. New forms of defining the hidden discrete logarithm problem. *SPIIRAS Proceedings*, 2019, vol. 18, no. 2, pp. 504–529. doi:10.15622/sp.18.2.504-529
24. Moldovyan N. A., Moldovyanu P. A. New primitives for digital signature algorithms. *Quasigroups and Related Systems*, 2009, vol. 17, no. 2, pp. 271–282.
25. Moldovyan N. A. Fast signatures based on non-cyclic finite groups. *Quasigroups and Related Systems*, 2010, vol. 18, no. 1, pp. 83–94.
26. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem. *Computer Science Journal of Moldova*, 2018, vol. 26, no. 3(78), pp. 301–313.
27. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions. *Quasigroups and Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.
28. Jozsa R. Quantum algorithms and the fourier transform. *Proc. Roy. Soc. London*, *Ser A*, 1988, vol. 454, pp. 323–337.
29. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 1996, vol. 68, pp. 733–752.
30. Ding J., Schmidt D. Rainbow, a new multivariable polynomial signature scheme. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2005, vol. 3531, pp. 164–175.

УДК 003.26
doi:10.31799/1684-8853-2020-6-21-29

Новый метод построения постквантовых схем цифровой подписи

Д. Н. Молдовян[a], канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru
А. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0001-5480-6016
Н. А. Молдовян[a], доктор техн. наук, главный научный сотрудник, orcid.org/0000-0002-4483-5048
[a]Санкт-Петербургский институт информатики и автоматики РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ

Введение: разработка постквантовых схем цифровой подписи является одним из вызовов в области криптографии. Недавно предложены схемы цифровой подписи, основанные на скрытой задаче дискретного логарифмирования. Развитие этого подхода представляет существенный прикладной интерес, поскольку он позволяет разработать практичные схемы подписи, обладающие малыми размерами открытого ключа и подписи в сравнении с известными аналогами. **Цель:** разработка метода построения постквантовых схем подписи, соответствующих ему новых форм задания скрытой задачи дискретного логарифмирования и схем подписи на его основе. **Результаты:** предложен метод построения постквантовых схем цифровой подписи. Суть метода состоит в задании зависимости элементов открытого ключа от маскирующих множителей, устраняющих периодичность, зависящую от значения дискретного логарифма, в периодических функциях, построенных на основе открытых параметров криптосхемы. На основе метода разработаны две новые формы задания скрытой задачи дискретного логарифмирования в конечных ассоциативных алгебрах. Первая позволила использовать коммутативные алгебры, а вторая — некоммутативные алгебры в качестве алгебраического носителя разработанных схем цифровой подписи. **Практическая значимость:** разработанные алгоритмы цифровой подписи представляют интерес как кандидаты на практичные постквантовые криптосхемы, обладающие существенно меньшим размером открытого ключа и подписи при примерно равной производительности в сравнении с известными аналогами.

Ключевые слова — постквантовые криптосхемы, компьютерная безопасность, электронная цифровая подпись, задача дискретного логарифмирования, конечные коммутативные группы, некоммутативные ассоциативные алгебры.

Для цитирования: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Информационно-управляющие системы*, 2020, № 6, с. 21–29. doi:10.31799/1684-8853-2020-6-21-29

For citation: Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. A novel method for development of post-quantum digital signature schemes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 21–29. doi:10.31799/1684-8853-2020-6-21-29

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other..., используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = –.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Coreldraw (*.cdr); Excel (*.xls); Word (*.docx); Adobe Illustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Правила для авторов».

Контакты

Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru

UDC 621.396
doi:10.31799/1684-8853-2020-6-30-36

Application of permutation frequency modulation signals manipulated with a constant weight code to increase the noise immunity of decameter radio communications

S. V. Dvornikov[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0002-4889-0001, practicdsv@yandex.ru*
A. A. Balykov[b], *Researcher, Post-Graduate Student, orcid.org/0000-0001-9311-1807*
S. S. Dvornikov[b], *PhD, Tech., Head of a Laboratory, orcid.org/0000-0001-7426-6475*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*
[b]*S. M. Budenny Military Academy of Communication, 3, Tikhoretskii Pr., 194064, Saint-Petersburg, Russian Federation*

Introduction: *The operation of radio lines in the decameter range, as a rule, occurs in a complex interference environment, characterized by the presence of fast and slow fading. Therefore, one of the most relevant areas of research in this subject area is the development of new technical solutions aimed at improving the noise immunity of reception.* ***Purpose:*** *Development of signals with permuted frequency modulation that allow detecting single errors at the physical level by selecting combinations of subcarriers of each character in accordance with the alphabet of the code with a constant weight.* ***Results:*** *Theoretical aspects of formation of the permutation signals with frequency modulation, the choice manipulating code to select subcarriers within a signal symbol, presents an analytical approach for the derivation of the generalized expression evaluation of noise immunity of the developed signals of permutation modulation in a channel with variable parameters in incoherent processing, we obtained the estimation of the values of probability of bit error for new signals in comparison with the known results.* ***Practical relevance:*** *The developed signal with permuted frequency modulation is proposed to be used in decameter radio communication systems operating in a narrow frequency band in the ionospheric channel.* ***Discussion:*** *Further research is associated with optimization of decision-making procedures for demodulating the developed signals, as well as the search for effective ways to encode signals with permuted frequency modulation at the physical level, allowing to increase the data transfer rate while maintaining the noise immunity of reception.*

Keywords *— permutation frequency modulation, code manipulation with constant weight, decameter radio communication, noise immunity, probability of bit error, non-coherent signal processing, slow fading.*

For citation: Dvornikov S. V., Balykov A. A., Dvornikov S. S. Application of permutation frequency modulation signals manipulated with a constant weight code to increase the noise immunity of decameter radio communications. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 30–36. doi:10.31799/1684-8853-2020-6-30-36

Introduction

Decameter radio systems operating in the ionospheric channel are characterized by slow fading. These fading are associated with the simultaneous reception of the direct and reflected beam. The main cause of fading is the passage of a reflected or scattered signal along several paths with different delay times [1].

In the case of slow fading, the waveform remains constant, but its power and phase change. This leads to a significant decrease in the quality of reception, although to a lesser extent than as a result of the effects of fast and selective fading, which significantly change the signal shape [2].

In practice, one of the main ways to eliminate intersymbol interference that occurs when radio waves pass in a fading ionospheric channel is to increase the chip duration. But this leads to a significant decrease in the bit rate, therefore, as a solution to this problem, it is proposed to use signals generated on the basis of permutation frequency modulation (PFM) [3].

The PFM methodology and various aspects of its application have been sufficiently studied [4–13]. Including the properties of PFM signals were investigated by Russian scientists [4, 8, 11, 13]. So, in [11], the following features of PFM are highlighted, which made it possible to consider it as a promising direction for radio communication systems in the decameter range:

— each PFM signal symbol has the same energy;

— demodulation of messages is carried out at the stage of detecting signal symbols of the code word;

— the PFM implementation guarantees the same error probability when receiving any codewords from the allowed alphabet.

It is important to note that PFM, with relatively simple signal processing algorithms, provides a sufficiently high transmission rate while maintaining acceptable noise immunity.

Taking these circumstances into account, this article presents the results of a study of the noise immunity of signals developed in [4], with their incoherent processing in a channel with variable parameters. The peculiarity of the developed PFM signals is that in them the choice of the current combination of subcarriers for each symbol is carried out in accordance with the alphabet determined by the code with constant weight, which makes it possible to detect single errors already at the physical level [8].

Theoretical aspects of the formation of signals of permutation frequency modulation for radio communication systems in the decameter range

In general, PFM signals can be viewed as a kind of Multiple Frequency Shift Keying (FM-m), where m is the number of frequency positions for subcarriers.

The synthesis of PFM-m/k signals can be carried out in accordance with the expression

$$s_{\text{PFM-}m/k}(t)=\frac{1}{N}\sum_{i=1}^{m}s_i(t)\otimes\mathbf{A}. \qquad (1)$$

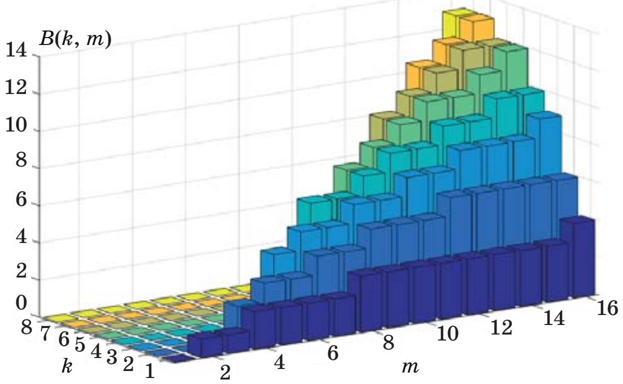
Here $s_i(t)$ are harmonics per m subcarriers within the signal bandwidth; **A** is a vector of dimension m, the elements of which are “0” and “1”, and “1” indicates the active subchannel on the duration of the signal element (the number of units of vector **A** is determined by the value k), the number “0” — on the passive one.

In contrast to multi-position frequency shift keying, in which each signal symbol is determined by the position of only one subcarrier in a given frequency band, in PFM it is formed by choosing a certain combination of several subcarriers, total number k, where $k\in[1;\lfloor m/2\rfloor]$ (here $\lfloor * \rfloor$ is the integer division operation). The use of permutation modulation can significantly expand the alphabet, and thereby increase the transmission rate. So, if the signals of multi-frequency modulation FM-m information bit rate R_b is related to the symbol rate R_s by the following relationship [2]:

$$R_b=R_s\times\lfloor\log_2 m\rfloor, \qquad (2)$$

then for PFM-m/k signals the specified connection will be as follows:

$$R_b=R_s\times\left\lfloor\log_2 C_m^k\right\rfloor=R_s\times\left\lfloor\log_2\frac{m!}{k!(m-k)!}\right\rfloor. \qquad (3)$$



■ ***Fig. 1.*** Dependence of dimension symbol on the number of frequency positions m, for a different number of active subcarriers k

To clarify the essence of this feature, in Fig. 1 is a three-dimensional diagram showing the dependence of the distribution of bits per symbol $B(m)$, on the number of frequency positions m, on the duration of the signal element for a different value of k, which determines the number of involved subcarriers (active subchannels), in accordance with the expression

$$B(m)=\left\lfloor\log_2\frac{m!}{k!(m-k)!}\right\rfloor. \qquad (4)$$

The analysis presented in Fig. 1 of the result shows that in relation to decameter communication channels, for which, as a rule, signal structures with a dimension of more than 16 are not used [14], a significant gain occurs in the case when the parameter k in its value approaches m. It should be borne in mind that an increase in k leads to a significant decrease in the energy falling on each of the subcarriers. This ultimately degrades the noise immunity of transmissions based on PFM signals [8, 13].

Therefore, a compromise is needed between the ratio of k and m.

Thus, the analysis of the ALE 2G standard (automatic installation of the 2nd generation channel) [15] shows that for radio communication systems in the decameter range, the choice of eight-position frequency-shift keying signals (FM-8 signals) with a bandwidth of about 2 kHz is justified. This signal provides a symbol rate of 125 baud. The indicated value is confirmed by the long-term practice of message transmission via the ionospheric channel (channel with variable parameters). Therefore, when choosing the value of m for transmission with PFM signals, it is advisable to focus on the frequency band determined by the symbol rate in the range from 100 to 250 baud.

The diagram obtained in the course of the study, shown in Fig. 1, clearly illustrates the obviousness of the choice with the total number of subchannels $m = 8$, the parameter value $k = 3$. The expediency of such a choice is due to the fact that in this case, each symbol of the PFM-7/3 signal will provide the transmission of five bits, with a slight decrease in energy indicators attributable to recalculation for each active subcarrier.

The choice of the manipulating code for the formation of signals PFM-7/3

For efficient transmission of information, the choice of active subcarriers on the chip duration must be determined in accordance with a given alphabet. The capacity (size) of the alphabet will be determined by the values $m = 8$ and $k = 3$, in accordance with the following combination formula [8]

$$C_m^k = \frac{m!}{k!(m-k)!}. \tag{5}$$

According to formula (5), for the indicated values of m and k, the capacity of the alphabet will be 35 elements. Moreover, for a seven-digit symbol, the number of elements of the alphabet is $2^7 = 128$. The analysis of existing codes in [4] showed the advisability of choosing for the indicated combinations of the International Telegraph Alphabet (ITA) with a constant weight of the ITA-3. The choice of this code is due to its properties, which make it possible to detect an error in a code combination if the odd parity of the units contained in it is violated. Exceptions are situations that result in offset errors. The occurrence of these errors is associated with the mutual transition of the allowed “0” to “1” and vice versa, the allowed “1” to “0”. Such errors lead to the combination allowed for the alphabet. But it should be borne in mind that the combination obtained in this case does not correspond to the combination transmitted by the received symbol.

Thus, the use of ITA-3 for coding subcarriers will allow, even before demodulation, to inform the recipient about the presence of an error in the received symbol, based on the results of evaluating the odd parity violation of active subchannels. This circumstance emphasizes the originality of the solution associated with the choice of the ITA-3 code for encoding the signal symbols PFM-7/3.

Evaluation of the noise immunity of the PFM-7/3 signals in the channel with variable parameters with incoherent processing

In [9], the following expression was proposed for calculating the error probability for PFM signals under the conditions of their incoherent demodulation:

$$P_{\text{PFM}} = \int_0^\infty \left[1 - \left(1 - \exp\left[\frac{z^2 m}{2\sigma^2}\right]^{m-k}\right)\right] \times$$

$$\times \left[\begin{aligned} &1 - \operatorname{erf}\left(\left[z - \frac{u\sqrt{2}}{\sqrt{k}}\right]\sqrt{m}\sigma^{-1}\right)^{k-1} \times \\ &\times k\frac{\sqrt{m}}{\sqrt{2\pi}\sigma}\exp\left[-\frac{\left[z - \frac{u\sqrt{2}}{\sqrt{k}}\right]^2 m}{2\sigma^2}\right]\end{aligned}\right] \mathrm{d}z. \tag{6}$$

Here u is the root-mean-square voltage of the signal in the channel; σ is the root-mean-square noise voltage in the channel; z is the accepted implementation of the signal in noise.

It should be noted that expression (6) has a rather complex analytical representation for its interpretation and modeling, therefore, a different approach is proposed to substantiate the formula for evaluating the noise immunity of the PFM-7/3 signals with their incoherent processing. In particular, in Fig. 2 shows the spectra of the signals PFM-2/1 $|F_{\text{PFM-2/1}}(f)|$ (frequency telegraphy) and PFM-7/3 $|F_{\text{PFM-7/3}}(f)|$.

With regard to orthogonal systems with an active pause, with incoherent reception in a channel with variable parameters, the probability of a symbolic error is determined using the expression:

$$P_s = \sum_{n=1}^{m-1} (-1)^{n+1} C_{m-1}^n \frac{1}{nh^2 + n + 1}. \tag{7}$$

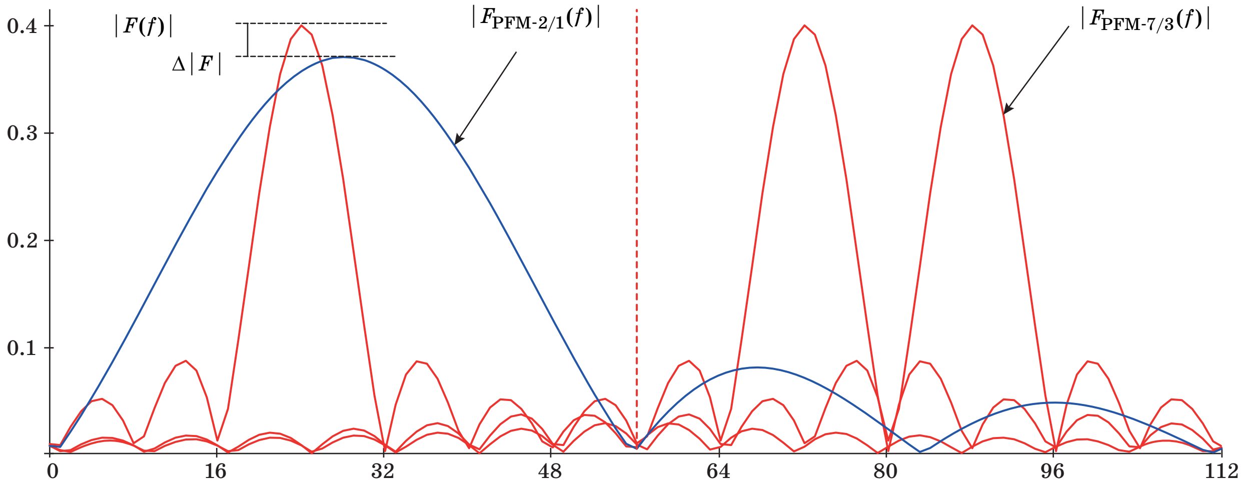
Here h^2 is the average ratio of the signal energy to the power spectral density of the noise (interference).

Next, we recalculate the probability of a symbolic error into a bit error

$$P_b = \frac{m/2}{m-1} P_s. \tag{8}$$

Now, in the interest of obtaining an expression for estimating the potential noise immunity of a signal with an orthogonal permutable frequency modulation of the PFM-m/k, formed by coding active subcarriers with a constant weight code at the physical level, it is necessary to consider the independent reception of k active tones on the signal chip duration. In this case, it is necessary to take into account that the energy of each of the tone oscillations at its own sub-frequency will decrease k times. Moreover, the signal symbol will be correctly identified only if each of the tonal fluctuations is reliably received. This is possible only if the condition

$$h^2 \to \frac{h^2}{k}. \tag{9}$$



■ ***Fig. 2.*** Functions of envelope spectra of signals of transmissions of permutation manipulation on symbol duration within the limited channel

Condition (9) can be interpreted in such a way that correct reception is possible only when the average level of each of the k active tonal oscillations exceeds the average value of the signal level together with interference within the passive subchannels [16], for which, according to formula (1), the element of vector **A** is "0". For further derivation of the required expression, we turn to the concept of the probability of error-free reception, which is the inverse for P_s:

$$P_0 = 1 - P_s. \tag{10}$$

Taking into account the assumptions made, the expression for calculating the probability of symbolic error for a channel with variable parameters will be as follows:

$$P_s = 1 - \left[1 - \sum_{n=1}^{m-1} (-1)^{n+1} C_{m-1}^{n} \frac{1}{\frac{nh^2}{k} + n + 1}\right]^k. \tag{11}$$

However, formula (11) does not take into account the fact that if the first tone waveform can be received on any of the m possible subchannels in the passband, then for the second tone waveform on the duration of the same symbol, only $m-1$ subchannels in within the same bandwidth, etc.

Taking into account the additions made, we transform expression (11) to the form:

$$P_s = 1 - \prod_{s=1}^{k} \left[1 - \sum_{n=1}^{m-s} (-1)^{n+1} C_{m-s}^{n} \frac{1}{\frac{nh^2}{k} + n + 1}\right]. \tag{12}$$

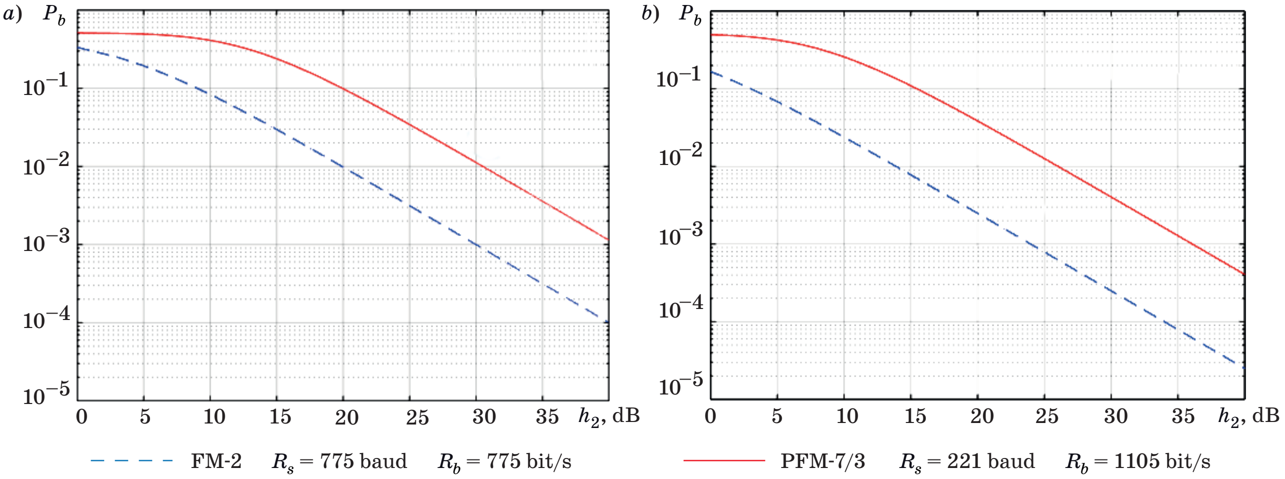
Now, to recalculate the probability of a symbolic error into a bit error, consider the formation of allowed combinations when encoding with a code with a constant weight (k, m). Note that a binary number will be associated with each allowed combination, and the number of such binary numbers L will not exceed the size of the allowed alphabet. Therefore, the number of used alphabet combinations is calculated by the formula

$$L = 2^{\left\lfloor \log_2 C_m^k \right\rfloor}. \tag{13}$$

And then, taking into account formulas (12) and (13), we obtain the resulting expression for calculating the bit error probability of orthogonal signals with permutational frequency modulation, encoded with a constant weight code at the physical layer. The expression is valid for the conditions of incoherent reception in a channel with variable parameters (ionospheric channel in the decameter range):

$$P_s = \frac{L/2}{L-1} \times$$
$$\times \left(1 - \prod_{s=1}^{k} \left[1 - \sum_{n=1}^{m-s} (-1)^{n+1} C_{m-s}^{n} \frac{1}{\frac{nh^2}{k} + n + 1}\right]\right). \tag{14}$$

According to expression (14), the decision on the transmitted symbol is made at the k maximum levels in the passbands of the corresponding tones. That is, in the received signal symbol, the position of k active subcarriers will correspond to the allowed constant weight code combination, which is k. This will allow implementing the property of the code to detect er-



■ ***Fig. 3.*** Dependence of the bit error probability on the ratio of bit energy to noise density (*a*) and of signal power to noise power (*b*) for FM-2 (PFM-2/1) and PFM-7/3 signals in a channel with variable parameters for incoherent reception

rors at the stage of signal reception. Only the resulting offset errors will not be detected.

In Figures 3, *a* and *b* show graphs of the dependence of the bit error probability for signals with permutable frequency modulation.

Analysis of the results presented in the form of graphs in Fig. 3 allows us to conclude that the use of signals PFM-7/3 leads to a decrease in the symbol rate, but at the same time the bit rate increases to 1105 bits per second. But precisely due to the decrease in the symbol rate from 775 to 221 baud compared to FM-2 signals in the 3100 Hz frequency band, the influence of intersymbol interference on the transmitted signal will no longer be so significant. The price for this is a loss in energy efficiency (up to 10–12 dB).

However, it should be borne in mind that if the achievement of energy performance in decameter radio communication systems can be achieved by selecting the optimal operating frequencies and increasing the power of the transmitters, then it is almost impossible to avoid problems with intersymbol interference, which leads to a sharp increase in the probability of error above the permissible at the symbol rate of 775 baud.

Conclusion

The physical simplicity of the formation and processing of signals of permutable frequency modulation makes them very interesting for practical use in radio communication systems of the decameter range.

In particular, the proposed PFM-7/3 signals, encoded by the ITA-3 code, make it possible to additionally detect symbolic errors at the physical level, which, according to the authors, will further increase the noise immunity of reception.

Another interesting aspect is seen in the application of correcting codes for subcarrier manipulation as well as wavelet signals.

The signals with permutational frequency modulation, formed on the basis of codes with constant weight, in a channel with variable parameters are inferior in noise immunity to signals of multi-position frequency modulation. This is due to the fact that the transmitter power is evenly distributed between the passbands of the active sub-frequencies in accordance with the given coding. But the loss in the energy aspect, in a sense, is compensated by the properties of higher spectral efficiency, which makes it possible to increase the number of bits per symbol.

In radio communication systems operating in ionospheric channels with multipath propagation, signals with permutational frequency modulation can serve as a good alternative to signals generated on the basis of technology with orthogonal frequency multiplexing of channels.

The authors associate further research with the search for optimal decision-making criteria when demodulating PFM signals.

References

1. Nguyen Minh Zhang. *Metod i algoritm prognozirovaniya uglov prikhoda dekametrovykh radiovoln pri ikh rasprostranenii v gorizontal'no — neodnorodnoy rasseivayushchey ionosphere.* Dis. kand. techn. nauk [Method and algorithm for predicting the angles of arrival of decameter radio waves during their propagation in a horizontally inhomogeneous scattering ionosphere. PhD tech. sci. diss.]. Irkutsk, Irkutskij nacional'nyj issledovatel'skij tekhnicheskij universitet Publ., 2017. 23 p. (In Russian).

2. Kandaurov N. A. *Signal'no-kodovyye konstruktsii dlya nizkoenergeticheskikh shirokopolosnykh radioliniy dekametrovogo diapazona*. Dis. kand. techn. nauk [Signal-code structures for low-energy broadband radio lines of the decameter range. PhD tech. sci. diss.]. Moscow, Moskovskij tekhnicheskij universitet svyazi i informatiki Publ., 2019. 23 p. (In Russian).
3. Naoki Ishikawa, Shinya Sugiura, and Lajos Hanzo. 50 years of permutation, spatial and index modulation: from classic RF to visible light communications and data storage. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, iss. 3, pp. 1–32. doi:10.1109/COMST.2018.2815642
4. Dvornikov S. V., Popov E. A., Balykov A. A., Dvornikov S. S. Interference stability of signals with transfer frequency modulation in channels with constant parameters when incorrect reception. *Radioengineering*, 2019, no. 12 (20), pp. 24–31 (In Russian). doi:10.18127/j00338486-201912(20)-04
5. Ishikawa N. Space-, time-, and frequency-domain permutation modulation designed for microwave and optical wireless communications. PhD dissertation, Tokyo University of Agriculture and Technology, 2017. Corpus ID: 67371011
6. Bian Y., Cheng X., Wen M., Yang L., Poor H. V., Jiao B. Differential spatial modulation. *IEEE Transactions on Vehicular Technology*, 2015, vol. 64, no. 7, pp. 3262–3268. doi:10.1109/TVT.2014.2348791
7. Ishikawa N., Rajashekar R., Sugiura S., Hanzo L. Generalized spatial modulation based Reduced-RF-Chain Millimeter-Wave communications. *IEEE Transactions on Vehicular Technology*, 2017, vol. 66, no. 1, pp. 879–883. doi:10.1109/TVT.2016.2555378
8. Dvornikov S. V., Ovchinnikov G. R., Balykov A. A. Programmed simulator of the ionospheric radio channel of the decameter range. *Information and Space*, 2019, no. 3, pp. 6–12 (In Russian).
9. Ishimura S., Kikuchi K. Multi-dimensional permutation-modulation format for coherent optical communications. *Optics Express*, 2015, vol. 23, iss. 12, pp. 15587–15597. doi:10.1364/OE.23.015587
10. Sugiura S., Ishihara T., Nakao M. State-of-the-art design of index modulation in the space, time, and frequency domains: Benefits and fundamental limitations. *IEEE Access*, 2017, vol. 5, pp. 21774–21790. doi:10.1109/ACCESS.2017.2763978
11. Bykhovsky M. A. Noise immunity of signal reception during permutation modulation. *T-Comm*: *Telecommunications and Transportation*, 2015, vol. 9, no. 4, pp. 12–16. doi:10.36724
12. Ishimura S., and Kikuchi K. Multi-dimensional permutation modulation aiming at both high spectral efficiency and high power efficiency. *Optical Fiber Communications Conference (OFC 2014)*, 2014, M3A.2. doi:10.1364/OFC.2014.M3A.2
13. Dvornikov S. V., Balykov A. A. Proposals for controlling the transmission rate and noise immunity of signals with permutable frequency modulation. *T-Comm: Telecommunications and Transportation*, 2020, vol. 14, no. 6, pp. 20–26. doi:10.36724/2072-8735-2020-14-6-20-26
14. Shagarova A. A. *Issledovaniye metodov i algoritmov povysheniya dostovernosti dannykh v sisteme aviatsionnoy elektrosvyazi dekametrovogo diapazona*. Dis. kand. techn. nauk [Research of methods and algorithms for increasing the reliability of data in the aviation telecommunication system of the decameter range. PhD tech. sci. diss.]. Ulyanovsk, Ul'yanovskij gosudarstvennyj tekhnicheskij universitet Publ., 2016. 16 p. (In Russian).
15. *Fixed HF radio communication systems*. Rep. ITU-R F.2061. Available at: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-F.2061-2006-PDF-R.pdf (accessed 30 August 2020).
16. Makoviy V. A. Numbering of permutation modulation channel symbols. *Teoriya i tekhnika radiosvyazi*, 2009, no. 4, pp. 17–22 (In Russian).

УДК 621.396
doi:10.31799/1684-8853-2020-6-30-36

Применение сигналов перестановочной частотной модуляции, манипулированных кодом с постоянным весом, для повышения помехоустойчивости радиосвязи декаметрового диапазона

С. В. Дворников[а], доктор техн. наук, профессор, orcid.org/0000-0002-4889-0001, practicdsv@yandex.ru
А. А. Балыков[б], соискатель, адъюнкт, orcid.org/0000-0001-9311-1807
С. С. Дворников[б], канд. техн. наук, начальник лаборатории кафедры применения войск связи, orcid.org/0000-0001-7426-6475
[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ
[б]Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ

Введение: работа радиолиний декаметрового диапазона, как правило, происходит в сложной помеховой обстановке, характеризующейся наличием быстрых и медленных замираний. Поэтому актуальным исследованием в данной предметной области является разработка новых технических решений, направленных на повышение помехоустойчивости приема. **Цель:** разработка сигналов с перестановочной частотной модуляцией, позволяющих на физическом уровне обнаруживать единичные ошибки за счет выбора сочетаний поднесущих каждого символа в соответствии с алфавитом кода с постоянным весом. **Результаты:** рассмотрены теоретические аспекты формирования сигналов с перестановочной частотной модуляцией; обоснован выбор манипулирующего кода для выбора поднесущих в пределах сигнального символа; представлен аналитический подход к выводу обобщенного выражения оценки помехоустойчивости разработанных сигналов перестановочной модуляции в канале с переменными параметрами при некогерентной обработке; приведены графики оценки значений вероятности битовой ошибки для новых сигналов в сравнении с известными результатами. **Практическая значимость:** разработанный сигнал с перестановочной частотной модуляцией предлагается использовать в системах декаметровой радиосвязи, работающих в узкой полосе частот в ионосферном канале. **Обсуждение:** дальнейшие исследования авторы связывают с оптимизацией процедур принятия решения при демодуляции разработанных сигналов, а также с поиском эффективных способов кодирования сигналов с перестановочной частотной модуляцией на физическом уровне, позволяющих повысить скорость передачи данных при сохранении помехоустойчивости приема.

Ключевые слова — перестановочная частотная модуляция, манипуляция кодом с постоянным весом, декаметровая радиосвязь, помехоустойчивость, вероятность битовой ошибки, некогерентная обработка сигналов, медленные замирания.

Для цитирования: Dvornikov S. V., Balykov A. A., Dvornikov S. S. Application of permutation frequency modulation signals manipulated with a constant weight code to increase the noise immunity of decameter radio communications. *Информационно-управляющие системы*, 2020, № 6, с. 30–36. doi:10.31799/1684-8853-2020-6-30-36

For citation: Dvornikov S. V., Balykov A. A., Dvornikov S. S. Application of permutation frequency modulation signals manipulated with a constant weight code to increase the noise immunity of decameter radio communications. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 30–36. doi:10.31799/1684-8853-2020-6-30-36

УВАЖАЕМЫЕ АВТОРЫ!

Научная электронная библиотека (НЭБ) продолжает работу по реализации проекта SCIENCE INDEX. После того как Вы зарегистрируетесь на сайте НЭБ (http://elibrary.ru/defaultx.asp), будет создана Ваша личная страничка, содержание которой составят не только Ваши персональные данные, но и перечень всех Ваших печатных трудов, имеющихся в базе данных НЭБ, включая диссертации, патенты и тезисы к конференциям, а также сравнительные индексы цитирования: РИНЦ (Российский индекс научного цитирования), h (индекс Хирша) от Web of Science и h от Scopus. После создания базового варианта Вашей персональной страницы Вы получите код доступа, который позволит Вам редактировать информацию, помогая создавать максимально объективную картину Вашей научной активности и цитирования Ваших трудов.

UDC 004.93'1

doi:10.31799/1684-8853-2020-6-37-49

Evaluation of EEG identification potential using statistical approach and convolutional neural networks

A. E. Sulavko[a]*, PhD, Tech., Associate Professor, orcid.org/0000-0002-9029-8028, sulavich@mail.ru*
P. S. Lozhnikov[a]*, Dr. Sc., Tech., Associate Professor, orcid.org/ 0000-0001-7878-1976*
A. G. Choban[a]*, Student, orcid.org/0000-0003-1834-6651*
D. G. Stadnikov[a]*, Student, orcid.org/0000-0002-5405-2450*
A. A. Nigrey[b]*, Post-Graduate Student, orcid.org/0000-0002-8391-5374*
D. P. Inivatov[a]*, Student, orcid.org/0000-0001-9911-1218*
[a]*Omsk State Technical University, 11, Mira Pr., 644050, Omsk, Russian Federation*
[b]*Omsk State Transport University, 35, Karl Marx Pr., 644046, Omsk, Russian Federation*

Introduction: *Electroencephalograms contain information about the individual characteristics of the brain activities and the psychophysiological state of a subject.* ***Purpose:*** *To evaluate the identification potential of EEG, and to develop methods for the identification of users, their psychophysiological states and activities performed on a computer by their EEGs using convolutional neural networks.* ***Results:*** *The information content of EEG rhythms was assessed from the viewpoint of the possibility to identify a person and his/her state. A high accuracy of determining the identity (98.5–99.99% for 10 electrodes, 96.47% for two electrodes Fp1 and Fp2) with a low transit time (2–2.5 s) was achieved. A significant decrease in accuracy was detected if the person was in different psychophysiological states during the training and testing. In earlier studies, this aspect was not given enough attention. A method is proposed for increasing the robustness of personality recognition in altered psychophysiological states. An accuracy of 82–94% was achieved in recognizing states of alcohol intoxication, drowsiness or physical fatigue, and of 77.8–98.72% in recognizing the user's activities (reading, typing or watching video).* ***Practical relevance:*** *The results can be applied in security and remote monitoring applications.*

Keywords *— deep learning, multilayer neural networks, biometrics, machine learning, feature extraction, electrical brain activity, psychophysiological state, pattern recognition, spectrograms.*

For citation: Sulavko A. E., Lozhnikov P. S., Choban A. G., Stadnikov D. G., Nigrey A. A., Inivatov D. P. Evaluation of EEG identification potential using statistical approach and convolutional neural networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 37–49. doi:10.31799/1684-8853-2020-6-37-49

Introduction

Today, technologies of creating neurocomputer interfaces transmitting commands to devices contact-free are actively developing. The majority of the neurointerfaces are based on the registration and interpretation of electroencephalograms (EEG), which reflect the dynamics of changes in brain electrical activity over time. The identification potential of electroencephalograms is extremely high — EEG analysis is used in tasks such as brain-computer interfaces [1], biometric identification and authentication [2], risky behavior identification [3], evaluation of a personal functional (physical, mental, emotional) state [4]. The last group of tasks is of particular interest since timely detection of the fact that the subject (an employee, an operator, a driver, a student) is asleep or intoxicated will help avoid emergencies. These states are characterized by reduced performance and reactions, distracted attention [5]. It is also possible to conclude the brain state (sleep, waking up, relaxation/meditation, concentration while performing heavy intellectual tasks) by analyzing the EEG. It allows building a continuous process of identifying not only a subject [2] but a type of a task as well (at work, in gaming, during distant examinations, etc.). Such methods are in particular demand when it is necessary to automatically monitor the subjects' activities without direct surveillance and to exclude the "human factor" in decision-making.

The automatic EEG analysis is difficult to perform as signals are noisy and depend on many factors: equipment (frequency of electrode interrogation, the number, and characteristics of electrodes), installation and location of electrodes, individual features of EEG subjects. Traditional EEG analysis methods based on frequency filtering and artifact removal provide under-represented results to be implemented; the resulted features prove to have low information value that leads to low accuracy in classifying EEG images.

This study focuses on the development of methods for recognizing the user identity, his or her psychophysiological state (PPS), and the tasks he or she performs on a computer using multilayer convolution neural networks (CNN) and deep learning methods [1]. These tasks are considered in one paper, as they are closely connected. The study focuses on this connection and estimates the informational value of EEG rhythms in terms of their ability to recognize the subject identity or particular states.

Psychophysiological state is a set of personal characteristics that reflect the biological aspects of adaptation to changing environmental conditions [6]. The following key PPS are considered in the paper: mild alcohol intoxication, drowsiness, physical fatigue, the norm. By the “norm” state it is understood that before the experiment, the test person has not been subjected to any physical or mental stress or taken any medication affecting the PPS.

The research has the following objectives.

1. To estimate the informational value of the EEG rhythms in terms of the possibility of identifying the user and his/her PPS.
2. To propose the architecture of convolutional networks for the recognition of EEG images.
3. To evaluate the accuracy (a ratio of correct decisions to the total number of experiments) of user identification, his or her PPS, as well as the tasks performed by the user in the “norm” state (watching an entertaining video, reading scientific literature, typing, inactivity/rest).

Base of EEG test persons

Data from the EEG was collected for 30 test persons. The location of the electrodes in all experiments was as shown in Fig. 1, according to the standard “10-20” scheme. The recording of the EEG in the “normal” state was done when the test users were performing fore tasks (each task preceded by the re-installation of the electrodes):

— the test user was sitting in a chair with his eyes closed (standard conditions);

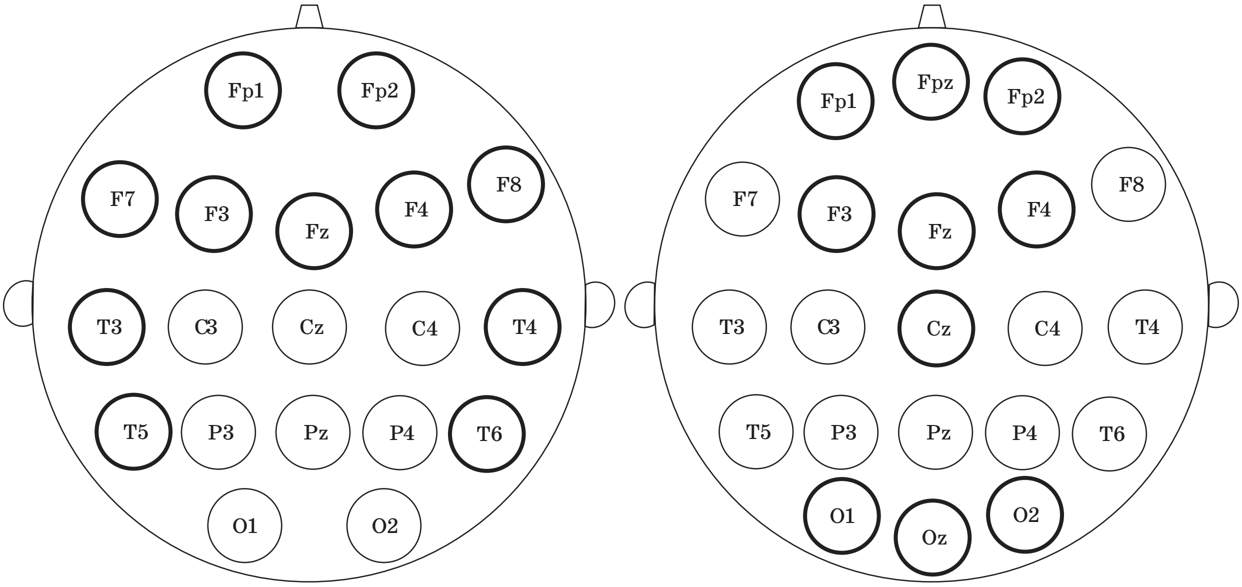
— the test user was typing a scientific and technical text on the keyboard;

— the user was reading a scientific article;

— the user was watching a comedy.

All the test persons have performed each task within 10 min. Experiments with the first task were carried out on different days and using two various devices: Mitsar EEG-201 (19 channels with a noise level of < 2 μV and a sampling rate (SN) of 250 Hz per channel) and Neuron Spectrum-4/P from Neurosoft (21 channels with a noise level less than 0.3 μV and SN 500 Hz per channel) in order to assess the variability of the EEG over time, depending on the installation and device. Neuron-Spectrum data for each test person were recorded 7 times on different days.

The recording of EEG data in states of intoxication, drowsiness, and fatigue was done only under standard conditions. In order to make the test person intoxicated, necessary doses of alcohol were calculated according to the modified formula Vidmark [see 7, formula (1)], based on a quantity of 0.7 ‰, which corresponds to the second stage of intoxication according to the Federal Aviation Regulation (CFR) 91.17 classification. In order to put the test persons into a state of drowsiness, they were asked to take 2 tablets of Leonurus cardiaca 200 mg and to be sitting in a chair for 20 min in a quiet and dark room just before starting EEG recording. To record the EEG in a fatigued state, the test persons experienced intensive physical activity before the experiment, the minimum amount of which was determined by the Martinet method (20 squats in 30 s), and then varied according to the physical abilities



■ ***Fig. 1.*** Mitsar connection diagram (left) and Neuron-Spectrum-4/P (right) of the person. EEG recordings were made for each subject in each state with a duration of 5 min. The EEG recordings for each of the test persons' states were made on a separate day.

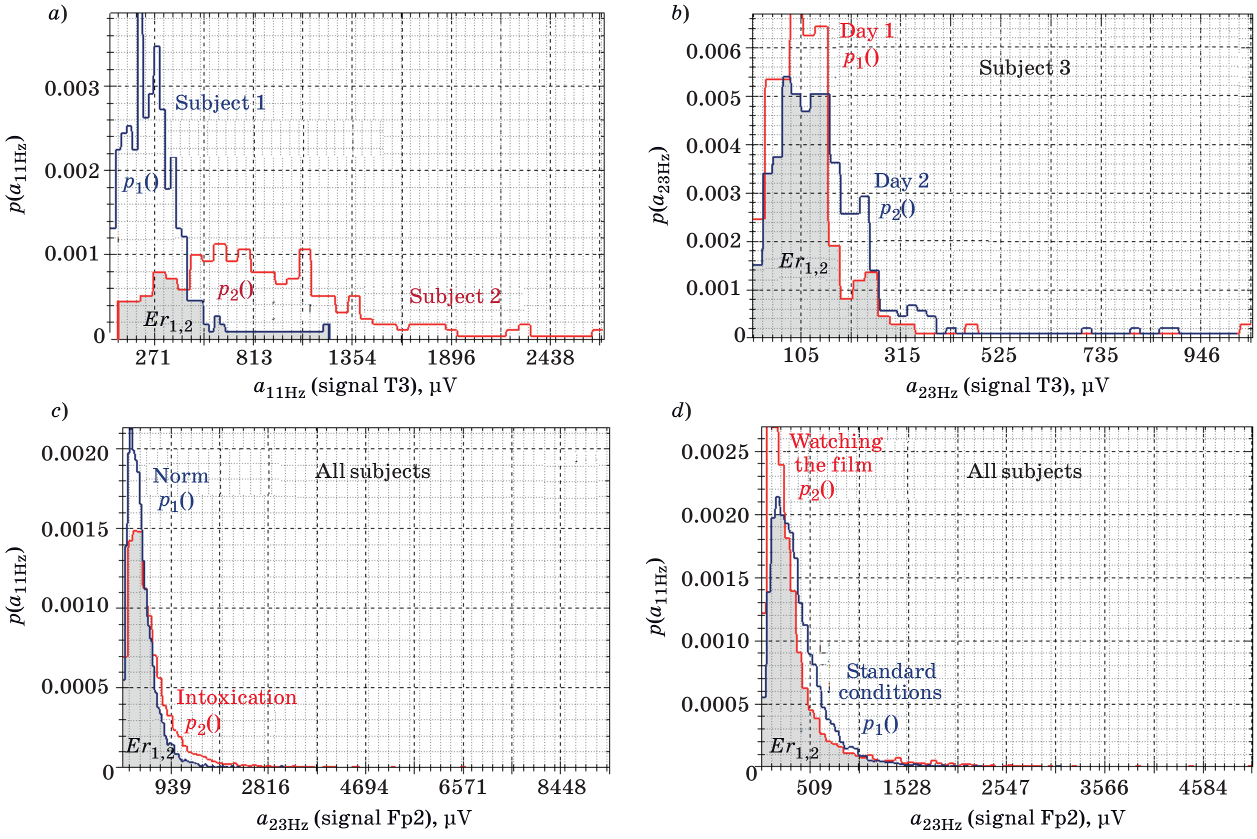
Estimation of the informational value of the EEG rhythms in terms of PPS

In this section, Mitsar data was analyzed, as only this data are obtained with the PPS in mind. In the first instance, a band-reject filter was applied to the original signals to suppress interference from power lines that operate at 50 Hz in Russia. EEG signals can have an ”overtone effect”, where interference is also observed at higher frequencies divisible by 50 Hz. The filtration was therefore performed in the 45–55, 95–105, and 145–155 Hz frequency bands.

The following EEG rhythms are distinguished by their frequency, duration, amplitude and waveform: delta (1–4 Hz), theta (4–8 Hz), alpha (8–14 Hz), beta (13–35 Hz), gamma (30–170 Hz), lambda (4–5 Hz), mu (7–13 Hz), kappa (8–12 Hz), tau (8–13 Hz), sigma (10–14 Hz). The main rhythms are the first five ones. Let us assess the informational value of the EEG rhythms in terms of the possibility of identifying the subject, the subject's PPS, and the task the subject is performing on a computer.

Spectrograms provide sufficient enough representation of the signal, in this study they were calculated by applying a short-term (window) rapid Fourier transform using a rectangular window (the duration is 1 s, a window overlap is 50%). If the amplitude a of each harmonic with the frequency ν is taken as a feature, it is possible to build a probability density function (PDF) of this harmonic for each image class (e. g. when identifying a PPS, a class for each state should be formed from one-second EEG images if the subjects who were in the corresponding state).

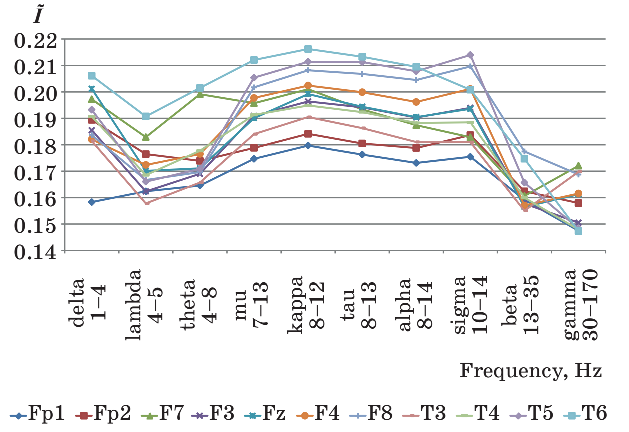
The area of intersection of the PDF values of a particular feature for two classes (with numbers j and i) is approximately equal to the probability of error $Er(\nu)_{j,i}$ of the two-class identification of images by this feature (Fig. 2, *a–d*). The probability of correct classification is numerically equal to $\dot{I}(\nu)_{j,i} = 1 - Er(\nu)_{j,i}$. The accuracy of this assessment depends on the sample size using which the relevant PDFs were built. The informational value of



■ ***Fig. 2.*** Examples of determining the error probability in the classification of EEG images by one feature: *a* — subject identification under standard conditions in the “norm” state; *b* — assessment of the subject EEG variability under standard conditions in the “norm” state; *c* — PPS identification under standard conditions; *d* — identification of the task performed by the subject in the “norm” state the feature for the majority of classes can be judged by the average probability estimation of the correct classification $\ddot{I}_\nu = m(\dot{I}(\nu)_{j,i})$ for all pairs of classes (the higher the $\ddot{I}_\nu$ is, the more informational value the frequency has). In a first approximation, in terms of the ability to identify a subject the informational value of the EEG rhythm can be calculated as the average of estimates $\breve{I} = m(\ddot{I}_\nu)$ in the corresponding frequency range. In addition, it must be borne in mind that the amplitude spectra of EEG signals may vary at different moments of time and depending on the installation of the electrodes. These changes can be estimated through the corresponding probability densities $p_{j,day\_1}(a_{\nu\mathrm{Hz}})$ and $p_{j,day\_2}(a_{\nu\mathrm{Hz}})$, which are derived from the EEG data of subjects recorded at identical PPS but on different days (see Fig. 2, *b*). Therefore, a correction of the informational value should be made to take into account the average probability of density mismatch $p_{j,day\_1}(a_{\nu\mathrm{Hz}})$ and $p_{j,day\_2}(a_{\nu\mathrm{Hz}})$ for all test persons in the "norm" state (hereinafter referred to as the Er_{norm}).

Figure 3 shows graphs of the informational values of EEG rhythms for the task of the user identification (under standard conditions of EEG recording), with a correction made to take into account the dependence of the EEG on the installation and the subject's PPS: $\tilde{I} = \breve{I} \cdot Er_{PPS} \cdot Er_{norm}$, where Er_{PPS} is the average error probability for the two-class identification in the state "norm", where the first class is the state "norm" and the second is any other state. This work reflects the probability of correct identification of the subject in a case of a mismatch between the installation and the PPS.

Figure 4, *a–f* shows graphs of the informational values of EEG rhythms for PPS identification tasks and the subject's activity. This assessment takes into account the dependence of the informational value on the individual features of the subjects' EEG and installation.



■ ***Fig. 3.*** Informational value of rhythms in multiclass subject identification under standard conditions in the "norm" state with respect to EEG variability due to changing mounting and a psychophysiological state

In general, all the rhythms individually are not informative enough for highly accurate automatic identification, both of the subject identity and the PPS. However, some results should be noted. The most information-bearing signal for EEG identification is recorded in the rear right temporal zones (T6). In this area, the most information-bearing rhythm is kappa rhythm, as well as mu and tau rhythms. The frequency range of 7–14 Hz in this area is very information-bearing when recognizing types of activity that require concentration (watching films, reading). The most information-bearing rhythms ($\tilde{I} \approx 0{,}395$) are lambda and theta rhythms in the right frontal area (Fp2) when recognizing the subject's intense activity related to typing on a computer, and sigma rhythm recorded in the rear left side of the temporal area (T5) when identifying a subject. High frequencies contain less information about the subject's individual EEG characteristics.

Based on the analysis carried out, it can be concluded that it is not worth excluding any frequencies from the input data while building a classifier, since all rhythmic oscillations carry parts of information for certain classes of images (states or subjects).

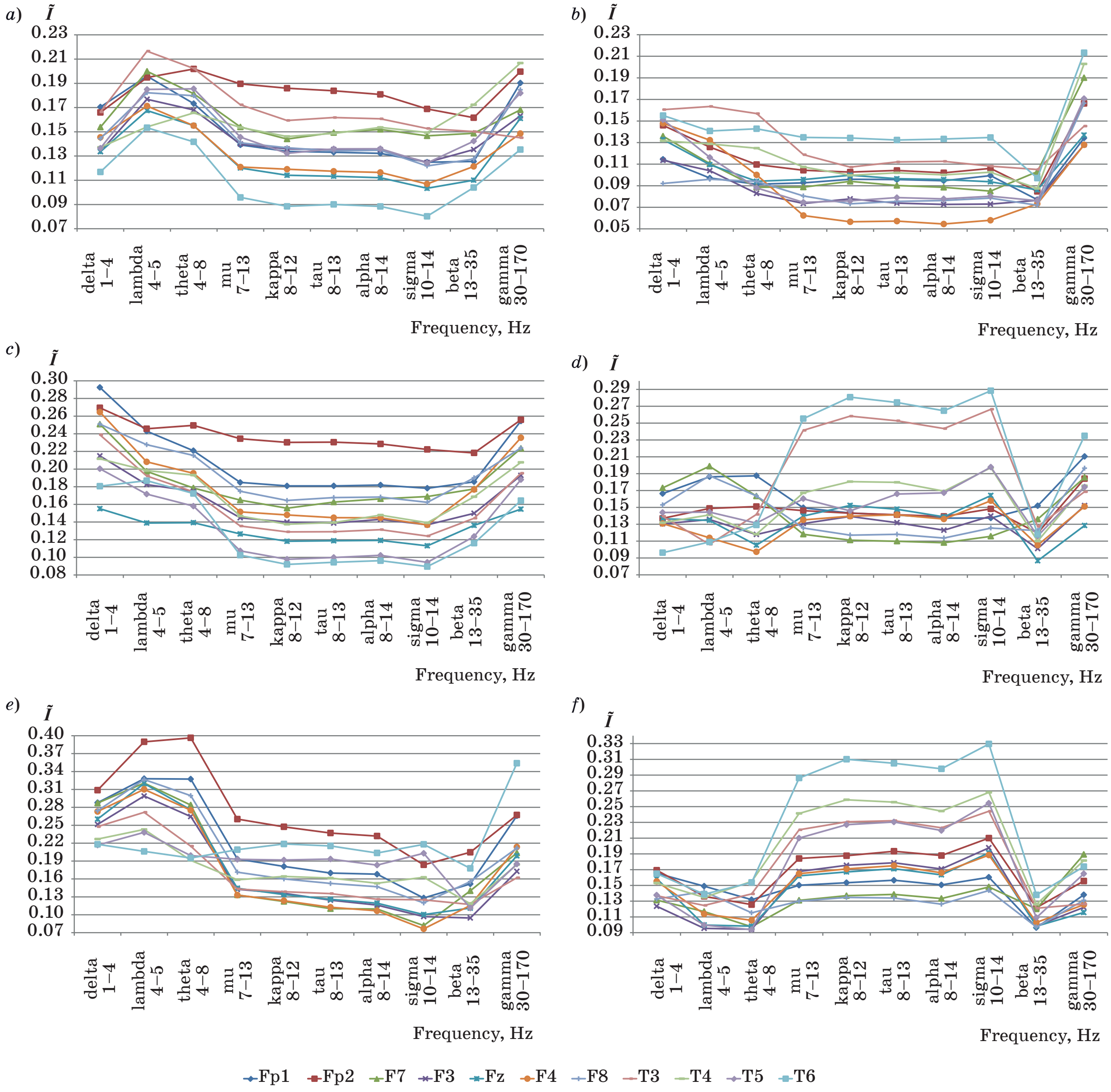
The mutual correlation between the amplitudes of harmonics with different frequencies has been assessed (Fig. 5, *a–d*).

Figure 5, *d* demonstrates that on average (for all subjects and all PPS) approximately 50% of the harmonic vibrations of the EEG signals have a remarkable or high mutual correlation relationship (over 0.3). The nature of the correlation relationships varies both from subject to subject and from PPS to PPS, as shown in Fig. 5. Pattern recognition methods should therefore be used that take into account the nature of correlative relationships between features (e. g., in this case, the Bayesian naive classification scheme is ineffective). In this respect, convolutional neural networks can be preferred because they can take into account the peculiarities of spectrum changes over time as well as the correlation links between different rhythms and electrodes.

Identification of EEG images

Two series of experiments were carried out.

1. Identification of a subject (from a closed set). The data generated by this study (Mitsar, Neuron-Spectrum) and the Physionet data set (64-channel EEGs with a duration of one minute, 109 test subjects in the "norm" state recorded under standard conditions with a sampling rate of 160 Hz) were used. The Physionet data set is one of the most rep-



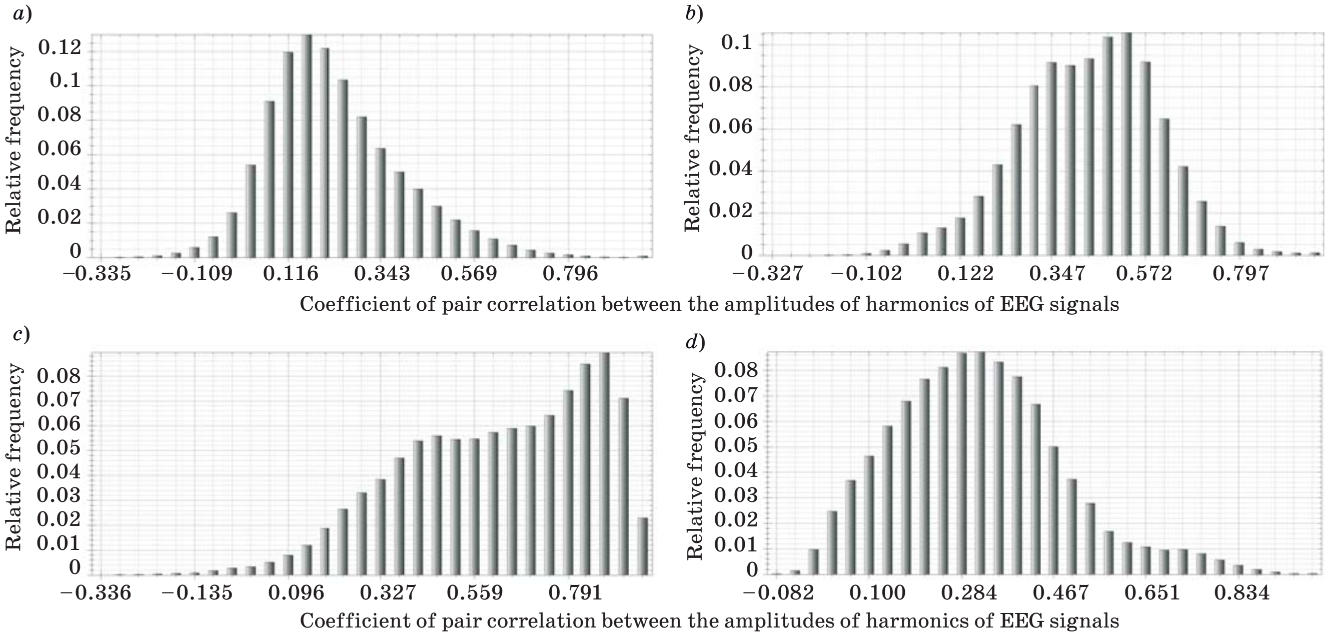
■ ***Fig. 4.*** The informational value of rhythms in the two-class identification of psychophysiological state and the tasks performed by the subject, where the first class is the "norm" state, and the second is: *a* — intoxication; *b* — drowsiness; *c* — fatigue; *d* — watching a movie; *e* — typing; *f* — reading

resentative as it includes many test subjects and is often used to compare EEG classification methods [8]. The training was carried out based on the EEGs recorded in the "norm" state on one or more days, and testing was carried out by cross-checking for data not used in training (in the "norm" state or other PPS).

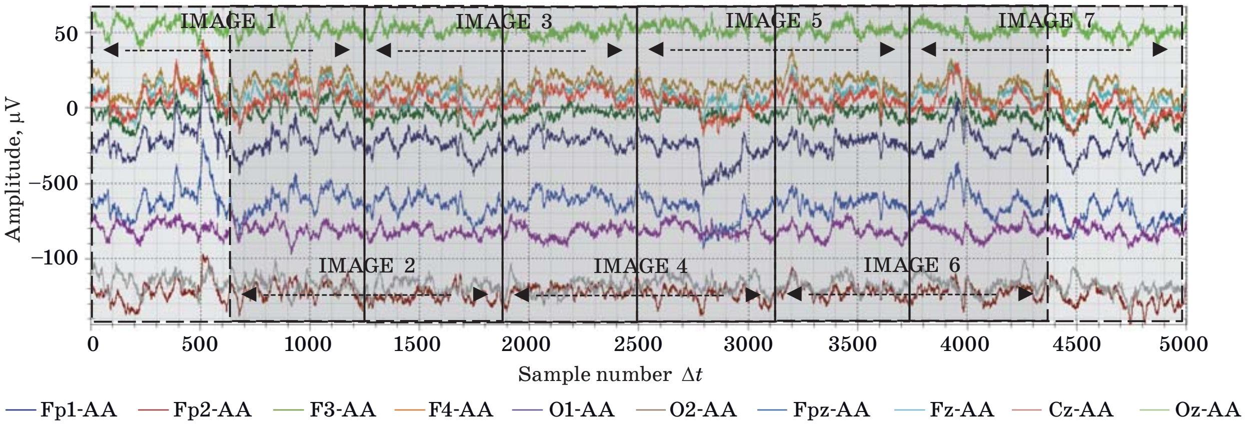
2. Identification of the PPS and the activity of the subjects (from a closed set). Only the Mitsar data set was used (30 subjects). The training sample was formed from all EEG data of 25 subjects, data from other subjects (not included in the training sample) were used for testing.

Electroencephalograms records were divided (with a 50% window overlapping) into shorter fragments: 2.5 s each (for Neuron-Spectrum data), 5 s each (for Mitsar data) and 2 s each (for Physionet data), as shown in Fig. 6. Each fragment obtained is an EEG image.

Images were submitted to the artificial neural network (ANN) input in two variants: as initial signals (IS) and as spectrograms (SG). The spectro-



■ ***Fig. 5.*** Histograms of the relative frequencies of the pair correlation coefficients between the amplitudes of different harmonics (with frequencies from 1 to 128 Hz): *a* — for the test subject 1 in the "norm" state; *b* — for the test subject 2 in the "norm" state; *c* — for the test subject 1 in a state of intoxication; *d* — for all subjects in all states



■ ***Fig. 6.*** Division of EEG into fragments of 2.5 s (Neuron-Spectrum data)

grams were calculated with window 64 and step 16 of the reports and further normalized to the minimum and maximum amplitude values of all signals for all subjects (to bring them to a single amplitude value interval [0; 1]).

Many ANN architectures were formed, focused on both IS and SG processing. Each architecture was built with respect to the peculiarities of a particular data set: sampling frequency, the number of electrodes, the number of identifiable classes (test subjects). The process of creating a network model based on some architecture consisted of several stages. At the architecture design stage, the neural network structure (the number of layers, the number of neurons in layers) was selected and hyperparameter calibration was done. The model was trained 10 times, and each time the EEG data were randomly divided into training and test samples (in the proportions originally set). During the training, an initial accuracy assessment was made on the validation sample (which was a subset of the test sample and includes 5–10% of the test examples). The primary accuracy estimates for each model were averaged. Next, the best models (with an accuracy margin of more than 10%) were fully tested (using the full test sample), after which the average Q accuracy estimates for each model were determined.

The networks were formed from constructions in a form of BLOCKS (from two to four per network). Each *BLOCK* consisted of two convolution layers (CL) with ReLu neuron activation functions, one layer of batch normalization (BN) and a dropout layer. The categorical cross entropy was used as an error function [9]. Each network also included an input (IL) and two fully connected layers (FL).

■ ***Table 1.*** Configuration of one of the promising ANNs for analysis of spectrograms

Layer Type		Layer Parameters
Input Layer		Dimension = 11, 32, 75 ([channel][frequency][time])
BLOCK_2d	Convolutional 2D	Number of filters = 10, convolution window = 3.3, stride = 2.2
	Convolutional 2D	Number of filters = 10, convolution window = 3.3, stride = 2.2
	Batch Normalization	
	Dropaut	Rate = 0.125
BLOCK_2d	Convolutional 2D	Number of filters = 20, convolution window = 3.3, stride = 2.2
	Convolutional 2D	Number of filters = 20, convolution window = 3.3, stride = 2.2
	Batch Normalization	
	Dropaut	Rate = 0.175
BLOCK_2d	Convolutional 2D	Number of filters = 30, convolution window = 2.1, stride = 1.1
	Convolutional 2D	Number of filters = 30, convolution window = 1.5, stride = 1.1
	Batch Normalization	
	Dropaut	Rate = 0.25
Fully connected layer		Number of neurons = 30, activation function: sigmoid
Fully connected layer		Number of neurons = number of classes, activation: softmax

■ ***Table 2.*** The results of subject identification by EEG

Input, quantity of channels	ANN structure	Quantity of epochs, batch size	Training sample per 1 man	Test sample (PPS)	Q, %
Neuron-Spectrum (30 classes, transit time (image size) 2.5 s, sampling rate 500 Hz)					
IS, 10	IL + 3BLOCKS_1d + + 2FL	20, 50	Day 1 (4 min), day 2 (1 min)	Norm, day 2	≥ 99.99
IS, 2 (Fp1, Fp2)					95
SG, 10	IL + 3BLOCKS_2d + + FL + BN + FL				≥ 99.99
SG, 2 (Fp1, Fp2)					96.47
Mitsar (30 classes, transit time (image size) 5 s, sampling rate 250 Hz)					
IS, 11	IL + 3BLOCKS_1d + + 2FL	100, 20	Day 1 (5 min)	Norm	94
		100, 20		Intoxication, drowsiness, fatigue	28.3
SG, 11	IL + 3BLOCKS_2d + + 2FL (Table 1)	20, 20		Norm	98.5
		20, 20		Intoxication, drowsiness, fatigue	41.8
		25, 20	Days 1 & 2 (2.5 min each)		64
		35, 30	Days 1, 2 & 3 (2.5 min each)		78.7
		50, 30	7 days (2.5 min each)		97.59
Physionet (109 classes, transit time (image size) 2 s, sampling rate 160 Hz)					
IS, 64	IL + 4BLOCKS_1d + + FL + BN + FL	70, 50	40 s	Norm	96.97
SG, 64	IL + 2BLOCKS_2d + + FL + BN + FL	100, 50			98.5

■ ***Table 3.*** The results of the identification of the subject's PPS and activity by the EEG

Input, quantity of channels	ANN structure	Quantity of epochs, batch size	Classes	*Q*, %
IS, 11	IL + 3BLOCKS_1d + 2FL	100, 50	4 (norm, intoxication, drowsiness, fatigue)	35
SG, 11	IL + 3BLOCKS_2d + 2FL (Table 1)	40, 50		41.5
IS, 11	IL + 3BLOCKS_1d + 2FL	100, 50	4 (norm, typing, reading, watching a movie)	56.68
SG,11	IL + 3BLOCKS_2d + 2FL (Table 1)	40, 50		59.21
SG,11	IL + 3BLOCKS_2d + 2FL (Table 1)	20, 25	2 (norm, fatigue)	94
	IL + 3BLOCKS_2d + FL + BN + FL	20, 25	2 (norm, reading)	92
		20, 25	2 (norm, drowsiness)	84
		20, 25	2 (norm, intoxication)	82
IS,11	IL + 3BLOCKS_1d + FL + BN + FL	50, 25		72
SG,11	IL + 3BLOCKS_2d + 2FL (Table 1)	20, 25	2 (norm, movie)	98.72
		20, 25	2 (norm, typing)	77.8

Thus, each neural network included from six to ten hidden layers (CL and FL). The parameters of the convolutions differed in various network implementations. One-dimensional convolutions were used for the IS analysis (time series analysis [9]), and two-dimensional convolutions were used for SG (image analysis [9]). Table 1 provides a description of one of the CNN architectures used in the experiment. The most representative results, as well as consolidated data on the parameters of the experiment (a number of training epochs, a mini-batch size, layers used, description of samples, etc.), are presented in Tables 2 and 3 (these tables describe CNN architectures in a shorter form).

Analysis of the obtained results for the identification of the EEG and their comparison with previous achievements

The survey has shown that traditional methods of signal analysis (frequency filtering, removal of artifacts, reduction of feature space dimension by the principal component analysis method (PCA)) and pattern recognition (k-nearest neighbors method (k-NN), support vector machine (SVM), C4.5 decision tree algorithm, etc.) are used more often to solve the problems under consideration [2, 4]. Artificial neural networks (ANNs) are also used in EEG analysis, with CNN giving better results in some tasks (emotion recognition in particular) [10].

The great majority of known studies consider the problems of identity recognition and human PPS identification as independent [2, 4]. There is little data available on the robustness of the identification results obtained in cases where subjects were in different PPS during the training and testing phases. The use of the EEG method of identification in practice requires that the results are consistent in a case of changes in the installation, and a state of the subject is identified.

The experiment carried out has shown that the accuracy of identification by EEG is reduced to unsatisfactory results if the subject's PPSs do not coincide during the training and testing stages. This indicates a high variability of the EEG depending on the subject's state (and possibly installation). In previous studies, this aspect has either not been taken into account or has been taken into account indirectly (for example, by normalizing signals to alpha rhythm [8], that does not guarantee their independence from PPS). It is proposed the network to be trained on EEG data recorded by the subject on different days. This has led to a significant increase in the reliability of the identification, including when the PPS changes, which follows from the results obtained — training with the 2-day data increases the accuracy by 22.2%, with the 5-day data by 53.5% (see Table 2).

When identifying an individual without respect to PPS (see Table 2), the high accuracy was obtained — it was 98.5% for Mitsar (30 classes) and Physionet (109 classes). When using the Neuron-Spectrum-4/P device, which has an increased sampling rate and low internal noise levels, the accuracy exceeded 99.99% (no errors were recorded). It is significant that when only two frontal electrodes were used, the accuracy on this device was 96.47%.

The percentage of correct decisions for two-class identification of PPS (see Table 3) ranged from 82 to 94%, and for two-class identification of tasks performed by a user on a computer — from 77.8 to 98.72%. For multiclass identification, the accuracy is significantly reduced (approximately twofold). The most difficult to identify is when the user is typing texts in real time on the keyboard (for this task, the accuracy was 77.8%).

Based on the results, it can be concluded that recognition accuracy and training rates increase (fewer epochs are required) if spectrograms are used as input data (see Tables 2 and 3).

Let us give a brief summary of the achieved accuracy rates of the subject's recognition and the PPS identification by EEG (Tables 4 and 5). The results of the analytical study on these issues are described in more detail in [2, 4].

As can be seen (see Table 4), convolution networks allow obtaining higher EEG identification accuracy with much shorter transit times. The result achieved in this paper surpasses the previous results.

The accuracy achieved in this paper in detecting drowsiness using the EEG is comparable to that obtained by other researchers; for intoxication, the result is on average slightly lower. However, the results of the recognition of fatigue, as well as the tasks performed by the user on the computer, are quite high. No direct analogy of these results have been found in the literature for direct comparison. The paper [3] should be mentioned that presents several hypotheses about the possibility of defining a subject's "risky behavior" based on EEG data (the possibility of performing dangerous or illegal actions), and a number of experiments have been carried out to test them. Sixty-two volunteers

■ ***Table 4.*** Comparison of the results of user recognition by EEG

Number of test persons	Methods	Transit time, s	Accuracy, %
45	Analysis of the activity of the brain areas responsible for reading and recognizing words based on artificial neural networks. A combination of 3 classifiers was used: cross-correlation, "naive" Bayes and feed forward ANN. Single-channel EEGs were used	50	97 [11]
50	Evaluation of individual brain reactions to various stimuli: primary visual perception, recognition of familiar faces, tastes. A time series cross correlation (fragments of EEG signals) was used as a classifier. Testing was repeated to account for the effect of EEG variability on the result over time. PPS was not monitored. The test subjects were placed in a camera protected from radio frequencies	27	No error recorded [12]
15	The application of an algorithm of generating 256-bit EEG-based keys using P300 evoked potential and two-layer neural networks trained in accordance with GOST R 52633.5.2011 (EEG authentication, one-to-one comparison). To be authenticated the user made a certain movement with his eyes (left, right, up, down etc.)	Over 10	10^{-10} [13]
80	Conversion of the test subjects' EEG in the "norm" state into a cryptographic key based on the fuzzy extractor method (EEG authentication, one-to-one comparison). The effect of alcohol ingestion on accuracy was studied		Before alcohol: 0.9742 After: 0.9389 [14]
109 (Physionet)	The EEG was recorded under standard conditions. The EEG was normalized by level, a bandpass filter (1–50 Hz), STFT (Hemming window) and the Fisher linear discriminant classifier were applied. The accuracy is higher at the moment of relaxation of the test subjects (alpha rhythm determines the optimal moment for authentication)	10	95.3–97.2 (64 electrodes) 93 (1 electrode) [8]
	The results obtained. Identification of images using CNN (EEG spectrogram analysis), one-to-many comparison. The impact of different PPSs was taken into account	2	98.5 (PPS is norm)
30 (Neuron-Spectrum)		2.5	No errors recorded (PPS is norm)
30 (Mitsar)		5	98.5 (norm) 97.59 (modified)

■ ***Table 5.*** Comparison of results of recognizing subject's states and actions by EEG

Test persons, electrodes	Methods	Accuracy, %
Sleep stage/ drowsiness		
29 test persons, Fp1, A1	SVM	72.7 [15]
10 test persons, 19 electrodes: Fp1-2, F3-4, C3-4, P3-4, O1-2, F7-8, T3-6, Fz, Cz, Pz	ANN	83.3 [7]
12 test persons, 32 electrodes	SVM, ANN, random tree and k-NN	93–97 [16]
6 test persons, 32 electrodes	SVM, k-NN	95 [17]
–	Hurst method	52.2 [18]
–	Higher-order spectrum analysis	88.7 [19]
–	Fuzzy logic, cluster analysis, Euclidian distance	80 [20]
30 test persons, 11 electrodes: Fp1, Fp2, Fz, F3-8, T3-6	Achieved result (drowsiness recognition)	**84**
Intoxication stages (the first stage — soberness)		
Alcohol ingestion: 50 ml, 40% ABV, 3 times a day (3 stages), electrodes: AF3-4, F3-8, FC5-6, P7-8, T7-8, O1-2	The signal is divided into fragments: 1 s each with a step of 0.5 s. 11 features are extracted from each fragment	89.95 (4 stages) [21]
The test persons ingested beer (750 and 1500 ml), 1 electrode Fp1	ANN	92.3 and 59.2 (2 and 7 stages) [22]
50 test persons in a "norm" state and 50 intoxicated persons, 64 electrodes	ANN, training — 40 subjects for each class, and 10 subjects for a test	95 (1200 training epochs) [23]
40 test persons in a "norm" state and 40 intoxicated persons	SVM, the training sample contains 20 subjects per class, the test sample contains 20 subjects. EEG has been processed with a filter (0.5–50 Hz)	98.83 [24]
50 intoxicated persons and in a "norm" state	Features are Yule — Walker equations autocorrelation coefficients. A training sample contains 40 users, a test sample contains 10 subjects	95 [25]
1341 visual records of evoked potentials (EP) (1129 — for training and 212 — for a test)	Power spectrum of EEG signals, average and dispersion of EP reports, PCA, fuzzy output	98.11 [26]
10 test persons in the "norm" state and intoxicated, 64 electrodes (sampling rate is 256 Hz)	PCA, C4.5, k-NN, SVM	79.3 (1 electrode) and 96.8 (64 electrodes) [27]
30 test persons, 11 electrodes: Fp1, Fp2, Fz, F3-8, T3-6	Obtained results (recognition of intoxication)	**82**
Other states (obtained results)		
30 test persons, 11 electrodes: Fp1, Fp2, Fz, F3-8, T3-6	Movie	**98.72**
	Fatigue	**94**
	Reading scientific articles	**92**
	Typing	**77.8**

(16 women and 46 men) were invited to conduct the experiments. The EEG was registered at 128 scalp areas. It was found that risk behavior is effectively predicted by the EEG through event-related electrical potentials.

Conclusion

The tasks of identification of an individual and the PPS by EEG are closely connected. The EEG contains information on both the individual characteristics of the subject's brain and the subject's state, as well as states that depend on his or her activity in real time. This paper estimates the informational value of EEG rhythms for recognizing a subject and a subject's PPS (with respect to the variability of the EEG over time, in a case of changes in installation and in dependence on PPS), recorded by the electrodes Fp1, Fp2, Fz, F3-8, T3-6 (in accordance with the "10-20" scheme). The most informative personal identification signal is recorded in the rear right (especially kappa, mu and tau rhythms) and left (sigma rhythm) temporal zones. The frequency range of 7–14 Hz in the posterior right temporal area is also meaningful when recognizing types of activity that require concentration (watching movies, reading). When recognizing typing activities on a computer, the lambda and theta rhythms in the right frontal lobe are the most meaningful.

Based on the results of the experiments, the convolution neural networks showed a higher accuracy of EEG identification (98.5–99.99% for 10 or more electrodes), with a shorter transit time (from 2 to 5 s) compared to the previously achieved level. It is significant that high accuracy is observed when only two frontal sensors are used (96.47%), which makes it possible to use "dry" electrodes that come into direct contact with the skin.

The use of the EEG method of identification requires results to be consistent in a case of changes in the installation and a state of the identified subject. Without the PPS, EEG-based identification results are of limited value. Our experiments have shown a significant drop in the accuracy of identification if the subject was in different PPSs during the training and testing phase of the EEG. In the course of previous studies, insufficient attention was paid to this aspect, and the tasks of identifying (authenticating) a subject and recognizing his or her EEG-based PPSs were perceived as independent. In this work, it has been suggested that the network should be trained on EEG data recorded by the subject on different days (without the control of the PPS). The results we have obtained indicate that this could significantly improve the reliability of identification, including the cases when the subject's PPS changes. If systems are trained on EEG data recorded on several different days, the recognition results become almost robust regardless of the condition of the subjects.

The accuracy of recognition of PPS by EEG achieved in this paper is comparable to the level obtained by other researchers. The percentage of correct decisions for two-class identification ranges from 82 to 94% (depending on the PPS detected — "norm", alcohol intoxication, drowsiness, physical fatigue). For multiclass identification, the accuracy is several times lower. However, it is worth noting that accuracy is achieved when there are 25 test subjects in a training sample, which indicates a high potential for the convolution networks in this task.

It was also possible to obtain the following estimates of the accuracy of the two-class identification of tasks performed by the user on the computer (where the first class characterizes inactivity/rest when the EEG is recorded under standard conditions, the second one is one of the following tasks): reading scientific texts 92%; watching an entertainment video 98.72%; typing a text on the keyboard 77.8%. For multiclass identification, the accuracy drops to 59.21 per cent. It is the first time these results are obtained, and they can be used when it is necessary to automatically monitor the activity of subjects without the ability to directly observe them (for example, when taking examinations remotely).

Financial support

This work was supported by Russian Foundation for Basic Research, No. 18-41-550002.

References

1. Craik A., He Y., Contreras-Vidal J. L. Deep learning for electroencephalogram (EEG) classification tasks: a review. *Journal of Neural Engineering*, 2019, no. 3, vol. 16. doi:10.1088/1741-2552/ab0ab5
2. Sulavko A. E., Kuprik A. I., Starkov M. A., Stadnikov D. G. Analysis of methods for recognizing human images by the characteristics of electroencephalograms (Review). *Information Security Questions*, 2018, no. 4, pp. 36–46 (In Russian).
3. Vance A., Anderson B. B., Kirwan B. C., Eargle D. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 2014, vol. 15, no. 10, pp. 679–722. doi:10.17705/1jais.00375
4. Nigrey A. A., Zhumazhanova S. S., Sulavko A. E. Methods for automatic assessment of the psychophysiological state of a person according to the parameters of electroencephalograms (review). *Biomedical Radioelectronics*, 2020, no. 5, pp. 5–18 (In Russian).
5. Yazdani A., Setaterhdan S. K. Classification of EEG signal correlated with alcohol abusers. *Proceedings of the ISSPA Conference Sharjah UAE*, 2007. doi: 10.1109/ISSPA.2007.4555309
6. Bogomolov A. V., Gridin L. A., Kukushkin Yu. A., Ushakov I. B. *Diagnostika sostoyaniya cheloveka: matematicheskie podxody* [Diagnosis of human con-

dition: mathematical approaches]. Moscow, Medicina Publ., 2003. 464 p. (In Russian).

7. Schmitz A., Grillon C. Assessing fear and anxiety in humans using the threat of predictable and unpredictable aversive events (the NPU-threat test). *Nature Protocols*, 2012, pp. 527–532. doi:10.1038/nprot.2012.001
8. Suppiah R., Vinod A. P. Biometric identification using single channel EEG during relaxed resting state. *IET Biometrics*, 2018, vol. 7, pp. 342–348. doi:10.1049/iet-bmt.2017.0142
9. Deng L., Yu D. Deep learning: methods and applications. *Foundations and Trends in Signal Processing*, 2014, vol. 7, no. 3–4, pp. 197–387.
10. Yang H., Han J., Min K. A multi-column CNN model for emotion recognition from EEG signals. *Sensors*, 2019, vol. 19, iss. 21. doi:10.3390/s19214736
11. Armstrong B., Blondet M. R., Khalifian N., Kurtz K. J., Zhanpeng Jin, Laszlo S. Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP. *Neurocomputing*, 2015, vol. 166, pp. 59–67. doi:10.1016/j.neucom.2015.04.025
12. Ruiz-Blondet M. V., Zhanpeng Jin, Laszlo S. CEREBRE: A novel method for very high accuracy event-related potential biometric identification. *IEEE Transactions on Information Forensics and Security*, 2016, vol. 11, pp. 1618–1629. doi:10.1109/TIFS.2016.2543524
13. Goncharov S. M., Borshevnikov A. E. Neural network transformer "Biometry — access code" based on the electroencephalogram in modern cryptographic applications. *Vestnik SibGUTI*, 2016, no. 1, pp. 17–22. (In Russian).
14. Nguyen D., Tran D., Sharma D., Ma W. On the study of impacts of brain conditions on eeg-based cryptographic key generation systems. *Procedia Computer Science*, 2018, vol. 126, pp. 713–722.
15. Ogino M., Mitsukura Y. Portable drowsiness detection through use of a prefrontal single-channel electroencephalogram. *Sensors*, 2018, vol. 18, no. 12. doi:10.3390/s18124477
16. Zunhammer M., Eberle H., Eichhammer P., Busch V. Somatic symptoms evoked by exam stress in university students: the role of alexithymia, neuroticism, anxiety and depression. *PLOS One*, 2013, vol. 8, iss. 12, pp. 1–11.
17. Güntekin B., Basar E. A review of brain oscillations in perception of faces and emotional pictures. *Neuropsychologia*, 2014, pp. 33–51. doi:10.1016/j.neuropsychologia.2014.03.014
18. Antipov O. I., Zakharov A. V., Poverennova I. E., Neganov V. A., Erofeev A. E. Facilities of different methods of automatic recognition of sleep stages. *Saratov Journal of Medical Scientific Research*, 2012, vol. 8, no. 2, pp. 374–379 (In Russian).
19. Rajendra Acharya U., Eric Chern-Pin Chua, Kuang Chua, Lim Choo, Toshiyo Tamura. Analysis and automatic identification of sleep stages using higher order spectra. *International Journal of Neural Systems*, 2010, vol. 20, no. 6, pp. 509–530.
20. Zaharov E. S. Automated sleep stage recognition. *Izvestiya SFedU. Engineering sciences*, 2008, no. 5, pp. 117–120 (In Russian).
21. Tzimourta K. D., Tsoulos I. G., Bilero T., Tzallas A. T., Tsipouras M., Giannakeas N. Direct assessment of alcohol consumption in mental state using brain computer interfaces and grammatical evolution. *Inventions*, 2018, vol. 3, no. 3, 51 p. doi:10.3390/inventions3030051
22. Karungaru S., Yoshida T., Seo T., Fukumi M., Terada K. Monotonous tasks and alcohol consumption effects on the brain by EEG analysis using neural networks. *International Journal of Computational Intelligence and Applications*, 2012, vol. 11, no. 03. doi:10.1142/S1469026812500150
23. Sarraf J., Chakrabarty S., Pattnaik P. K. EEG based oscitancy classification system for accidental prevention. *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, 2017, pp. 235–243. doi:10.1007/978-981-10-3156-4_24
24. Thangarajah V., Denshiya D. A., Senaka A., Jayalath E. BCI-based alcohol patient detection. *17th World Congress of International Fuzzy Systems Association and 9th International Conference on Soft Computing and Intelligent*, 2017. doi:10.1109/IFSA-SCIS.2017.8305564
25. Ziya E., Akif A., Mehmet R. B. The classification of EEG signals recorded in drunk and non-drunk people. *International Journal of Computer Applications*, 2013, vol. 68, no. 10, pp. 40–44.
26. Yazdani A., Ataee P., Setarehdan K., Araabi B. N., Lucas C. Neural, fuzzy and neurofuzzy approach to classification of normal and alcoholic electroencephalograms. *Proceedings of the 5th International Symposium on Image and Signal Processing and Analysis*, 2007. doi:10.1109/ISPA.2007.4383672
27. Shuaifang Wang, Yan Li, Pen Wen, Guohun Zhu. Analyzing EEG signals using graph entropy based principle component analysis and J48 decision tree. *International Journal of Signal Processing Systems*, 2016, vol. 4, no. 1, pp. 67–72. doi:10.12720/ijsps.4.1.67-72

УДК 004.93'1
doi:10.31799/1684-8853-2020-6-37-49

Оценка идентификационного потенциала электроэнцефалограмм с использованием статистического подхода и сверточных нейронных сетей

А. Е. Сулавко[а], канд. техн. наук, доцент, orcid.org/0000-0002-9029-8028, sulavich@mail.ru
П. С. Ложников[а], доктор техн. наук, доцент, orcid.org/0000-0001-7878-1976
А. Г. Чобан[а], студент, orcid.org/0000-0003-1834-6651
Д. Г. Стадников[а], студент, orcid.org/0000-0002-5405-2450
А. А. Нигрей[б], аспирант, orcid.org/0000-0002-8391-5374
Д. П. Иниватов[а], студент, orcid.org/0000-0001-9911-1218
[а]Омский государственный технический университет, Мира пр., 11, Омск, 644050, РФ
[б]Омский государственный университет путей сообщения, К. Маркса пр., 35, Омск, 644046, РФ

Введение: электроэнцефалограммы содержат информацию об индивидуальных особенностях работы мозга и психофизиологическом состоянии субъекта. **Цель исследования:** оценить идентификационный потенциал электроэнцефалограмм; разработать методы идентификации личности и психофизиологического состояния субъектов, а также действий пользователя, выполняемых на компьютере, по электроэнцефалограмме с использованием аппарата сверточных нейронных сетей. **Результаты:** оценена информативность ритмов электроэнцефалограмм с точки зрения возможности идентификации человека и его состояния. Достигнута высокая точность идентификации личности (98,5–99,99 % для 10 электродов, 96,47 % для двух электродов Fp1 и Fp2) при низком времени прохода (2–2,5 с). Обнаружено существенное падение точности идентификации, если на этапе обучения и тестирования сети субъект находился в разных психофизиологических состояниях. (В ранних исследованиях данному аспекту уделялось недостаточно внимания.) Предложен способ повышения робастности распознавания личности в измененных состояниях. Достигнута точность 82–94 % при распознавании состояний алкогольного опьянения, сонливости, физической усталости и 77,8–98,72 % при распознавании действий пользователя (чтение, набор текста, просмотр видео). **Практическая значимость:** результаты будут востребованы в приложениях информационной безопасности и удаленного мониторинга субъектов (при отсутствии возможности непосредственно наблюдать за ними).

Ключевые слова — глубокое обучение, многослойные нейронные сети, биометрия, машинное обучение, извлечение признаков, электрическая активность мозга, психофизиологическое состояние, распознавание образов, спектрограммы.

Для цитирования: Sulavko A. E., Lozhnikov P. S., Choban A. G., Stadnikov D. G., Nigrey A. A., Inivatov D. P. Evaluation of EEG identification potential using statistical approach and convolutional neural networks. *Информационно-управляющие системы*, 2020, № 6, с. 37–49. doi:10.31799/1684-8853-2020-6-37-49

For citation: Sulavko A. E., Lozhnikov P. S., Choban A. G., Stadnikov D. G., Nigrey A. A., Inivatov D. P. Evaluation of EEG identification potential using statistical approach and convolutional neural networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 37–49. doi:10.31799/1684-8853-2020-6-37-49

В опубликованную статью Зотин А. Г., Фаворская М. Н. Применение штрихкодирования для цифрового маркирования видеопоследовательностей на основе частотных преобразований, 2020, № 5, авторы вносят дополнение.

Финансовая поддержка

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 19-07-00047 А.

UDC 57.087.1::616-006.4
doi:10.31799/1684-8853-2020-6-50-59

Building and evaluation of bioinformatic pipeline for determination of clonal profiles in myelodysplastic syndrome

D. S. Bug[a]***,*** *M. D., orcid.org/0000-0002-5849-1311, dmitriybs@1spbgmu.ru*
A. A. Prikhodko[a]***,*** *Student, orcid.org/0000-0002-0001-7932*
E. A. Bakin[a,b]***,*** *PhD, Tech., Associate Professor, orcid.org/0000-0002-5694-4348*
A. V. Tishkov[a]***,*** *PhD, Phys.-Math., Associate Professor, orcid.org/0000-0002-4282-8717*
N. V. Petukhova[a]***,*** *PhD, Biol., orcid.org/0000-0001-6397-824X*
I. M. Barkhatov[a]***,*** *PhD, Med., orcid.org/0000-0002-8000-3652*
E. V. Morozova[a]***,*** *PhD, Med., Associate Professor, orcid.org/0000-0002-9605-485X*
I. S. Moiseev[a]***,*** *Dr. Sc., Med., Associate Professor, orcid.org/0000-0002-4332-0114*
[a]*Pavlov First Saint Petersburg State Medical University, 6-8, L'va Tolstogo St., 197022, Saint-Petersburg, Russian Federation*
[b]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*

Introduction: *There is growing evidence of a connection between tumor clonal profile and its clinical impact. However, there is a lack of a feasible and reliable method for clonal profiling in actual clinical practice. Myelodysplastic syndrome is a clonal hematopoietic stem cell disorder characterized by morphological dysplasia, cytopenia and a high risk of evolution to acute myeloid leukemia. The clinical outcome of myelodysplastic syndrome is greatly heterogeneous; therefore, specific examination of clonal profiles is needed to resolve the prognosis of patients with such complex disorders.* ***Purpose:*** *Development of a pipeline specifically for determining the clonal profiles in patients with myelodysplastic syndrome on the basis of target next-generation sequencing data.* ***Results:*** *The pipeline was developed and evaluated on a set of 35 patients with high-risk myelodysplastic syndrome. It is possible to use the target sequencing data in order to assess the heterogeneity of clonal profiles and characterize their genetic features. This approach allows you to identify the consistency between a specific individual profile and the disease prognosis, which can be critical for the treatment decision. Herein, the characterization and analysis of clonal profiles are presented.* ***Practical relevance:*** *The information about relation patterns between clonal profile characteristics (number of subclones, mutations-per-clone rate) and clinical outcome can be used by doctors in current practice for a more accurate therapy selection depending on the identified individual specificity of the disease.*

Keywords *— myelodysplastic syndrome, bioinformatics pipeline, clonal profile, primary mutation, subclone, target sequencing, next-generation sequencing.*

For citation: Bug D. S., Prikhodko A. A., Bakin E. A., Tishkov A. V., Petukhova N. V., Barkhatov I. M., Morozova E. V., Moiseev I. S. Building and evaluation of bioinformatic pipeline for determination of clonal profiles in myelodysplastic syndrome. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 50–59. doi:10.31799/1684-8853-2020-6-50-59

Introduction

Adult myelodysplastic syndrome (MDS) occurs as a result of the gradual accumulation of somatic mutations [1]. A set of cells derived from a mutated cell is called a clone. Subclones arise from a primary clone (so-called subclones) in the process of acquiring new somatic mutations (tumor progression, clonal evolution), therefore, they are also considered as clones. To predict the tumor development pathway, it is essential to characterize the clone with its subclones [2].

Each clone is defined by its unique mutational profile providing to trace the relation between clone genotype and prognosis of the disease. The presence of subclones with driver mutations in oncogenes has been shown to negatively affect the outcome of the disease in case of chronic lymphocytic leukemia [3]. A correlation between a large number of subclones and an unfavorable prognosis was identified in lung, breast, prostate, kidney tumors, as well as low-grade glioma [4–6].

One of the main approaches of next-generation sequencing (NGS) is targeted sequencing (TS) method focused on specific genes panel in order to determine the current mutation load. High precision, relatively low cost, multiple genes analysis at once are the main advantages of TS. However, there are some technical issues associated with the implementation of this technique in actual clinical practice: lack of verification methods and standard pipelines for analysis of sequencing data, a need to adapt for particular diseases. TS method used with additional bioinformatic tools could be helpful in clonal profile deduction.

Thus, the purpose of present work is to build an analytical pipeline using modern bioinformatic tools specifically adapted for determination of the clonal profiles in patients with MDS on the basis of TS. Such evaluation might help to derive the relation and corresponding patterns between the number and the genotype of subclones, and subsequent disease prognosis.

Materials and methods

1. **Group selection.**

Next-generation sequencing of 35 patients with high-risk MDS was performed (Table 1) [7].

2. **DNA sequencing.**

Genomic DNA was extracted from bone marrow using TriZ reagent extraction Kit (Inogene, Russia) and stored at −80 °C. The quality of the samples was analyzed with Qubit 4.0 (Thermo Fisher, CA, USA). The libraries for target sequencing of the genes were prepared using KAPA HyperPlus Kit (Roche, Switzerland). The enrichment of targeted genome sequences was performed using SeqCap EZ Target Enrichment System (Roche, Switzerland). Sequencing was performed by MiSeq benchtop sequencer using MiSeq Reagent Kits v2 (Illumina, USA).

■ ***Table 1***. Characteristics of patients before and after filtering of germinal and false positive variants

Parameter	Value	
	before filtering	after filtering
Age median (interval), years	49 (18–80)	46,4 (18–80)
Male/female	21/14	16/11
After bone marrow transplant	25 (71,4%)	20 (74,1%)
Secondary MDS (after prior chemo- or radiotherapy)	5 (14,3%)	5 (18,5%)
Diagnosis		
5q deletion	1 (2,9%)	1 (3,7%)
Excess of blasts I	13 (37,1%)	10 (37,0%)
Excess of blasts II	19 (54,3%)	14 (51,9%)
Multilineage dysplasia	2 (5,7%)	2 (7,4%)
Risk according to IPSS-R		
Very low	0	0
Low	1 (2,9%)	1 (37%)
Intermediate	5 (14,3%)	4 (14,8%)
High	15 (42,8%)	12 (33,3%)
Very high	14 (40,0%)	13 48,1%)

3. **Data preprocessing.**

The quality of sequencing reads was analyzed using FastQC (http://www.bioinformatics.babraham.ac.uk/projects/fastqc/); adapters were eliminated by Trimomatic 0.39 [8].

4. **Alignment, analysis and generation of the detected variants list.**

Bioinformatic analysis was performed according to the GATK-4 manual [9], with alignment to the GRCh38 version of the human genome using BWA 0.7.17 [10], and determination of somatic variants was accomplished with Mutect2 4.1.5.0 [11]. The resulting list of variants was annotated using Ensemble Variant Effect Predictor 99 [12] and ANNOVAR [13].

The custom scripts used in the analysis on the basis of GATK Best Practices pipelines, were deposited to the Github portal (https://github.com/bugds/BashGATK). Parallelization was performed using GNU Parallel [14].

5. **Filtering of the germinal variants.**

When analyzing the identified gene variants, we excluded those variants whose frequency in different populations according to GnomAD [15] exceeds 1%, and the allelic load (taking into account the chimerism) was in the range of 30–70% and 90–100% [16].

6. **Removing false positives.**

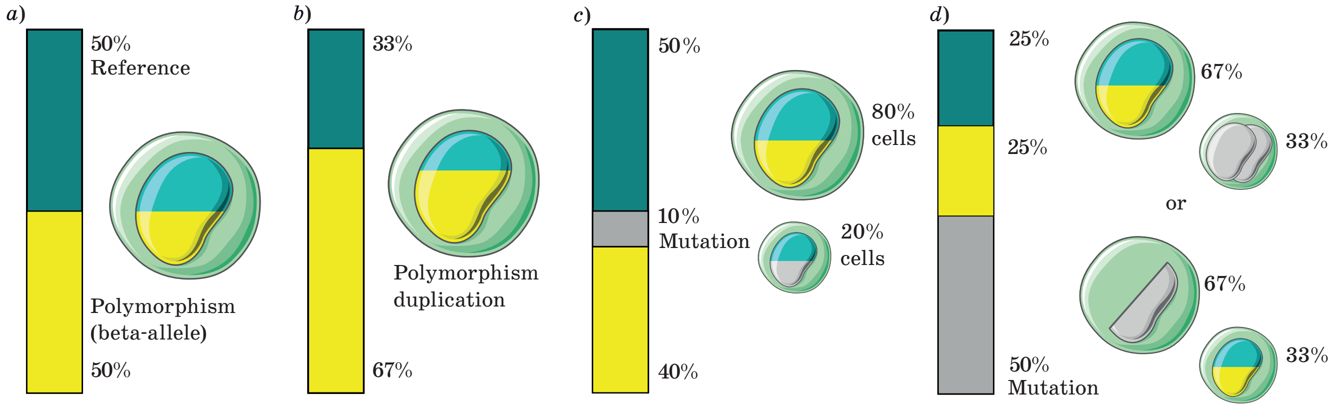
Variants not filtered by Mutect2 were not taken into account. Additionally, variants found in two or more samples with the same allelic load were removed from the analysis that indicate a direct sign of mispriming [17].

Samples were removed from the analysis in cases where less than two variants remained as a result of filtering (the study of tumor progression is based on comparing allelic loads of variants and is possible only if there are two or more variants). Finally, 27 patient samples remained in the study (see Table 1).

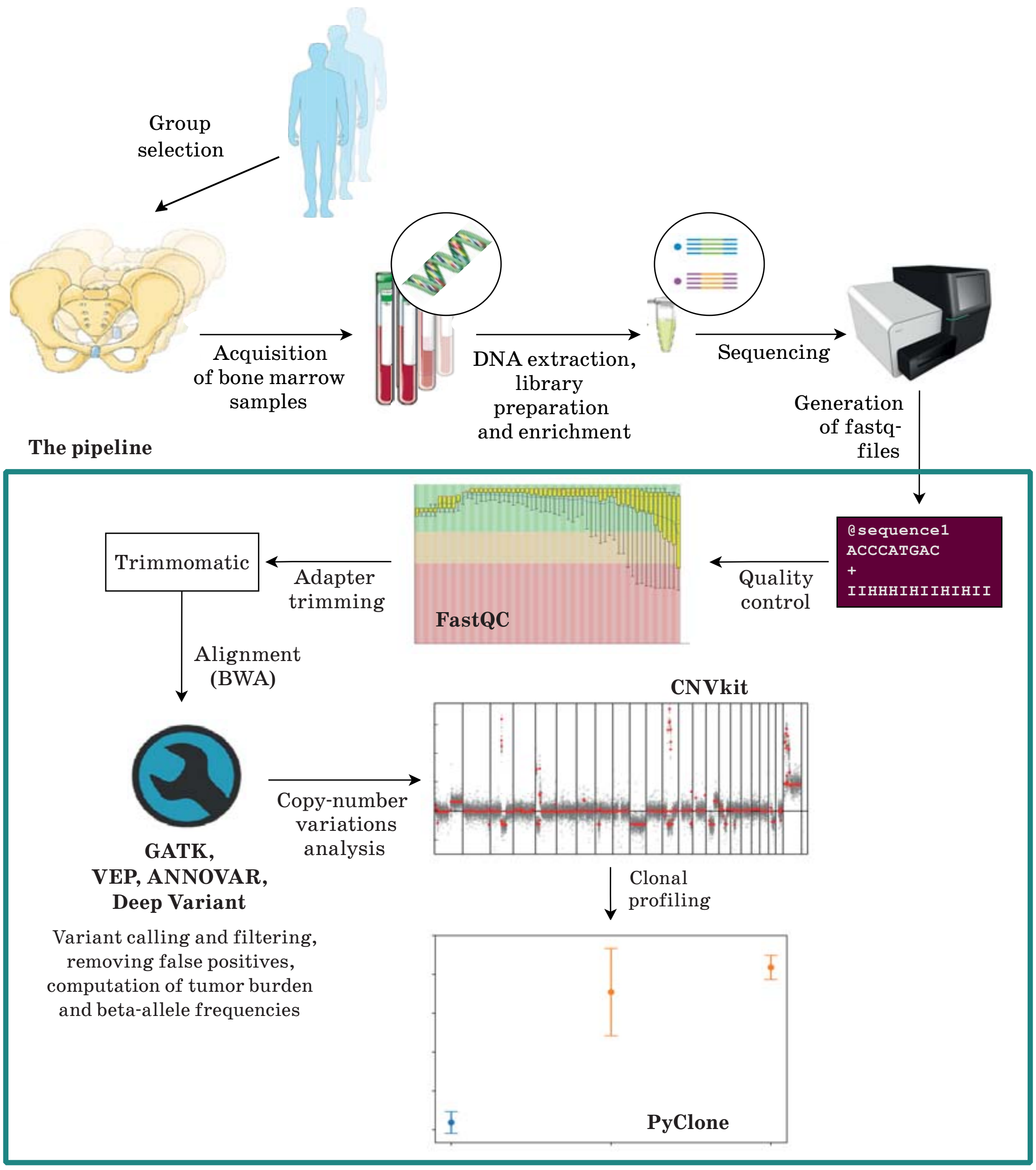
7. **Computation of tumor burden and beta-allele frequencies.**

Beta-alleles are the polymorphisms detected during sequencing (Fig. 1, *a*). Their allelic load must be taken into account when calculating copy-number variations (see point 8): for instance, a germinal variant in a heterozygous state with an allelic load of about 33 or 67% indicates a duplication of this region (Fig. 1, *b*). The Deep Variant 0.10.0 software tool was used to determine polymorphisms [18].

In each sample, variants with the maximum allelic load were identified — they are primary, and approximately reflect the proportion of tumor cells in the sample. In this case, we assume that the variants with the maximum allelic frequency in each sample are not located in the regions of the genome with a copy-number variation (insertions and deletions), and are also heterozygous. In this case, the pro-



■ *Fig. 1.* Compliance between the allelic load detected during sequencing (columns) and the genotype configuration in normal (*a*), with polymorphism duplication (*b*), the presence of a mutation in 20% of cells (*c*) and the 50% allelic load of the mutation (*d*)



```
@sequence1
ACCCATGAC
+
IIHHHIHIIHIHII
```

■ *Fig. 2.* The workflow of clonal profiling portion of tumor cells can be calculated as the double number of variant allelic loads (Fig. 1, *c*). Cases where variants with maximum loads are located in regions of the genome with copy-number variation require high-attention. For example, if a variant is found in 50% of the reads, this may indicate both a 100% tumor load and the above phenomena associated with a copy-number variation (Fig. 1, *d*). Similar phenomena can be suspected when studying allelic loads of the other variants found in the same sample. They were analyzed manually, and if interpretation was not possible, they were excluded (it was considered that there is copy-number variation when identifying stable change of reading depth in the region with an allele mutation with the maximum frequency, and the mutation with the maximum allelic frequency cannot be considered primary).

8. **Copy-number variations analysis.**

To determine the copy-number variation, CNVkit 0.9.5 was used, an algorithm that utilizes both target gene reads and non-specifically captured non-target reads to identify the copy-numbers evenly across the entire genome [19]. This tool has a relatively high accuracy [20] and is designed specifically for detecting acquired copy-number variation together with TS. To study somatic insertions and deletions, it is necessary to take into account the proportion of tumor cells in the sample determined at the previous stage (see point 7). The copy-number is calculated by comparing the reading depth in certain positions in the control and pathological samples, taking into account the proportion of tumor cells and the size of the beta allele. In CNVkit, a pooled or single reference can be used as a reference material. In this study, the usage of a sample with more than 99% chimerism and a normal karyotype was chosen as a reference, which corresponds to complete cytogenetic remission taken from a patient 4 weeks after bone marrow transplantation.

9. **Clonal profiling.**

PyClone 0.13.1 software tool was used to determine the clonal profiles [21] — the algorithm performs Bayesian clustering method to group somatic mutations into assumed clonal clusters with an assessment of their cellular prevalence (the proportion of affected cells) and taking into account the allelic imbalances introduced by copy-number variations and contamination of normal cells.

The complete workflow of analysis is presented in Fig. 2.

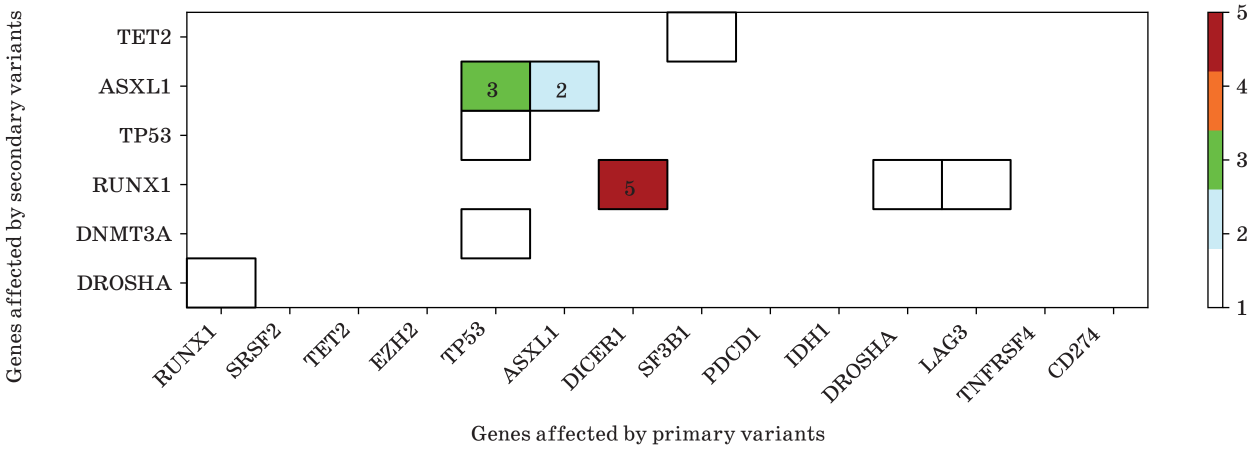
Results

The whole analysis took 7 hours 2 minutes (Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz, 32G).

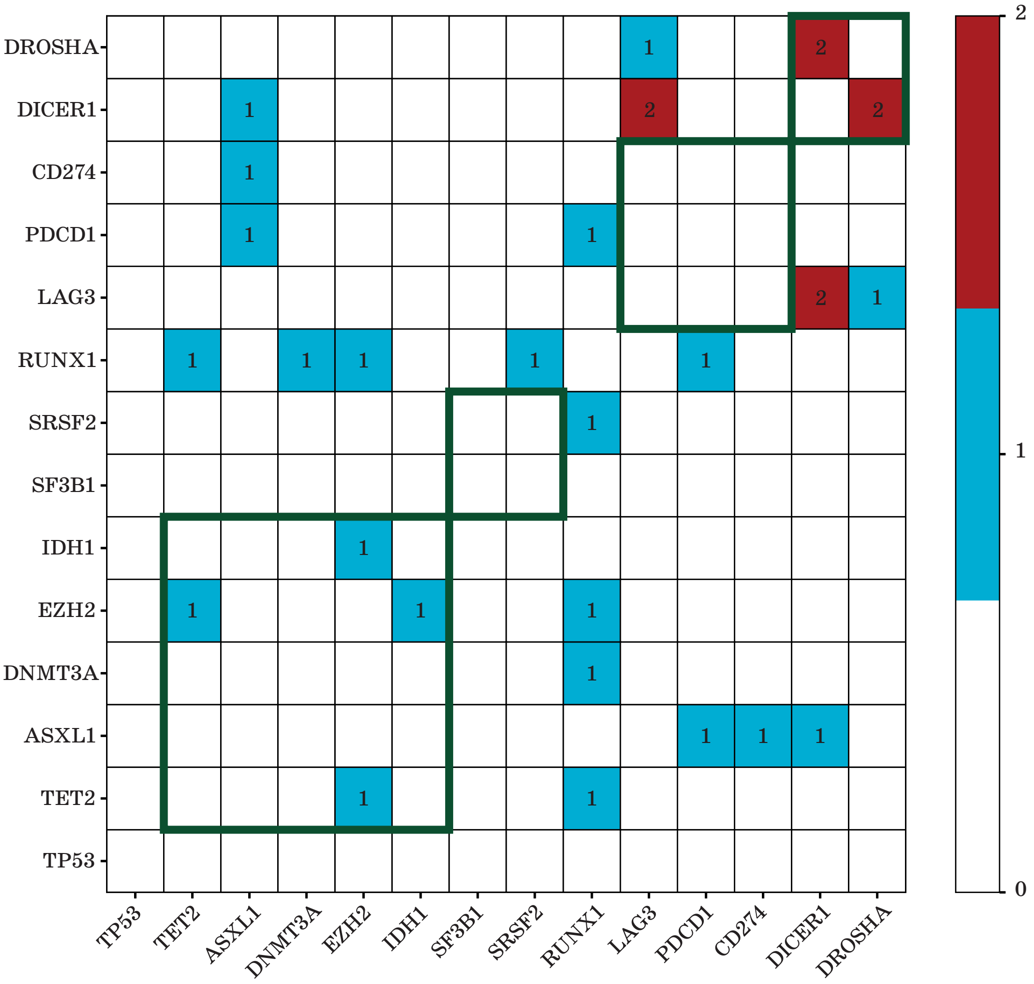
Under the analysis, one of the main issues was the lack of an out-of-the-box tool for reformatting the CNVkit output format into the one suitable for PyClone. However, our pipeline avoids the majority of such complications by using a single package (GATK) for the most part of the analysis.

Mutational profiles of the patients were derived in form of tables; each variant was annotated with its original allele frequency, the calculated tumor load (i. e. a fraction of cells where this variant was observed), the standard deviation of the tumor load, and the cluster-ID that included the variant itself, based on the calculated tumor burden. Two matrices were obtained based on the patients' clonal profiles: one, depicting the co-occurrence of primary and secondary variants from the genes perspective (Fig. 3), and another, describing genes affected by mutations in the same clusters (Fig. 4).

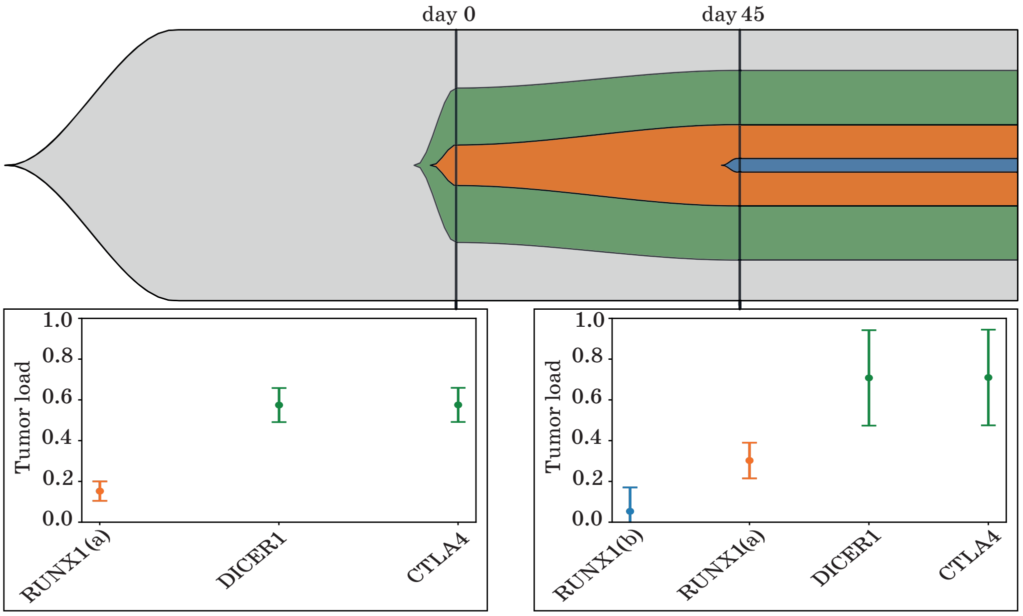
The dynamics of tumor progression was described for a patient, who was sequenced twice with samples taken in 45 days (Fig. 5 [22]). A subclone with *RUNX1* mutation overcame the detection



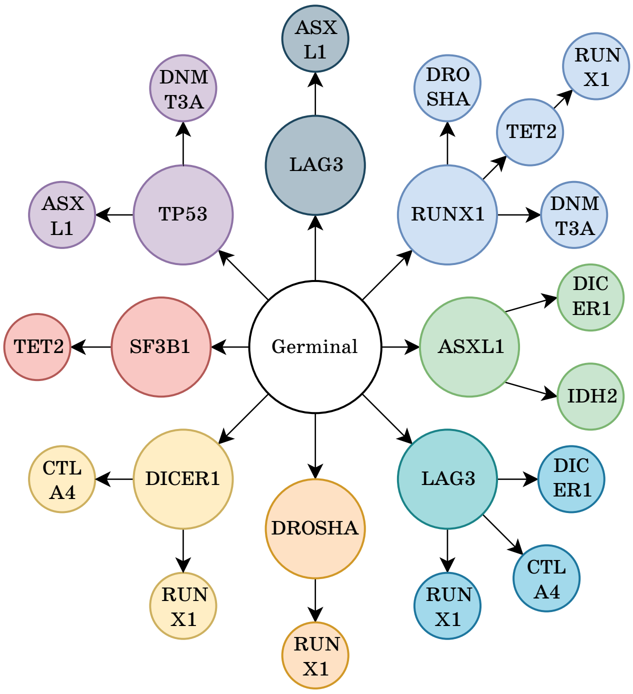
■ ***Fig. 3.*** Matrix of co-occurrence of primary and secondary gene variants. The numbers *1–5* of such events are differentiated by colors



■ ***Fig. 4.*** Matrix of co-occurrence of gene variants in the same clusters. The numbers *0–2* of identified clusters with a certain combination of variants are represented by different colors. Combinations of variants affecting genes of a single functional group are marked by bold frames



■ ***Fig. 5.*** Dynamics of tumor progression



■ ***Fig. 6.*** Schematic representation of all possible paths of tumor progression for variants with >10% load discovered across all analyzed samples

threshold, and two other clones identified previously have grown.

Discovered paths of tumor progression were plotted (Fig. 6). Moving along the arrows depicts acquiring a mutation in a specific gene by a clone. The diagram demonstrates all variants of tumor progression that may be inferred from the observable clonal profiles.

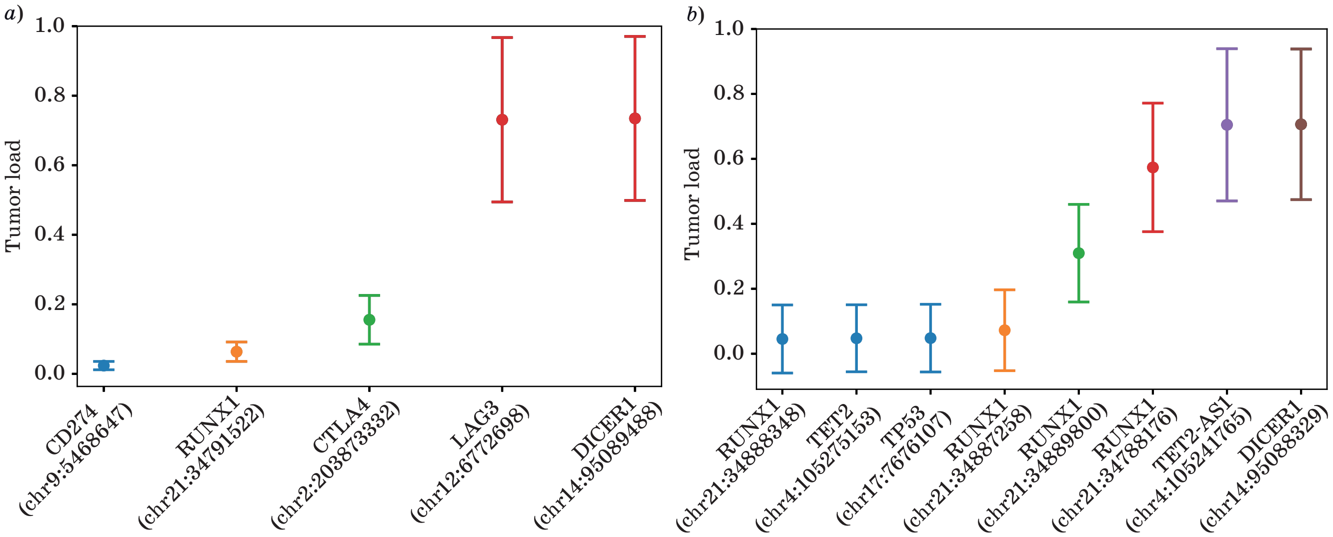
Discussion

We have developed and tested the pipeline for clonal profiles determination in patients with MDS. It is advantageous to identify the correlation between the clonal profile, their genotypic features and disease prognosis, that has been effectively demonstrated for other pathologies [3–6].

Genotypes of clones and subclones were plotted (Fig. 7). Whiskers indicate the standard deviation of tumor burden of a certain variant. The color of a mark shows the affiliation to a specific cluster (clone or subclone). Genes affected by a variant and its genomic position in chromosomes are marked on a horizontal axis.

Five mutations were found in the same sample (Fig. 7, *a*) herewith two variants (in *LAG3*, *DICER1* genes) grouped in a single cluster. This fact, considering their high tumor load (> 50%), can be interpreted as their coexistence in the same cells. Otherwise, such a clonal profile would only be observed if the mutation occurs again in the same position, which is highly improbable.

In the other case (Fig. 7, *b*), eight mutations were discovered in genes: *DICER1*, *TET2-AS1*, *RUNX1*, *TP53*, and *TET2*. Probably, the variant present in the largest number of cells (marked brown, mutation in *DICER1*) occurred almost simultaneously with the mutation in *TET2-AS1*, which led to the neoplasm formation. Then, all the other variants developed within the proliferating tumor. Three mutations located in the same cluster (marked in blue) appeared in a small fraction of cells, thereby having relatively low clonal load, and therefore, their coexistence and contribution to the current clinical course is questionable. Such variants probably in-



■ ***Fig. 7.*** The clonal profiling of the variants detected in particular patients: *a* — a probe with five mutations in fore clusters; *b* — another probe with eight mutations in six clusters dicate the possibility of new subclones genesis, and the diversification of a further clonal population within the existing tumor.

Matrix of primary and secondary mutations (see Fig. 3) shows that the primary mutations mostly developed in *DICER1*, *TP53*, and *ASXL1* among the examined samples. It is in compliance with the well-known fact that *ASXL1* gene is frequently affected primarily in patients with MDS [23]. A clonal evolution path with *TP53* as a driver mutation was also described [24]. *RUNX1* and *ASXL1* lesions were the most frequent among the secondary mutations.

Matrix of variants co-occurring in the same clusters (see Fig. 4) illustrates the lack of coexistence of mutations in genes of common biological function: different splicing genes (*SRSF2*, *SF3B1*), immune response genes (*LAG3*, *PDCD1*, *CD274*), which corresponds to the common trend of negative cooperativity where functionally similar genes are rarely affected together [25]. However, we have identified inconsistencies of such tendency: mutations in genes of microRNA processing (*DICER1*, *DROSHA*) appeared in the same clusters. Additionally, it is true for genes of epigenetic regulation (*TET2*, *ASXL1*, *EZH2*, *DNMT3A*, and *IDH1*), that was also observed in another research [23]. Such distinguishing tendencies might be related to the interdependent participation of these genes in the same biological pathway. It should be noted that the cluster variants with the lowest tumor burden (up to 10%) and duplicated probes were omitted from the resulting matrices, since their mutational load is comparable with the size of a method error [16].

One of the main potential applications of the tumor subclones identification and characterization is the monitoring of their size and genetic features in dynamics. Fig. 5 demonstrates an example of a negative tendency for disease progression where the growth of a primary clone and its subclone led to the emergence of another subclone.

For more reliable identification and subsequent exclusion of irrelevant polymorphisms from the list of detected variants, matching control material can be sequenced for each patient using tissue with a germinal genotype. This could also improve the copy-number variations calling as both tumor and normal genotype files can be introduced to CNVkit.

In some cases the tumor load can be evaluated by tissue morphology (in case of solid tumors) or flow cytometry: this would be beneficial to avoid the assumptions about the maximum allele frequency being indicative which were included when determining the tumor load using only NGS data: we hypothesized this indicative variant is heterozygous and not affected by indels (in the absence of obvious signs of the opposite).

■ ***Table 2.*** Comparison of TS and WGS requirements

Platform	Cost (per sample, USD)	Depth	Data size (processed bam)
WGS	1000–3000	30–60	Depending on coverage ~60–350 GB
WES	500–2000	150–200	Depending on coverage ~5–20 GB
TS	300–1000	200–1000	Varies by panel size and coverage ~0.1–5 GB

The importance of subclones in tumor development has also been proven in other studies. In case of ovarian cancer heterogeneous clonal profiles of metastases led to different courses of tumor progression in each metastasis, which caused poor response to immunotherapy, limiting treatment options [26]. Clonal structure in MDS was also described earlier [1], but both papers imply the methods yet unavailable in clinical practice. In another study, clonal architecture of prostate cancer was reconstructed by different methods, and PyClone was shown to be appropriate in this case [27]. For their turn, we have demonstrated the suitability of computational methods in MDS, endorsing this technique and its beneficial prognostic value into clinical practice.

PyClone uses beta-binomial distribution to model mutation frequencies. There are alternatives: PhyloWGS [28] and DPClust [29] based on binomial distribution; but these tools were shown to be not applicable in all cases [27]: DPClust failed with the rate of 3.1% due to excessive computational memory (more than 250 GB), and PhyloWGS demanded inordinate runtime (more than 3 months). On the contrary, PyClone successfully completes all samples in the same study, which was confirmed by our work.

Moreover, the majority of these tools request data from the whole genome or exome sequencing (WGS, WES), which greatly exceeds the storage and computational resources needed for the same analysis performed with TS (Table 2 [30]).

In conclusion, the analysis of the clonal structure, being a modern trend in predicting the outcomes of tumors, is of highest importance for the prognosis and the selection of treatment, which establishes the relevance for pipeline development in case of MDS and other clonal diseases.

The authors have no conflicts of interest.

Financial support

This work was supported by the Russian Science Foundation under the grant No. 17-75-20145-П from 03.08.2020 “Search for potential therapeutic targets and biological prognostic factors in patients with myelodysplastic syndrome”.

References

1. Nagata Y., Makishima H., Kerr C. M., Przychodzen B. P., Aly M., Goyal A., Awada H., Asad M. F., Kuzmanovic T., Suzuki H., Yoshizato T., Yoshida K., Chiba K., Tanaka H., Shiraishi Y., Miyano S., Mukherjee S., LaFramboise T., Nazha A., Sekeres M. A., Radivoyevitch T., Haferlach T., Ogawa S., Maciejewski J. P. Invariant patterns of clonal succession determine specific clinical features of myelodysplastic syndromes. *Nature Communications*, 2019, vol. 10, no. 1, p. 5386. doi:10.1038/s41467-019-13001-y
2. Montalban-Bravo G., Takahashi K., Patel K., Wang F., Xingzhi S., Nogueras G. M., Huang X., Pierola A. A., Jabbour E., Colla S., Gañan-Gomez I., Borthakur G., Daver N., Estrov Z., Kadia T., Pemmaraju N., Ravandi F., Bueso-Ramos C., Chamseddine A., Konopleva M., Zhang J., Kantarjian H., Futreal A., Garcia-Manero G. Impact of the number of mutations in survival and response outcomes to hypomethylating agents in patients with myelodysplastic syndromes or myelodysplastic/myeloproliferative neoplasms. *Oncotarget*, 2018, vol. 9, no. 11, pp. 9714–9727. doi:10.18632/oncotarget.23882
3. Landau D. A., Carter S. L., Stojanov P., McKenna A., Stevenson K., Lawrence M. S., Sougnez C., Stewart C., Sivachenko A., Wang L., Wan Y., Zhang W., Shukla S. A., Vartanov A., Fernandes S. M., Saksena G., Cibulskis K., Tesar B., Gabriel S., Hacohen N., Meyerson M., Lander E. S., Neuberg D., Brown J. R., Getz G., Wu C. J. Evolution and impact of subclonal mutations in chronic lymphocytic leukemia. *Cell*, 2013, vol. 152, no. 4, pp. 714–726. doi:10.1016/j.cell.2013.01.019
4. Andor N., Graham T. A., Jansen M., Xia L. C., Aktipis C. A., Petritsch C., Ji H. P., Maley C. C. Pan-cancer analysis of the extent and consequences of intratumor heterogeneity. *Nature Medicine*, 2016, vol. 22, no. 1, pp. 105–113. doi:10.1038/nm.3984
5. Morris L. G. T., Riaz N., Desrichard A., Şenbabaoğlu Y., Hakimi A. A., Makarov V., Reis-Filho J. S., Chan T. A. Pan-cancer analysis of intratumor heterogeneity as a prognostic determinant of survival. *Oncotarget*, 2016, vol. 7, no. 9, pp. 10051–10063. doi:10.18632/oncotarget.7067
6. Zhang J., Fujimoto J., Zhang J., Wedge D. C., Song X., Zhang J., Seth S., Chow C.-W., Cao Y., Gumbs C., Gold K. A., Kalhor N., Little L., Mahadeshwar H., Moran C., Protopopov A., Sun H., Tang J., Wu X., Ye Y., William W. N., Lee J. J., Heymach J. V., Hong W. K., Swisher S., Wistuba I. I., Futreal P. A. Intratumor heterogeneity in localized lung adenocarcinomas delineated by multiregion sequencing. *Science*, 2014, vol. 346, no. 6206, pp. 256–259. doi:10.1126/science.1256930
7. Tsvetkov N. Yu., Morozova E. V., Barkhatov I. M., Moiseev I. S., Barabanshchikova M. V., Tishkov A. V., Bug D. S., Petukhova N. V., Izmailova E. A., Bondarenko S. N., Afanasyev B. V. Prognostic value of next-generation sequencing data in patients with myelodysplastic syndrome. *Clinical Oncohematology*, 2020, vol. 13, no. 2, pp. 170–175 (In Russian). doi:10.21320/2500-2139-2020-13-2-170-175
8. Bolger A. M., Lohse M., Usadel B. Trimmomatic: a flexible trimmer for Illumina sequence data. *Bioinformatics*, 2014, vol. 30, no. 15, pp. 2114–2120. doi:10.1093/bioinformatics/btu170
9. Poplin R., Ruano-Rubio V., DePristo M. A., Fennell T. J., Carneiro M. O., Van der Auwera G. A., Kling D. E., Gauthier L. D., Levy-Moonshine A., Roazen D., Shakir K., Thibault J., Chandran S., Whelan C., Lek M., Gabriel S., Daly M. J., Neale B., MacArthur D. G., Banks E. Scaling accurate genetic variant discovery to tens of thousands of samples. *Genomics*, 2017. doi:10.1101/201178
10. Li H., Durbin R. Fast and accurate short read alignment with Burrows — Wheeler transform. *Bioinformatics*, 2009, vol. 25, no. 14, pp. 1754–1760. doi:10.1093/bioinformatics/btp324
11. Benjamin D., Sato T., Cibulskis K., Getz G., Stewart C., Lichtenstein L. Calling somatic snvs and indels with mutect2. *Bioinformatics*, 2019. doi:10.1101/861054
12. McLaren W., Gil L., Hunt S. E., Riat H. S., Ritchie G. R. S., Thormann A., Flicek P., Cunningham F. The ensembl variant effect predictor. *Genome Biology*, 2016, vol. 17, no. 1, p. 122. doi:10.1186/s13059-016-0974-4
13. Wang K., Li M., Hakonarson H. ANNOVAR: functional annotation of genetic variants from high-throughput sequencing data. *Nucleic Acids Research*, 2010, vol. 38, no. 16, pp. e164–e164. doi:10.1093/nar/gkq603
14. Tange O. Gnu parallel-the command-line power tool. *The USENIX Magazine*, 2011, vol. 36, no. 1, pp. 42–47.
15. Genome Aggregation Database Consortium. Karczewski K. J., Francioli L. C., Tiao G., Cummings B. B., Alföldi J., Wang Q., Collins R. L., Laricchia K. M., Ganna A., Birnbaum D. P., Gauthier L. D., Brand H., Solomonson M., Watts N. A., Rhodes D., Singer-Berk M., England E. M., Seaby E. G., Kosmicki J. A., Walters R. K., Tashman K., Farjoun Y., Banks E., Poterba T., Wang A., Seed C., Whiffin N., Chong J. X., Samocha K. E., Pierce-Hoffman E., Zappala Z.,

O'Donnell-Luria A. H., Minikel E. V., Weisburd B., Lek M., Ware J. S., Vittal C., Armean I. M., Bergelson L., Cibulskis K., Connolly K. M., Covarrubias M., Donnelly S., Ferriera S., Gabriel S., Gentry J., Gupta N., Jeandet T., Kaplan D., Llanwarne C., Munshi R., Novod S., Petrillo N., Roazen D., Ruano-Rubio V., Saltzman A., Schleicher M., Soto J., Tibbetts K., Tolonen C., Wade G., Talkowski M. E., Neale B. M., Daly M. J., MacArthur D. G. The mutational constraint spectrum quantified from variation in 141,456 humans. *Nature*, 2020, vol. 581, no. 7809, pp. 434–443. doi:10.1038/s41586-020-2308-7

16. Judkins T., Leclair B., Bowles K., Gutin N., Trost J., McCulloch J., Bhatnagar S., Murray A., Craft J., Wardell B., Bastian M., Mitchell J., Chen J., Tran T., Williams D., Potter J., Jammulapati S., Perry M., Morris B., Roa B., Timms K. Development and analytical validation of a 25-gene next generation sequencing panel that includes the BRCA1 and BRCA2 genes to assess hereditary cancer risk. *BMC Cancer*, 2015, vol. 15, no. 1, p. 215. doi:10.1186/s12885-015-1224-y
17. McCall C. M., Mosier S., Thiess M., Debeljak M., Pallavajjala A., Beierl K., Deak K. L., Datto M. B., Gocke C. D., Lin M.-T., Eshleman J. R. False positives in multiplex pcr-based next-generation sequencing have unique signatures. *The Journal of Molecular Diagnostics*, 2014, vol. 16, no. 5, pp. 541–549. doi:10.1016/j.jmoldx.2014.06.001
18. Poplin R., Chang P.-C., Alexander D., Schwartz S., Colthurst T., Ku A., Newburger D., Dijamco J., Nguyen N., Afshar P. T., Gross S. S., Dorfman L., McLean C. Y., DePristo M. A. A universal SNP and small-indel variant caller using deep neural networks. *Nature Biotechnology*, 2018, vol. 36, no. 10, pp. 983–987. doi:10.1038/nbt.4235
19. Talevich E., Shain A. H., Botton T., Bastian B. C. Cnvkit: genome-wide copy number detection and visualization from targeted dna sequencing. *PLoS Computational Biology*, 2016, vol. 12, no. 4, p. e1004873. doi:10.1371/journal.pcbi.1004873
20. Soong D., Stratford J., Avet-Loiseau H., Bahlis N., Davies F., Dispenzieri A., Sasser A. K., Schecter J. M., Qi M., Brown C., Jones W., Keats J. J., Auclair D., Chiu C., Powers J., Schaffer M. CNV Radar: an improved method for somatic copy number alteration characterization in oncology. *BMC Bioinformatics*, 2020, vol. 21, no. 1, p. 98. doi:10.1186/s12859-020-3397-x
21. Roth A., Khattra J., Yap D., Wan A., Laks E., Biele J., Ha G., Aparicio S., Bouchard-Côté A., Shah S. P. PyClone: statistical inference of clonal population structure in cancer. *Nature Methods*, 2014, vol. 11, no. 4, pp. 396–398. doi:10.1038/nmeth.2883
22. Miller C. A., McMichael J., Dang H. X., Maher C. A., Ding L., Ley T. J., Mardis E. R., Wilson R. K. Visualizing tumor evolution with the fishplot package for R. *BMC Genomics*, 2016, vol. 17, no. 1, p. 880. doi:10.1186/s12864-016-3195-z
23. Li X., Xu F., Wu L.-Y., Zhao Y.-S., Guo J., He Q., Zhang Z., Chang C.-K., Wu D. A genetic development route analysis on MDS subset carrying initial epigenetic gene mutations. *Scientific Reports*, 2020, vol. 10, no. 1, p. 826. doi:10.1038/s41598-019-55540-w
24. Chen J., Kao Y.-R., Sun D., Todorova T. I., Reynolds D., Narayanagari S.-R., Montagna C., Will B., Verma A., Steidl U. Myelodysplastic syndrome progression to acute myeloid leukemia at the stem cell level. *Nature Medicine*, 2019, vol. 25, no. 1, pp. 103–110. doi:10.1038/s41591-018-0267-4
25. Sperling A. S., Gibson C. J., Ebert B. L. The genetics of myelodysplastic syndrome: from clonal haematopoiesis to secondary leukaemia. *Nature Reviews Cancer*, 2017, vol. 17, no. 1, pp. 5–19. doi:10.1038/nrc.2016.112
26. Jiménez-Sánchez A., Memon D., Pourpe S., Veeraraghavan H., Li Y., Vargas H. A., Gill M. B., Park K. J., Zivanovic O., Konner J., Ricca J., Zamarin D., Walther T., Aghajanian C., Wolchok J. D., Sala E., Merghoub T., Snyder A., Miller M. L. Heterogeneous tumor-immune microenvironments among differentially growing metastases in an ovarian cancer patient. *Cell*, 2017, vol. 170, no. 5, pp. 927–938.e20. doi:10.1016/j.cell.2017.07.025
27. Liu L. Y., Bhandari V., Salcedo A., Espiritu S. M. G., Morris Q. D., Kislinger T., Boutros P. C. Quantifying the influence of mutation detection on tumour subclonal reconstruction. *Cancer Biology*, 2018. doi:10.1101/418780
28. Deshwar A. G., Vembu S., Yung C. K., Jang G. H., Stein L., Morris Q. PhyloWGS: Reconstructing subclonal composition and evolution from whole-genome sequencing of tumors. *Genome Biology*, 2015, vol. 16, no. 1, p. 35, doi:10.1186/s13059-015-0602-8
29. Nik-Zainal S., Van Loo P., Wedge D. C., Alexandrov L. B., Greenman C. D., Lau K. W., Raine K., Jones D., Marshall J., Ramakrishna M., Shlien A., Cooke S. L., Hinton J., Menzies A., Stebbings L. A., Leroy C., Jia M., Rance R., Mudie L. J., Gamble S. J., Stephens P. J., McLaren S., Tarpey P. S., Papaemmanuil E., Davies H. R., Varela I., McBride D. J., Bignell G. R., Leung K., Butler A. P., Teague J. W., Martin S., Jönsson G., Mariani O., Boyault S., Miron P., Fatima A., Langerød A., Aparicio S. A. J. R., Tutt A., Sieuwerts A. M., Borg Å., Thomas G., Salomon A. V., Richardson A. L., Børresen-Dale A.-L., Futreal P. A., Stratton M. R., Campbell P. J. The life history of 21 breast cancers. *Cell*, 2012, vol. 149, no. 5, pp. 994–1007. doi:10.1016/j.cell.2012.04.023
30. Bewicke-Copley F., Arjun Kumar E., Palladino G., Korfi K., Wang J. Applications and analysis of targeted genomic sequencing in cancer studies. *Computational and Structural Biotechnology Journal*, 2019, vol. 17, pp. 1348–1359. doi:10.1016/j.csbj.2019.10.004

УДК 57.087.1::616-006.4
doi:10.31799/1684-8853-2020-6-50-59

Построение и апробация биоинформатического пайплайна для определения клональных профилей при миелодиспластическом синдроме

Д. С. Буг[а], специалист, orcid.org/0000-0002-5849-1311, dmitriybs@1spbgmu.ru
А. А. Приходько[а], студентка, orcid.org/0000-0002-0001-7932
Е. А. Бакин[а,б], канд. техн. наук, доцент, orcid.org/0000-0002-5694-4348
А. В. Тишков[а], канд. физ.-мат. наук, доцент, orcid.org/0000-0002-4282-8717
Н. В. Петухова[а], канд. биол. наук, orcid.org/0000-0001-6397-824X
И. М. Бархатов[а], канд. мед. наук, orcid.org/0000-0002-8000-3652
Е. В. Морозова[а], канд. мед. наук, доцент, orcid.org/0000-0002-9605-485X
И. С. Моисеев[а], доктор мед. наук, доцент, orcid.org/0000-0002-4332-0114
[а]Первый Санкт-Петербургский государственный медицинский университет им. акад. И. П. Павлова, Льва Толстого ул., 6-8, Санкт-Петербург, 197022, РФ
[б]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

Введение: результаты последних научных исследований показывают более очевидной связь между клональным профилем опухоли и его клиническим значением. Однако в настоящее время отсутствует доступный в клинической практике и надежный метод для клонального профилирования. Миелодиспластический синдром представляет собой сложную клональную патологию гемопоэтической стволовой клетки, характеризующуюся морфологической дисплазией, цитопенией и высоким риском трансформации в острый миелоидный лейкоз. Клинический исход миелодиспластического синдрома может быть чрезвычайно гетерогенным, поэтому для выяснения истинного состояния гемопоэтической системы и дальнейшего прогноза больных с такими сложными нарушениями необходимо специфическое изучение клональных профилей. **Цель исследования:** разработка пайплайна, предназначенного для определения клональных профилей пациентов с миелодиспластическим синдромом на основе данных таргетного секвенирования следующего поколения. **Результаты:** пайплайн был разработан и апробирован на выборке из 35 пациентов с миелодиспластическим синдромом преимущественно высокого риска. Показана возможность использовать данные таргетного секвенирования для оценки гетерогенности клональных профилей и характеристики их генных свойств. Данный подход позволит идентифицировать соответствие между типом индивидуального профиля и прогнозом заболевания, влиять на выбор терапии. Продемонстрированы характеристики полученных клональных профилей и описан процесс их анализа. **Практическая значимость:** информация о выявленных закономерностях и взаимосвязи между характеристиками клонального профиля (количеством субклонов, частотой мутаций на клон) и клиническим исходом может быть использована врачами в современной практике для более точного подбора терапии в зависимости от выявленной индивидуальной специфичности заболевания.

Ключевые слова — миелодиспластический синдром, биоинформатический пайплайн, клональный профиль, первичная мутация, субклон, таргетное секвенирование, секвенирование следующего поколения.

Для цитирования: Bug D. S., Prikhodko A. A., Bakin E. A., Tishkov A. V., Petukhova N. V., Barkhatov I. M., Morozova E. V., Moiseev I. S. Building and evaluation of bioinformatic pipeline for determination of clonal profiles in myelodysplastic syndrome. *Информационно-управляющие системы*, 2020, № 6, с. 50–59. doi:10.31799/1684-8853-2020-6-50-59

For citation: Bug D. S., Prikhodko A. A., Bakin E. A., Tishkov A. V., Petukhova N. V., Barkhatov I. M., Morozova E. V., Moiseev I. S. Building and evaluation of bioinformatic pipeline for determination of clonal profiles in myelodysplastic syndrome. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 50–59. doi:10.31799/1684-8853-2020-6-50-59

UDC 004.895

doi:10.31799/1684-8853-2020-6-60-69

Generative augmentation to improve lung nodules detection in resource-limited settings

N. F. Gusarova[a]*, PhD, Tech., Associate Professor, orcid.org/0000-0002-1361-6037, natfed@list.ru*
A. P. Klochkov[a]*, Student, orcid.org/0000-0002-6843-7888*
A. A. Lobantsev[a]*, Software Engineer, orcid.org/0000-0002-8314-5103*
A. S. Vatian[a]*, PhD, Tech., Associate Professor, orcid.org/0000-0002-5483-716X*
M. V. Kabyshev[a]*, Post-Graduate Student, orcid.org/0000-0002-1006-0408*
A. A. Shalyto[a]*, Dr. Sc., Tech., Professor, orcid.org/0000-0002-2723-2077*
A. A. Tatarinova[b]*, PhD, Med., Senior Researcher, orcid.org/0000-0001-5955-2529*
T. V. Treshkur[b]*, PhD, Med., Associate Professor, orcid.org/0000-0001-5955-2529*
Min Li[c]*, PhD, Professor, orcid.org/0000-0002-1361-6037*
[a]*ITMO University, 49, Kronverksky Pr., 197101, Saint-Petersburg, Russian Federation*
[b]*Almazov National Medical Research Centre, 2, Akkuratova St., 197341, Saint-Petersburg, Russian Federation*
[c]*School of Computer Science and Engineering, Central South University, 932, South Lushan Road, Changsha, Hunan, 410083 P.R., China*

Introduction: *Lung cancer is one of the most formidable cancers. The use of neural network technologies in its diagnostics is promising, but the datasets collected from real clinical practice cannot cover various lung cancer manifestations.* ***Purpose:*** *Assessment of the possibility of improving pulmonary nodules classification quality utilizing generative augmentation of available datasets under resource constraints.* ***Methods:*** *The LIDC-IDRI dataset was used. We used the StyleGAN architecture, to generate artificial lung nodules and the VGG11 model as a classifier.* ***Results:*** *We generated pulmonary nodules using the proposed pipeline and invited four experts to evaluate them visually. Four experimental datasets with different types of augmentation were formed, including the use of synthesized data. We compared the effectiveness of the classification performed by the VGG11 network when training for each dataset. For an expert assessment, 10 generated nodules in each group of characteristics were presented: parietal nodules, ground-glass, sub-solid, solid nodules. In all cases, expert assessments of similarity with real nodules were obtained with a Fleiss's kappa coefficient* $\kappa = 0.7–0.9$*. We got the values of AUROC=0.9867 and AUPR=0.9873 with the proposed approach of a generative augmentation.* ***Discussion:*** *The obtained efficiency metrics are superior to the baseline results obtained using comparably small training datasets and slightly less than the best results achieved using much more powerful computational resources. We have shown that one can effectively use StyleGAN for augmenting an unbalanced dataset with a combination of VGG11 as a classifier, which does not require extensive computing resources and a sizeable initial dataset for training.*

Keywords *— lung nodules classification, data augmentation, generative adversarial networks, StyleGAN, CT image.*

For citation: Gusarova N. F., Klochkov A. P., Lobantsev A. A., Vatian A. S., Kabyshev M. V., Shalyto A. A., Tatarinova A. A., Treshkur T. V., Li Min. Generative augmentation to improve lung nodules detection in resource-limited settings. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 60–69. doi:10.31799/1684-8853-2020-6-60-69

Introduction

Lung cancer is one of the most formidable cancers, both in terms of the development rate and the severity of the prognosis [1]. In this case, it is a vital necessity to get the earliest possible and accurate diagnosis. During the initial examination and screening of the population, procedures such as chest radiography and sputum cytology are widespread. However, when detecting the suspicions of lung cancer, the patient requires stronger diagnostic procedures, including bronchoscopic biopsies and computed tomography (CT) of the lungs. A bronchial biopsy is a highly invasive procedure. It involves the participation of proficient experts, is accompanied by complications and side effects, and cannot be used as a regular diagnostic procedure. Simultaneously, CT of the lungs is a non-invasive procedure, which does not adversely affect the patient's health, and CT scanners are now widely used medical equipment. In this regard, increasing the efficiency of CT in the diagnosis of lung cancer is today one of the essential tasks of information technology.

The use of machine learning technologies and, above all, deep convolutional neural networks in this task has led to promising results in recent years. For instance, for the classification of malignant and benign nodes, the following results are given in literature: $\text{accuracy} = 92.0\%$, $\text{sensitivity} = 100\%$ [2]; $\text{accuracy} = 96.0\%$, $\text{sensitivity} = 97\%$ [3]. However, such high values of metrics are achieved, as a rule, on typical datasets (most often, the Lung Image Database Consortium and Image Database Resource Initiative (LIDC-IDRI) dataset [4] is used). When moving to other datasets or real practice, the values of metrics drop dramatically. For example, the accuracy achieved by [3] on a relatively large proprietary dataset of 2054 images was 86% only.

The reason for such a fall in efficiency is mainly is as follows: benign and malignant nodes in lung cancer are very similar, both in objectively measurable features (such as diameter, optical density, etc.); in terms of integral visual assessment (such as smooth, lobulated, or irregular and spiculated margins, etc.) [5]. The existing datasets collected from real clinical practice cannot cover such a variety of lung cancer manifestations. Their size is not enough for full-fledged training of neural networks, which, as a result, leads to the explicit overfitting on a specific dataset and the drop in efficiency when switching to new datasets. An increase the dataset volume due to traditional augmentation methods, such as shifts, rotations, reflections, etc., does not give the desired improvement in the results of lung cancer classification. Therefore, generative adversarial networks (GAN) are considered a promising technology for solving this problem.

Generative adversarial network, proposed in [6], is a model to approximate an arbitrary distribution only by sampling from that distribution. The model consists of two parts — the generator and the discriminator. The generator aims to learn the sample distribution. It takes random noise and tries to generate the sample from the learned distribution. The discriminator tries to distinguish these generated objects from the real objects from the training sample with an arbitrary distribution and returns the results to the generator via gradient back-propagation. Thus, during training, the generator generates objects that are more and more similar to a sample.

Modern implementations of GAN technologies provide realistic-looking images, for example, pictures for an online store, avatars for games, and video clips. A significant advantage for the application of GAN in medicine is the fact that they provide the extraction of visual features by discovering the high dimensional latent distribution of the input data [7, 8]. Thus, in principle, it becomes possible to generate an unlimited number of images of benign and malignant nodes belonging to the same distribution as real nodes in a particular dataset and thereby augment this dataset to a size sufficient for effective training of the classifier. The article discusses the challenges of using GAN for generative augmentation of small datasets gathered in real clinical practice. To improve the availability of generative augmentation to the research community, this article focuses on the resource efficiency of the proposed methods.

Background and related works

As the literature review shows [8], today, GANs are actively used to analyze high-tech images in various medical applications, including diagnostics and treatment of diseases of the brain, lungs, spine, cardiovascular system, etc. Within the framework of this article, we highlight the work related to the diagnosis of lung status. In the total flow of the publications, the share of works devoted to using GANs in pulmonology problems is relatively small. They can be divided into two groups — applying GANs for chest X-ray and CT images.

As concerning the first one, one should first of all mention the work [9], where the authors use a deep convolutional GAN (DCGAN) for mimicking common chest pathologies and then augment a labeled set of chest X-rays for the training of the deep CNN across five pathological classes. The authors in [10] use conditional GAN for improving lung segmentation in chest X-ray. But, as the authors themselves note, their construction is resource expensive and requires high computing power.

The authors [11] solve a complicated problem — predicting the dynamics of lung position during breathing. To do this, they use two CNNs, each of which is built according to the GAN scheme. The solution is very resource-intensive: to register images between any two breath phases, it uses a powerful NVIDIA Tesla V100 GPU within 1 min. The authors [12] also solve a dynamic problem — to visualize chronic obstructive pulmonary disease progress. They proposed a method of visualization for regression with GAN, which is also very resource-intensive.

The research [13] aims to balance dataset used in training CNN for pneumonia prediction via oversampling with CycleGAN [14] producing X-ray images with pneumonia from images with no pneumonia. The advantage of the proposed augmentation technique is that it does not require extensive computational resources (a single NVIDIA 1070 graphical card is enough).

Going to the overview of applying GANs for CT images, it is worth noting that the general concept behind GANs of [6] has been transformed here in various architectures. For example, to generate high-quality images of pulmonary nodes on CT scans, the authors [15] use DCGANs [16]. With a relatively simple architecture, their implementation required extensive computational resources (up to 110,000 iterations), while the generated images showed low results on the Turing test (58%). Attempts have been made to use a more complicated architecture for the same purpose: the authors of [17] used a 3D conditional GAN [18], and the approach in [19] suggest to apply a sophisticated variant called 3D multi-conditional GAN. In both works, the authors generate pulmonary nodes and their immediate environment (context) and then embed them into the general CT images. For this, they condition the GAN basing on a volume of interest whose central part containing the nodule has been erased. Nevertheless, despite the sharp increase in the architecture complexity and a significant increase in computing resource requirements, the generated images are easily distinguished by qualified radiologists due to artifacts in synthetic samples [8].

Thus, as the analysis of existing achievements shows, it is hardly advisable today to set the task of creating realistic images of pulmonary nodes with the help of GAN having limited resources. Instead, researchers move on to modeling the characteristic components of the desired images. For pulmonary nodes, such a component is the maximum intensity projection (MIP) image. MIP [20, 21] is a postprocessing method that projects 3D voxels with maximum intensity to the projection plane. The advantage of MIP is that its formation is a 2D task and therefore requires less computing resources. Besides, radiologists use MIP images as more easily interpretable concepts during the nodule screening stage in their routine clinical practice.

A typical pipeline for detecting neoplasms in the lungs using high-tech images consists of two independently solvable tasks — detecting nodules and their subsequent classification. When organizing research having only small proprietary datasets, the second task is more topical. As our analysis evidence, in the literature, works using GANs for detection tasks [17, 19, 22] are presented more widely and thoroughly than concerning classification tasks [23–26]. They used axial sections of the volume of interest centered on the pulmonary nodule as a generated characteristic component.

The authors [24] aiming to generate high-quality synthetic nodules images proposed a new GAN architecture named forward and backward GAN (F&BGAN) and formed a hierarchical learning framework based on multi-scale VGG11 network as a classifier. They tested different augmentation approaches including traditional methods, DCGAN generative augmentation, and proposed F&BGAN generative augmentation. The part of LIDC-IDRI [28] was used as the initial dataset. The accuracy from 88.09% up to 95.24% was obtained depending on the augmentation approach.

In [25], the authors used Wasserstein GAN (WGAN) to generate malignant nodes differing by the only feature — the presence of spicules. They used a relatively small proprietary CT dataset consisting of 60 cases for training. Due to the low resolution of the formed nodes, the authors obtained not very good classification accuracy values — up to 63.0% for benign nodes and 84.8% for malignant nodes. In [26], they improved these metrics by increasing the network complexity (moving to three CNNs).

In [23], the authors used LUNA16 [27] database to extract candidate areas of images and nodules and imitate them using GAN. The authors divided the nodules extracted from the dataset into three groups: large, medium, and small. Then, they generated artificial nodules using the GAN for each group separately. Synthesized nodules allowed them to change the distribution of node sizes in the generated dataset by weighting each group's share. As the authors write, they tested their method for 15 variants of the CNN of six different feature extraction types and classifiers on the newly generated images dataset. They received accuracy values with a wide scatter — from 78.21 to 95.13%. Unfortunately, no technical details of the development are provided, making it impossible to reproduce their results.

Considering all of the above, in our article, we set the task of experimentally testing the possibility of improving pulmonary node classification into malignant and benign utilizing generative augmentation of available datasets under resource constraints. The problem is solved in the 2D projection.

Method and materials

Initial dataset and data preprocessing

As the source of lung cancer nodules, we used the LIDC-IDRI dataset containing more than 1018 CT scans in DICOM format from about 1010 different patients. The characteristics of lesions in the dataset and specifics of the annotation of the data can be accessed in [28]. It should be noted that authors of the dataset are aware that the term nodule is more appropriately used for a spectrum of abnormalities in lung tissue, and according to that, they state that during the annotation procedure, each of four participating radiologists provided their own "noduleness" interpretation.

For the experiments, we selected only those DICOM series that contain tumor nodules. The DICOM series is a 3D scan of the lungs, and the tumor nodule is a 3D image. Therefore, by capturing part of the images from a series of images, we can extract the 3D nodule. The extraction of a nodule is performed as follows. We form a cube circumscribing the desired nodule. The bounding cube size is selected to capture the nodule completely and, if necessary, a small margin around the nodule. In our experiments, we used circumscribing cubes with a side length from 1 to 40 mm.

After extracting the bounding cube with a nodule, we resampled it to a size of 128 × 128 × 128 pixels, and cut off the pixel values that are outside the range [–1000, 800] on the Hounsfield scale [29] according to the formula

$$\mathrm{pixel}_{\mathrm{value}}^{\mathrm{new}} = \min\Big(800,\ \max\Big(-1000,\ \mathrm{pixel}_{\mathrm{value}}^{\mathrm{old}}\Big)\Big)$$

The resulting pixel values are scaled to the range [–1, 1] by the formula

$$x = 2(x_{\text{in}} - \text{in}_{\min}) / ((\text{in}_{\max} - \text{in}_{\min}) - 1),$$

where $\text{in}_{\max} = 800$, $\text{in}_{\min} = -1000$ are boundary values on the Hounsfield scale. As a result, we got 695 cubes, of which 294 have a malignant nodule. Examples of nodules which were used as input data to train the generative network are shown in Fig. 1, *a–e*.

As discussed in the previous section, there are two ways to go from 3D to a 2D image of a nodule: either to select a central slice (i. e., passing through the center of the nodule) in one of the projections or to build MIP for the central slice. As our experiments have shown, using MIP projection provides some advantages, namely:

— it shows the picture of the lungs in more detail;

— it rather clearly displays the nodules;

— it allows representing the nodules with the context around.

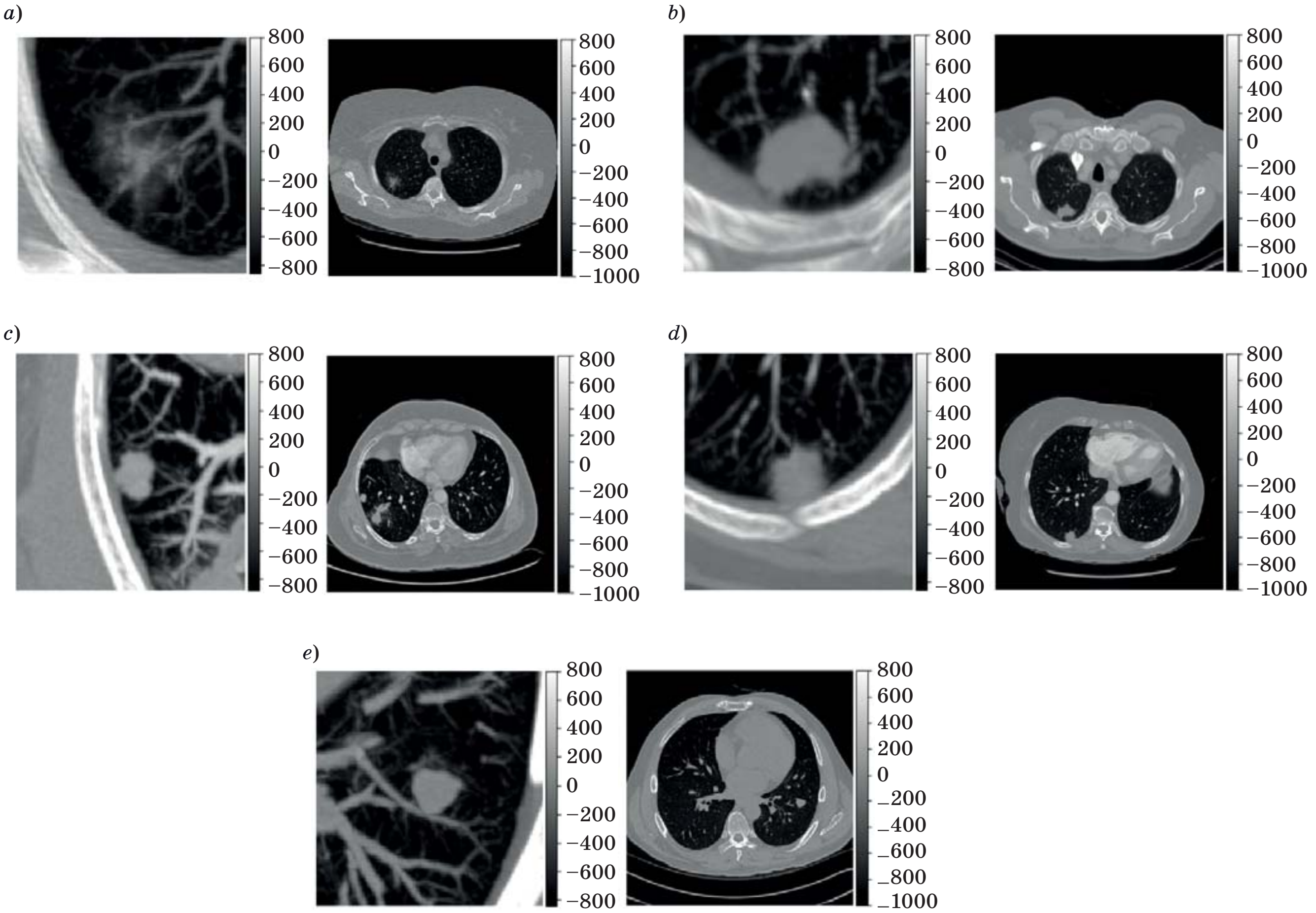
All of the above simplifies facilitates the task of classifying a cancerous tumor. We have performed a MIP lookup operation using the NumPy package.

Models and model training

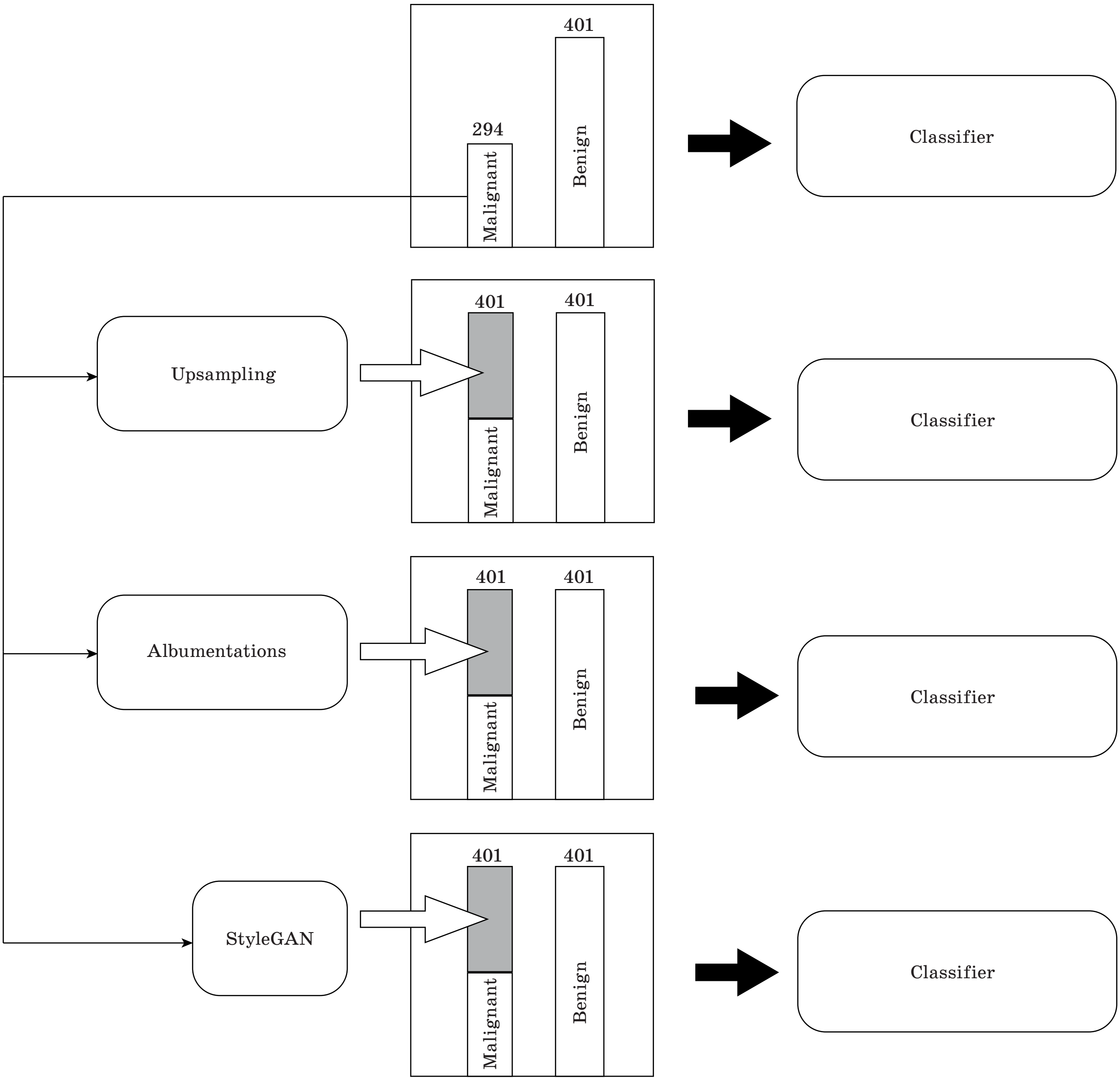
The complete pipeline of our experiments is shown in Fig. 2.

As an architecture for GAN, we chose StyleGAN [30] — one of the leading in the generation of photorealistic images. Considering that generating nodes in 2D is not more difficult than generating faces (on the example of StyleGAN was tested), this choice can be regarded as justified.

The paper aims to increase the cancer nodules classification quality under resource constraints. Hence the model with a simpler and more lightweight architecture suits better. Experiments show that VGG11 is the most appropriate model, which gives competitive results. We used the VGG11 model [31] as a classifier — a reasonably clear and easy-to-understand classifier model, which is often the baseline for research. We used the *torchvision* package to implement the model.



■ ***Fig. 1.*** Examples of extracted nodules (left column — nodules; right column — a corresponding lung slice): *a* — ground glass nodules; *b–d* — nodules of parietal localization; *e* — solid nodule



■ ***Fig. 2.*** Pipeline of our experiments

■ ***Table 1.*** Classifier training parameters

Name	Value
Model	VGG-11
batch_size	16
learning_rate	1e-5
optimizer	Adam
Loss function type	BinaryCrossEntropy
Training epochs	300

It should be emphasized that both models are relatively undemanding in terms of computing resources and can be applied in everyday machine learning practice [32].

To adapt the StyleGAN architecture following the prepared data, we made some changes to the model. The original implementation is configured to work with 3-channel images. To adjust the model in accordance with the prepared data, we have transformed the number of channels in the input and output layers in such a way as to be able to work with single-channel images. Besides, we made changes to the parameters of the model presented in Table 1.

Experimental datasets

To test the hypothesis that the binary classification of cancerous tumors in the lungs is better performed on a dataset augmented with synthesized GAN data, we formed four experimental datasets:

1) dataset A: original dataset with class imbalance;

2) dataset B: with the elimination of class imbalance by random copying of data of a smaller class (upsampling);

3) dataset C: with the elimination of class imbalance by transforming data of one class (vertical and horizontal reflection, and elastic transformation from the albumentations package [33]);

4) dataset D: balanced dataset using synthesized data. The imbalance was eliminated by generating new data using a pre-trained GAN model.

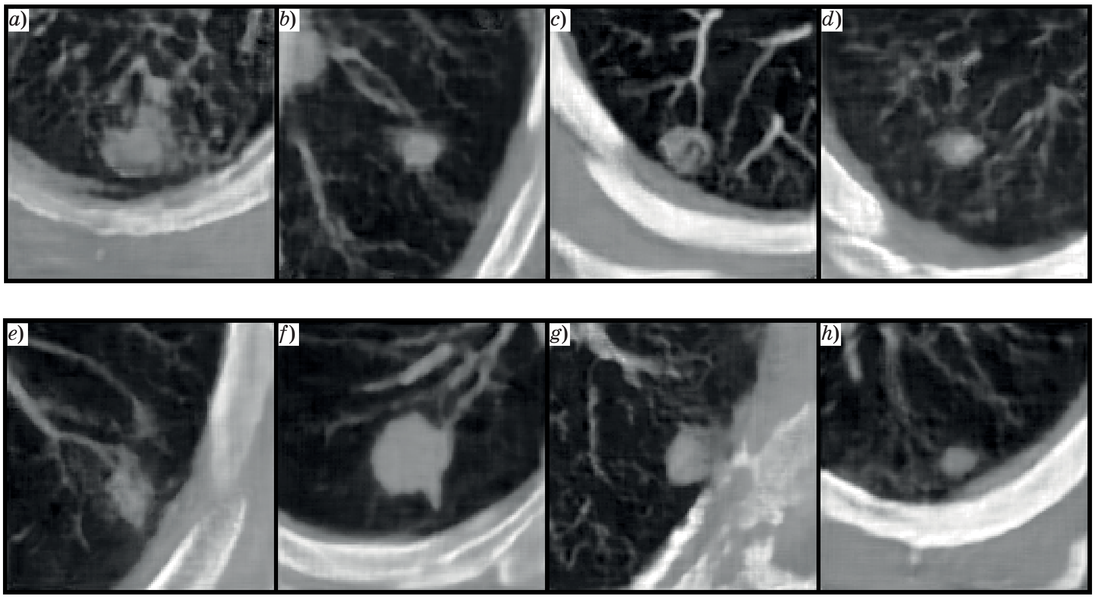
Results and discussion

Examples of nodules generated by our GAN model are presented in Fig. 3, *a–h*. As shown in the previous section, it is not required to achieve an exhaustive execution of the Turing test on the generated nodules in the task under consideration. Therefore, we carried out an expert assessment of the “similarity” of the generated nodules for individual characteristics, including parietal nodule, solid nodule, subsolid nodule, ground-glass nodule. Four qualified radiologists participated in the examination, ten nodules in each group of characteristics were presented for assessment. In all cases, positive expert assessments were obtained with a good Fleiss’s kappa coefficient κ = 0,7–0,9.

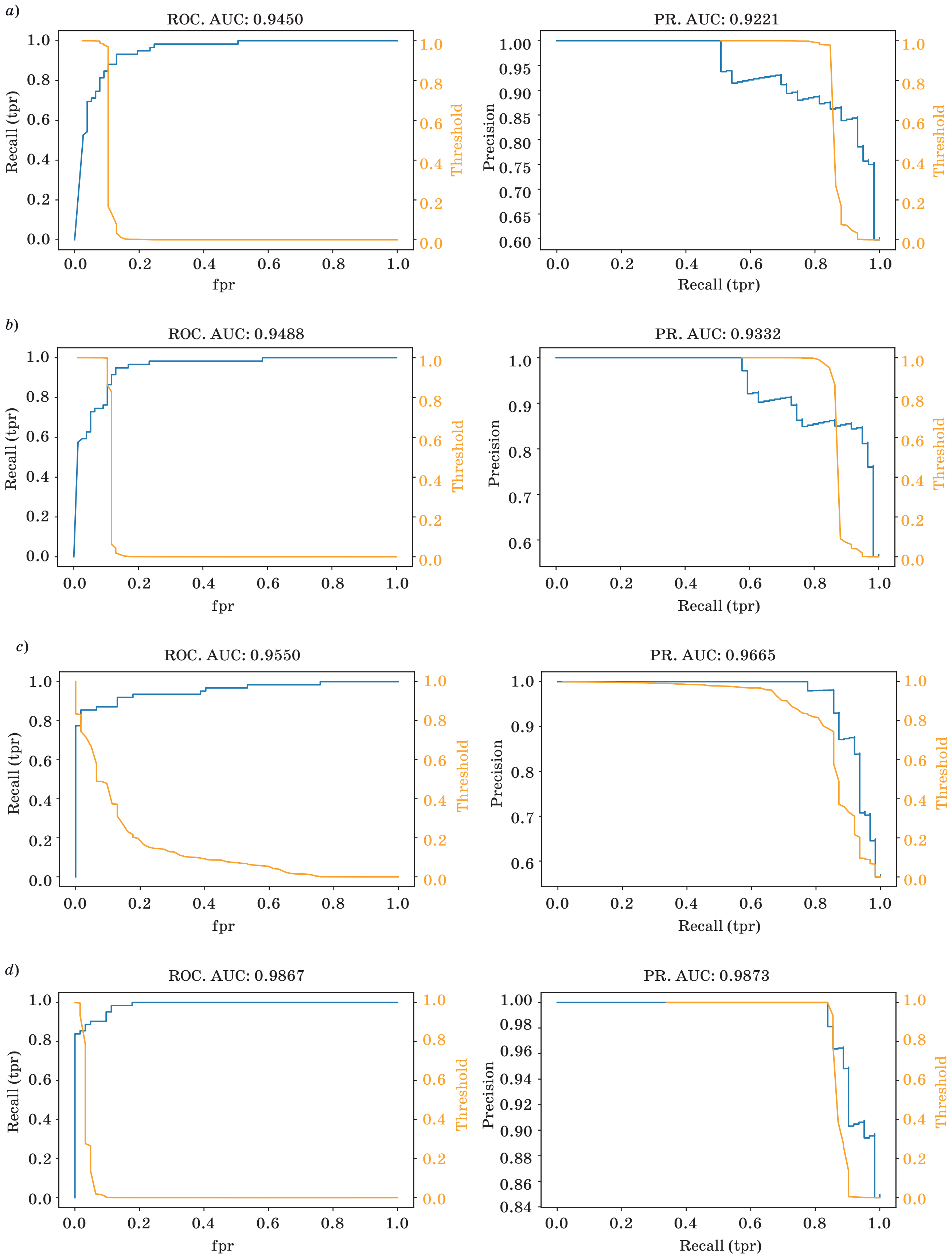
Figure 4 shows the ROC-curves for the best learning epochs for each experimental dataset described above, which makes it possible to compare the efficiency of the different augmenetation techniques. As can be seen, the best values of AUROC: 0.9867, AUPR: 0.9873, accuracy: 94.35% were obtained with the proposed approach of a generative augmentation (see Fig. 3, *d*). Note that the obtained values are superior to the [25] results obtained using comparable training datasets (balanced accuracy: 81.7%), [26], (balanced accuracy: 85.6%), and comparable with the results of [24] (best accuracy: 95.24%, best AUROC: 0.984). Worth noting that the classifier model in [24] has approx-

■ ***Table 2.*** Results

Dataset	Accuracy, %	AUROC	AUPR
Original (A)	84.68	0.945	0.922
Upsampling (B)	87.50	0.949	0.933
Augmentation (C)	91.13	0.955	0.967
Synthetic (D)	94.35	0.987	0.987



■ ***Fig. 3.*** Examples of generated nodules: *a*, *g* — subsolid nodules of parietal localization nodules; *b–d*, *f*, *h* — solid nodules; *e* — subsolid nodule



■ ***Fig. 4.*** ROC- and PR-curves for the datasets: *a* — dataset A; *b* — dataset B; *c* — dataset C; *d* — dataset D imately 143 million trainable parameters, while used VGG11 has 128 million trainable parameters. Hence, our proposed method has a lower GPU memory consumption with comparative quality results (Table 2).

Conclusion

It is not rare in common practice when a machine learning practitioner can encounter a lack of data to train the classification model properly. However, as our experiments have shown, augmenting an unbalanced dataset with synthetic data improves the classifier efficiency with comparatively no significant effort. Regarding the classification of pulmonary nodules, we have shown that one can effectively use a combination of StyleGAN and VGG11, which does not require extensive computing resources and a sizeable initial dataset for training. We suggest that in future works, the use of StyleGAN in generative augmentation can be extended to conditional augmentation to synthesize the nodules with the specific parameters.

Financial support

This work was financially supported by Russian Science Foundation, Grant 19-19-00696.

References

1. *Cancer Facts & Figures 2020*. Atlanta, American Cancer Society, 2020. Available at: https://www.cancer.org/content/dam/cancer-org/research/cancer-facts-and-statistics/annual-cancer-facts-and-figures/2020/cancer-facts-and-figures-2020.pdf (accessed 18 September 2020).
2. Makajua S., Prasad P. W. C., Alsadoona A., Singhb A. K., Elchouemic A. Lung cancer detection using CT scan images. *Procedia Computer Science*, 2018, vol. 125, pp. 107–114.
3. Wang S., Dong L., Wang X., and Wang X. Classification of pathological types of lung cancer from CT images by deep residual neural networks with transfer learning strategy. *Open Medicine*, 2020, vol. 15, iss. 1, pp. 190–197.
4. *Lung Image Database Consortium image collection (LIDC-IDRI)*. Available at: https://wiki.cancerimagingarchive.net/display/Public/LIDC-IDRI (accessed 18 September 2020).
5. Purandare N. C., and Rangarajan V. Imaging of lung cancer: implications on staging and management. *The Indian Journal of Radiology and Imaging*, 2015, vol. 25, iss. 2, p. 109.
6. Goodfellow I. J., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. Generative adversarial nets. *Proceedings of Advances in Neural Information Processing Systems*, 2014, pp. 2672–2680.
7. Creswell A., White T., Dumoulin V., Arulkumaran K., Sengupta B., and Bharath A. A. Generative adversarial networks: An overview. *IEEE Signal Processing Magazine*, 2018, vol. 35, iss. 1, pp. 53–65.
8. Kazeminia S., Baur C., Kuijper A., van Ginneken B., Navab N., Albarqouni S., and Mukhopadhyay A. GANs for medical image analysis. *Artificial Intelligence in Medicine*, 2020, p. 101938.
9. Salehinejad H., Valaee S., Dowdell T., Colak E., and Barfett J. Generalization of deep neural networks for chest pathology classification in X-rays using generative adversarial networks. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018, pp. 990–994.
10. Munawar F., Azmat S., Iqbal T., Grönlund C., and Ali H. Segmentation of lungs in chest X-ray image using generative adversarial networks. *IEEE Access*, 2020, no. 8, pp. 153535–153545.
11. Fu Y., Lei Y., Wang T., Higgins K., Bradley J. D., Curran W. J., Liu T., Yanga X. LungRegNet: an unsupervised deformable image registration method for 4D-CT lung. *Medical Physics*, 2020, vol. 47, iss. 4, pp. 1763–1774.
12. Lanfredi R. B., Schroeder J. D., Vachet C., and Tasdizen T. Adversarial regression training for visualizing the progression of chronic obstructive pulmonary disease with chest X-rays. *International Conference on Medical Image Computing and Computer-Assisted Intervention*, 2019, pp. 685–693.
13. Malygina T., Ericheva E., and Drokin I. GANs' N Lungs: improving pneumonia prediction. arXiv preprint arXiv:1908.00433, 2019. Available at: https://arxiv.org/pdf/1908.00433 (accessed 18 September 2020).
14. Zhu J. Y., Park T., Isola P., and Efros A. A. Unpaired image-to-image translation using cycle-consistent adversarial networks. *Proceedings of the IEEE International Conference on Computer Vision*, 2017, pp. 2223–2232.
15. Chuquicusma M. J. M., Hussein S., Burt J. R, Bagci U. How to fool radiologists with generative adversarial networks? A visual turing test for lung cancer diagnosis. *2018 IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018)*, 2018, pp. 240–244.
16. Radford A., Metz L., and Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434, 2015. Available at: https://arxiv.org/pdf/1511.06434.pdf%C3 (accessed 18 September 2020).

17. Jin D., Xu Z., Tang Y., Harrison A. P., and Mollura D. J. CT-realistic lung nodule simulation from 3D conditional generative adversarial networks for robust lung segmentation. *International Conference on Medical Image Computing and Computer-Assisted Intervention*, 2018, pp. 732–740.
18. Mirza M., and Osindero S. Conditional generative adversarial nets. preprint arXiv:1411.1784, 2014. Available at: https://arxiv.org/pdf/1411.1784.pdf (accessed 18 September 2020).
19. Han C., Kitamura Y., Kudo A., Ichinose A., Rundo L., Furukawa Y., Umemoto K., Li Y., Nakayama H. Synthesizing diverse lung nodules wherever massively: 3D multi-conditional GAN-based CT image augmentation for object detection. *International Conference on 3D Vision (3DV)*, 2019, pp. 729–737.
20. Zhang J., Xia Y., Zeng H., and Zhang Y. NODULe: Combining constrained multi-scale LoG filters with densely dilated 3D deep convolutional neural network for pulmonary nodule detection. *Neurocomputing*, 2018, vol. 317, pp. 159–167.
21. Zheng S., Guo J., Cui X., Veldhuis R. N., Oudkerk M., and Van Ooijen P. M. Automatic pulmonary nodule detection in CT scans using convolutional neural networks based on maximum intensity projection. *IEEE Transactions on Medical Imaging*, 2019, vol. 39, iss. 3, pp. 797–805.
22. Gao C., Clark S., Furst J., and Raicu D. *Augmenting LIDC dataset using 3D generative adversarial networks to improve lung nodule detection*. In: *Medical Imaging 2019: Computer-Aided Diagnosis*, 2019, vol. 10950, p. 109501K.
23. Esmaeilishahmirzadi N., Mortezapour H. A novel method for enhancing the classification of pulmonary data sets using generative adversarial networks. *Biomedical Research*, 2018, vol. 29, iss. 14, pp. 3022–3027.
24. Zhao D., Zhu D., Lu J., Luo Y., and Zhang G. Synthetic medical images using F&BGAN for improved lung nodules classification by multi-scale VGG16. *Symmetry*, 2018, vol. 10, iss. 10, p. 519.
25. Onishi Y., Teramoto A., Tsujimoto M., Tsukamoto T., Saito K., Toyama H., Imaizumi K., Fujita H. Automated pulmonary nodule classification in computed tomography images using a deep convolutional neural network trained by generative adversarial networks. *BioMed Research International*, 2019, vol. 2019, Article ID 6051939. https://doi.org/10.1155/2019/6051939
26. Onishi Y., Teramoto A., Tsujimoto M., Tsukamoto T., Saito K., Toyama H., Imaizumi K., Fujita H. Multiplanar analysis for pulmonary nodule classification in CT images using deep convolutional neural network and generative adversarial networks. *International Journal of Computer Assisted Radiology and Surgery*, 2020, vol. 15, iss. 1, pp. 173–178.
27. Setio A. A. A., Traverso A., De Bel T., Berens M. S., van den Bogaard C., Cerello P., ... and van der Gugten R. Validation, comparison, and combination of algorithms for automatic detection of pulmonary nodules in computed tomography images: the LUNA16 challenge. *Medical Image Analysis*, 2017, vol. 42, pp. 1–13.
28. Armato III S. G., McLennan G., Bidaut L., McNitt-Gray M. F., Meyer C. R., Reeves A. P., ... and Kazerooni E. A. The lung image database consortium (LIDC) and image database resource initiative (IDRI): A completed reference database of lung nodules on CT scans. *Medical Physics*, 2011, vol. 38, iss. 2, pp. 915–931.
29. Feeman T. G. *The Mathematics of Medical Imaging: A Beginner's Guide*. Springer Undergraduate Texts in Mathematics and Technology. Springer, 2015. 197 p.
30. Karras T., Laine S., and Aila T. A style-based generator architecture for generative adversarial networks. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019, pp. 4401–4410.
31. Simonyan K., and Zisserman A. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014. Available at: https://arxiv.org/pdf/1409.1556.pdf (accessed 18 September 2020).
32. Iglovikov V., and Shvets A. Ternausnet: U-net with vgg11 encoder pre-trained on imagenet for image segmentation. arXiv preprint arXiv:1801.05746, 2018. Available at: https://arxiv.org/pdf/1801.05746 (accessed 18 September 2020).
33. Buslaev A., Iglovikov V. I., Khvedchenya E., Parinov A., Druzhinin M., and Kalinin A. A. Albumentations: fast and flexible image augmentations. *Information*, 2020, vol. 11, iss. 2, p. 125.

УДК 004.895
doi:10.31799/1684-8853-2020-6-60-69

Генеративная аугментация для улучшения обнаружения узелков в легких в условиях ограниченных ресурсов

Н. Ф. Гусарова[а], канд. техн. наук, доцент, orcid.org/0000-0002-1361-6037, natfed@list.ru
А. П. Клочков[а], студент, orcid.org/0000-0002-6843-7888
А. А. Лобанцев[а], инженер-программист, orcid.org/0000-0002-8314-5103
А. С. Ватьян[а], канд. техн. наук, доцент, orcid.org/0000-0002-5483-716X
М. В. Кабышев[а], аспирант, orcid.org/0000-0002-1006-0408
А. А. Шалыто[а], доктор техн. наук, профессор, orcid.org/0000-0002-2723-2077
А. А. Татаринова[б], канд. мед. наук, старший научный сотрудник, orcid.org/0000-0001-5955-2529
Т. В. Трешкур[б], канд. мед. наук, доцент, orcid.org/0000-0001-5955-2529
Мин Ли[в], доктор наук, профессор, orcid.org/0000-0002-1361-6037
[а]Университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ
[б]НМИЦ им. В. А. Алмазова, Аккуратова ул., 2, Санкт-Петербург, 97341, РФ
[в]Школа компьютерных наук и инженерии, Центральный Южный университет, 932, Союф Люшан роуд, Чанша, Хунан, 410083 P.R., Китай

Введение: рак легкого — один из самых опасных видов рака. Использование технологий нейронных сетей для его диагностики является многообещающим, но датасеты, собранные из реальной клинической практики, не могут охватить различные проявления рака легких. **Цель:** оценка возможности улучшить классификацию легочных узлов посредством генеративной аугментации доступных датасетов при ограниченных ресурсах. **Методы:** использован датасет LIDC-IDRI, архитектура StyleGAN для создания искусственных изображений легочных узлов и модель VGG11 в качестве классификатора. **Результаты:** проведены генерация изображений легочных узлов с помощью предложенной схемы и их визуальная оценка с привлечением четырех экспертов. Сформированы четыре экспериментальных датасета с различными типами аугментации, включая использование синтезированных данных, и проведено сравнение эффективности классификации, выполняемой сетью VGG11 при обучении на каждом датасете. Для экспертизы отобраны по 10 генерированных изображений легочных узлов в каждой группе характеристик. Во всех случаях получены экспертные оценки схожести с реальными экземплярами с коэффициентом каппа Флейса κ = 0,7–0,9. Предложенный подход генеративной аугментации позволил получить значения AUROC = 0,9867 и AUPR = 0,9873. **Обсуждение:** полученные показатели эффективности превосходят результаты бейзлайна с использованием сравнительно небольших обучающих датасетов и немного уступают лучшим результатам, достигнутым с применением гораздо более мощных вычислительных ресурсов. Тем самым показано, что для аугментации несбалансированного датасета можно эффективно использовать StyleGAN в комбинации с VGG11 классификатором, которая не требует больших вычислительных ресурсов, а также большого начального датасета для обучения.

Ключевые слова — классификация легочных узлов, аугментация данных, генеративные состязательные сети, StyleGAN, КТ-изображение.

Для цитирования: Gusarova N. F., Klochkov **A.** P., Lobantsev A. A., Vatian A. S., Kabyshev **M.** V., Shalyto A. A., Tatarinova A. A., Treshkur T. V., Li Min. Generative augmentation to improve lung nodules detection in resource-limited settings. *Информационно-управляющие системы*, 2020, № 6, с. 60–69. doi:10.31799/1684-8853-2020-6-60-69
For citation: Gusarova N. F., Klochkov **A.** P., Lobantsev A. A., Vatian A. S., Kabyshev **M.** V., Shalyto A. A., Tatarinova A. A., Treshkur **T.** V., Li Min. Generative augmentation to improve lung nodules detection in resource-limited settings. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 60–69. doi:10.31799/1684-8853-2020-6-60-69

СВЕДЕНИЯ ОБ АВТОРАХ

БАЛОНИН
Николай
Алексеевич

Профессор кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.

В 1982 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика».

В 2008 году защитил диссертацию на соискание ученой степени доктора технических наук.

Является автором более 100 научных публикаций, в том числе трех монографий.

Область научных интересов — теория динамических систем, теория идентификации, теория операторов, теория матриц, вычислительные методы, интернет-робототехника, интернет-книги с исполняемыми алгоритмами, научные социальные сети.

Эл. адрес: korbendfs@mail.ru

БАКИН
Евгений
Александрович

Доцент кафедры проблемно-ориентированных вычислительных комплексов Санкт-Петербургского государственного университета аэрокосмического приборостроения.

В 2008 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Радиоэлектронные системы».

В 2012 году защитил диссертацию на соискание ученой степени кандидата технических наук.

Является автором 25 научных публикаций и семи патентов на изобретения.

Область научных интересов — компьютерное моделирование сложных систем, биоинформатика, биостатистика.

Эл. адрес: jenyb@mail.ru

БАЛЫКОВ
Антон
Александрович

Адъюнкт кафедры радиосвязи Военной академии связи им. С. М. Буденного, Санкт-Петербург.

В 2010 году окончил Ставропольский военный институт связи ракетных войск по специальности «Эксплуатация наземных средств и комплексов радиосвязи».

Является автором 11 научных публикаций, пяти свидетельств на программные продукты для ЭВМ и двух изобретений.

Область научных интересов — цифровая обработка сигналов, распространение радиоволн.

Эл. адрес: etomoiadres@mail.ru

БАРХАТОВ
Ильдар
Мунерович

Заведующий лабораторией трансплантологии и молекулярной гематологии Научно-исследовательского института детской онкологии, гематологии и трансплантологии им. Р. М. Горбачевой.

В 2001 году окончил Первый Санкт-Петербургский государственный медицинский университет им. И. П. Павлова по специальности «Лечебное дело».

В 2007 году защитил диссертацию на соискание ученой степени кандидата медицинских наук.

Является автором 67 научных публикаций и трех патентов на изобретения.

Область научных интересов — молекулярная биология, генетика, анализ мутаций.

Эл. адрес:
i.barkhatov@gmail.com

БУГ
Дмитрий
Сергеевич

Старший лаборант Научно-исследовательского центра биоинформатики Научно-образовательного института биомедицины Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова.

В 2018 году окончил Первый Санкт-Петербургский государственный медицинский университет им. И. П. Павлова по специальности «Лечебное дело», в 2020 году — по специальности «Клиническая лабораторная диагностика».

Является автором четырех научных публикаций.

Область научных интересов — биоинформатика, генетика, гематология, секвенирование.

Эл. адрес: dmitriybs@1spbgmu.ru

ВАТЬЯН
Александра
Сергеевна

Доцент факультета инфокоммуникационных технологий Университета ИТМО, Санкт-Петербург.

В 2014 году окончила Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики по специальности «Прикладная информатика».

В 2019 году защитила диссертацию на соискание ученой степени кандидата технических наук.

Является автором 31 научной публикации и 11 результатов интеллектуальной деятельности.

Область научных интересов — машинное обучение, искусственный интеллект, автоматное программирование, системы поддержки принятия клинических решений.

Эл. адрес: alexvatyan@gmail.com

ГУСАРОВА Наталия Федоровна

Старший научный сотрудник, доцент факультета инфокоммуникационных технологий Университета ИТМО, Санкт-Петербург.

В 1974 году окончила Ленинградский институт точной механики и оптики по специальности «Оптико-электронные приборы».

В 1984 году защитила диссертацию на соискание ученой степени кандидата технических наук.

Является автором 95 научных публикаций и 47 свидетельств о регистрации программного продукта.

Область научных интересов — машинное обучение, искусственный интеллект, автоматное программирование.

Эл. адрес: natfed@list.ru

ДВОРНИКОВ Сергей Сергеевич

Начальник лаборатории кафедры применения войск связи Военной академии связи им. С. М. Буденного, Санкт-Петербург.

В 2015 году окончил Санкт-Петербургский государственный политехнический университет по специальности «Радиотехника и телекоммуникация».

В 2018 году защитил диссертацию на соискание ученой степени кандидата технических наук.

Является автором 20 научных публикаций и десяти патентов на изобретения.

Область научных интересов — теория связи, помехоустойчивые радиосистемы.

Эл. адрес: dvornikov_s_s@mail.ru

КАБЫШЕВ Максим Васильевич

Аспирант Университета ИТМО, Санкт-Петербург.

В 2020 году окончил магистратуру Университета ИТМО по специальности «Экстренные вычисления и обработка сверхбольших объемов данных».

Область научных интересов — большие данные, мобильная разработка на платформе iOS, применение технологий машинного обучения при разработке программных систем, применяемых в медицинской сфере.

Эл. адрес: maxk6971@gmail.com

ДВОРНИКОВ Сергей Викторович

Профессор кафедры радиотехнических и оптоэлектронных комплексов Санкт-Петербургского государственного университета аэрокосмического приборостроения, заслуженный изобретатель Российской Федерации.

В 1998 году окончил Военную академию связи им. С. М. Буденного по специальности «Организация применения и эксплуатации радиоэлектронных систем».

В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.

Является автором 200 научных публикаций и 100 патентов на изобретения.

Область научных интересов — теория связи, помехозащищенность инфокоммуникационных каналов радиотехнических систем, методы совместной частотно-временной обработки сигналов.

Эл. адрес: practicdsv@yandex.ru

ИНИВАТОВ Даниил Павлович

Студент бакалавриата Омского государственного технического университета.

Является автором 41 научной публикации.

Область научных интересов — искусственный интеллект и машинное обучение.

Эл. адрес: daniilini@mail.ru

КЛОЧКОВ Антон Павлович

Магистрант программы «Разработка программного обеспечения» Университета ИТМО, Санкт-Петербург.

В 2020 году окончил бакалавриат Университета ИТМО по специальности «Информационные системы и технологии».

Область научных интересов — глубокое обучение, оптимизация использования вычислительных ресурсов, проектирование информационных систем.

Эл. адрес: tklochkov@gmail.com

ЛИ Мин

Профессор Школы компьютерных наук и инженерии Центрального Южного университета, Чанша, Хунан, Китай.
В 1985 году окончила бакалавриат Хэнаньского университета по специальности «Традиционная китайская медицина», в 1988 году — магистратуру Университета китайской медицины Гуанчжоу, Китай.
В 2001 году защитила диссертацию на соискание ученой степени доктора наук (PhD) на медицинском факультете Университета Токай, Япония.
Является автором более 100 научных публикаций, в том числе 20 монографий.
Область научных интересов — исследование эффективности и безопасности традиционной китайской медицины в лечении нейродегенеративных заболеваний.
Эл. адрес: limin@hkbu.edu.hk

ЛОБАНЦЕВ Артем Андреевич

Инженер-программист факультета информационных технологий и программирования Университета ИТМО, Санкт-Петербург.
В 2020 году окончил аспирантуру Университета ИТМО по специальности «Информатика и вычислительная техника».
Является автором 14 научных публикаций.
Область научных интересов — применение нейросетевых моделей в медицине, робототехника, байесовские методы в машинном обучении.
Эл. адрес: lobantseff@gmail.com

ЛОЖНИКОВ Павел Сергеевич

Заведующий кафедрой комплексной защиты информации Омского государственного технического университета.
В 2000 году окончил Омский государственный технический университет по специальности «Автоматизированные системы обработки информации и управление».
В 2005 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и четырех патентов на изобретения.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: lozhnikov@gmail.com

МОИСЕЕВ Иван Сергеевич

Доцент кафедры гематологии, трансфузиологии и трансплантологии ФПО с курсом детской онкологии, заместитель директора по науке Научно-исследовательского института детской онкологии, гематологии и трансплантологии им. Р. М. Горбачевой.
В 2007 году окончил Первый Санкт-Петербургский государственный медицинский университет им. И. П. Павлова по специальности «Лечебное дело».
В 2019 году защитил диссертацию на соискание ученой степени доктора медицинских наук.
Является автором 95 научных публикаций.
Область научных интересов — гематология, миелодиспластический синдром, лимфомы, аллогенная трансплантация гемопоэтических стволовых клеток.
Эл. адрес: moisiv@mail.ru

МОЛДОВЯН Александр Андреевич

Профессор, главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации РАН.
В 1974 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматизированные системы управления».
В 2005 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций и 60 патентов на изобретения.
Область научных интересов — компьютерная безопасность, защита информации, криптография, протоколы электронной цифровой подписи.
Эл. адрес: maa1305@yandex.ru

МОЛДОВЯН Дмитрий Николаевич

Научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации РАН.
В 2009 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Компьютерная безопасность».
В 2012 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 79 научных публикаций и шести патентов на изобретения.
Область научных интересов — информационная безопасность, защита информации, криптосистемы с открытым ключом, постквантовая криптография, конечные некоммутативные алгебры.
Эл. адрес: mdn.spectr@mail.ru

МОЛДОВЯН
Николай
Андреевич

Профессор, заведующий научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН, заслуженный изобретатель РФ.
В 1975 году окончил Кишиневский политехнический институт по специальности «Полупроводниковые приборы».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций и 60 патентов на изобретения.
Область научных интересов — информационная безопасность, криптография, электронная цифровая подпись, блочные шифры.
Эл. адрес: nmold@mail.ru

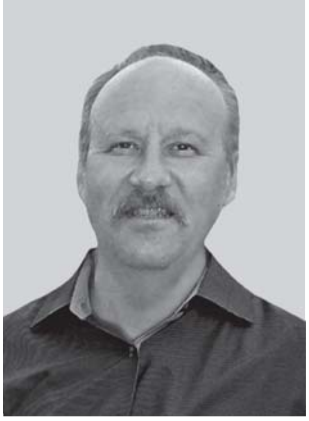
НИГРЕЙ
Алексей
Андреевич

Инженер Департамента систем планирования и оптимизации дирекции производственных систем ООО «Автоматика — Сервис», аспирант Омского государственного университета путей сообщения.
В 2017 году окончил Омский государственный университет путей сообщения по специальности «Информационная безопасность автоматизированных систем».
Является автором 32 научных публикаций.
Область научных интересов — биометрические системы идентификации и распознавания психофизиологических состояний.
Эл. адрес: aa.nig@yandex.ru

ПЕТУХОВА
Наталья
Витальевна

Руководитель НИЦ биоинформатики Научно-образовательного института биомедицины Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова.
В 2010 году окончила Московский государственный университет по специальности «Биохимия», в 2020 году — магистратуру Университета ИТМО по специальности «Прикладная математика и информатика».
В 2013 году защитила диссертацию на соискание ученой степени кандидата биологических наук.
Является автором 13 научных публикаций и двух патентов на изобретения.
Область научных интересов —молекулярная биология, геномика, протеомика, биоинформатика, молекулярное моделирование.
Эл. адрес: petuhovanv@1spbgmu.ru

ПИМЕНОВ
Виктор
Игоревич



Профессор, директор специализированного центра новых информационных технологий, заведующий кафедрой информационных технологий Санкт-Петербургского государственного университета промышленных технологий и дизайна.
В 1983 году окончил Ленинградский механический институт по специальности «Системы автоматического управления».
В 2009 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 170 научных публикаций и 11 свидетельств об интеллектуальной собственности.
Область научных интересов — распознавание образов, интеллектуальный анализ данных, 3D-моделирование.
Эл. адрес: v_pim@mail.ru

ПИМЕНОВ
Илья
Викторович

Доцент кафедры вычислительных систем и информатики государственного университета морского и речного флота им. адмирала С. О. Макарова, Санкт-Петербург.
В 2011 году окончил Санкт-Петербургский государственный университет технологии и дизайна по специальности «Прикладная информатика».
В 2017 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 40 научных публикаций и двух свидетельств об интеллектуальной собственности.
Область научных интересов — интеллектуальные системы, методы извлечения знаний, мультимедиа-технологии.
Эл. адрес: i-pim@mail.ru

ПРИХОДЬКО
Алена
Андреевна

Студентка Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова.
Область научных интересов — биоинформатика, генетика, молекулярная биология.
Эл. адрес: aljonaprich@gmail.com

СЕБЕРРИ
Дженифер

Профессор, директор Центра компьютерных исследований безопасности Австралийского государственного университета Вуллонгонг (Wollongong), основатель школы криптографии Австралии, Вуллонгонг, Австралия.
В 1966 году получила степень бакалавра в университете Нового Южного Уэльса, в 1969 году — магистра естественных наук в университете Ла Троб, Австралия.
В 1971 году защитила диссертацию на соискание ученой степени доктора наук (PhD).
Является автором более 450 научных публикаций и шести монографий.
Область научных интересов — дискретная математика, комбинаторика, матрицы Адамара, безопасные криптоалгоритмы, передача информации.
Эл. адрес: jennie@uow.edu.au

СИНИЦИНА
Ольга
Игоревна

Аспирант кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2008 году окончила Санкт-Петербургский университет телекоммуникаций им. проф. М. А. Бонч-Бруевича по специальности «Автоматизация технологических процессов и производств».
Является автором одной научной публикации.
Область научных интересов — теория динамических систем, теория матриц, вычислительные методы.
Эл. адрес: libra18@yandex.ru

СУЛАВКО
Алексей
Евгеньевич

Доцент кафедры комплексной защиты информации Омского государственного технического университета.
В 2009 году окончил Сибирскую государственную автомобильно-дорожную академию по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».
В 2014 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 130 научных публикаций и одного патента на изобретение.
Область научных интересов — распознавание образов, машинное обучение, биометрия, искусственный интеллект, защита информации, искусственные нейронные сети.
Эл. адрес: sulavich@mail.ru

СЕРГЕЕВ
Михаил
Борисович

Профессор, директор Института вычислительных систем и программирования, заведующий кафедрой вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения, почетный работник высшего профессионального образования РФ.
В 1980 году окончил ЛЭТИ по специальности «Электронные вычислительные машины».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций и 14 патентов на изобретения.
Область научных интересов — теория разрядных вычислений, методы проектирования спецпроцессоров для систем контроля и управления и др.
Эл. адрес: mbse@mail.ru

СТАДНИКОВ
Денис
Геннадьевич

Студент Омского государственного технического университета.
Является автором 21 научной публикации
Область научных интересов — распознавание образов, моделирование систем биометрической аутентификации.
Эл. адрес: sdg250598@inbox.ru

ТАТАРИНОВА
Анна
Андреевна

Старший научный сотрудник научно-исследовательской лаборатории электрокардиологии, ассистент кафедры внутренних болезней Института медицинского образования Национального медицинского исследовательского центра им. В. А. Алмазова, Санкт-Петербург.
В 2004 году с отличием окончила Санкт-Петербургский медицинский университет им. акад. И. П. Павлова по специальности «Лечебное дело».
В 2011 году защитила диссертацию на соискание ученой степени кандидата медицинских наук.
Является автором девяти научных публикаций.
Область научных интересов — этиология, патофизиология, диагностика и лечение желудочковых нарушений ритма различного характера и нарушений сердечной проводимости.
Эл. адрес: antsvet.18@mail.ru

ТИШКОВ
Артем
Валерьевич

Доцент, заведующий кафедрой физики, математики и информатики, старший научный сотрудник НИЦ биоинформатики Научно-образовательного института биомедицины Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова.

В 1996 году окончил Санкт-Петербургский государственный университет по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».

В 1999 году защитил диссертацию на соискание ученой степени кандидата физ.-мат. наук.

Является автором 101 научной публикации, в том числе трех патентов на изобретения.

Область научных интересов — молекулярная биология, генетика, анализ мутаций.

Эл. адрес: artem.tishkov@gmail.com

ЧОБАН
Адиль
Гаврилович

Студент бакалавриата Омского государственного технического университета.

Является автором 11 научных публикаций и трех свидетельств о регистрации электронных ресурсов.

Область научных интересов — биометрическая идентификация и аутентификация личности, машинное обучение, искусственные нейронные сети.

Эл. адрес: adil_choban@mail.ru

ТРЕШКУР
Татьяна
Васильевна

Заведующая НИЛ электрокардиологии, доцент кафедры внутренних болезней института медицинского образования Национального медицинского исследовательского центра им. В. А. Алмазова, Санкт-Петербург.

В 1972 году окончила 1-й Ленинградский медицинский институт им. акад. И. П. Павлова по специальности «Терапия».

В 1988 году защитила диссертацию на соискание ученой степени кандидата медицинских наук.

Является автором более 100 научных публикаций, семи монографий и пяти патентов.

Область научных интересов — нарушения сердечного ритма, электрокардиография, холтеровское мониторирование с телеметрической передачей данных через интернет маркеров внезапной сердечной смерти.

Эл. адрес: meinetvt@mail.ru

ШАЛЫТО
Анатолий
Абрамович

Профессор факультета информационных технологий и программирования Университета ИТМО, ученый секретарь НПО «Аврора», Санкт-Петербург.

В 1971 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика».

В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.

Является автором более 250 научных публикаций, трех монографий и 70 изобретений.

Область научных интересов — системы логического управления, автоматное программирование.

Эл. адрес: shalyto@mail.ifmo.ru

СОДЕРЖАНИЕ ЖУРНАЛА «ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ» ЗА 2020 г. [№ 1–6]

	№	Стр.
Sulavko A. E., Lozhnikov P. S., Choban A. G., Stadnikov D. G., Nigrey A. A., Inivatov D. P. Evaluation of EEG identification potential using statistical approach and convolutional neural networks	6	37
Алёшкин А. П., Владимиров В. В., Невзоров В. И., Савочкин П. В. Метод повышения разрешающей способности и точности радиолокационных угловых измерений на основе последовательной пространственно-временной обработки принимаемых сигналов	2	37
Арсеньев В. Н., Хомоненко А. Д., Ядренкин А. А. Взвешенный учет априорной и опытной информации в задаче оценивания эффективности функционирования системы управления при распределении числа испытаний по закону Паскаля	3	39
Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И. Окружности на решетках и матрицы максимума детерминанта	6	2
Браницкий А. А., Дойникова Е. В., Котенко И. В. Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям	1	24
Волков В. Ю. Адаптивная многопороговая селекция объектов на изображениях в системах дистанционного зондирования	3	12
Гейдаров П. Ш. Алгоритм вычисления значений весов синапсов первого слоя нейронной сети на основе метрических методов распознавания. Часть 1	2	20
Гейдаров П. Ш. Алгоритм вычисления значений весов синапсов первого слоя нейронной сети на основе метрических методов распознавания. Часть 2	3	25
Горбунова М. В., Омётов А. Я., Комаров М. М., Беззатеев С. В. Обзор проблем внедрения технологии распределенного реестра	2	10
Грачев П. Г., Муравьев С. Б., Фильченков А. А., Шалыто А. А. Генерация автоматов на основе рекуррентных нейросетей и автоматического выбора кластеризации	1	34
Двойникова А. А., Карпов А. А. Аналитический обзор подходов к распознаванию тональности русскоязычных текстовых данных	4	20
Дворников С. В., Конюховский В. С., Симонов А. Н. Способ частотно-пространственной селекции радиоизлучений с помощью триортогональной антенной системы	1	63
Демьянов В. В., Халиманов Д. С., Федоров М. Э., Имарова О. Б. Оценка качества алгоритма контроля доступности WAAS в условиях умеренной геомагнитной бури	2	46
Дикий Д. И. Метод обнаружения DoS-атак на прикладном уровне в сетях «издатель-подписчик»	4	50
Доронина Ю. В., Скатков А. В. Каскадно-иерархическое моделирование в задачах анализа динамики ресурсных характеристик сложных систем	3	48
Зотин А. Г., Фаворская М. Н. Применение штрихкодирования для цифрового маркирования видеопоследовательностей на основе частотных преобразований	5	12
Куц А. К., Максименко В. А., Храмова М. В., Храмов А. Е. Исследование процесса обработки зрительной информации в зависимости от ориентации стимулов по многоканальным записям ЭЭГ	1	73
Мальцев Г. Н., Джумков В. В. Аддитивная граница вероятности ошибки в дискретном канале передачи информации с помехоустойчивым кодированием и группированием ошибок	4	78
Мартынова Л. А., Киселев Н. К., Мысливый А. А. Метод выбора архитектуры мультиагентной системы управления автономного необитаемого подводного аппарата	4	31
Молдовян Д. Н., Молдовян А. А., Гурьянов Д. Ю. Протоколы слепой цифровой подписи на основе скрытой задачи дискретного логарифмирования	3	71
Осипов В. Ю., Милосердов Д. И. Нейросетевое прогнозирование событий для роботов с непрерывным обучением	5	33
Памяти Н. Н. Красильникова	1	81
Пятаев А. С., Фаворская М. Н. Классификация состояния деревьев по визуальным данным на основе нечеткой логики	3	2

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность
за достоверность и точность рекламных материалов несут рекламодатели.