

Информатика и её применения

Том 20 Выпуск 3 Год 2026

СОДЕРЖАНИЕ

Некоторые свойства кода квадратичных отношений и его использование
в задаче декодирования линейного кода

И. В. Чижев 2

Оптимальное управление марковскими скачкообразными процессами
по бесшумовым наблюдениям с задержками I: универсальный
стохастический базис и проблема мартингалов

А. В. Борисов, Ю. Н. Куринов 23

Устойчивые алгоритмы адаптивного оценивания состояний динамических
систем при случайных временных задержках наблюдений

А. В. Босов, С. А. Босов, И. В. Урюпин 33

Асимптотический анализ методов пороговой обработки
в разреженных моделях с пуассоновским числом наблюдений

Е. И. Мележников, О. В. Шестаков 47

Анализ загрузки многопользовательской сети при смешанных стратегиях
маршрутизации

Ю. Е. Малащенко, И. А. Назарова, М. В. Козлов 58

Интерпретация кластерной структуры данных на основе эллипсоидов

М. П. Кривенко 67

Самообучаемое инкрементальное обнаружение классов
на основе вероятностно-информированного непрерывного обучения

А. М. Достовалова, А. К. Горшенин 77

Методы порождения метрик на множествах объектов
в контексте топологической теории анализа данных.
Часть 2. Экспериментальное порождение метрик на объектах
в контексте метрических алгоритмов числового прогнозирования

И. Ю. Торшин 87

Моделирование автоматической многоаспектной идентификации проблемы
в гибридных интеллектуальных многоагентных системах

С. В. Листопад 96

Атаки на управляющие сетевые системы
с использованием обмана

**А. А. Грушо, Н. А. Грушо, М. И. Забежайло, А. А. Зацаринный,
В. О. Писковский** 104

Об авторах 110

Правила подготовки рукописей 112

НЕКОТОРЫЕ СВОЙСТВА КОДА КВАДРАТИЧНЫХ ОТНОШЕНИЙ И ЕГО ИСПОЛЬЗОВАНИЕ В ЗАДАЧЕ ДЕКОДИРОВАНИЯ ЛИНЕЙНОГО КОДА

И. В. Чижов¹

Аннотация: В 2023 г. был предложен подход к взлому криптосистемы Мак-Элиса, базирующийся на изучении так называемых кодов квадратичных отношений, которые связаны с произведением Шура–Адамара. Эти коды строятся из квадратичных форм, обращающихся в ноль на столбцах порождающей матрицы линейного кода. Эффективность такого подхода показана в недавней работе, где строится атака на криптосистему Мак-Элиса, основанную на двоичных кодах Гоппы малой степени; при этом в атаке используется тот факт, что в коде квадратичных отношений существует квадратичная форма небольшого ранга. В настоящей работе проводится систематическое изучение линейных кодов, у которых в коде квадратичных отношений имеются формы ранга 2 и ниже. Рассматривается специальный случай, когда в коде квадратичных отношений имеется приводимая квадратичная форма, т. е. раскладывающаяся в произведение ненулевых линейных форм. В финальной части работы рассматривается вопрос решения задачи декодирования для кодов, у которых в коде квадратичных отношений нет приводимых квадратичных форм либо их относительно мало.

Ключевые слова: код квадратичных отношений; квадрат Шура–Адамара кода; криптосистема Мак-Элиса; минимальный код; задача декодирования

DOI: 10.14357/19922264260301

EDN: IKIBAT

1 Введение

Постквантовая криптография представляет собой раздел криптографии, изучающий криптографические механизмы, реализуемые на классических вычислителях, для которых в настоящее время неизвестны эффективные алгоритмы взлома в модели нарушителя, обладающего квантовым вычислителем достаточной мощности.

Процесс разработки постквантовых алгоритмов и их стандартизации ведется как на международном, так и на национальном уровне. Он перешел в активную фазу в 2017 г., когда Национальный институт стандартов и технологий США (NIST) объявил конкурс на создание перспективных постквантовых схем электронной подписи и схем инкапсуляции секретного ключа. В ноябре 2022 г. аналогичный конкурс был объявлен также Научно-исследовательским институтом национальной безопасности Республики Корея (NSR) и Национальной разведывательной службой Республики Корея (NIS). В России также ведется разработка постквантовых криптографических механизмов в рамках рабочей группы технического комитета № 26 Росстандарта РФ.

Один из важных классов постквантовых криптографических механизмов представляют механиз-

мы, построенные на основе задачи декодирования линейного кода. Исторически первой такой криптосистемой с открытым ключом стала криптосистема, предложенная в 1978 г. Р. Мак-Элисом [1]. Криптосистема Мак-Элиса представляет собой не одну конкретную криптосистему, а некоторый каркас для построения криптосистем на различных семействах линейных кодов. Вариант Нидеррайтера [2] этой криптосистемы участвует в конкурсах по стандартизации и в настоящее время предлагается для стандартизации на международном уровне в рамках ISO.

В 2010 г. для криптографического анализа криптосистемы Мак-Элиса, основанной на подкодах обобщенного кода Рида–Соломона [3], была применена операция произведения Шура–Адамара линейных кодов [4]. Позднее, в 2014 г., эта операция была применена для построения эффективной атаки на криптосистему Мак-Элиса, основанную на двоичных кодах Рида–Маллера [5]. К настоящему времени с использованием этой операции построены атаки на большое число вариантов криптосистемы Мак-Элиса, в которых применяются различные классы линейных кодов. Среди них отметим подкоды алгебро-геометрических кодов [6], специальную конструкцию на обобщенных кодах Рида–Соломона [7], скрученные коды Рида–Соломо-

¹Московский государственный университет имени М. В. Ломоносова; Федеральный исследовательский центр «Информатика и управление» Российской академии наук, chizhoviv@my.msu.ru

на [8], подкоды кодов Рида–Маллера [9], последовательно соединенные коды Рида–Маллера [10] и др.

В 2023 г. был предложен подход к взлому криптосистемы Мак–Элиса [11], базирующийся на изучении так называемых кодов квадратичных отношений, которые связаны с произведением Шура–Адамара. Эти коды строятся из квадратичных форм, которые обращаются в ноль на столбцах порождающей матрицы линейного кода. Эффективность такого подхода недавно показана в работе [12], где строится атака на криптосистему Мак–Элиса, основанную на двоичных кодах Гоппы малой степени. При этом в атаке используется тот факт, что в коде квадратичных отношений существует квадратичная форма небольшого ранга.

В настоящей работе проводится систематическое изучение линейных кодов, у которых в коде квадратичных отношений имеются квадратичные формы ранга не выше 2. Рассматривается содержательный частный случай, когда в коде квадратичных отношений имеется приводимая над базовым полем квадратичная форма, т. е. раскладывающаяся в нетривиальное произведение линейных форм. В конце статьи рассматривается вопрос решения задачи декодирования для кодов, у которых в коде квадратичных отношений нет приводимых квадратичных форм, либо когда их относительно мало.

2 Основные термины и определения

Если $\mathbb{F}_q$ — конечное поле из q элементов, то для произвольного натурального числа n через $\mathbb{F}_q^n$ обозначим линейное пространство векторов длины n над полем $\mathbb{F}_q$. Тогда линейным блоковым кодом длины n над полем $\mathbb{F}_q$ (или просто $[n]_q$ -кодом) называется произвольное линейное подпространство $\mathcal{C}$ пространства $\mathbb{F}_q^n$.

Линейный код $\mathcal{C}$ как подпространство конечномерного пространства имеет некоторую размерность k , которая называется размерностью кода $\mathcal{C}$. Линейный код длины n и размерности k над полем $\mathbb{F}_q$ будем называть $[n, k]_q$ -кодом. Векторы $c \in \mathbb{F}_q^n$, лежащие в $\mathcal{C}$, называются кодовыми словами (или просто словами) $\mathcal{C}$.

В дальнейшем для произвольных натуральных чисел k и n через $\mathbb{F}_q^{k \times n}$ будем обозначать множество всех $(k \times n)$ -матриц над полем $\mathbb{F}_q$. Матрица $G_C \in \mathbb{F}_q^{k \times n}$, у которой строки образуют базис $[n, k]_q$ -кода $\mathcal{C}$ как линейного пространства, называется порождающей матрицей кода $\mathcal{C}$.

Матрицы $G_1, G_2 \in \mathbb{F}_q^{k \times n}$ порождают один и тот же код $\mathcal{C}$, если и только если для некоторой невырожденной $(k \times k)$ -матрицы A с элементами из поля $\mathbb{F}_q$ (т. е. $A \in \text{GL}_k(q)$) выполняется равенство $G_2 = A \cdot G_1$.

Систематической порождающей матрицей кода $\mathcal{C}$ называется порождающая матрица вида $G = (I_k | G')$, где I_k — единичная $(k \times k)$ -матрица, а G' — произвольная $(k \times (n - k))$ -матрица. Заметим, что в общем случае у линейного кода может не быть систематической порождающей матрицы, однако у него всегда существует порождающая матрица, которая отличается от систематической только перестановкой столбцов. В такой порождающей матрице единичная подматрица занимает, возможно, не первые k позиций, однако каждый столбец этой подматрицы с единицей в строке i , $i = \overline{1, k}$, находится в исходной матрице всегда правее всех остальных столбцов той же самой подматрицы, имеющих ненулевые позиции в строках j , $j < i$. Поэтому далее, когда будем говорить о систематической порождающей матрице, то будем под ней понимать матрицу описанного обобщенного вида. Отметим, что иногда в литературе такую порождающую матрицу называют полусистематической или почти систематической.

Для $[n, k]_q$ -кода $\mathcal{C}$ можно определить дуальный код $\mathcal{C}^\perp$ как множество всех векторов $x \in \mathbb{F}_q^n$, которые ортогональны каждому слову $\mathcal{C}$, т. е.

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c^\top = 0 \quad \forall c \in \mathcal{C}\}.$$

Ясно, что $\mathcal{C}^\perp$ является $[n, n - k]_q$ -кодом. Его порождающая $((n - k) \times n)$ -матрица H называется проверочной матрицей кода $\mathcal{C}$. Несложно увидеть, что $c \in \mathcal{C}$, если и только если $H \cdot c^\top = 0$.

Весом Хемминга (или просто весом) вектора $x \in \mathbb{F}_q^n$ называется целое число $\text{wt}(x)$, равное числу его ненулевых координат. Минимальным расстоянием $d(\mathcal{C})$ кода $\mathcal{C}$ будем называть минимальный вес ненулевых кодовых слов $\mathcal{C}$, т. е. если $\mathcal{C} = [n, k]_q$ -код, то $d(\mathcal{C}) = \min_{c \in \mathcal{C}, \text{wt}(c) \neq 0} \text{wt}(c)$. Если $[n, k]_q$ -код $\mathcal{C}$ имеет минимальное расстояние d , то такой код будем называть $[n, k, d]_q$ -кодом.

Справедливо следующее утверждение (см. [13]).

Утверждение 1 (граница Синглтона). Для любого $[n, k, d]_q$ -кода выполняется неравенство $d \leq n - k + 1$.

С каждым вектором $x \in \mathbb{F}_q^n$ можно связать множество $\text{supp}(x)$ номеров его ненулевых координат, которое в дальнейшем будем называть носителем вектора x . Таким образом, если $[n] \stackrel{\text{def}}{=} \{1, 2, \dots, n\}$, то

$$\text{supp}(x) \stackrel{\text{def}}{=} \{i \in [n] \mid x_i \neq 0\},$$

где $x = (x_1, x_2, \dots, x_n)$.

Для произвольного множества векторов $X \subseteq \mathbb{F}_q^n$ определим носитель $\text{supp}(X)$ этого множества как объединение носителей векторов x , принадлежащих X , т. е.

$$\text{supp}(X) = \bigcup_{x \in X} \text{supp}(x).$$

Таким образом, можно говорить о носителе $\text{supp}(\mathcal{C})$ кода $\mathcal{C}$. Если для кода $\mathcal{C}$ выполняется равенство $\text{supp}(\mathcal{C}) = \llbracket n \rrbracket$, то $\mathcal{C}$ будем называть кодом с полным носителем. Код имеет полный носитель, если и только если его порождающая матрица не имеет нулевых столбцов; это также эквивалентно тому, что минимальное расстояние $d(\mathcal{C}^\perp)$ дуального кода $\mathcal{C}^\perp$ не меньше двух: $d(\mathcal{C}^\perp) \geq 2$.

3 Произведение Шура–Адамара, квадратичные формы и код квадратичных отношений

Произведением Шура–Адамара (произведением Шура, произведением Адамара или покомпонентным произведением) $[n]_q$ -кодов $\mathcal{C}$ и $\mathcal{B}$ будем называть $[n]_q$ -код $\mathcal{A} = \mathcal{C} \circ \mathcal{B}$, который порожден линейной оболочкой векторов:

$$\left\{ c \circ b = (c_1, \dots, c_n) \circ (b_1, \dots, b_n) \stackrel{\text{def}}{=} \right. \\ \left. \stackrel{\text{def}}{=} (c_1 \cdot b_1, \dots, c_n \cdot b_n) \mid c \in \mathcal{C}, b \in \mathcal{B} \right\}.$$

Если $s \in \mathbb{N}$, то степень Шура–Адамара кода $\mathcal{C}$ будем называть код

$$\mathcal{C}^{\circ s} = \underbrace{\mathcal{C} \circ \mathcal{C} \circ \dots \circ \mathcal{C}}_{s \text{ раз}}.$$

Тогда квадратом Шура–Адамара кода $\mathcal{C}$ называется вторая степень Шура–Адамара этого кода, т. е. код $\mathcal{C}^{\circ 2} = \mathcal{C} \circ \mathcal{C}$. Для любого $[n, k]_q$ -кода $\mathcal{C}$ выполняется неравенство

$$\dim \mathcal{C}^{\circ 2} \leq \min \left(n, \frac{k(k+1)}{2} \right).$$

Если $\mathbb{F}_q[x_1, \dots, x_k] = \mathbb{F}_q[x]$ — кольцо многочленов от переменных $x = (x_1, x_2, \dots, x_k)$, то через $\mathbb{F}_q[x_1, \dots, x_k]^{(d)} = \mathbb{F}_q[x]^{(d)}$ обозначим линейное пространство всех однородных многочленов степени d . В частности, $\mathbb{F}_q[x_1, \dots, x_k]^{(1)} = \mathbb{F}_q[x]^{(1)}$ — линейное пространство всех линейных форм, которое состоит из многочленов вида

$$L(x_1, \dots, x_k) = a_1 x_1 + a_2 x_2 + \dots + a_k x_k, \\ a_1, a_2, \dots, a_k \in \mathbb{F}_q.$$

Тогда $\mathbb{F}_q[x_1, \dots, x_k]^{(2)} = \mathbb{F}_q[x]^{(2)}$ — пространство квадратичных форм, т. е. всех многочленов вида

$$Q(x_1, x_2, \dots, x_k) = \sum_{1 \leq i \leq j \leq k} a_{i,j} x_i x_j, \quad a_{i,j} \in \mathbb{F}_q.$$

Зафиксируем некоторый кортеж (упорядоченное множество) $U = (u_1, u_2, \dots, u_n)$ векторов из $\mathbb{F}_q^k$, т. е. $U \in (\mathbb{F}_q^k)^n$ и $u_i = (u_{i,1}, u_{i,2}, \dots, u_{i,k}) \in \mathbb{F}_q^k$ для всех $i = \overline{1, n}$. Определим линейный оператор $\text{eval}_U : \mathbb{F}_q[x] \rightarrow \mathbb{F}_q^n$, который каждому многочлену $f(x_1, x_2, \dots, x_k)$ ставит в соответствие его вектор значений на элементах U , т. е.

$$f(x_1, x_2, \dots, x_k) \rightarrow (f(u_1), f(u_2), \dots, f(u_n)) \in \mathbb{F}_q^n,$$

где $f(u_i) \stackrel{\text{def}}{=} f(u_{i,1}, u_{i,2}, \dots, u_{i,k}) \in \mathbb{F}_q$ — значение полинома f на векторе u_i , $i = \overline{1, n}$.

Пусть $G \in \mathbb{F}_q^{k \times n}$ и $G = (g^{(1)}, g^{(2)}, \dots, g^{(n)})$, где $g^{(i)} = (g_{1,i}, g_{2,i}, \dots, g_{k,i})$ — столбец с номером i , $i = \overline{1, n}$, матрицы G . Тогда G можно рассматривать как кортеж ее столбцов и поэтому будет определено отображение eval_G , которое $f \in \mathbb{F}_q[x]$ ставит в соответствие вектор значений f на столбцах матрицы G , т. е.

$$\text{eval}_G(f) = (f(g^{(1)}), f(g^{(2)}), \dots, f(g^{(n)})) \in \mathbb{F}_q^n.$$

В дальнейшем потребуется сужение $\text{eval}_G^{(1)}$ операторов eval_G на пространство линейных форм $\mathbb{F}_q[x]^{(1)}$, т. е. $\text{eval}_G^{(1)} : \mathbb{F}_q[x]^{(1)} \rightarrow \mathbb{F}_q^n$ и $\text{eval}_G^{(1)}(L) \stackrel{\text{def}}{=} \text{eval}_G(L)$. Кроме того, будем также рассматривать сужение $\text{eval}_G^{(2)}$ оператора на пространство квадратичных форм $\mathbb{F}_q[x]^{(2)}$.

Утверждение 2. Если $G \in \mathbb{F}_q^{k \times n}$ и $\text{rank } G = k$, то $\ker \text{eval}_G^{(1)} = \{0\}$, т. е. отображение $\text{eval}_G^{(1)}$ инъективно и устанавливает биекцию между $\mathbb{F}_q[x]^{(1)}$ и $[n, k]_q$ -кодом $\mathcal{C}$, порожденным матрицей G .

Если $a = (a_1, a_2, \dots, a_k) \in \mathbb{F}_q^k$ и $G \in \mathbb{F}_q^{k \times n}$ является порождающей матрицей $[n, k]_q$ -кода $\mathcal{C}$, то оператор $\text{eval}_G^{(1)}$ каждой линейной форме $L = a_1 x_1 + a_2 x_2 + \dots + a_k x_k$ ставит в соответствие кодовое слово $c = a \cdot G \in \mathcal{C}$. При этом согласно утверждению 2 это сопоставление взаимно однозначно.

Утверждение 3 [14]. Если матрица $G \in \mathbb{F}_q^{k \times n}$ порождает код $\mathcal{C}$, то справедливо равенство $\text{Imeval}_G^{(2)} = \mathcal{C}^{\circ 2}$.

Из утверждения 3 следует, что для любой невырожденной матрицы $A \in \text{GL}_k(q)$ выполняется

равенство $\text{Imeval}_G^{(2)} = \text{Imeval}_{A \cdot G}^{(2)}$, т. е. образ оператора $\text{eval}_G^{(2)}$ не зависит от выбора порождающей матрицы линейного кода.

Ситуация меняется, если вместо образа оператора $\text{eval}_G^{(2)}$ рассмотреть его ядро. В общем случае $\ker \text{eval}_G^{(2)}$ и $\ker \text{eval}_{A \cdot G}^{(2)}$ не совпадают, поэтому ядро этого оператора зависит от выбора порождающей матрицы линейного кода.

С $\ker \text{eval}_G^{(2)}$ можно связать другой линейный код [11].

Если

$$\text{coeff}(Q) \stackrel{\text{def}}{=} (a_{1,1}, a_{1,2}, \dots, a_{1,k}, a_{2,2}, \dots, a_{k,k}) \in \mathbb{F}_q^{k(k+1)/2},$$

то код $\mathcal{Q}_G$ состоит из векторов $\text{coeff}(Q)$, $Q \in \ker \text{eval}_G^{(2)}$. Ясно, что если k_2 — размерность квадрата $\mathcal{C}^{\circ 2}$ кода $\mathcal{C}$, порождаемого матрицей G , то $\mathcal{Q}_G$ представляет собой $[k(k+1)/2, k(k+1)/2 - k_2]_q$ -код. Код $\mathcal{Q}_G$ называется кодом квадратичных отношений, связанных с порождающей матрицей G кода $\mathcal{C}$.

В работе будут рассматриваться квадратичные формы $Q \in \ker \text{eval}_G^{(2)}$, которые можно разложить на линейные множители, т. е. для которых существуют такие $L_1, L_2 \in \mathbb{F}_q[x_1, x_2, \dots, x_k]^{(1)}$, что

$$Q(x_1, x_2, \dots, x_k) = L_1(x_1, x_2, \dots, x_k) \cdot L_2(x_1, x_2, \dots, x_k).$$

Определение 1. Квадратичную форму $Q \in \mathbb{F}_q[x]^{(2)}$ будем называть *приводимой*, если существуют такие $L_1, L_2 \in \mathbb{F}_q[x]^{(1)}$, $L_1, L_2 \neq 0$, что $Q = L_1 \cdot L_2$. При этом если для линейной формы $L_1 \in \mathbb{F}_q[x]^{(1)}$ существует такая линейная форма $L_2 \in \mathbb{F}_q[x]^{(1)}$, что выполняется равенство $Q = L_1 \cdot L_2$, то будем говорить, что L_1 делит Q или служит делителем Q .

Ненулевую квадратичную форму, которая не является приводимой, будем называть простой.

Каждой квадратичной форме Q можно поставить в соответствие ее матрицу $M_Q = (m_{i,j}) \in \mathbb{F}_q^{k \times k}$ следующим образом:

$$m_{i,j} = \begin{cases} a_{i,j}, & \text{если } 1 \leq i \leq j \leq k; \\ 0 & \text{иначе.} \end{cases}$$

Тогда можно рассмотреть симметрическую матрицу $B_Q = M_Q + M_Q^\top$, которая фактически является матрицей билинейной формы, соответствующей квадратичной форме Q . Если характеристика поля $\mathbb{F}_q$ отлична от двух, то соответствие $Q \leftrightarrow B_Q$ биективно. В случае когда поле $\mathbb{F}_q$ имеет характеристику 2, можно говорить только о биективном соответствии между B_Q и фактор-пространством $\mathbb{F}_q[x]^{(2)} / \langle x_1^2, \dots, x_k^2 \rangle$.

Несложно понять, что если квадратичная форма Q представима в виде $Q = L_1 \cdot L_2$, то ранг матрицы B_Q не больше 2. В работе [11] предлагается подход к анализу криптосистемы Мак-Элиса, построенной на основе кодов, у которых в коде квадратичных отношений есть векторы, связанные с квадратичными формами ранга не более 3 или 4. Таким образом, наличие в коде квадратичных отношений слов, связанных с приводимыми квадратичными формами, позволяет говорить, что в нем содержатся слова, отвечающие формам небольшого ранга.

Далее постараемся ответить на два вопроса. Во-первых, приводимых квадратичных форм в $\ker \text{eval}_G^{(2)}$ может не быть, поэтому необходимо изучить условия, при которых такие формы существуют. Во-вторых, интерес представляет алгебраическая структура делителей L_1 и L_2 таких квадратичных форм.

4 Условия существования в коде квадратичных отношений слов, связанных с приводимыми квадратичными формами

Начнем с установления простого, но важного свойства отображения eval_U .

Утверждение 4. Для любых $F_1, F_2 \in \mathbb{F}_q[x]$ и любого кортежа $U \in (\mathbb{F}_q^k)^n$ выполняется равенство

$$\text{eval}_U(F_1 \cdot F_2) = \text{eval}_U(F_1) \circ \text{eval}_U(F_2). \quad (1)$$

Доказательство. Справедливость утверждения прямо следует из определения eval_U и того факта, что для любого $u \in \mathbb{F}_q^k$ выполняется равенство $(F_1 \cdot F_2)(u) = F_1(u) \cdot F_2(u)$. $\square$

Из утверждения 4 следует, что если $Q = L_1 \cdot L_2$, то

$$\begin{aligned} \text{eval}_G^{(2)}(Q) &= \text{eval}_G(Q) = \text{eval}_G(L_1) \circ \text{eval}_G(L_2) = \\ &= \text{eval}_G^{(1)}(L_1) \circ \text{eval}_G^{(1)}(L_2). \end{aligned}$$

Несложно доказать следующее

Утверждение 5. Если $L_1, L_2 \in \mathbb{F}_q[x]^{(1)}$, то равенство $\text{eval}_G^{(1)}(L_1) \circ \text{eval}_G^{(1)}(L_2) = 0$ выполняется, если и только если множества ненулевых координат векторов $\text{eval}_G^{(1)}(L_1)$ и $\text{eval}_G^{(1)}(L_2)$ не пересекаются, т. е. $\text{supp}(\text{eval}_G^{(1)}(L_1)) \cap \text{supp}(\text{eval}_G^{(1)}(L_2)) = \emptyset$.

Теперь в качестве следствия из утверждения 5 получим следующее

Утверждение 6. Если двоичный $[n, k]_2$ -код $\mathcal{C}$ с порождающей матрицей G содержит вектор 1^n , состоящий из n единиц, и $k \geq 2$, то $\ker \text{eval}_G^{(2)}$ содержит приводимые квадратичные формы Q .

Доказательство. Для доказательства утверждения достаточно заметить, что если в $\mathcal{C}$ имеется вектор 1^n и размерность $\mathcal{C}$ не меньше 2, то в $\mathcal{C}$ найдется еще хотя бы один вектор $c \neq 1^n, 0^n$.

Значит, можно рассмотреть векторы $c_1 = c$ и $c_2 = c + 1^n$, $c_1, c_2 \neq 0^n$.

Тогда в двоичном случае $c_1 \circ c_2 = 0^n$, и поэтому если $c_1 = \text{eval}_G^{(1)}(L_1)$ и $c_2 = \text{eval}_G^{(1)}(L_2)$, то, во-первых, $L_1, L_2 \neq 0$, потому что на основании утверждения 2 отображение $\text{eval}_G^{(1)}$ биективно, а во-вторых, на основании утверждения 5 верно включение $Q = L_1 \cdot L_2 \in \ker \text{eval}_G^{(2)}$, так как по построению $\text{supp}(c_1) \cap \text{supp}(c_2) = \emptyset$. $\square$

Продолжим характеризацию кодов, в ядре Шур-Адамара которых имеются приводимые квадратичные формы.

Если $T \subseteq [n]$ и $v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$, то через $v|_T$ обозначим подвектор вектора v , составленный из координат с номерами из множества T , т. е. $v|_T = (v_i, i \in T) \in \mathbb{F}_q^{|T|}$.

Далее определим еще два вектора: $v_{\setminus T}$ и v_T . Вектор $v_{\setminus T} \in \mathbb{F}_q^{n-|T|}$ имеет длину $n - |T|$ и состоит из тех координат вектора v , номера которых не лежат в множестве T , т. е. $v_{\setminus T} = v|_{[n] \setminus T}$ и он получается из v удалением координат с номерами из множества T . Вектор $v_T \in \mathbb{F}_q^n$ имеет ту же длину, что v , и получается из v обнулением координат, имеющих номера из множества T . Получается, что если $v_T = (u_1, u_2, \dots, u_n)$, то для всех $i \in [n] \setminus T$ выполняется равенство $u_i = v_i$, а для $i \in T$ — равенство $u_i = 0$, т. е. $(v_T)|_T = 0^{|T|}$ и $(v_T)_{\setminus T} = v_{\setminus T}$.

Аналогичную систему обозначений перенесем и на матрицы.

Определение 2. Пусть $I \subseteq [n]$. Традиционно множество I называется информационным окном или информационным множеством $[n, k]_q$ -кода $\mathcal{C}$ с порождающей матрицей G , если $|I| = k$ и подматрица $G|_I$, составленная из столбцов G с номерами из I , невырожденна.

Определение 3. Для $[n]_q$ -кода $\mathcal{C}$ и множества $T \subseteq [n]$ через $\mathcal{C}_T$ обозначим $[n]_q$ -код, состоящий из c_T для всех $c \in \mathcal{C}$. Назовем T -выколотым (или просто выколотым) кодом $[n - |T|]_q$ -код $\mathcal{C}_{\setminus T}$, который состоит из векторов $c_{\setminus T}$ для всех $c \in \mathcal{C}$. И, наконец, T -укороченным (или просто укороченным) кодом назовем $[n]_q$ -код $\mathcal{C}^T = \mathcal{C}_T \cap \mathcal{C}$.

Легко понять, что если $T \neq \emptyset$, то, вообще говоря, $\mathcal{C}_{\setminus T}$ не будет подкодом кода $\mathcal{C}$. Код $\mathcal{C}_T$ станет под-

кодом кода $\mathcal{C}$, если и только если $T \cap \text{supp}(\mathcal{C}) = \emptyset$. И $\mathcal{C}^T$ — подкод $\mathcal{C}$ по построению.

Утверждение 7. Пусть $c \in \mathcal{C}$ и $T \subseteq [n]$. Тогда $c \in \mathcal{C}^T$, если и только если $\text{supp}(c) \cap T = \emptyset$.

Размерность подкода $\mathcal{C}^T$ устанавливает следующее утверждение.

Утверждение 8. Если $[n, k]_q$ -код $\mathcal{C}$ имеет порождающую матрицу G , а $T \subset [n]$, то $\mathcal{C}^T$ является $[n, k - \text{rank } G|_T]_q$ -кодом.

Используя несложные соображения из линейной алгебры, можно доказать следующее

Утверждение 9. Множество $I \subseteq [n]$, $|I| = k$, будет информационным для $[n, k]_q$ -кода $\mathcal{C}$, если и только если выполнено одно из условий:

- (1) $\mathcal{C}^I = \{0^n\}$;
- (2) для любого $c \in \mathcal{C}$ из равенства $c|_I = c_{\setminus ([n] \setminus I)} = 0^k$ следует, что $c = 0^n$, т. е. для любого ненулевого кодового слова c его подвектор, состоящий из координат с номерами из I , не равен нулевому вектору.

Зададимся вопросом, при каком условии для заданной линейной формы $L \in \mathbb{F}_q[x]^{(1)}$, $L \neq 0$, существует такая линейная форма $K \in \mathbb{F}_q[x]^{(1)}$, $K \neq 0$, что $Q = L \cdot K$ принадлежит $\ker \text{eval}_G^{(2)}$.

Для каждой линейной формы $L \in \mathbb{F}_q[x]^{(1)}$ определим множество

$$Z_G(L) = \left\{ K \in \mathbb{F}_q[x]^{(1)} \mid Q = L \cdot K \in \ker \text{eval}_G^{(2)} \right\} \subseteq \mathbb{F}_q[x]^{(1)}.$$

Заметим, что $Z_G(L)$ — линейное подпространство $\mathbb{F}_q[x]^{(1)}$. Более того, если $c = \text{eval}_G^{(1)}(L)$, то существует взаимно однозначное соответствие (т. е. изоморфизм) между $Z_G(L)$ и $\mathcal{C}^{\text{supp}(c)}$. Оно устанавливается следующим утверждением.

Утверждение 10. Если L — линейная форма, то $K \in Z_G(L)$ тогда и только тогда, когда $b = \text{eval}_G^{(1)}(K) \in \mathcal{C}^T$, где $T = \text{supp}(c)$ и $c = \text{eval}_G^{(1)}(L)$.

Доказательство. Линейная форма $K \in \mathbb{F}_q[x]^{(1)}$ принадлежит $Z_G(L)$, если и только если $Q = L \cdot K \in \ker \text{eval}_G^{(2)}$, т. е. $\text{eval}_G^{(1)}(K) \circ \text{eval}_G^{(1)}(L) = 0^n$. На основании утверждения 5 выполнение равенства $\text{eval}_G^{(1)}(K) \circ \text{eval}_G^{(1)}(L) = 0^n$ равносильно выполнению соотношения $T \cap \text{supp}(\text{eval}_G^{(1)}(K)) = \emptyset$. Это, в свою очередь, эквивалентно включению $b \in \mathcal{C}^T$. $\square$

Как следствие из утверждения 10 докажем следующее

Утверждение 11. Пусть G — порождающая матрица $[n, k]_q$ -кода $\mathcal{C}$, $L \in \mathbb{F}_q[x]^{(1)}$, $L \neq 0$, и $c = \text{eval}_G^{(1)}(L)$. Тогда существует такая линейная форма $K \in \mathbb{F}_q[x]^{(1)}$, что $K \neq 0$ и $Q = L \cdot K \in \ker \text{eval}_G^{(2)}$, если и только если $\text{supp}(c)$ не содержит информационное множество кода $\mathcal{C}$. Или, что то же самое, $\dim Z_G(L) \geq 1$, если и только если $\text{supp}(c)$ не содержит информационное множество кода $\mathcal{C}$.

Доказательство. Если существует такая ненулевая форма $K \in \mathbb{F}_q[x]^{(1)}$, что $Q = K \cdot L \in \ker \text{eval}_G^{(2)}$, то на основании утверждения 10 выполняется включение $b = \text{eval}_G^{(1)}(K) \in \mathcal{C}^T$.

В силу утверждения 2 выполнено неравенство $b \neq 0^n$, так как $K \neq 0$. Поэтому в данном случае код $\mathcal{C}^T$ будет содержать ненулевое кодовое слово.

Для произвольного подмножества S множества T справедливо включение $\mathcal{C}^T \subseteq \mathcal{C}^S$, поэтому код $\mathcal{C}^S$ для любого подмножества $S \subseteq T$ будет содержать ненулевой вектор. Но тогда, применяя к S пункт 1 утверждения 9, получим, что все эти подмножества S не относятся к информационным множествам кода $\mathcal{C}$, т. е. T не содержит информационное множество этого кода.

Обратно: пусть T не содержит информационное множество $\mathcal{C}$, тогда опять из утверждения 9 следует наличие в коде $\mathcal{C}^T$ ненулевого кодового слова b , которое и будет соответствовать ненулевой линейной форме K из пространства $Z_G(L)$. $\square$

С учетом утверждения 8 получим размерность $Z_G(L)$.

Утверждение 12. Пусть матрица G порождает $[n, k]_q$ -код $\mathcal{C}$. Если L — линейная форма и $T = \text{supp}(\text{eval}_G^{(1)}(L))$, то $\dim Z_G(L) = \dim \mathcal{C}^T = k - \text{rank } G|_T$.

Из утверждения 10 следует простой способ проверки того, существует ли для данной линейной формы L такая линейная форма $K \neq 0$, что $Q = L \cdot K \in \ker \text{eval}_G^{(2)}$. Для этого следует вычислить размерность кода $\mathcal{C}^T$, $T = \text{supp}(\text{eval}_G^{(1)}(L))$, и сравнить ее с нулем. Если размерность этого кода не равна нулю, то такая K существует, а если она равна нулю, то таких K нет.

Из утверждения 11 в качестве следствия сформируем ряд теорем.

Теорема 1. Пусть G — порождающая матрица кода $\mathcal{C}$. Тогда $\ker \text{eval}_G^{(2)}$ не содержит приводимые квадратичные формы, если и только если носитель каждого ненулевого кодового слова $\mathcal{C}$ содержит информационное множество.

Теорема 2. Если $\mathcal{C}$ — $[n, k, d]_q$ -код, $d < k$, и G — его порождающая матрица, то $\ker \text{eval}_G^{(2)}$ содержит приводимые квадратичные формы.

Доказательство. Так как $d < k$, то найдется кодовое слово, у которого носитель содержит меньше k элементов, поэтому носитель этого слова не может содержать информационное множество. Значит, из теоремы 1 следует, что $\ker \text{eval}_G^{(2)}$ для любой порождающей матрицы G кода $\mathcal{C}$ содержит квадратичную форму вида $Q = L \cdot K \neq 0$. $\square$

В 1984 г. в работе [15] было введено понятие пересекающегося кода.

Определение 4. Код $\mathcal{C}$ называется пересекающимся, если для любой пары линейно независимых кодовых слов кода $\mathcal{C}$ их носители пересекаются, т. е. для любых $c_1 \in \mathcal{C}$, $c_1 \neq 0$, и $c_2 \in \mathcal{C}$, $c_2 \neq 0$, $c_1 \neq a \cdot c_2$ для всех $a \in \mathbb{F}_q$, выполняется неравенство $\text{supp}(c_1) \cap \text{supp}(c_2) \neq \emptyset$.

Из утверждения 5 прямо следует утверждение

Утверждение 13. Если $G \in \mathbb{F}_q^{k \times n}$ имеет ранг k , то $\ker \text{eval}_G^{(2)}$ не содержит приводимые квадратичные формы тогда и только тогда, когда матрица G порождает пересекающийся код $\mathcal{C}$.

Интересно, что в поле из двух элементов коды, для которых ядро Шура–Адамара не содержит квадратичных форм, представимых в виде произведения ненулевых линейных форм, могут быть охарактеризованы через наличие или отсутствие в них неминимальных кодовых слов.

Начнем с определения минимального кодового слова.

Определение 5. Кодовое слово c называется минимальным для $[n]_q$ -кода $\mathcal{C}$, если для любого кодового слова $c' \in \mathcal{C}$ из включения $\text{supp}(c') \subseteq \text{supp}(c)$ следует, что $c' = a \cdot c$ для некоторой константы $a \in \mathbb{F}_q$.

Таким образом, носитель минимальных кодовых слов не содержит носитель других линейно независимых с ним кодовых слов.

Понятие минимальных кодовых слов было впервые введено в работе [16], а их систематическое изучение начато в работе [17].

Лемма 1. Если c — ненулевое кодовое слово $[n]_2$ -кода $\mathcal{C}$, не являющееся минимальным, то существуют такие ненулевые кодовые слова c_1 и c_2 , что $c = c_1 + c_2$ и $\text{supp}(c_1) \cap \text{supp}(c_2) = \emptyset$.

Доказательство следует из леммы 2.1 работы [17]. $\square$

Утверждение 14. Пусть $[n]_q$ -код $\mathcal{C}$ порождается матрицей G . Если ядро оператора $\text{eval}_G^{(2)}$ содержит приводимую квадратичную форму, то в коде $\mathcal{C}$ есть кодовые слова, не являющиеся минимальными.

Доказательство. Если для некоторой $Q \neq 0$ существуют такие линейные формы K и L , что

$Q = K \cdot L$, то на основании утверждений 2 и 5 носители кодовых слов $c_1 = \text{eval}_G^{(1)}(K)$ и $c_2 = \text{eval}_G^{(1)}(L)$, во-первых, не пустые множества, а во-вторых, не пересекаются. Поэтому носитель кодового слова $c = c_1 + c_2$ содержит строго носитель каждого из векторов c_1 и c_2 , а значит, c не может быть линейно зависимым ни с одним из векторов c_1 и c_2 , и поэтому он не является минимальным кодовым словом. $\square$

Утверждение 15. Пусть $[n]_2$ -код C порождается матрицей G . Тогда ядро оператора $\text{eval}_G^{(2)}$ содержит приводимую квадратичную форму, если и только если в коде C есть кодовые слова, не являющиеся минимальными.

Доказательство следует из леммы 1 и утверждения 5 с учетом утверждения 14. $\square$

Следуя работе [18], введем следующее

Определение 6. Коды, в которых все кодовые слова минимальные, называются минимальными.

Получается, что в случае поля $\mathbb{F}_2$ множество матриц G , для которых в $\ker \text{eval}_G^{(2)}$ нет приводимых квадратичных форм, совпадает с множеством порождающих матриц минимальных двоичных кодов, т. е. справедлива

Теорема 3. Пусть G — $(k \times n)$ -матрица максимального ранга с элементами из поля $\mathbb{F}_2$. Тогда ядро $\ker \text{eval}_G^{(2)}$ не содержит приводимых квадратичных форм, если и только если G порождает минимальный двоичный код.

В произвольном конечном поле можно утверждать только то, что множество матриц G , для которых в $\ker \text{eval}_G^{(2)}$ есть приводимые квадратичные формы, содержится в множестве порождающих матриц неминимальных кодов.

Следующая теорема устанавливает, что для некоторых параметров n и k для порождающей матрицы G любого $[n, k]_q$ -кода ядро $\ker \text{eval}_G^{(2)}$ содержит приводимые квадратичные формы.

Теорема 4. Пусть G — порождающая матрица $[n, k]_q$ -кода C . Тогда если $n < 2k - 1$, то $\ker \text{eval}_G^{(2)}$ содержит хотя бы одну приводимую квадратичную форму.

Доказательство. Воспользуемся границей Синглтона. Согласно утверждению 1 для любого $[n, k, d]_q$ -кода C справедливо неравенство $d \leq n - k + 1$. Значит, если $n < 2k - 1$, то $d \leq n - k + 1 < 2k - 1 - k + 1 = k$. И теперь, применяя теорему 2, получим требуемое. $\square$

В работе [11] (утверждение 10, с. 16) говорится, что ядро отображения $\text{eval}_R^{(2)}$ для порождающей матрицы R случайного линейного $[n, k]_q$ -кода $\mathcal{R}$ при $n < 2k - 1$ в предположении, что матричный

код квадратичных отношений, который получается из $\mathcal{Q}_R$ представлением каждого вектора коэффициентов квадратичной формы в виде соответствующей симметрической матрицы квадратичной формы, имеет распределение весов, характерное для случайного матричного кода, с **непренебрежимой** вероятностью содержит квадратичные формы ранга не более чем 2.

Теорема 4 утверждает, что для таких параметров n и k в ядре оператора $\text{eval}_G^{(2)}$ для порождающей матрицы G **любого** кода содержится приводимая квадратичная форма, т. е. содержится форма ранга 2 с вероятностью 1, а не просто с **непренебрежимой** вероятностью.

Утверждение 16. Пусть код C с порождающей матрицей G — $[n, k, d]_q$ -код и при этом $d \geq k$. Если дуальный код $C^\perp$ имеет такое минимальное расстояние $d^\perp$, что $d^\perp \geq k + 1$, то ядро $\ker \text{eval}_G^{(2)}$ не содержит приводимых квадратичных форм.

Доказательство. Будем действовать от противного. Пусть в $\ker \text{eval}_G^{(2)}$ найдется такая квадратичная форма $Q \neq 0$, что $Q = K \cdot L$. Рассмотрим $c = \text{eval}_G^{(1)}(K)$. Так как $Q \neq 0$, то и $K \neq 0$, поэтому и $c \neq 0^n$. Из утверждения 11 следует, что $\text{supp}(c)$ не содержит информационного множества кода C . По определению информационного множества это означает, что матрица $G|_{\text{supp}(c)}$ имеет ранг строго меньше k . Кроме того, $|\text{supp}(c)| \geq d \geq k$, поэтому существует такой ненулевой вектор $v \in \mathbb{F}_q^{|\text{supp}(c)|}$, что $G|_{\text{supp}(c)} \cdot v^\top = 0$.

Более того, так как ранг $G|_{\text{supp}(c)}$ меньше или равен $k - 1$, то в $G|_{\text{supp}(c)}$ найдется система из не более чем k столбцов, ненулевая линейная комбинация которых равна 0, поэтому можно считать, что $\text{wt}(v) \leq k$.

По v построим $h \in \mathbb{F}_q^n$ следующим образом: на множестве $\text{supp}(c)$ он совпадает с v , а все координаты не из $\text{supp}(c)$ равны 0, т. е. $h|_{\text{supp}(c)} = v$ и $h|_{\text{supp}(c)^c} = 0^{n-\text{wt}(c)}$. С учетом выбора v и построения h выполняется цепочка равенств $G \cdot h^\top = G|_{\text{supp}(c)} \cdot v^\top + G|_{[n] \setminus \text{supp}(c)} \cdot h|_{\text{supp}(c)}^\top = 0$, т. е. $h \in C^\perp$.

Теперь, так как $v \neq 0$, то $h \neq 0$. Вес Хемминга ненулевого кодового слова h кода $C^\perp$ не может быть меньше минимального расстояния $C^\perp$, т. е. $d^\perp$, поэтому $\text{wt}(h) \geq d^\perp$. А значит, $\text{wt}(v) = \text{wt}(h) \geq d^\perp \geq k + 1$. Но по построению $\text{wt}(v) \leq k < k + 1$, что невозможно. Получено противоречие. $\square$

Из границы Синглтона (утверждение 1) следует, что минимальное расстояние $d^\perp$ кода, дуального к $[n, k]_q$ -коду C , не превосходит $n - (n - k) + 1 = k + 1$. При этом коды, для которых $d = n - k + 1$, называются кодами с максимальным дистанцион-

ным расстоянием (МДР-кодами). Код, дуальный к МДР-коду, сам является МДР-кодом, поэтому $d^\perp = k + 1$. Таким образом, из утверждения 16 вытекает справедливость следующей теоремы.

Теорема 5. Если $[n, k, d]_q$ -код C является МДР-кодом и $n \geq 2k - 1$, то для порождающей матрицы G кода C ядро $\ker \text{eval}_G^{(2)}$ не содержит приводимые квадратичные формы.

Установим связь между размерностью пространства $Z_G(L)$ и весом вектора $c = \text{eval}_G^{(1)}(L)$. Для этого введем еще одно понятие.

Определение 7. Для произвольного $[n, k]_q$ -кода C и числа $r \in \mathbb{N}$ определим $d_r(C) \in \mathbb{N}$ как минимальную мощность носителя всех $[n, r]_q$ -подкодов D кода C , т. е.

$$d_r \stackrel{\text{def}}{=} \min \{ |\text{supp}(D)| : D \text{ — подкод размерности } r \text{ кода } C \}.$$

Число $d_r(C)$ называется r -м обобщенным расстоянием Хемминга кода C .

Ясно, что $d_1 = d$ — минимальное расстояние кода C .

Обобщенное расстояние Хемминга линейных кодов впервые введено в работе [19]. В той же работе доказано следующее утверждение, которое является естественным обобщением границы Синглтона.

Утверждение 17. Для любого $[n, k]_q$ -кода C и любого $r \in \mathbb{N}$ справедливо неравенство $d_r \leq n - k + r$.

Обобщенные минимальные расстояния строго возрастают с ростом r , т. е. справедливо утверждение [19].

Утверждение 18. Для любого $[n, k]_q$ -кода C справедливо неравенства

$$0 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n.$$

Используя утверждение 17, докажем следующее

Утверждение 19. Пусть G — порождающая матрица $[n, k]_q$ -кода C и $L \in \mathbb{F}_q[x]^{(1)}$ и $c = \text{eval}_G^{(1)}(L)$. Тогда если выполняется неравенство $\dim Z_G(L) \geq r$, то $\text{wt}(c) \leq n - d_r(C)$.

Доказательство. По условию $Z_G(L)$ содержит r линейно независимых линейных форм $K_1, K_2, \dots, K_r \in \mathbb{F}_q[x]^{(1)}$. Пусть $T = \text{supp}(\text{eval}_G^{(1)}(L))$. Из утверждения 10 следует, что линейная форма K_i , $i = \overline{1, r}$, принадлежит $Z_G(L)$, если и только если $c_i = \text{eval}_G^{(1)}(K_i) \in C^T$.

Заметим, что в силу утверждения 2 векторы $c_1, c_2, \dots, c_r$ линейно независимы, так как $K_1, K_2, \dots, K_r$ линейно независимы.

Итак, код C^T , с одной стороны, является подкодом кода C , а с другой — имеет размерность по меньшей мере r . Рассмотрим D — произвольный подкод кода C^T размерности r . По определению обобщенного расстояния Хемминга $d_r = d_r(C)$ должно выполняться неравенство $d_r \leq |\text{supp}(D)|$. Но $\text{supp}(D) \subseteq \text{supp}(C^T)$, поэтому $d_r \leq |\text{supp}(C^T)|$.

Но $|\text{supp}(C^T)| \leq n - |T|$, а значит, должно выполняться неравенство $d_r \leq n - |T|$. Осталось заметить, что по построению $|T| = \text{wt}(\text{eval}_G^{(1)}(L)) = \text{wt}(c)$. $\square$

Следующее утверждение — прямое следствие утверждения 19.

Утверждение 20. Пусть G — порождающая матрица $[n, k, d]_q$ -кода C , $L \in \mathbb{F}_q[x]^{(1)}$ и $c = \text{eval}_G^{(1)}(L)$. Тогда если существует такая линейная форма $K \in \mathbb{F}_q[x]^{(1)}$, что $K \neq 0$ и $Q = L \cdot K \in \ker \text{eval}_G^{(2)}$, то $\text{wt}(c) \leq n - d$.

Выходит, что если линейная форма L делит хотя бы одну квадратичную форму из $\ker \text{eval}_G^{(2)}$, то она соответствует кодовому слову c небольшого веса. И, более того, из утверждения 19 следует, что чем больше квадратичных форм делит L , тем меньший вес имеет c . Поэтому поиск в $\ker \text{eval}_G^{(2)}$ квадратичных форм ранга 2 может оказаться в общем случае вычислительно сложной задачей.

В завершение раздела докажем утверждение о максимально возможной размерности $Z_G(L)$. Если код C имеет порождающую матрицу G , то можно рассмотреть величину

$$z(C) \stackrel{\text{def}}{=} \max_{\substack{L \in \mathbb{F}_q[x]^{(1)}, \\ L \neq 0}} \dim Z_G(L).$$

Так как $\max \dim Z_G(L)$ не зависит от выбора порождающей матрицы кода C , то величина $z(C)$ определена корректно и служит характеристикой кода C , а не его порождающей матрицы.

Утверждение 21. Если r — такое минимальное натуральное число, что для линейного $[n]_q$ -кода C выполняется неравенство $d_r(C) + d_1(C) > n$, то $z(C) \leq r - 1$.

Доказательство. Пусть G — порождающая матрица C . Для любой ненулевой линейной формы L выполняется неравенство $\dim Z_G(L) < r$. Действительно, пусть для линейной формы L выполнено $\dim Z_G(L) \geq r$. Из утверждения 19 следует, что в этом случае для кодового слова $c = \text{eval}_G^{(1)}(L)$ верно неравенство $\text{wt}(c) \leq n - d_r(C)$. Но по условию $d_r(C) + d_1(C) > n$, поэтому $\text{wt}(c) < d_1(C)$. Вес кодового слова может быть меньше минимального расстояния только в случае, когда это слово нулевое, т. е. $c = 0$. Отсюда следует, что если $\dim Z_G(L) \geq r$, то $L = 0$.

Итак, для любой ненулевой линейной формы L выполняется неравенство $\dim Z_G(L) < r$. Это же неравенство должно выполняться и для максимального значения $\dim Z_G(L)$ по всем ненулевым L , т. е. $z(C) = \max_L \dim Z_G(L) < r$. $\square$

Для величины $z(C)$ можно установить следующую оценку снизу.

Утверждение 22. Если в $[n, k]_q$ -коде C существует кодовое слово c веса w , то выполняется неравенство $z(C) \geq k - w$. В частности, если d — минимальное расстояние C , то $z(C) \geq k - d$.

Доказательство. Зафиксируем порождающую матрицу G кода C и рассмотрим такую $L \in \mathbb{F}_q[x]^{(1)}$, что $c = \text{eval}_G^{(1)}(L)$.

Пусть $T = \text{supp}(c)$. Тогда в силу утверждения 12 выполняется неравенство

$$z(C) \geq \dim Z_G(L) = k - \text{rank } G|_T.$$

Так как матрица $G|_T$ имеет w столбцов, то $\text{rank } G|_T \leq w$, и поэтому $z(C) \geq k - w$. Неравенство $z(C) \geq k - d$ следует из того, что по определению минимального расстояния кода выполняется неравенство $w \geq d$. $\square$

Теорема 6. Если у $[n, k, d]_q$ -кода C дуальный к нему код $C^\perp$ имеет минимальное расстояние $d^\perp$, то $k - d \leq z(C) \leq k - \min(d, d^\perp - 1)$.

Доказательство. Неравенство $z(C) \geq k - d$ прямо следует из утверждения 22.

Далее, если $c \in C$ имеет носитель T и для $L \in \mathbb{F}_q[x]^{(1)}$ выполняется равенство $c = \text{eval}_G^{(1)}(L)$, то из утверждения 12 следует, что $z(C) \leq k - \min_{c \in C, c \neq 0} \text{rank } G|_T$.

Так как любая система из $d^\perp - 1$ столбцов матрицы G линейно независима, то $\text{rank } G|_T \geq \min(|T|, d^\perp - 1)$, а T — носитель кодового вектора кода C , поэтому $|T| \geq d$. Значит, $\min_{c \in C, c \neq 0} \text{rank } G|_T \geq \min(d, d^\perp - 1)$. $\square$

На основании теоремы 6 параметр $z(C)$ можно качественно интерпретировать как характеристику близости C к классу МДР-кодов.

5 Задача декодирования кодов, у которых в ядре Шура—Адамара нет приводимых квадратичных форм

В этом разделе рассматривается вопрос о том, как наличие приводимых квадратичных форм

в ядре оператора $\text{eval}_G^{(2)}$ можно использовать для построения алгоритма декодирования произвольного линейного кода. Идея состоит в том, чтобы свести задачу декодирования к задаче поиска приводимой квадратичной формы специального вида в ядре кода, пополненного вектором ошибки. Сначала сформулируем эту задачу формально и установим соответствующее сведение (разд. 5.1), затем опишем алгоритм построения пространства $Z_G(L)$ (разд. 5.2), на основе которого построим алгоритм декодирования (разд. 5.3). В разд. 5.4 проведем вероятностный анализ среднего числа итераций, а в разд. 5.5 сравним предложенный алгоритм с известными методами на конкретных параметрах.

5.1 Сведение задачи декодирования к поиску приводимой формы

Начнем с формальной постановки задачи декодирования и покажем, что при $t < k$ ее можно эквивалентным образом переформулировать как задачу поиска приводимой квадратичной формы в ядре оператора $\text{eval}_G^{(2)}$, связанного с расширенным кодом.

Для произвольного $[n, k]_q$ -кода C введем задачу декодирования.

Определение 8. Пусть y — некоторый вектор длины n над полем $\mathbb{F}_q$, а t — натуральное число. Тогда задачей декодирования $\text{DEC}_C(y, t)$ кода C называется задача поиска такого кодового слова $c \in C$, что $\text{wt}(y - c) = t$.

Обычно код C задан своей порождающей (G) или проверочной (H) матрицей. Поэтому когда требуется в задаче $\text{DEC}_C(y, t)$ конкретизировать, каким способом задан C , будем писать $\text{DEC}_C(G, y, t)$, если C задан порождающей матрицей G , и $\text{DEC}_C(H, y, t)$ — если проверочной матрицей H .

Получается, что на вход задачи $\text{DEC}_C(G, y, t)$ подается $(k \times n)$ -матрица G , вектор y и число t , а на вход задачи $\text{DEC}_C(H, y, t)$ также подаются вектор y и число t , а вместо порождающей матрицы подается проверочная $((n - k) \times n)$ -матрица H .

Если G — порождающая $(k \times n)$ -матрица $[n, k]_q$ -кода C и $y \in \mathbb{F}_q^n$, $y \notin C$, то рассмотрим код $y + C$, который порождается $((k + 1) \times n)$ -матрицей $(G; y)$, т. е. $(G; y)$ получается из G добавлением строки y . Несложно увидеть, что код $y + C$ представляет собой объединение кода C и смежных классов $\{a \cdot y\} + C \stackrel{\text{def}}{=} \{a \cdot y + c \mid c \in C\}$, $a \in \mathbb{F}_q$, $a \neq 0$, т. е. $y + C = C \sqcup \bigsqcup_{a \in \mathbb{F}_q, a \neq 0} (\{a \cdot y\} + C)$.

Из утверждения 11 следует

Утверждение 23. Пусть G — $(k \times n)$ -матрица, порождающая $[n, k]_q$ -код C , и $e \in \mathbb{F}_q^n$, $e \notin C$, имеет вес Хемминга $t < k$. Рассмотрим код $e + C$, порождаемый

матрицей $(G; e)$. Если $L \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$ — такая линейная форма, что $e = \text{eval}_{(G;e)}^{(1)}(L)$, то существует такая $K \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$, $K \neq 0$, что $Q = L \cdot K \in \ker \text{eval}_{(G;e)}^{(2)}$, т.е. $Z_{(G;e)}(L) \neq \{0\}$.

Утверждение 24. Пусть $G \in \mathbb{F}_q^{k \times n}$ — порождающая матрица некоторого $[n, k]_q$ -кода $\mathcal{C}$, $y \in \mathbb{F}_q^n$, $y \notin \mathcal{C}$, и $t < k$.

Задача декодирования $\text{DEC}_{\mathcal{C}}(G, y, t)$ имеет решение, если и только если в $\ker \text{eval}_{(G;y)}^{(2)}$ существует приводимая квадратичная форма $Q = L \cdot K$, $L, K \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$, у которой сомножитель L имеет ненулевой коэффициент при переменной x_{k+1} , а вектор $\text{eval}_{(G;y)}^{(1)}(L)$ имеет вес t .

Доказательство. Пусть задача $\text{DEC}_{\mathcal{C}}(G, y, t)$ имеет решение, т.е. существует такое $c \in \mathcal{C}$, что вектор $e = y - c$ имеет вес t . Так как строки матрицы $(G; y)$ образуют базис кода $y + \mathcal{C}$, а $e \in y + \mathcal{C}$, то существует единственная линейная форма $L \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$, для которой $e = \text{eval}_{(G;y)}^{(1)}(L)$. Если $c = a \cdot G$ для $a = (a_1, \dots, a_k) \in \mathbb{F}_q^k$, то $L = -a_1 x_1 - \dots - a_k x_k + x_{k+1}$, поэтому коэффициент при x_{k+1} у L равен 1, т.е. отличен от нуля. Так как $\text{wt}(e) = t < k$, то носитель кодового слова e не может содержать информационное множество, поэтому из утверждения 11 следует существование такой линейной формы $K \neq 0$, что $Q = L \cdot K \in \ker \text{eval}_{(G;y)}^{(2)}$. Форма Q приводима и удовлетворяет всем требованиям утверждения.

Обратно. Пусть $Q = L \cdot K \in \ker \text{eval}_{(G;y)}^{(2)}$, у L коэффициент a_{k+1} при x_{k+1} отличен от нуля и $e' = \text{eval}_{(G;y)}^{(1)}(L)$ имеет вес t . По построению кода $y + \mathcal{C}$ выполняется равенство $e' = a_{k+1} \cdot y + c_0$ для некоторого $c_0 \in \mathcal{C}$. Положим $c = y - a_{k+1}^{-1} \cdot e'$. Тогда $c = y - a_{k+1}^{-1} (a_{k+1} \cdot y + c_0) = -a_{k+1}^{-1} \cdot c_0 \in \mathcal{C}$ и при этом $\text{wt}(y - c) = \text{wt}(a_{k+1}^{-1} \cdot e') = \text{wt}(e') = t$. Значит, c — решение задачи $\text{DEC}_{\mathcal{C}}(G, y, t)$. $\square$

Сформулированное утверждение показывает, что задача декодирования при $t < k$ полностью эквивалентна задаче поиска приводимой формы специального вида.

Отметим ограничение $t < k$: при $t \geq k$ метод неприменим. Таким образом, центральной для дальнейшего изложения становится задача построения линейных форм L , для которых пространство $Z_{(G;y)}(L)$ нетривиально.

5.2 Вычисление базиса пространства $Z_G(L)$

Для практической реализации алгоритма декодирования потребуется эффективная процедура по-

строения базиса пространства $Z_G(L)$ для заданной линейной формы L .

Можно использовать два подхода. Первый заключается в построении базиса $Q_1, Q_2, \dots, Q_m$ ядра $\ker \text{eval}_G^{(2)}$, где $m = \dim \ker \text{eval}_G^{(2)}$. И далее, зафиксировав предварительно порядок мономов $x_i x_j$, поделить каждую Q_i на L и вычислить остаток R_i от этого деления. Теперь каждое решение $b = (b_1, b_2, \dots, b_m)$ уравнения

$$b_1 R_1 + b_2 R_2 + \dots + b_m R_m = 0$$

будет соответствовать квадратичной форме $Q = b_1 Q_1 + b_2 Q_2 + \dots + b_m Q_m$, которая и делится на L , а значит, частное $K = Q/L$ является линейной формой, которая лежит в $Z_G(L)$. Общая трудоемкость первого способа оценивается величиной $O(k^6)$ операций в поле $\mathbb{F}_q$.

Второй способ основан на утверждении 10. По определению $Z_G(L)$ состоит из всех линейных форм K , для которых $L \cdot K \in \ker \text{eval}_G^{(2)}$. Но в силу утверждения 10 линейная форма K принадлежит $Z_G(L)$, если и только если $c = \text{eval}_G^{(1)}(K)$ лежит в коде $\mathcal{C}^T$ для $T = \text{supp}(\text{eval}_G^{(1)}(L))$. Получается, что для построения $Z_G(L)$ достаточно вычислить базис укорочения кода $\mathcal{C}$ по носителю кодового слова, соответствующего L . Построение базиса этого кода осуществляется с помощью применения алгоритма исключения Гаусса, который требует не более $O(k^2 \cdot n)$ операций в поле $\mathbb{F}_q$. В приложениях обычно работают с кодами, у которых $n < k^2$, поэтому трудоемкость этого способа меньше, чем первого. Далее на основе этой идеи опишем алгоритм построения $Z_G(L)$.

Несложно доказать следующее

Утверждение 25. Алгоритм 1 требует не более $O(k^2 n)$ операций в поле $\mathbb{F}_q$ и возвращает нулевую строку, если $\dim Z_G(L) = 0$.

Тем самым задача построения базиса $Z_G(L)$ решена, и алгоритм 1 будет использоваться дальше как подпрограмма в алгоритме декодирования.

5.3 Алгоритм декодирования

Согласно утверждению 24 задача декодирования сводится к поиску приводимой формы $Q = L \cdot K$ в ядре расширенного кода. Естественная стратегия — перебирать линейные формы L и для каждой проверять, существует ли подходящая $K \in Z_{(G;y)}(L)$, дающая решение. Опишем процедуру, выполняющую такую проверку для заданной L .

Следующая лемма устанавливает связь размерности пространства $Z_{(G;y)}(L)$ для расширенного кода через характеристику $z(\mathcal{C})$ исходного кода, а не его расширения. Это позволяет переложить анализ

Алгоритм 1. Алгоритм построения $Z(L)$ **Вход:** G — $(k \times n)$ -матрица, $L = a_1x_1 + \dots + a_kx_k$ — линейная форма над $\mathbb{F}_q$.**Выход:** $B_L \in \mathbb{F}_q^{r \times k}$ — матрица, строки которой служат векторами коэффициентов линейных форм, образующих базис $Z_G(L)$, здесь $r = \dim Z_G(L)$, либо 0^k , если $\dim Z_G(L) = 0$.

```

1   $a \leftarrow (a_1, a_2, \dots, a_k) \stackrel{\text{def}}{=} \text{coeff}(L)$ ;
2   $c \leftarrow a \cdot G$ ;
3   $w \leftarrow \text{wt}(c)$ ;
4   $i_1, i_2, \dots, i_w \leftarrow \text{supp}(c)$ ;
5   $(g^{(1)}, g^{(2)}, \dots, g^{(n)}) \leftarrow c \circ G$ ; // вычисляется произведение Адамара вектора  $c$  на каждую строку матрицы  $G$ 
6   $F \leftarrow (g^{(i_1)}, g^{(i_2)}, \dots, g^{(i_w)})$ ; //  $F \in \mathbb{F}_q^{k \times w}$ 
7   $F \leftarrow (F \ I_k)$ ; //  $I_k$  — единичная  $(k \times k)$ -матрица,  $F \in \mathbb{F}_q^{k \times (w+k)}$ 
8   $F = (f^{(1)}, f^{(2)}, \dots, f^{(w)}, f^{(w+1)}, f^{(w+2)}, \dots, f^{(w+k)}) \leftarrow \text{rref}(F)$ ;
9   $s \leftarrow \text{rank}(f^{(1)}, f^{(2)}, \dots, f^{(w)})$ ;
10 if  $s = k$  then
11   | return  $0^k$ ; //  $\dim Z_G(L) = 0$ 
12 end
13  $B = (b_{(1)}, b_{(2)}, \dots, b_{(k)}) \leftarrow \text{rows}(F|_{\{w+1, \dots, w+k\}})$ ; // строки  $(k \times k)$ -подматрицы  $F|_{\{w+1, \dots, w+k\}}$ , составленной из последних  $k$  столбцов матрицы  $F$ 
14  $B_L \leftarrow (b_{(s+1)}, b_{(s+2)}, \dots, b_{(k)})$ ; // берем последние  $k - s$  строк
15 return  $B_L$ 

```

сложности алгоритма с расширенного кода на исходный, для которого $z(C)$ — известный инвариант.

Лемма 2. Пусть G — порождающая $(k \times n)$ -матрица $[n, k]_q$ -кода C , $y \in \mathbb{F}_q^n$, $y \notin C$, а $L \in \mathbb{F}_q[x_1, \dots, x_{k+1}]^{(1)}$ — линейная форма с нулевым коэффициентом при x_{k+1} , т.е. $L(x_1, \dots, x_{k+1}) = L_0(x_1, \dots, x_k) + 0 \cdot x_{k+1}$, где $L_0 \in \mathbb{F}_q[x_1, \dots, x_k]^{(1)}$ — некоторая ненулевая линейная форма от первых k переменных.

Тогда

$$\dim Z_{(G;y)}(L) \leq \dim Z_G(L_0) + 1 \leq z(C) + 1.$$

Кроме того, если r — такое минимальное натуральное число, что $d_r(C) + d(C) > n$, то $\dim Z_{(G;y)}(L) \leq r$.

Доказательство. Заметим, что $L = L_0(x_1, \dots, x_k) + 0 \cdot x_{k+1}$, поэтому $c = \text{eval}_{(G;y)}^{(1)}(L)$ соответствует кодовому слову кода C с порождающей матрицей G . Рассмотрим код $y + C$, который порождается матрицей $(G; y)$.

Положим $T = \text{supp}(c)$. В силу утверждения 8 выполняется равенство

$$\dim(y + C)^T = k + 1 - \text{rank}(G; y)|_T.$$

Так как добавление строки к матрице либо не изменяет ранга матрицы, либо увеличивает его ровно на 1, то

$$k + 1 - \text{rank}(G; y)|_T \leq k + 1 - \text{rank } G|_T.$$

откуда получим неравенство

$$\dim(y + C)^T \leq \dim C^T + 1,$$

а значит,

$$\dim Z_{(G;y)}(L) \leq \dim Z_G(L_0) + 1 \leq z(C) + 1.$$

Отсюда получаем первую часть утверждения.

Выберем такое минимальное r , что $d_r(C) + d(C) > n$. Из утверждения 21 следует, что $z(C) \leq r - 1$ и, значит, верна вторая часть утверждения. $\square$

Утверждение 26. Пусть матрица G — порождающая матрица $[n, k]_q$ -кода C . Тогда алгоритм 2 требует не более $O(q^{z(C)}kn + k^2n)$ операций в поле $\mathbb{F}_q$.

Если r — такое минимальное натуральное число, что $d_r(C) + d(C) > n$, то алгоритм 2 требует не более $O(q^{r-1}kn + k^2n)$ операций в поле $\mathbb{F}_q$.

Доказательство. В алгоритме 2 перебираются в цикле все элементы множества $Z_{(G;y)}(L) \subseteq \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$, у которых коэффициент при переменной x_{k+1} , отвечающей вектору y , не равен 0. При переборе отождествляются линейные формы вида $a \cdot K$ для всех $a \in \mathbb{F}_q$, $a \neq 0$. Это связано с тем, что кодовые слова, соответствующие таким линейным формам, имеют один и тот же носитель.

Общее число итераций основного цикла алгоритма не превосходит величины $q^{\ell-1}$, где $\ell = \dim Z_{(G;y)}(L)$. Каждая итерация требует не более $O(kn)$ операций в поле $\mathbb{F}_q$, поэтому общая

Алгоритм 2. Алгоритм тестирования линейных форм

Вход: $G \leftarrow (k \times n)$ -матрица, порождающая $[n, k]_q$ -код $\mathcal{C}$, $y \in \mathbb{F}_q^n$ — вектор для декодирования,
 $t \in \mathbb{N}$ — число ошибок, $L = a_1x_1 + \dots + a_kx_k$ — линейная форма над $\mathbb{F}_q$.

Выход: $e \in \mathbb{F}_q^n$, $\text{wt}(e) = t$ и $y - e \in \mathcal{C}$, либо символ $\perp$

```

1  $L \leftarrow L + 0 \cdot x_{k+1}$  ; // Рассматриваем  $L$  как элемент  $\mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$ 
2  $B \leftarrow \text{basis}(Z_{(G;y)}(L))$  ; // алгоритм 1,  $B \in \mathbb{F}_q^{\ell \times (k+1)}$ , где  $\ell = \dim Z_{(G;y)}(L)$ 
   //  $B \stackrel{\text{def}}{=} (b^{(1)}, b^{(2)}, \dots, b^{(k+1)}) \stackrel{\text{def}}{=} (b_{(1)}, b_{(2)}, \dots, b_{(\ell)})$ 
3  $i' \leftarrow 0$  ;
4 for  $i = 1, 2, \dots, \ell$  do
5   if  $b_{i,k+1} \neq 0$  then
6      $i' \leftarrow i$  ;
7     break
8   end
9 end
10 if  $i' = 0$  then
11   return  $\perp$ 
12 end
   //  $b^{(k+1)} \neq 0^\ell$ 
13  $b_{(1)}, b_{(i')} = b_{(i')}, b_{(1)}$  ;
14  $b_{(1)} \leftarrow b_{1,k+1}^{-1} \cdot b_{(1)}$  ;
15 for  $i = 2, 3, \dots, \ell$  do
16    $b_{(i)} \leftarrow b_{(i)} - b_{i,k+1} \cdot b_{(1)}$  ;
17 end
18 for  $a' \in \mathbb{F}_q^{\ell-1}$  do
19    $a \leftarrow (1; a') \in \mathbb{F}_q^\ell$  ;
20    $e \leftarrow (a \cdot B) \cdot (G; y) \in \mathbb{F}_q^n$  ;
21   if  $\text{wt}(e) = t$  then
22     return  $e$ 
23   end
24 end
25 return  $\perp$ 

```

трудоемкость алгоритма не превосходит $O(q^{\ell-1}kn)$. Теперь, используя лемму 2 для оценки ℓ , получим справедливость требуемого утверждения. $\square$

Алгоритм 2 требует выбора линейной формы L . Случайный выбор крайне неэффективен: вероятность того, что произвольная L делит хотя бы одну форму из $\ker \text{eval}_{(G;y)}^{(2)}$, мала.

Утверждение 20 подсказывает разумный источник кандидатов: если L делит форму из ядра, то соответствующее ей кодовое слово $c = \text{eval}_G^{(1)}(L)$ имеет вес не более $n - d$, т.е. оказывается словом относительно небольшого веса в коде $\mathcal{C}$.

Более того, если минимальное расстояние d кода $\mathcal{C}$ удовлетворяет неравенству $d \geq k - 1$, то кодовые слова, которые соответствуют приводимым формам, должны иметь вес не более $n - d \leq n - k + 1$. Такие слова легко находить, так как их естественным источником служит систематическая матрица линейного кода. Описанная идея реализована в алгоритме 3.

Оценка сложности одной итерации алгоритма 3 устанавливается следующим утверждением.

Утверждение 27. *Одна итерация алгоритма 3 требует не более $O(q^{z(C)}(t+1) \cdot kn + (t+1)k^2n)$ операций в поле $\mathbb{F}_q$.*

Отметим, что оценка утверждения 27 соответствует худшему случаю $\text{rank } G|_I = k$. Если $\text{rank } G|_I < k$, то на итерации выполняется ровно один вызов алгоритма 2.

Остается вопрос о числе итераций алгоритма 3.

5.4 Вероятностный анализ среднего числа итераций

Для конкретного кода число прогонов алгоритма 3 зависит от деталей структуры кода. Чтобы получить осмысленную оценку для типичного кода, перейдем к вероятностной модели случайной порождающей матрицы. В этой модели оценим

Алгоритм 3. Алгоритм декодирования выбором векторов из систематической матрицы

Вход: $G \leftarrow (k \times n)$ -матрица, порождающая $[n, k]_q$ -код $\mathcal{C}$, $y \in \mathbb{F}_q^n$ — вектор для декодирования, $t \in \mathbb{N}$ — количество ошибок.

Выход: $e \in \mathbb{F}_q^n$, $\text{wt}(e) = t$ и $y - e \in \mathcal{C}$

```

1 while true do
2    $I \leftarrow \{J \subseteq [n], |J| = k\}$ ;
3    $R, A \leftarrow \text{rref}(G|_I)$ ;           // Построение приведенного ступенчатого вида  $R$  матрицы  $G|_I$ ,
                                     // возвращает  $R$  и матрицу преобразования  $A$ , т. е.  $R = A \cdot G|_I$ .
   //  $A = (a_{(1)}, a_{(2)}, \dots, a_{(k)})$ 
4    $\rho \leftarrow \text{rank } R$ ;
5   if  $\rho = k$  then
6      $M \leftarrow \{1, 2, \dots, t + 1\}$ ;
7   else
8      $M \leftarrow \{\rho + 1\}$ ;
9   end
10  for  $i \in M$  do
11     $a_1, a_2, \dots, a_k \leftarrow a_{(i)}$ ;
12     $L \leftarrow a_1 x_1 + a_2 x_2 + \dots + a_k x_k$ ;
13     $e \leftarrow \text{testLF}(G, y, t, L)$ ; // алгоритм 2
14    if  $e \neq \perp$  then
15      return  $e$ 
16    end
17  end
18 end

```

среднее число «удачных» k -подмножеств I , при выборе которых алгоритм находит решение.

Введем следующую вероятностную схему. Будем случайно, равновероятно и независимо друг от друга выбирать векторы $g_1, g_2, \dots, g_n$ из $\mathbb{F}_q^k$. Сформируем из этих векторов $(k \times n)$ -матрицу $G = (g^{(1)}, g^{(2)}, \dots, g^{(n)})$, в которой столбец $g^{(i)}$ с номером i , $i = \overline{1, n}$, равен вектору g_i : $g^{(i)} = g_i$. Построение матрицы G описанным способом будем обозначать как $G \leftarrow \$_{\mathbb{F}_q^{k \times n}}$.

Если $L_e \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$ и $e = \text{eval}_{(G; y)}^{(1)}(L_e)$, то, чтобы оценить вероятность нахождения решения на одной итерации алгоритма 3, необходимо оценить количество таких подмножеств $I \subseteq [n]$, что матрица $A \cdot G$ в строках, проверяемых алгоритмом, будет содержать $c \in \mathcal{C}$, соответствующий линейной форме $K \in \mathbb{F}_q[x_1, \dots, x_k]^{(1)}$, $c = \text{eval}_G^{(1)}(K)$, для которой линейная форма $K + 0 \cdot x_{k+1} \in \mathbb{F}_q[x_1, \dots, x_k, x_{k+1}]^{(1)}$ лежит в множестве $Z_{(G; y)}(L_e)$. Так как

$$\text{eval}_{(G; y)}^{(1)}(K + 0 \cdot x_{k+1}) = \text{eval}_G^{(1)}(K) = c,$$

то согласно утверждениям 10 и 7 включение $K + 0 \cdot x_{k+1} \in Z_{(G; y)}(L_e)$ выполняется, если и только если

$$\text{supp}(c) \cap \text{supp}(e) = \emptyset.$$

Выходит, что для успеха итерации алгоритма достаточно, чтобы было выбрано такое подмножество $I \subseteq [n]$, что среди множества строк матрицы $A \cdot G$, проверяемых алгоритмом, содержится вектор $c \in \mathcal{C}$, у которого множество ненулевых координат не пересекается с множеством ненулевых координат вектора ошибок e .

Утверждение 28. Зафиксируем вектор $e \in \mathbb{F}_q^n$ веса t . Пусть $\mathcal{J}$ — множество всех k -подмножеств I множества $[n]$, для которых среди проверяемых алгоритмом 3 строк матрицы $A \cdot G$ содержится кодовое слово c с носителем, не пересекающимся с $\text{supp}(e)$, т. е.

$$\mathcal{J} = \{I \subseteq [n] \mid |I| = k, \exists i \in M : \text{supp}((A \cdot G)_{(i)}) \cap \text{supp}(e) = \emptyset\}.$$

Здесь, как и в алгоритме 3, $A \leftarrow (k \times k)$ -матрица, которая приводит подматрицу $G|_I$ к приведенной ступенчатой форме, а M — множество номеров проверяемых строк:

$$M = \begin{cases} \{1, 2, \dots, t + 1\}, & \text{если } \text{rank } G|_I = k; \\ \{\text{rank } G|_I + 1\} & \text{иначе.} \end{cases}$$

Тогда справедливо неравенство

$$\mathbb{E}_{G \leftarrow \$_{\mathbb{F}_q^{k \times n}}}[\|\mathcal{J}\|] \geq \max_{\substack{s \in \mathbb{Z}, \\ s \in [0, \min(t, k-1)]}} q^{-(t-s)} \binom{t}{s} \binom{n-t}{k-s}. \quad (2)$$

Доказательство. Выберем и зафиксируем некоторое число $s \in \mathbb{Z}$, $0 \leq s \leq t$.

Для каждого $I \subseteq \llbracket n \rrbracket$ рассмотрим индикатор $\delta_I \in \{0, 1\}$, который принимает значение 1, если и только если $I \in \mathcal{J}$, т. е.

$$\delta_I = \begin{cases} 1, & \text{если } I \in \mathcal{J}; \\ 0 & \text{иначе.} \end{cases}$$

Найдем математическое ожидание суммы $|\mathcal{J}| = \sum_{I \subseteq \llbracket n \rrbracket, |I|=k} \delta_I$. По свойству линейности получим

$$\begin{aligned} \mathbb{E}_{G \leftarrow \mathbb{F}_q^{k \times n}}[|\mathcal{J}|] &= \sum_{I \subseteq \llbracket n \rrbracket, |I|=k} \mathbb{E}_{G \leftarrow \mathbb{F}_q^{k \times n}}[\delta_I] = \\ &= \sum_{I \subseteq \llbracket n \rrbracket, |I|=k} \Pr_{G \leftarrow \mathbb{F}_q^{k \times n}}[I \in \mathcal{J}]. \end{aligned}$$

Обозначим через $\mathcal{I}_s$ множество тех $I \subseteq \llbracket n \rrbracket$, $|I| = k$, которые пересекаются с $\text{supp}(e)$ ровно по s координатам.

Если $I \notin \mathcal{I}_s$, то оценим вероятность $\Pr[I \in \mathcal{J}]$ тривиально нулем. Для каждого s получим неравенство

$$\begin{aligned} \sum_{I \subseteq \llbracket n \rrbracket, |I|=k} \Pr_{G \leftarrow \mathbb{F}_q^{k \times n}}[I \in \mathcal{J}] &\geq \\ &\geq \sum_{I \in \mathcal{I}_s} \Pr_{G \leftarrow \mathbb{F}_q^{k \times n}}[I \in \mathcal{J}]. \end{aligned}$$

Теперь оценим вероятность $\Pr_{G \leftarrow \mathbb{F}_q^{k \times n}}[I \in \mathcal{J}]$ для тех I , которые лежат в $\mathcal{I}_s$.

При $s \geq k$ вероятность $\Pr[I \in \mathcal{J}]$ оценим тривиально нулем.

В остальных случаях воспользуемся формулой полной вероятности

$$\Pr[I \in \mathcal{J}] = \sum_{F \in \mathbb{F}_q^{k \times k}} \Pr[I \in \mathcal{J} | G|_I = F] \cdot \Pr[G|_I = F].$$

Пусть I содержит s , $s \leq \min(t, k-1)$, номеров из $\text{supp}(e)$. Покажем, что среди проверяемых алгоритмом строк найдется строка с таким номером $i_0 \in M$, что слово $a_{(i_0)} \cdot G$ имеет нули на всех позициях из множества $I \cap \text{supp}(e)$. Если $\text{rank } G|_I = k$, то $\text{rref}(G|_I) = I_k$, поэтому каждая строка матрицы $A \cdot G$ имеет внутри I ровно одну ненулевую позицию. Позиций из множества $I \cap \text{supp}(e)$ не более s , поэтому среди строк с номерами $1, 2, \dots, s+1$, $s+1 \leq t+1$, найдется хотя бы одна строка, у которой на всех позициях из $I \cap \text{supp}(e)$ стоят нули. Если же $\rho = \text{rank } G|_I < k$, то строка с номером $\rho+1$ матрицы $\text{rref}(G|_I)$ нулевая, поэтому проверяемая в этом случае строка $a_{(\rho+1)} \cdot G$ имеет нули на всем множестве I и тем более на множестве $I \cap \text{supp}(e)$.

Функция rref детерминированная, поэтому для каждой $(k \times k)$ -матрицы F однозначно определены матрица A , приводящая F к приведенной ступенчатой форме, множество M и минимальный номер $i_0 \in M$, для которого строка i_0 матрицы $A \cdot G$ в координатах с номерами из $I \cap \text{supp}(e)$ содержит нули. Обозначим через $\bar{I}$ множество, состоящее из всех оставшихся номеров столбцов из $\text{supp}(e)$, которые не попали в I , т. е. $\bar{I} = \text{supp}(e) \setminus I$. Тогда, чтобы носитель слова $a_{(i_0)} \cdot G$ не пересекался с $\text{supp}(e)$, достаточно выполнения равенства $a_{(i_0)} \cdot G|_{\bar{I}} = 0$. Значит, для каждой фиксированной матрицы F будет выполняться неравенство

$$\Pr[I \in \mathcal{J} | G|_I = F] \geq \Pr[a_{(i_0)} \cdot G|_{\bar{I}} = 0].$$

При этом здесь $a_{(i_0)}$ — константа, которая зависит только от F . Общее число векторов из $\mathbb{F}_q^k$, ортогональных фиксированному вектору, не меньше чем q^{k-1} , поэтому

$$\Pr[a_{(i_0)} \cdot G|_{\bar{I}} = 0] \geq \left(\frac{q^{k-1}}{q^k} \right)^{|\bar{I}|} = q^{-(t-s)}.$$

Значит, если $s \leq \min(t, k-1)$, то, поскольку $|\bar{I}| = t-s$,

$$\Pr[I \in \mathcal{J}] \geq q^{-(t-s)}$$

и

$$\sum_{I \in \mathcal{I}_s} \Pr_{G \leftarrow \mathbb{F}_q^{k \times n}}[I \in \mathcal{J}] \geq |\mathcal{I}_s| q^{-(t-s)}.$$

Осталось заметить, что

$$|\mathcal{I}_s| = \binom{t}{s} \binom{n-t}{k-s}.$$

С учетом того, что целое s было выбрано произвольно из отрезка $[0, \min(t, k-1)]$, окончательно получим неравенство (2). $\square$

Теорема 7. Зафиксируем вектор $e \in \mathbb{F}_q^n$ веса t . Рассмотрим произвольный вектор y , для которого $y - e \in \mathcal{C}$. Пусть P — вероятность того, что при случайном и равновероятном выборе множества $I \subseteq \llbracket n \rrbracket$, $|I| = k$, алгоритм 3 на очередной итерации находит решение задачи декодирования $\text{DEC}_{\mathcal{C}}(G, y, t)$. Тогда выполняется неравенство

$$\begin{aligned} \mathbb{E}_{G \leftarrow \mathbb{F}_q^{k \times n}}[P] &\geq \\ &\geq \binom{n}{k}^{-1} \cdot \max_{\substack{s \in \mathbb{Z}, \\ s \in [0, \min(t, k-1)]}} q^{-(t-s)} \binom{t}{s} \binom{n-t}{k-s}. \end{aligned}$$

Доказательство. Будем использовать систему обозначений из формулировки утверждения 28.

Пусть $\mathcal{I} = \{I \subseteq \llbracket n \rrbracket, |I| = k\}$. Если выбранное алгоритмом множество I попадает в $\mathcal{J}$, то итерация алгоритма находит решение, поэтому для каждой фиксированной матрицы G и вектора e веса t верно неравенство

$$P \geq \Pr_{I \leftarrow \mathcal{I}}[I \in \mathcal{J}].$$

Ясно, что

$$\Pr_{I \leftarrow \mathcal{I}}[I \in \mathcal{J}] = \frac{|\mathcal{J}|}{|\mathcal{I}|},$$

поэтому из утверждения 28 с учетом равенства

$$|\mathcal{I}| = \binom{n}{k}$$

получим справедливость теоремы. $\square$

Из теоремы 7 получаем, что ожидаемое число итераций алгоритма 3 оценивается как $\sim 1/P$, где P — типичное значение вероятности успеха одной итерации. Тогда с учетом утверждения 27 можно ожидать, что совокупное число операций в поле $\mathbb{F}_q$, которое нужно выполнить в алгоритме 3, примерно равно величине

$$N = \left(q^{z(C)}(t+1) \cdot kn + (t+1)k^2n \right) \cdot \binom{n}{k} \times \\ \times \min_{s \in \mathbb{Z}, s \in [0, \min(t, k-1)]} q^{(t-s)} \binom{t}{s}^{-1} \binom{n-t}{k-s}^{-1}.$$

При этом число операций получено в предположении единственности решения задачи декодирования.

Полученная оценка N носит эвристический характер: формально $\mathbb{E}[1/P] \neq 1/\mathbb{E}[P]$ (по неравенству Йенсена), и правильнее интерпретировать N как типичный порядок числа операций, а не точное математическое ожидание.

Поскольку оценка N экспоненциально зависит от $z(C)$, эффективность алгоритма существенно определяется тем, мала ли эта характеристика.

Теорема 6 устанавливает двустороннюю оценку $k - d \leq z(C) \leq k - \min(d, d^\perp - 1)$, а асимптотический результат работы [17] (следствие 2.4) показывает, что для случайного линейного кода почти все ненулевые кодовые слова минимальны. Поэтому можно ожидать, что для типичных кодов в подходящем диапазоне параметров $z(C)$ будет небольшой константой.

Заметим, что если минимальное расстояние d некоторого $[n, k]_q$ -кода меньше k , то величина $z(C)$ может быть достаточно большой. Поэтому для эффективного применения алгоритма желателен режим параметров, в котором возможен широкий

диапазон значений d , включающий область $d \geq k$. По границе Синглтона $d \leq n - k + 1 = (1 - R)n + 1$, и условие $d \geq k = Rn$ выполнимо только при $R \leq 1/2 + 1/(2n) \approx 1/2$. Например, при $R \approx 1/3$ возможные значения d лежат в отрезке $[k, 2k]$, что и оставляет место для кодов с относительно малой $z(C)$, и для этого диапазона параметров можно ожидать наибольшее ускорение алгоритма 3 по сравнению с известными общими алгоритмами декодирования.

5.5 Эмпирическое сравнение

Сравним сложность работы алгоритма 3 с другими известными алгоритмами декодирования линейных кодов в описанном диапазоне параметров.

В настоящее время существуют следующие наиболее значимые алгоритмы декодирования линейных кодов.

1. Алгоритм декодирования на основе информационных множеств, версия Е. Пранга [20] (далее обозначается как Prange).
2. Алгоритмы типа «встреча посередине»: алгоритм Ж. Штерна [21] (далее — Stern) и алгоритм И. Думера [22] (далее — Dumer).
3. Алгоритмы, комбинирующие деревья поиска и технику представления входных данных: алгоритм BJMM (Becker–Joux–May–Meurer) [23], усовершенствованная версия алгоритма BJMM, представленная в работе [24] (далее — BJMMPlus) и алгоритм MMT (May–Meurer–Thomae) [25].
4. Алгоритмы декодирования на основе поиска ближайшего соседа: алгоритм Л. Бота и А. Мея [26] (далее — BothMay) и алгоритм А. Мея и И. Озерова [27] (далее — MayOzerov).
5. И, наконец, алгоритм Д. Бернштейна, Т. Ланге и К. Петерс [28], который использует технику поиска коллизий (далее — BallCollision).

В силу сложности получения оценок трудоемкости перечисленных алгоритмов практически во всех работах, в которых приводятся оценки их сложности, указывается лишь экспоненциальный множитель, доминирующий с ростом длины кода. Поэтому сравнение алгоритмов для конкретных n , k и t будем проводить с использованием специального программного обеспечения CryptographicEstimators, которое оценивает трудоемкость алгоритмов. Это программное обеспечение реализовано в виде веб-сервиса, и оно доступно по ссылке <https://estimators.cryptotii.ae>. Подробное описание CryptographicEstimators и принципы его функционирования можно найти в работе [29].

Сделаем одну важную оговорку: CryptographicEstimators рассчитывает сложность алгоритмов декодирования для случайных кодов, поэтому оно учитывает распределение числа векторов в коде заданного веса в своих оценках. Например, если решается задача декодирования для $[n, k]_q$ -кода и вектора ошибок веса t , то сначала оценивается примерная величина d для случайного $[n, k]_q$ -кода. При $t > (d-1)/2$ задача декодирования перестает иметь единственное решение, и тогда достаточно найти хотя бы одно из них. Для случайного кода среднее число решений задачи декодирования будет равно (см., например, п. 6.1 в [30])

$$N_q(n, k, t) = q^{-(n-k)}(q-1)^t \binom{n}{t}.$$

Поскольку CryptographicEstimators оценивает сложность поиска хотя бы одного решения, а оценка сложности алгоритма 3 делалась в предположении единственности решения задачи декодирования, то для сравнения необходимо учитывать поправку на число решений и либо увеличивать результат вывода CryptographicEstimators на величину $\log_2 N_q(n, k, t)$, либо уменьшать сложность алгоритма 3 на ту же величину. В дальнейшем для удобства выберем второй подход.

Прежде чем перейти к таблицам, отметим важное обстоятельство. Стандартные алгоритмы декодирования на информационных множествах (Information Set Decoding, ISD) — такие как Prange, Stern, BJMM и др. — сформулированы для задачи уникального декодирования и эффективны при $t \leq t_{GV}$, где t_{GV} — граница Варшавова–Гилберта линейного кода, т.е. $t_{GV} \approx \tau \cdot n$, где τ — наименьший корень уравнения

$$-\tau \log_q \tau - (1-\tau) \log_q (1-\tau) + \tau \log_q (q-1) = 1 - \frac{k}{n}.$$

При $t > t_{GV}$ задача переходит в режим списочного декодирования: число допустимых решений экспоненциально велико, и ISD-методы находят «случайное» решение из этого множества. Алгоритм 3

работает в обоих режимах, но его относительное преимущество оказывается выше в режиме $t > t_{GV}$.

Для сравнения алгоритмов выберем параметры кодов с учетом ограничений $n \approx 3k$ и $t \approx k/2$:

- (1) $q = 2$, $n = 850$, $k = 320$, $t = 160$, $\log_2 N_2(n, k, t) \approx 58$, $t_{GV} \approx 0,15554 \cdot 850 = 132,209$;
- (2) $q = 2$, $n = 900$, $k = 300$, $t = 160$, $\log_2 N_2(n, k, t) \approx 3$, $t_{GV} \approx 0,174 \cdot 900 = 156,6$;
- (3) $q = 2$, $n = 1200$, $k = 400$, $t = 276$, $\log_2 N_2(n, k, t) \approx 128$, $t_{GV} \approx 0,174 \cdot 1200 = 208,8$;
- (4) $q = 2$, $n = 3000$, $k = 1000$, $t = 720$, $\log_2 N_2(n, k, t) \approx 379$, $t_{GV} \approx 0,174 \cdot 3000 = 522$;
- (5) $q = 2^8$, $n = 208$, $k = 104$, $t = 78$, $\log_2 N_q(n, k, t) \approx -14$.

Кроме того, будем считать, что $z(C) \approx 0$.

Результаты приведены в табл. 1–5. При этом сложность алгоритма 3 в таблицах уменьшена на величину $\log_2 N_q(n, k, t)$, если она положительна.

Особо выделим табл. 5, в которой рассматривается недвоичный линейный код. Программное обеспечение CryptographicEstimators для таких кодов поддерживает вычисление оценки сложности только базовых алгоритмов Stern и Prange, а также алгоритма LeeBrickell [31], который не рассматривается в двоичном случае.

Из таблиц видны три закономерности.

Во-первых, в режиме большого превышения границы Варшавова–Гилберта (см. табл. 1, 3 и 4) предложенный алгоритм превосходит по сложности базовый алгоритм декодирования Prange, но наилучшим оказывается только в табл. 1 и 4; в табл. 3, несмотря на большой избыток решений, выигрыш поправки $\log_2 N_q$ не компенсирует разрыв с продвинутыми алгоритмами декодирования с использованием информационных множеств.

Во-вторых, в пограничном случае (см. табл. 2), где t лишь слегка превышает t_{GV} (поправка

Таблица 1 Трудоемкость для $[850, 320]$ -кода

Алгоритм	Операции	Память
BallCollision	75	35
BJMM	72	68
BJMMPlus	71	64
BothMay	73	45
Dumer	75	40
MayOzerov	72	50
Prange	102	19
Stern	75	35
Алгоритм 3	68	19

Таблица 2 Трудоемкость для $[900, 300]$ -кода

Алгоритм	Операции	Память
BallCollision	112	35
BJMM	109	61
BJMMPlus	109	60
BothMay	110	44
Dumer	112	35
MayOzerov	109	72
Prange	129	19
Stern	112	29
Алгоритм 3	130	19

Таблица 3 Трудоемкость для [1200, 400]-кода

Алгоритм	Операции	Память
BallCollision	69	47
BJMM	67	60
BJMMPlus	67	49
BothMay	68	38
Dumer	69	62
MayOzerov	67	37
Prange	89	20
Stern	69	52
Алгоритм 3	78	20

Таблица 5 Трудоемкость для $[208, 104]_{256}$ -кода

Алгоритм	Операции	Память
Prange	137	17
Stern	127	26
LeeBrickell	129	17
Алгоритм 3	141	17

$\log_2 N_q \approx 3$), алгоритм проигрывает Prange один бит сложности и существенно уступает более совершенным ISD-алгоритмам. Основная причина состоит в том, что хотя вероятность успеха на одной итерации и выше, чем у многих ISD-алгоритмов, но при этом, когда решений задачи декодирования немного, она не может компенсировать высокую цену каждой итерации.

В-третьих, в случае большого алфавита (см. табл. 5) преимущество полностью теряется: алгоритм оказывается хуже даже базового Prange.

В завершение раздела обсудим реалистичность ключевого предположения $z(C) \approx 0$ и обозначим границы применимости метода.

Согласно работе [17] (следствие 2.4), для случайного линейного кода фиксированной скорости R почти все ненулевые кодовые слова минимальны при больших n . Для двоичных кодов равенство $z(C) = 0$ эквивалентно минимальности кода (теорема 3), а в общем случае — тому, что код пересекающийся, и указанный асимптотический результат дает основания ожидать, что для случайного кода $z(C)$ мала. Поэтому для типичных кодов в соответствующем диапазоне параметров множитель $q^{z(C)}$ в оценке сложности оказывается небольшой константой.

Вместе с тем алгоритм имеет несколько четко выраженных ограничений. Он применим только при $t < k$ (см. утверждение 24). Его эффективность падает при больших значениях мощности q конечного поля. Наконец, в режиме уникального декодирования (при $t \leq t_{GV}$) предложенный алгоритм, как правило, проигрывает специализированным ISD-методам.

Таблица 4 Трудоемкость для [3000, 1000]-кода

Алгоритм	Операции	Память
BallCollision	124	121
BJMM	118	108
BJMMPlus	118	97
BothMay	120	62
Dumer	123	118
MayOzerov	120	63
Prange	151	22
Stern	123	120
Алгоритм 3	103	22

Естественная область применимости алгоритма — двоичные коды небольшой и средней скорости, для которых $z(C)$ с большой вероятностью мала (по результату [17]), в режиме $t > t_{GV}$, где список допустимых решений обширен.

6 Заключение

В настоящей работе установлена связь между минимальными кодами и кодами, у которых в ядре $\text{eval}_G^{(2)}$ отсутствуют приводимые квадратичные формы: в двоичном случае эти два класса совпадают (теорема 3).

Получена двусторонняя оценка характеристики $z(C)$ через минимальные расстояния кода и дуального к нему (теорема 6), уточняющая результаты работы [11].

Также предложен новый алгоритм декодирования, который оказывается в ряде случаев эффективнее известных алгоритмов декодирования, когда задача декодирования имеет много решений.

Отметим, что предложенный алгоритм декодирования, скорее всего, не дает преимуществ для высокоскоростных кодов Гоппы, которые обычно используются в теоретико-кодовых криптосистемах, так как для таких кодов величина $z(C)$ немногим меньше размерности кода.

В целом задача поиска приводимых квадратичных форм в коде квадратичных отношений сводится к построению векторов относительно небольшого веса в коде, что в общем случае относится к NP-трудным задачам [32]. Тем не менее для специфических классов кодов с дополнительной структурой задача может решаться эффективнее. Дальнейшие исследования ее сложности, например с использованием наработок в области геометрии пересекающихся кодов (см. [33]), позволят оценить криптографическую применимость подхода — в частности, перспективы построения постквантовых схем электронной подписи на его основе.

Литература

1. McEliece R. J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report, 1978. Vol. 42–44. P. 114–116.
2. Niederreiter H. Knapsack type cryptosystems and algebraic coding theory // Probl. Control Inform., 1986. Vol. 15. No. 2. P. 159–166.
3. Berger T. P., Loidreau P. How to mask the structure of codes for a cryptographic use // Design. Code. Cryptogr., 2005. Vol. 35. No. 1. P. 63–79. doi: 10.1007/s10623-003-6151-2.
4. Wieschebrink C. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes // Post-quantum cryptography / Ed. N. Sendrier. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2010. Vol. 6061. P. 61–72. doi: 10.1007/978-3-642-12929-2_5.
5. Бородин М. А., Чижов И. В. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера // Дискретная математика, 2014. Т. 26. № 1. С. 10–20. doi: 10.4213/dm1264.
6. Couvreur A., Márquez-Corbella I., Pellikaan R. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes // Algebraic geometry modeling in information theory / Eds. R. Pellikaan, X. Wu, S. Yao. — Ser. on number theory and its applications. — World Scientific, 2015. Vol. 8. P. 201–234. doi: 10.1142/9789814678701_0010.
7. Couvreur A., Otmani A., Tillich J.-P., Gauthier-Umaña V. A polynomial-time attack on the BBRS scheme // Public-key cryptography / Ed. J. Katz. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2015. Vol. 9020. P. 175–193. doi: 10.1007/978-3-662-46447-2_8.
8. Lavauzelle J., Renner J. Cryptanalysis of a system based on twisted Reed–Solomon codes // Design. Code. Cryptogr., 2020. Vol. 88. P. 1285–1300. doi: 10.1007/s10623-020-00747-6.
9. Чижов И. В., Бородин М. А. Классификация произведений Адамара подкодов коразмерности 1 кодов Рида-Маллера // Дискретная математика, 2020. Т. 32. № 1. С. 115–134. doi: 10.4213/dm1583.
10. Чижов И. В., Конюхов С. А., Давлетшина А. М. Эффективная структурная атака на криптосистему Мак-Элиса–Сидельникова // Int. J. Open Information Technologies, 2020. Т. 8. № 7. С. 1–10. EDN: JPOKHW.
11. Couvreur A., Mora R., Tillich J.-P. A new approach based on quadratic forms to attack the McEliece cryptosystem // Advances in cryptology / Eds. J. Guo, R. Steinfeld. — Lecture notes in computer science ser. — Singapore: Springer, 2023. Vol. 14444. P. 3–38. doi: 10.1007/978-981-99-8730-6_1.
12. Mora R. On the matrix code of quadratic relationships for a Goppa code // Adv. Math. Commun., 2025. Vol. 19. No. 3. P. 829–852. doi: 10.3934/amc.2024026.
13. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки / Пер. с англ. под ред. Л. А. Бассалыго. — М.: Связь, 1979. 744 с.
14. (MacWilliams F. J., Sloane N. J. A. The theory of error-correcting codes. — Amsterdam: North-Holland, 1977. 762 p.)
15. Randriambololona H. On products and powers of linear codes under componentwise multiplication // Algorithmic arithmetic, geometry, and coding theory / Eds. S. Ballet, J.-M. Couveignes, D. Kohel, R. Rolland. — Contemporary mathematics ser. — Providence, RI, USA: American Mathematical Society, 2015. Vol. 637. P. 3–78. doi: 10.1090/conm/637/12749.
16. Miklós D. Linear binary codes with intersection properties // Discrete Appl. Math., 1984. Vol. 9. No. 2. P. 187–196. doi: 10.1016/0166-218X(84)90018-0.
17. Hwang T.-Y. Decoding linear block codes for minimizing word error rate // IEEE T. Inform. Theory, 1979. Vol. 25. No. 6. P. 733–737. doi: 10.1109/TIT.1979.1056120.
18. Ashikhmin A., Barg A. Minimal vectors in linear codes // IEEE T. Inform. Theory, 1998. Vol. 44. No. 5. P. 2010–2017. doi: 10.1109/18.705584.
19. Ding C., Yuan J. Covering and secret sharing with linear codes // Discrete mathematics and theoretical computer science / Eds. C. S. Calude, M. J. Dinneen, V. Vajnovszki. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2003. Vol. 2731. P. 11–25. doi: 10.1007/3-540-45066-1_2.
20. Wei V. K. Generalized Hamming weights for linear codes // IEEE T. Inform. Theory, 1991. Vol. 37. No. 5. P. 1412–1418. doi: 10.1109/18.133259.
21. Prange E. The use of information sets in decoding cyclic codes // IEEE T. Inform. Theory, 1962. Vol. 8. No. 5. P. 5–9. doi: 10.1109/TIT.1962.1057777.
22. Stern J. A method for finding codewords of small weight // Coding theory and applications / Eds. G. Cohen, J. Wolfmann. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 1989. Vol. 388. P. 106–113. doi: 10.1007/BFb0019850.
23. Думер И. И. Два алгоритма декодирования линейных кодов // Проблемы передачи информации, 1989. Т. 25. № 1. С. 24–32.
24. Becker A., Joux A., May A., Meurer A. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding // Advances in cryptology / Eds. D. Pointcheval, T. Johansson. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2012. Vol. 7237. P. 520–536. doi: 10.1007/978-3-642-29011-4_31.
25. Both L., May A. Optimizing BJMM with nearest neighbors: Full decoding in $2^{2n/21}$ and McEliece security // 10th Workshop (International) on Coding and Cryptography Proceedings. — Saint-Petersburg: SUAI, 2017. P. 214–225.
26. May A., Meurer A., Thomae E. Decoding random linear codes in $\tilde{O}(2^{0.054n})$ // Advances in cryptology / Eds. D. H. Lee, X. Wang. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2011. Vol. 7073. P. 107–124. doi: 10.1007/978-3-642-25385-0_6.

26. Both L., May A. Decoding linear codes with high error rate and its impact for LPN security // Post-quantum cryptography / Eds. T. Lange, R. Steinwandt. — Lecture notes in computer science ser. — Cham: Springer, 2018. Vol. 10786. P. 25–46. doi: 10.1007/978-3-319-79063-3_2.
27. May A., Ozerov I. On computing nearest neighbors with applications to decoding of binary linear codes // Advances in cryptology / Eds. E. Oswald, M. Fischlin. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2015. Vol. 9056. P. 203–228. doi: 10.1007/978-3-662-46800-5_9.
28. Bernstein D. J., Lange T., Peters C. Smaller decoding exponents: ball-collision decoding // Advances in cryptology / Ed. P. Rogaway. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 2011. Vol. 6841. P. 743–760. doi: 10.1007/978-3-642-22792-9_42.
29. Esser A., Verbel J., Zweydinger F., Bellini E. SoK: CryptographicEstimators — a software library for cryptographic hardness estimation // 19th ACM Asia Conference on Computer and Communications Security Proceedings. — New York, NY, USA: ACM, 2024. P. 560–574. doi: 10.1145/3634737.3645007.
30. Chailloux A., Debris-Alazard T. A tight security reduction in the quantum random oracle model for code-based signature schemes. — Cornell University, 2017. 22 p. arXiv:1709.06870 [quant-ph].
31. Lee P. J., Brickell E. F. An observation on the security of McEliece's public-key cryptosystem // Advances in cryptology / Ed. C. G. Günther. — Lecture notes in computer science ser. — Berlin, Heidelberg: Springer, 1988. Vol. 330. P. 275–280. doi: 10.1007/3-540-45961-8_25.
32. Berlekamp E. R., McEliece R. J., van Tilborg H. C. A. On the inherent intractability of certain coding problems // IEEE T. Inform. Theory, 1978. Vol. 24. No. 3. P. 384–386. doi: 10.1109/TIT.1978.1055873.
33. Borello M., Schmid W., Scotti M. The geometry of intersecting codes and applications to additive combinatorics and factorization theory // J. Comb. Theory A, 2025. Vol. 214. Art. 106023. 44 p. doi: 10.1016/j.jcta.2025.106023.

Поступила в редакцию 04.05.2026

Принята к публикации 15.08.2026

SOME PROPERTIES OF THE CODE OF QUADRATIC RELATIONSHIPS AND ITS APPLICATION TO THE DECODING PROBLEM FOR LINEAR CODES

I. V. Chizhov^{1,2}

¹M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation

²Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: In 2023, an approach to attacking the McEliece cryptosystem was proposed that is based on the study of so-called quadratic relationship codes, which are closely connected with the Schur–Hadamard product. These codes are constructed from quadratic forms that vanish on the columns of a generator matrix of a linear code. The effectiveness of this approach was recently demonstrated by an attack on the McEliece cryptosystem built upon binary Goppa codes of small degree. This attack exploits the fact that the quadratic relationship code contains a quadratic form of a relatively small rank. In the present paper, a systematic study is carried out of linear codes whose quadratic relationship code contains forms of rank 2 and lower. A special case is considered where the quadratic relationship code contains a reducible quadratic form, i.e., a form that decomposes into a product of two nonzero linear forms. Finally, the decoding problem is addressed for codes whose quadratic relationship codes contain no reducible quadratic forms or contain relatively few of them.

Keywords: code of quadratic relationships; Schur–Hadamard square of a code; McEliece cryptosystem; minimal code; decoding problem

DOI: 10.14357/19922264260301

EDN: IKIBAT

References

1. McEliece, R. J. 1978. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report* 42–44:114–116.
2. Niederreiter, H. 1986. Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control Inform.* 15(2):159–166.
3. Berger, T. P., and P. Loidreau. 2005. How to mask the structure of codes for a cryptographic use. *Design. Code. Cryptogr.* 35(1):63–79. doi: 10.1007/s10623-003-6151-2.
4. Wieschebrink, C. 2010. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. *Post-quantum cryptography*. Ed. N. Sendrier. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 6061:61–72. doi: 10.1007/978-3-642-12929-2_5.

5. Borodin, M. A., and I. V. Chizhov. 2014. Effective attack on the McEliece cryptosystem based on Reed–Muller codes. *Discrete Mathematics Applications* 24(5):273–280. doi: 10.1515/dma-2014-0024. EDN: UFJEAV.
6. Couvreur, A., I. Márquez-Corbella, and R. Pellikaan. 2015. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. *Algebraic geometry modeling in information theory*. Eds. R. Pellikaan, X. Wu, and S. Yao. Ser. on number theory and its applications. World Scientific. 8:201–234. doi: 10.1142/9789814678701_0010.
7. Couvreur, A., A. Otmani, J.-P. Tillich, and V. Gauthier-Umaña. 2015. A polynomial-time attack on the BBKRS scheme. *Public-key cryptography*. Ed. J. Katz. Lecture notes in computer science. Berlin, Heidelberg: Springer. 9020:175–193. doi: 10.1007/978-3-662-46447-2_8.
8. Lavauzelle, J., and J. Renner. 2020. Cryptanalysis of a system based on twisted Reed–Solomon codes. *Design. Code. Cryptogr.* 88(7):1285–1300. doi: 10.1007/s10623-020-00747-6.
9. Chizhov, I., and M. Borodin. 2022. Classification of Hadamard products of one-codimensional subcodes of Reed–Muller codes. *Discrete Mathematics Applications* 32(5):297–311. doi: 10.1515/dma-2022-0025. EDN: EGVLOK.
10. Chizhov, I. V., S. A. Konyukhov, and A. M. Davletshina. 2020. Effektivnaya strukturnaya ataka na kriptosistemu Mak-Elisa–Sidel’nikova [Effective structural attack on McEliece–Sidel’nikov public-key cryptosystem]. *Int. J. Open Information Technologies* 8(7):1–10. EDN: JPOKHW.
11. Couvreur, A., R. Mora, and J.-P. Tillich. 2023. A new approach based on quadratic forms to attack the McEliece cryptosystem. *Advances in cryptology*. Eds. J. Guo and R. Steinfeld. Lecture notes in computer science ser. Singapore: Springer. 14444:3–38. doi: 10.1007/978-981-99-8730-6_1.
12. Mora, R. 2025. On the matrix code of quadratic relationships for a Goppa code. *Adv. Math. Commun.* 19(3):829–852. doi: 10.3934/amc.2024026.
13. MacWilliams, F. J., and N. J. A. Sloane. 1977. *The theory of error-correcting codes*. Amsterdam: North-Holland. 762 p.
14. Randriambololona, H. 2015. On products and powers of linear codes under componentwise multiplication. *Algorithmic arithmetic, geometry, and coding theory*. Eds. S. Ballet, J.-M. Couveignes, D. Kohel, and R. Rolland. Contemporary mathematics ser. Providence, RI: American Mathematical Society. 637:3–78. doi: 10.1090/conm/637/12749.
15. Miklós, D. 1984. Linear binary codes with intersection properties. *Discrete Appl. Math.* 9(2):187–196. doi: 10.1016/0166-218X(84)90018-0.
16. Hwang, T.-Y. 1979. Decoding linear block codes for minimizing word error rate. *IEEE T. Inform. Theory* 25(6):733–737. doi: 10.1109/TIT.1979.1056120.
17. Ashikhmin, A., and A. Barg. 1998. Minimal vectors in linear codes. *IEEE T. Inform. Theory* 44(5):2010–2017. doi: 10.1109/18.705584.
18. Ding, C., and J. Yuan. 2003. Covering and secret sharing with linear codes. *Discrete mathematics and theoretical computer science*. Eds. C. S. Calude, M. J. Dinneen, and V. Vajnovszki. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 2731:11–25. doi: 10.1007/3-540-45066-1_2.
19. Wei, V. K. 1991. Generalized Hamming weights for linear codes. *IEEE T. Inform. Theory* 37(5):1412–1418. doi: 10.1109/18.133259.
20. Prange, E. 1962. The use of information sets in decoding cyclic codes. *IEEE T. Inform. Theory* 8(5):5–9. doi: 10.1109/TIT.1962.1057777.
21. Stern, J. 1989. A method for finding codewords of small weight. *Coding theory and applications*. Eds. G. Cohen and J. Wolfmann. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 388:106–113. doi: 10.1007/BFb0019850.
22. Dumer, I. I. 1989. Two decoding algorithms for linear codes. *Probl. Inf. Transm.* 25(1):17–23.
23. Becker, A., A. Joux, A. May, and A. Meurer. 2012. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. *Advances in cryptology*. Eds. D. Pointcheval and T. Johansson. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 7237:520–536. doi: 10.1007/978-3-642-29011-4_31.
24. Both, L., and A. May. 2017. Optimizing BJMM with nearest neighbors: Full decoding in $2^{2n/21}$ and McEliece security. *10th Workshop (International) on Coding and Cryptography Proceedings*. Saint-Petersburg, Russia: SUAI. 214–225.
25. May, A., A. Meurer, and E. Thomae. 2011. Decoding random linear codes in $\tilde{O}(2^{0.054n})$. *Advances in cryptology*. Eds. D. H. Lee and X. Wang. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 7073:107–124. doi: 10.1007/978-3-642-25385-0_6.
26. Both, L., and A. May. 2018. Decoding linear codes with high error rate and its impact for LPN security. *Post-quantum cryptography*. Eds. T. Lange and R. Steinwandt. Lecture notes in computer science ser. Cham: Springer. 10786:25–46. doi: 10.1007/978-3-319-79063-3_2.
27. May, A., and I. Ozerov. 2015. On computing nearest neighbors with applications to decoding of binary linear codes. *Advances in cryptology*. Eds. E. Oswald and M. Fischlin. Lecture notes in computer science. Berlin, Heidelberg: Springer. 9056:203–228. doi: 10.1007/978-3-662-46800-5_9.
28. Bernstein, D. J., T. Lange, and C. Peters. 2011. Smaller decoding exponents: Ball-collision decoding. *Advances in cryptology*. Ed. P. Rogaway. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 6841:743–760. doi: 10.1007/978-3-642-22792-9_42.
29. Esser, A., J. Verbel, F. Zweyding, and E. Bellini. 2024. SoK: CryptographicEstimators — a software library for cryptographic hardness estimation. *19th ACM*

- Asia Conference on Computer and Communications Security Proceedings*. New York, NY: ACM. 560–574. doi: 10.1145/3634737.3645007.
30. Chailloux, A., and T. Debris-Alazard. 2017. A tight security reduction in the quantum random oracle model for code-based signature schemes. Cornell University. 22 p. Available at: <https://arxiv.org/pdf/1709.06870> (accessed August 17, 2026).
31. Lee, P. J., and E. F. Brickell. 1988. An observation on the security of McEliece's public-key cryptosystem. *Advances in cryptology*. Ed. C. G. Günther. Lecture notes in computer science ser. Berlin, Heidelberg: Springer. 330:275–280. doi: 10.1007/3-540-45961-8_25.
32. Berlekamp, E. R., R. J. McEliece, and H. C. A. van Tilborg. 1978. On the inherent intractability of certain coding problems. *IEEE T. Inform. Theory* 24(3):384–386. doi: 10.1109/TIT.1978.1055873.
33. Borello, M., W. Schmid, and M. Scotti. 2025. The geometry of intersecting codes and applications to additive combinatorics and factorization theory. *J. Comb. Theory A* 214:106023. 44 p. doi: 10.1016/j.jcta.2025.106023.

Received May 4, 2026

Accepted August 15, 2026

Contributor

Chizhov Ivan V. (b. 1984) — Candidate of Science (PhD) in physics and mathematics, associate professor, Department of Information Security, Faculty of Computational Mathematics and Cybernetics, M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation; senior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; chizhoviv@my.msu.ru

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ МАРКОВСКИМИ СКАЧКООБРАЗНЫМИ ПРОЦЕССАМИ ПО БЕСШУМОВЫМ НАБЛЮДЕНИЯМ С ЗАДЕРЖКАМИ I: УНИВЕРСАЛЬНЫЙ СТОХАСТИЧЕСКИЙ БАЗИС И ПРОБЛЕМА МАРТИНГАЛОВ*

А. В. Борисов¹, Ю. Н. Куринов²

Аннотация: Первая часть цикла представляет теоретические основы корректной постановки и решения одной из задач оптимального стохастического управления на конечном отрезке времени по неполной информации. Объект управления — класс марковских скачкообразных процессов (МСП) с конечным множеством состояний. Критерием оптимальности выступает некоторая интегральная функция потерь. Для синтеза управления доступны наблюдения, представляющие собой некоторые функции состояния системы, наблюдаемые без шума, но с некоторой фиксированной временной задержкой. Класс допустимых управлений содержится в множестве процессов, предсказуемых относительно фильтрации, порожденной наблюдениями, и стесненных комплексом геометрических и интегральных ограничений. Представлен стохастический базис с фильтрацией, обеспечивающий на нем решение проблемы мартингалов для рассматриваемых управляемых МСП. Предложены условия, обеспечивающие непрерывную зависимость управляемого состояния и критерия оптимальности от примененного управления.

Ключевые слова: управляемый марковский скачкообразный процесс; пространство Винера–Пуассона; проблема мартингалов; пуассоновская стохастическая мера

DOI: 10.14357/19922264260302

EDN: AZXCMB

1 Введение

Задачам оптимального управления МСП по различным комплексам доступной информации традиционно уделяется большое внимание [1–4]. Теоретические результаты в этой области широко применяются в телекоммуникациях [5–7], динамическом распределении ресурсов и заданий [8–10], оптимизации функционирования реальных систем массового обслуживания [11, 12] и пр. [13]. Помимо самостоятельного использования МСП часто выступают в роли процессов смены режимов в управляемых стохастических системах переменной структуры [14–17].

Корректная постановка задачи управления состояниями МСП значительно сложнее, чем для диффузионных процессов [18]. Для объяснения этого факта рассмотрим общий вариант управляемой стохастической дифференциальной системы (СДС) с винеровским процессом в правой части:

$$x_t^u = x_0 + \int_0^t a(s, x_s^u, u_s) ds + \int_0^t b(s, x_s^u, u_s) dw_s, \quad (1)$$

где x_t^u — управляемое состояние; u_t — управление; w_t — независимый от x_0 винеровский процесс. Замечательным представляется тот факт, что для этой

СДС имеется единое естественное вероятностное пространство (в англоязычной литературе — *real-world probability*), порожденное x_0 и w_t , в котором состояние x_t^u корректно определено и обладает рядом полезных свойств для достаточно широкого класса допустимых управлений. Например, в случае если $u_t = u(t, x_{t-}^u)$, процесс x_t^u обладает марковским свойством. В общем же случае, когда управление u_t $\mathcal{F}_t$ -предсказуемо, процесс x_t^u теряет свойство марковости, однако остается семимартингалом, допускающим представление (1).

Эти свойства управляемых процессов дают возможность использовать эффективный математический аппарат стохастического анализа [19]. С физической точки зрения управление в таких системах выглядит вполне естественно: оно заключается в оптимизации в реальном масштабе времени коэффициентов сноса и диффузии, в то время как внешнее входное воздействие — винеровский процесс w_t — остается неизменным. Качество управления, определяемое значением средних потерь, может быть вычислено для любого допустимого управления в едином вероятностном пространстве. При этом возможно потраекторное сравнение поведения управляемой системы в зависимости от выбранного управления.

* Работа выполнена при финансовой поддержке РНФ (проект № 25-21-00504).

¹ Федеральный исследовательский центр «Информатика и управление» Российской академии наук, aborisov@frccsc.ru

² Московский государственный университет имени М. В. Ломоносова, kurinovurij@gmail.com

Случай управляемых МСП значительно сложнее. Марковский скачкообразный процесс управляется через свою матрицу интенсивностей переходов (МИП) $\Lambda(t, u_t)$. В случае если управление u_t — неслучайная функция, МСП X_t^u допускает следующее представление:

$$X_t^u = X_0 + \int_0^t \Lambda^\top(s, u_s) X_s^u ds + M_t^u, \quad (2)$$

где M_t^u — некоторый $\mathcal{F}_t^X$ -согласованный мартингал с квадратичной характеристикой, зависящей от $\Lambda(t, u_t)$. Выбирая u_t , можно формировать вероятностные базисы, индивидуальные для используемого управления [20, 21]. Вероятностные пространства порождены самим МСП, и потраекторное сравнение поведения МСП для различных законов управления выглядит проблематичным. Сравнение их качества с помощью критерия оптимальности в виде математического ожидания выглядит не вполне корректным, так как осреднение выполняется по разным вероятностным мерам, зависящим от выбранного управления.

Теоретическая сложность заключается в том, что при использовании управления u_t из класса $\mathcal{F}_t$ -предсказуемых случайных процессов состояние X_t теряет не только марковское свойство, но и в общем случае возможность мартингального представления: процесс M_t^u в (2) перестает быть мартингалом.

Цель предлагаемой работы заключается в корректной постановке задачи оптимального стохастического управления МСП по косвенным наблюдениям состояния, поступающим без шумов, но с временной задержкой, а также решение мартингальной проблемы для представленной управляемой системы.

Работа организована следующим образом. Раздел 2 содержит корректную постановку задачи стохастического управления состоянием МСП, оптимального по интегральному критерию, при наличии комплекса геометрических и интегральных ограничений, предъявляемых к допустимому управлению.

Для управляемой системы разд. 3 представляет решение проблемы мартингалов [22]: предложено единое вероятностное пространство [23], основанное на пуассоновской стохастической мере, которое позволяет единым образом строить мартингалы в управляемых МСП. Таким образом, в общем случае управляемые МСП теряют марковское свойство, однако сохраняют мартингальное разложение (2) (в нем M_t^u остается мартингалом), что позволяет использовать развитый аппарат теории

мартингалов. В этом же разделе представлены условия, обеспечивающие непрерывную зависимость траекторий МСП и критерия качества от применяемого управления.

Раздел 4 содержит заключительные замечания.

2 Постановка задачи оптимального управления

Объектом управления выступает МСП X_t^u , $t \in [0, T]$, с конечным множеством состояний $\mathbb{S}^N \triangleq \{e_1, \dots, e_N\}$ — набором координатных ортов евклидова пространства $\mathbb{R}^N$. Управление применяется к МИП $\Lambda(t, u) : [0, T] \times \mathcal{U} \rightarrow \mathbb{R}^{N \times N}$. Здесь $\mathcal{U} \subset \mathbb{R}^M$ — компактное множество допустимых управлений, определяющее его мгновенные геометрические ограничения. Функция $\Lambda(t, u) = \|\Lambda^{ij}(t, u)\|_{i,j=\overline{1,N}}$ непрерывна по совокупности своих переменных на $[0, T] \times \mathcal{U}$, и для всех (t, u) функция $\Lambda(t, u)$ сохраняет свойства МИП, т. е. $\Lambda^{ij}(t, u) \geq 0$ для всех $i \neq j$, а также $\sum_{j=1}^N \Lambda^{ij}(t, u) \equiv 0$.

Критерий качества совпадает с представленным в [20, 21]:

$$J_0(U) \triangleq \mathbb{E} \left\{ \int_0^T f^0(s, u_s) X_s^u ds + \phi^0 X_T^u \right\}, \quad (3)$$

где $f^0(t, u) \triangleq \text{row}(f_1^0(t, u), \dots, f_N^0(t, u)) : [0, T] \times \mathcal{U} \rightarrow \mathbb{R}^{1 \times N}$ — вектор-функция, компоненты которой непрерывны по совокупности своих аргументов; $\phi^0 \triangleq \text{row}(\phi_1^0, \dots, \phi_N^0)$ — известная вектор-строка.

Допустимое управление может быть стеснено дополнительными интегральными ограничениями, аналогичными (3):

$$J_\ell(U) \triangleq \mathbb{E} \left\{ \int_0^T f^\ell(s, u_s) X_s^u ds + \phi^\ell X_T^u \right\} \leq 0, \quad \ell = \overline{1, L}, \quad (4)$$

где $f^\ell(t, u) \triangleq \text{row}(f_1^\ell(t, u), \dots, f_N^\ell(t, u)) : [0, T] \times \mathcal{U} \rightarrow \mathbb{R}^{1 \times N}$ — вектор-функции с непрерывными компонентами, $\phi^\ell \triangleq \text{row}(\phi_1^\ell, \dots, \phi_N^\ell)$ — известные вектор-строки.

Для синтеза управления доступны наблюдения ξ_t , представляющие собой некоторую функцию от управляемого состояния X^u , фиксируемую без шумов, но с временной задержкой Δ :

$$\xi_t = C X_{t-\Delta}^u, \quad \Delta \leq t \leq T, \quad \xi_t \equiv 0 \text{ при } t < \Delta,$$

где $C \in \mathbb{R}^{K \times N}$ — известная матрица, состоящая из 0 и 1; $\Xi_t \triangleq \sigma\{\xi_s : 0 \leq s \leq t\}$ — естественное семейство σ -алгебр, порожденных наблюдениями.

Если $\mathcal{U}'$ — множество управлений $U = \{u_t\}_{t \in [0, T]}$, образованное всеми Ξ_t -предсказуемыми Σ_t -процессами, удовлетворяющими мгновенным геометрическим ограничениям

$$P\{u_t \in U\} \equiv 1, \quad \forall t \in [0, T], \quad (5)$$

а также ограничениям интегрального типа (4), то задача

$$J_0(U) \rightarrow \min_{U \in \mathcal{U}'} \quad (6)$$

называется *задачей оптимального управления состоянием МСП по наблюдениям с задержками*.

Если $\mathcal{U}''$ — множество управлений вида $U = \{u(t, \xi_t)\}_{t \in [0, T]}$, зависящих только от текущего наблюдения ξ_t , удовлетворяющее геометрическим и интегральным ограничениям (4), (5), то задача

$$J_0(U) \rightarrow \min_{U \in \mathcal{U}''} \quad (7)$$

называется *задачей оптимального марковского управления состоянием МСП по наблюдениям с задержками*.

Пусть $\hat{X}_t^u \triangleq E\{X_t^u | \Xi_t\}$ — вектор условного распределения состояния МСП относительно имеющихся к моменту времени t наблюдений. Если $\mathcal{U}'''$ — множество управлений вида $U = \{u(t, \hat{X}_{t-}^u)\}_{t \in [0, T]}$, зависящих от наблюдений через условное распределение $\hat{X}_t^u$, удовлетворяющее интегральным и геометрическим ограничениям (4) и (5), то задача

$$J_0(U) \rightarrow \min_{U \in \mathcal{U}'''} \quad (8)$$

называется *задачей оптимального стохастического управления состоянием МСП по наблюдениям с задержками, основанного на принципе разделения*. В случае если решения задач (6) и (8) совпадают, говорят, что для рассмотренной задачи оптимального стохастического управления выполняется *теорема разделения* [24]. Решение задачи (8) представляется достаточно перспективным также в свете того, что вид условного распределения $\hat{X}_t^u$ известен для класса программных управлений — детерминированных функций u_t [25, 26].

Дальнейшее исследование (6)–(8) нуждается в решении проблемы мартингалов для управляемого МСП [22]: необходимо предложить такой канонический базис с фильтрацией $(\Omega, \mathcal{F}, P, \{\mathcal{F}_t\}_{t \in [0, T]})$, что

- для допустимых детерминированных управлений U управляемое состояние обладало бы марковским свойством и допускало мартингаловое разложение (2);

- для допустимых стохастических управлений $U \in \mathcal{U}'$, $\mathcal{U}''$ или $\mathcal{U}'''$ управляемое состояние было бы представимо в форме (2), где M_t^u — некоторый $\mathcal{F}_t$ -согласованный мартингал.

3 Универсальный стохастический базис и проблема мартингалов

Для построения канонического базиса с фильтрацией — пространства Винера–Пуассона — введем в рассмотрение следующие объекты:

- $\Omega^0 \triangleq \mathbb{S}^N$ — выборочное пространство начальных условий ω^0 процесса X_t^u ;
- Ω^{ij} , $i, j = \overline{1, N}$, $i \neq j$, — множество таких целочисленных мер ω^{ij} на $([0, T] \times [0, 1], \mathcal{B}([0, T] \times [0, 1]))$, что $\omega^{ij}([0, T] \times \{0\}) \equiv 0$; оно будет использовано при описании переходов $e_i \rightarrow e_j$ управляемого МСП X_t^u ;
- $\mathcal{F}^0 \triangleq 2^{\mathbb{S}^N}$;
- $\mathcal{F}^{ij} \triangleq \mathcal{B}([0, T] \times [0, 1])$; $\mathcal{F}_t^{ij} \triangleq \mathcal{B}([0, t] \times [0, 1])$, $t \in [0, T]$;
- P^0 — такая вероятностная мера на $(\Omega^0, \mathcal{F}^0)$, что $X_0(\omega^0) \triangleq \omega^0$ имеет распределение p_0 ;
- P^{ij} — вероятностные меры на $(\Omega^{ij}, \mathcal{F}^{ij})$, при которых меры $\pi^{ij}(\omega^{ij}, dt, dx) \triangleq \omega^{ij}(dt, dx)$ являются пуассоновскими с компенсаторами $\nu^{ij}(dt, dx) = C^{ij} dt dx$, где

$$C^{ij} \triangleq \max_{(t, u) \in [0, T] \times [0, 1]} \Lambda_{ij}(t, u).$$

Канонический базис с фильтрацией $(\Omega, \mathcal{F}, P, \{\mathcal{F}_t\}_{t \in [0, T]})$ имеет вид:

$$\begin{aligned} \Omega &\triangleq \Omega^0 \otimes \bigotimes_{i, j: i \neq j} \Omega^{ij}; \quad \mathcal{F} \triangleq \mathcal{F}^0 \otimes \bigotimes_{i, j: i \neq j} \mathcal{F}^{ij}; \\ P &\triangleq P^0 \times \prod_{i, j: i \neq j} P^{ij}; \quad \mathcal{F}_t \triangleq \mathcal{F}^0 \otimes \bigotimes_{i, j: i \neq j} \mathcal{F}_t^{ij}. \end{aligned}$$

Продemonстрируем, что $(\Omega, \mathcal{F}, P, \{\mathcal{F}_t\}_{t \in [0, T]})$ допускает решение проблемы мартингалов для рассматриваемого класса управляемых МСП. Для этого введем два множества процессов управления:

- $\mathcal{V}'$ — детерминированные процессы $v(t) : [0, T] \rightarrow U$ с *càdlàg*-траекториями;
- $\mathcal{V}''$ — $\mathcal{F}_t$ -предсказуемые процессы $v(\omega, t) : \Omega \times [0, T] \rightarrow U$ с *càdlàg*-траекториями.

Рассмотрим процессы

$$J_t^{v,ij} \triangleq \int_{[0,t] \times [0,1]} \mathbf{I}_{[0;\Lambda_{ij}(s,v(s))/C^{ij}]}(x) \pi^{ij}(ds, dx),$$

$$i, j = \overline{1, N}, i \neq j.$$

Из свойств интегралов по пуассоновской стохастической мере следует, что в случае если $v(t) \in \mathcal{V}'$, $J_t^{v,ij}$ представляет собой неоднородный пуассоновский процесс, имеющий независимые приращения и обладающий марковским свойством. Если $v(t) \in \mathcal{V}''$, то $J_t^{v,ij}$ — субмартингал с компенсатором

$$\nu_t^{ij} = \int_0^t \Lambda^{ij}(s, v(s)) ds. \quad (9)$$

При $v(t) \in \mathcal{V}'$ или $v(t) \in \mathcal{V}''$ верно разложение

$$J_t^{v,ij} = \nu_t^{v,ij} + \mu_t^{v,ij}, \quad (10)$$

где $\mu_t^{v,ij}$ — $\mathcal{F}_t$ -согласованный квадратично интегрируемый мартингал с квадратичной характеристикой $\langle \mu^{v,ij} \rangle_t = \nu_t^{v,ij}$. При этом мартингалы сильно ортогональны, т. е. $\langle \mu^{v,ij}, \mu^{v,k\ell} \rangle_t \equiv 0$ при $(i, j) \neq (k, \ell)$. Введем в рассмотрение случайный процесс X_t^v , определяемый уравнением

$$X_t^v = X_0^v + \int_0^t \sum_{i,j:i \neq j} e_i^\top X_{s-}^v (e_j - e_i) dJ_s^{v,ij}. \quad (11)$$

Из того, что $X_0^v \in \mathbb{S}^N$ Р-п. н., процессы $\{J_t^{v,ij}\}_{i \neq j}$ — чисто разрывные субмартингалы, а также из явного вида решения матричного уравнения Долеан [27] следует, что сильное решение (11) существует и единственно и что $X_t^v \in \mathbb{S}^N$ Р-п. н. Из представлений (9) и (10) следует, что

$$\begin{aligned} X_t^v &= X_0^v + \\ &+ \int_0^t \sum_{i,j:i \neq j} (e_j e_i^\top - \text{diag } e_i) \Lambda^{ij}(s, v(s)) X_{s-}^v ds + \\ &+ \int_0^t \sum_{i,j:i \neq j} (e_j e_i^\top - \text{diag } e_i) X_{s-}^v d\mu_s^{v,ij} = \\ &= X_0^v + \int_0^t \Lambda^\top(s, v(s)) X_{s-}^v ds + \\ &+ \underbrace{\int_0^t \begin{bmatrix} \sum_{i:i \neq 1} e_i^\top X_{s-}^v d\mu_s^{v,i1} \\ \vdots \\ \sum_{i:i \neq N} e_i^\top X_{s-}^v d\mu_s^{v,iN} \end{bmatrix}}_{\triangleq M_t^v}, \end{aligned}$$

где M_t^v как интеграл Ито предсказуемого интегранда по мартингалу также представляет собой некоторый $\mathcal{F}_t$ -согласованный мартингал. Так как $X_t^v \in \mathbb{S}^N$, то M_t^v — квадратично интегрируемый мартингал, и по обобщенному правилу Ито [19] и свойствам считающих процессов $\{J_t^{v,ij}\}_{i \neq j}$ можно получить его квадратичную характеристику

$$\begin{aligned} \langle M^v \rangle_t &= \int_0^t (\text{diag}(\Lambda^\top(s, v(s)) X_{s-}^v) - \\ &- \Lambda^\top(s, v(s)) \text{diag}(X_{s-}^v) - \\ &- \text{diag}(X_{s-}^v) \Lambda(s, v(s))) ds. \end{aligned}$$

Докажем, что при $v \in \mathcal{V}'$ процесс X_t^v обладает марковским свойством. Зафиксируем два момента времени $0 \leq s < t \leq T$. В силу свойств решения СДС с мартингалом в правой части и того факта, что на $[0, T]$ $X_{t-}^v \neq X_t^v$ не более чем в конечном числе точек, процесс X_t^v , $t \in [s, T]$, может быть представлен как решение СДС

$$X_t^v = X_s^v + \int_s^t \Lambda^\top(q, v(q)) X_q^v dq + (M_t^v - M_s^v).$$

Вычислим условное математическое ожидание (УМО) относительно $\mathcal{F}_s$ от левой и правой частей последнего равенства: в силу свойств УМО, детерминированности МИП $\Lambda(q, v(q))$ и мартингалности процесса M_t^v верно равенство

$$\mathbb{E}\{X_t^v | \mathcal{F}_s\} = X_s^v + \int_s^t \Lambda^\top(q, v(q)) \mathbb{E}\{X_q^v | \mathcal{F}_s\} dq.$$

Условное математическое ожидание $\mathbb{E}\{X_t^v | \mathcal{F}_s\}$, $0 \leq s < t \leq T$, представимо в виде

$$\mathbb{E}\{X_t^v | \mathcal{F}_s\} = \Phi^\top(s, t) X_s^v,$$

где $\Phi(s, t)$ — матрица Коши, т. е. решение задачи

$$\Phi'_t(s, t) = \Phi(s, t) \Lambda(t, v(t)), \quad s < t \leq T, \quad \Phi(s, s) = I.$$

Заметим, что

$$\begin{aligned} \mathbb{E}\{X_t^v | X_s^v\} &= \mathbb{E}\{\mathbb{E}\{X_t^v | \mathcal{F}_s\} | X_s^v\} = \\ &= \Phi^\top(s, t) X_s^v = \mathbb{E}\{X_t^v | \mathcal{F}_s\}, \end{aligned}$$

что подтверждает марковское свойство процесса X_t^v относительно $\mathcal{F}_t$ при любом детерминированном управлении $V \in \mathcal{V}'$.

Очевидно, что в множестве управлений $\mathcal{V}''$ имеются подмножества, изоморфные множествам управлений $\mathcal{U}'$ и $\mathcal{U}''$, представленных в предыдущем

разделе. Условное распределение $E\{X_t^u | \Xi_t\}$ описывается некоторым вариантом уравнения Кушнера–Стратоновича, решение которого представляет собой càdlàg-процесс [26], поэтому в $\mathcal{V}''$ также имеется подмножество, изоморфное множеству управлений $\mathcal{U}'''$. Таким образом, доказана

Теорема 1. В представленном каноническом базисе с фильтрацией Винера–Пуассона $(\Omega, \mathcal{F}, P, \{\mathcal{F}_t\}_{t \in [0, T]})$ существует решение задачи мартингалов для управляемых МСП X_t^u , в которых $u \in \mathcal{U}', \mathcal{U}'', \mathcal{U}'''$.

Ниже представлены условия, обеспечивающие непрерывную зависимость МСП и критерия оптимальности от выбранного управления.

A. Компоненты МИП $\Lambda^{ij}(t, v)$ — липшицевы с параметром K , т. е.

$$|\Lambda^{ij}(t, v') - \Lambda^{ij}(t, v'')|^2 \leq K^2 \|v' - v''\|^2$$

для $\forall i, j = \overline{1, N} : i \neq j; t \in [0, T], v', v'' \in U$.

Б. Последовательность процессов управления $\{v^n(\omega, t)\}_{n \in \mathbb{N}}$ и предельный процесс $v(\omega, t)$ таковы, что $\{v^n(\omega, t)\}_{n \in \mathbb{N}} \subset \mathcal{V}''$, $v^n(\omega, t) \in \mathcal{V}''$, и $v^n \xrightarrow{\mathcal{L}_2} v$ равномерно на $[0, T]$, т. е. существует такая последовательность $\{\varepsilon_n\}$, $\varepsilon_n \xrightarrow{n \rightarrow \infty} 0$, что

$$\sup_{t \in [0, T]} E\{\|v^n(\omega, t) - v(\omega, t)\|^2\} \leq \varepsilon_n^2.$$

В. Компоненты критерия $f^\ell(t, v)$ — липшицевы с параметром K , т. е.

$$|f^\ell(t, v') - f^\ell(t, v'')|^2 \leq K^2 \|v' - v''\|^2, \\ \ell = \overline{1, N} : \forall t \in [0, T], v', v'' \in U.$$

Теорема 2. Условия A–B обеспечивают непрерывную зависимость состояний управляемых МСП относительно управления, т. е.

$$E\{\|X_t^{v^n} - X_t^v\|^2\} \leq L_1(t) \varepsilon_n \xrightarrow{\varepsilon_n \rightarrow 0} 0, \quad (12)$$

а также непрерывность критерия качества

$$|J_0(V^n) - J_0(V)| \leq \\ \leq L_2(T) \varepsilon_n^{1/2} + L_3(T) \varepsilon_n \xrightarrow{\varepsilon_n \rightarrow 0} 0 \quad (13)$$

для некоторых положительных функций $L_1(t)$, $L_2(T)$ и $L_3(T)$.

Доказательство теоремы 2 дано в приложении.

4 Заключение

В работе сформулирована задача оптимального стохастического управления МСП с конечным

множеством состояний по неполной информации. Критерием управления выступают ожидаемые интегральные потери. Управления стеснены как геометрическими, так и интегральными ограничениями, а доступная информация представляет собой некоторую функцию измерений, фиксируемую без дополнительного шума, но с известной временной задержкой. Управления формируются как предсказуемые преобразования доступных наблюдений.

В работе решена проблема мартингалов. Предложен единый вероятностный триплет с фильтрацией, относительно которого управляемые МСП для произвольных допустимых управлений допускают мартингаловое представление, определенное классической формулой Дынкина. Представлены условия, обеспечивающие непрерывную зависимость МСП и критерия оптимальности от примененного управления.

Приложение

Рассмотрим два управляемых МСП, соответствующих допредельному и предельному управлению

$$X_t^{v^n} = x_0 + \int_0^t \Lambda^\top(s, v^n(s)) X_{s-}^{v^n} ds + M_t^{v^n}; \\ X_t^v = x_0 + \int_0^t \Lambda^\top(s, v(s)) X_{s-}^v ds + M_t^v,$$

и будем использовать следующие обозначения:

$$\tilde{X}_t \triangleq X_t^{v^n} - X_t^v; \\ \tilde{\Lambda}(t) \triangleq \Lambda(t, v^n(t)) - \Lambda(t, v(t)); \\ \tilde{M}_t \triangleq M_t^{v^n} - M_t^v.$$

Построим интегральное неравенство для $E\{\|\tilde{X}_t\|^2\}$ и воспользуемся для его оценки неравенством Гронуолла–Беллмана [28]. Выпишем уравнение для $\tilde{X}_t$

$$\tilde{X}_t = \\ = \int_0^t \left(\Lambda^\top(s, v^n(s)) X_{s-}^{v^n} - \Lambda^\top(s, v(s)) X_{s-}^v \right) ds + \tilde{M}_t = \\ = \int_0^t \left(\Lambda^\top(s, v^n(s)) \tilde{X}_{s-} + \tilde{\Lambda}^\top(s) X_{s-}^v \right) ds + \tilde{M}_t$$

и детализируем вид компонент мартингала $\tilde{M}_t$:

$$\tilde{M}_t = \begin{bmatrix} \int_0^t \sum_{i:i \neq 1} e_i^\top \left(X_{s-}^{v^n} d\mu^{v^n, i1} - X_{s-}^v d\mu^{v, i1} \right) \\ \vdots \\ \int_0^t \sum_{i:i \neq N} e_i^\top \left(X_{s-}^{v^n} d\mu^{v^n, iN} - X_{s-}^v d\mu^{v, iN} \right) \end{bmatrix}.$$

Для вычисления $\text{tr} \langle \widetilde{M} \rangle_t$ рассмотрим более подробно процессы $J_t^{v^n, ij}$ и $J_t^{v, ij}$, описывающие переходы $e_i \rightarrow e_j$ управляемых МСП $X_t^{v^n}$ и X_t^v . Обозначим

$$\begin{aligned}\underline{\Lambda}^{ij}(t) &\triangleq \min(\Lambda^{ij}(t, v^n(t)), \Lambda^{ij}(t, v(t))); \\ \overline{\Lambda}^{ij}(t) &\triangleq \max(\Lambda^{ij}(t, v^n(t)), \Lambda^{ij}(t, v(t))); \\ f_+(t) &\triangleq \max(f(t), 0).\end{aligned}$$

Тогда

$$J_t^{v^n, ij} = \underline{J}_t^{ij} + \widetilde{J}_t^{v^n, ij}, \quad J_t^{v, ij} = \underline{J}_t^{ij} + \widetilde{J}_t^{v, ij},$$

где

$$\begin{aligned}\underline{J}_t^{ij} &\triangleq \int_{[0; t] \times [0; 1]} \mathbf{I}_{\left[0, \frac{\underline{\Lambda}^{ij}(s)}{C^{ij}}\right]}(x) \pi^{ij}(ds, dx); \\ \widetilde{J}_t^{v^n, ij} &\triangleq \int_0^t \mathbf{I}(\Lambda^{ij}(s, v^n(s)) - \underline{\Lambda}^{ij}(s)) d\overline{J}_s^{ij}; \\ \widetilde{J}_t^{v, ij} &\triangleq \int_0^t \mathbf{I}(\Lambda^{ij}(s, v(s)) - \underline{\Lambda}^{ij}(s)) d\overline{J}_s^{ij}; \\ \overline{J}_t^{ij} &\triangleq \int_{[0; t] \times [0; 1]} \mathbf{I}_{\left[\frac{\underline{\Lambda}^{ij}(s)}{C^{ij}}, \frac{\overline{\Lambda}^{ij}(s)}{C^{ij}}\right]}(x) \pi^{ij}(ds, dx).\end{aligned}$$

Определенные выше процессы допускают следующие разложения:

$$\begin{aligned}\underline{J}_t^{ij} &= \int_0^t \underline{\Lambda}^{ij}(s) ds + \underline{\mu}_t^{ij}; \\ \widetilde{J}_t^{v^n, ij} &= \int_0^t (\Lambda^{ij}(s, v^n(s)) - \underline{\Lambda}^{ij}(s))_+ ds + \widetilde{\mu}_t^{v^n, ij}; \\ \widetilde{J}_t^{v, ij} &= \int_0^t (\Lambda^{ij}(s, v(s)) - \underline{\Lambda}^{ij}(s))_+ ds + \widetilde{\mu}_t^{v, ij}; \\ \overline{J}_t^{ij} &= \int_0^t (\overline{\Lambda}^{ij}(s) - \underline{\Lambda}^{ij}(s)) ds + \overline{\mu}_t^{ij},\end{aligned}$$

где $\underline{\mu}_t^{ij}$, $\widetilde{\mu}_t^{v^n, ij}$, $\widetilde{\mu}_t^{v, ij}$ и $\overline{\mu}_t^{ij}$ — мартингалы с квадратичными характеристиками

$$\begin{aligned}\langle \underline{\mu}^{ij}, \widetilde{\mu}^{v^n, ij} \rangle_t &= \langle \underline{\mu}^{ij}, \widetilde{\mu}^{v, ij} \rangle_t = \langle \widetilde{\mu}^{v^n, ij}, \widetilde{\mu}^{v, ij} \rangle_t \equiv 0; \\ \langle \underline{\mu}^{ij} \rangle_t &= \int_0^t \underline{\Lambda}^{ij}(s) ds; \\ \langle \widetilde{\mu}^{v^n, ij} \rangle_t &= \int_0^t (\Lambda^{ij}(s, v^n(s)) - \underline{\Lambda}^{ij}(s))_+ ds; \\ \langle \widetilde{\mu}^{v, ij} \rangle_t &= \int_0^t (\Lambda^{ij}(s, v(s)) - \underline{\Lambda}^{ij}(s))_+ ds; \\ \langle \overline{\mu}^{ij} \rangle_t &= \int_0^t (\overline{\Lambda}^{ij}(s) - \underline{\Lambda}^{ij}(s)) ds.\end{aligned}$$

При этом мартингалы $\widetilde{\mu}^{v^n, ij}$ и $\widetilde{\mu}^{v, ij}$ выражаются через $\overline{\mu}^{ij}$:

$$\begin{aligned}\widetilde{\mu}_t^{v^n, ij} &= \int_0^t \mathbf{I}(\Lambda^{ij}(s, v^n(s)) - \underline{\Lambda}^{ij}(s)) d\overline{\mu}_s^{ij}; \\ \widetilde{\mu}_t^{v, ij} &= \int_0^t \mathbf{I}(\Lambda^{ij}(s, v(s)) - \underline{\Lambda}^{ij}(s)) d\overline{\mu}_s^{ij}.\end{aligned}$$

Покомпонентное представление мартингала $\widetilde{M}_t$ через введенные выше ортогональные мартингалы

$$\begin{aligned}\widetilde{M}_t^\ell &= \int_0^t \sum_{i: i \neq \ell} e_i^\top \left(X_{s-}^{v^n} (d\underline{\mu}_s^{i\ell} + d\widetilde{\mu}_s^{v^n, i\ell}) - \right. \\ &\quad \left. - X_{s-}^v (d\underline{\mu}_s^{i\ell} + d\widetilde{\mu}_s^{v, i\ell}) \right) = \\ &= \int_0^t \sum_{i: i \neq \ell} e_i^\top \left(\widetilde{X}_{s-} d\underline{\mu}_s^{i\ell} + X_{s-}^{v^n} \widetilde{\mu}_s^{v^n, i\ell} - X_{s-}^v \widetilde{\mu}_s^{v, i\ell} \right), \\ &\quad \ell = 1, N,\end{aligned}$$

позволяет получить его квадратичную характеристику

$$\begin{aligned}\langle \widetilde{M}^\ell \rangle_t &= \int_0^t \sum_{i: i \neq \ell} \left(\left(\widetilde{X}_{s-}^i \right)^2 \underline{\Lambda}^{i\ell}(s) + \right. \\ &\quad \left. + \left(X_{s-}^{v^n, i} \right)^2 \left(\Lambda^{i\ell}(s, v^n(s)) - \underline{\Lambda}^{i\ell}(s) \right)_+ + \right. \\ &\quad \left. + \left(X_{s-}^{v, i} \right)^2 \left(\Lambda^{i\ell}(s, v(s)) - \underline{\Lambda}^{i\ell}(s) \right)_+ \right) ds, \quad \ell = 1, N.\end{aligned}$$

Далее найдем оценку сверху для $\text{tr} \langle \widetilde{M} \rangle$:

$$\begin{aligned}\text{tr} \langle \widetilde{M} \rangle_t &= \sum_{\ell=1}^N \langle \widetilde{M}^\ell \rangle_t = \\ &= \sum_{\ell=1}^N \sum_{i: i \neq \ell} \int_0^t \left(\left(\widetilde{X}_{s-}^i \right)^2 \underline{\Lambda}^{i\ell}(s) + \left(X_{s-}^{v^n, i} \right)^2 \times \right. \\ &\quad \times \left(\Lambda^{i\ell}(s, v^n(s)) - \underline{\Lambda}^{i\ell}(s) \right)_+ + \\ &\quad \left. + \left(X_{s-}^{v, i} \right)^2 \left(\Lambda^{i\ell}(s, v(s)) - \underline{\Lambda}^{i\ell}(s) \right)_+ \right) ds \leq \\ &\leq \int_0^t \left(\underbrace{\sum_{\ell=1}^N \sum_{i: i \neq \ell} \left(\widetilde{X}_{s-}^i \right)^2 \underline{\Lambda}^{i\ell}(s)}_{= \sum_{\ell=1}^N (\widetilde{X}_{s-}^i)^2 \sum_{i: i \neq \ell} \underline{\Lambda}^{i\ell}(s)} + \right. \\ &\quad \left. + \max_{\ell} \sum_{i: i \neq \ell} \left(\overline{\Lambda}^{i\ell}(s) - \underline{\Lambda}^{i\ell}(s) \right) \right) ds \leq \\ &\leq \int_0^t \left(\alpha_2^2 \|\widetilde{X}_{s-}\|^2 + \max_{\ell} \sum_{i: i \neq \ell} \left(\overline{\Lambda}^{i\ell}(s) - \underline{\Lambda}^{i\ell}(s) \right) \right) ds,\end{aligned}$$

где

$$\alpha_2^2 \triangleq \max_{\substack{i=1, N \\ (t, v) \in [0, T] \times U}} \sum_{\ell: \ell \neq i} \Lambda^{i\ell}(t, v).$$

По обобщенному правилу Ито

$$\begin{aligned} \|\tilde{X}_t\|^2 &= \tilde{X}_t^\top \tilde{X}_t = \int_0^t (\tilde{X}_{s-}^\top d\tilde{X}_s + d\tilde{X}_s^\top \tilde{X}_{s-}) + \text{tr}(\tilde{M})_t = \\ &= \int_0^t \left[\tilde{X}_{s-}^\top (\Lambda^\top(s, v^n(s)) \tilde{X}_{s-} + \tilde{\Lambda}^\top(s) X_{s-}^v) + \right. \\ &\quad \left. + (\tilde{X}_{s-}^\top \Lambda(s, v^n(s)) + (X_{s-}^v)^\top \tilde{\Lambda}(s)) \tilde{X}_{s-} \right] + \\ &\quad + \sum_{\ell=1}^N (\tilde{M}^\ell)_t + \mu_t, \quad (14) \end{aligned}$$

где μ_t — некоторый $\mathcal{F}_t$ -согласованный мартингал. Заметим, что

$$\tilde{X}_t^\top (\Lambda^\top(t, v^n(t)) + \Lambda(t, v^n(t))) \tilde{X}_t \leq \alpha_1^2 \|\tilde{X}_t\|^2,$$

где $\alpha_1^2 = \max_{(t,v) \in [0,T] \times U} \|\Lambda^\top(t, v) + \Lambda(t, v)\|$. В то же время

$$\begin{aligned} \tilde{X}_t^\top \tilde{\Lambda}^\top(t) X_t^v + (X_t^v)^\top \tilde{\Lambda}(t) \tilde{X}_t &\leq \\ &\leq 2 \max_{\substack{i=1, N, \\ s \in [0, T]}} |\tilde{\Lambda}^{ii}(t)| + 2 \max_{\substack{i, j=1, N: i \neq j, \\ s \in [0, T]}} |\tilde{\Lambda}^{ij}(t)|. \end{aligned}$$

Подставляя все оценки сверху в (14), получаем интегральное неравенство

$$\begin{aligned} \|\tilde{X}_t\|^2 &\leq \int_0^t (\alpha_1^2 + \alpha_2^2) \|\tilde{X}_{s-}\|^2 ds + \\ &+ \int_0^t \left[2 \left(\max_{\substack{i=1, N, \\ s \in [0, T]}} |\tilde{\Lambda}^{ii}(t)| + \max_{\substack{i, j=1, N: i \neq j, \\ s \in [0, T]}} |\tilde{\Lambda}^{ij}(t)| \right) + \right. \\ &\quad \left. + \max_{\ell} \sum_{i: i \neq \ell} (\bar{\Lambda}^{i\ell}(s) - \underline{\Lambda}^{i\ell}(s)) \right] ds + \mu_t. \end{aligned}$$

Из условия А следует, что

$$\begin{aligned} |\tilde{\Lambda}^{ij}(t)| &= \\ &= |\Lambda^{ij}(t, v^n(t)) - \Lambda^{ij}(t, v(t))| \leq K \|v^n(t) - v(t)\|. \end{aligned}$$

Обозначим $m_t^n \triangleq \mathbb{E}\{\|\tilde{X}_t\|^2\}$ и возьмем математическое ожидание от обеих частей последнего неравенства, учитывая условие Б:

$$\begin{aligned} m_t^n &\leq \int_0^t (\alpha_1^2 + \alpha_2^2) m_s^n ds + \\ &+ \int_0^t (3N-1) K \mathbb{E}\{\|v^n(s) - v(s)\|\} ds \leq \\ &\leq \int_0^t (\alpha_1^2 + \alpha_2^2) m_s^n ds + (3N-1) K \varepsilon_n. \end{aligned}$$

Тогда в силу неравенства Гронуолла–Беллмана

$$\begin{aligned} \mathbb{E}\{\|X_t^{v^n} - X_t^v\|^2\} &\leq \\ &\leq \underbrace{(3N-1) K (e^{(\alpha_1^2 + \alpha_2^2)t} - 1)}_{\triangleq L_1(t)} \varepsilon_n \xrightarrow{\varepsilon \rightarrow 0} 0. \end{aligned}$$

Сходимость (12) доказана.

Рассмотрим разность критериев качества для соответствующих управлений и построим ее оценку сверху:

$$\begin{aligned} |J_0(V^n) - J_0(V)| &= \\ &= \left| \mathbb{E} \left\{ \int_0^T (f^0(s, v_s^n) X_s^{v^n} - f^0(s, v_s) X_s^v) ds + \right. \right. \\ &\quad \left. \left. + \phi^0(X_T^{v^n} - X_T^v) \right\} \right| \leq \\ &\leq \int_0^T (\mathbb{E}\{|f^0(s, v^n(s)) \tilde{X}_s|\} + \mathbb{E}\{|f^0(s) X_s^v|\}) ds + \\ &\quad + \mathbb{E}\{|\phi^0 \tilde{X}_T|\} \leq \\ &\leq \int_0^T \left(\underbrace{\max_{(s,v) \in [0,T] \times U} \|f^0(s, v)\|}_{\triangleq \alpha_3} \sqrt{\mathbb{E}\{\|\tilde{X}_s\|^2\}} + \right. \\ &\quad \left. + \sqrt{\mathbb{E}\{\|\tilde{f}^0(s)\|^2\}} \right) ds + \|\phi^0\| \sqrt{\mathbb{E}\{\|\tilde{X}_T\|^2\}} = \\ &= \int_0^T (\alpha_3 \sqrt{L_1(t)} \varepsilon_n^{1/2} + K N \varepsilon_n) dt + \|\phi^0\| \sqrt{L_1(T)} \varepsilon_n^{1/2} = \\ &= \underbrace{\left(\int_0^T \alpha_3 \sqrt{L_1(t)} dt + \|\phi^0\| \sqrt{L_1(T)} \right)}_{\triangleq L_2(T)} dt \varepsilon_n^{1/2} + \\ &\quad + \underbrace{K N T}_{\triangleq L_3(T)} \varepsilon_n \xrightarrow{\varepsilon \rightarrow 0} 0. \end{aligned}$$

Сходимость (13) и теорема 2 доказаны.

Литература

1. Дынкин Е., Юшкевич А. Управляемые марковские процессы и их приложения. — М.: Наука, 1975. 338 с.
2. Davis M. Markov models and optimization. — London: Chapman and Hall, 1993. 308 p. doi: 10.1201/9780203748039.
3. Piunovskiy A., Zhang Y. Continuous-time Markov decision processes: Borel space models and general control strategies. — Cham: Springer, 2020. 583 p. doi: 10.1007/978-3-030-54987-9.

4. Босов А. Стабилизация автономного линейного выхода марковской цепи по квадратичному критерию на бесконечном горизонте // Информатика и её применения, 2024. Т. 18. Вып. 3. С. 38–44. doi: 10.14357/19922264240305. EDN: XVTFLH.
5. Low S., Paganini F., Doyle J. Internet congestion control // IEEE Contr. Syst. Mag., 2002. Vol. 22. Iss. 1. P. 28–43. doi: 10.1109/37.980245.
6. Altman E. Applications of Markov decision processes in communication networks // Handbook of Markov decision processes / Eds. E. A. Feinberg, and A. Shwartz. — International ser. in operations research and management science. — Boston, MA, USA: Springer, 2002. Vol. 40. P. 489–536. doi: 10.1007/978-1-4615-0805-2_16.
7. Миллер Б., Авраченко К., Степанян К., Миллер Г. Задача оптимального стохастического управления потоком данных по неполной информации // Проблемы передачи информации, 2005. Т. 41. № 2. С. 89–110.
8. McInnes D., Miller B. Optimal control of a large dam using time-inhomogeneous Markov chains with an application to flood control // IFAC PapersOn-Line, 2017. Vol. 50. Iss. 1. P. 3499–3504. doi: 10.1016/J.IFACOL.2017.08.936.
9. Shaldambayeva S., Zhumakhanova K., Sandygulova A., et al. Partially observable Markov decision processes in shared autonomy applications: A survey // IEEE Access, 2025. Vol. 13. P. 186937–186951. doi: 10.1109/ACCESS.2025.3625601.
10. Fox A., De Pellegrini F., Altman E., et al. Performing Load Balancing under Constraints // 23rd Symposium (International) on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks Proceedings. — IEEE 2025. P. 103–110. doi: 10.23919/WiOpt66569.2025.11123242.
11. Rieder U., Winter J. Optimal control of Markovian jump processes with partial information and applications to a parallel queueing model // Math. Method. Oper. Res., 2009. Vol. 70. P. 567–596. doi: 10.1007/s00186-009-0284-7.
12. Li Q., Ma J., Fan R., Xia L. An overview for Markov decision processes in queues and networks // Stochastic models in reliability, network security and system safety / Eds. Q. L. Li, J. Wang, H. B. Yu. — Communications in computer and information science ser. — Singapore: Springer, 2019. Vol. 1102. P. 44–71. doi: 10.1007/978-981-15-0864-6_3.
13. White D. A survey of applications of Markov decision processes // J. Oper. Res. Soc., 1996. Vol. 44. Iss. 11. P. 1073–1096. doi: 10.2307/2583870.
14. Shi P., Li F. A survey on Markovian jump systems: Modeling and design // Int. J. Control Autom., 2015. Vol. 13. Iss. 1. P. 1–16. doi: 10.1007/s12555-014-0576-4.
15. Борисов А. Рынок с марковской скачкообразной волатильностью I: мониторинг цены риска как задача оптимальной фильтрации // Информатика и её применения, 2023. Т. 17. Вып. 2. С. 27–33. doi: 10.14357/19922264230204. EDN: GAXCHQ.
16. Борисов А. Рынок с марковской скачкообразной волатильностью V: пополнение рынка деривативами // Информатика и её применения, 2024. Т. 18. Вып. 2. С. 9–16. doi: 10.14357/19922264240202. EDN: DQFSDO.
17. Босов А. Стабилизация траектории линейной системы со скачкообразным дрейфом при целочисленных ограничениях на управление // Информатика и её применения, 2025. Т. 19. Вып. 3. С. 10–18. doi: 10.14357/19922264250302. EDN: YZENCC.
18. Крылов Н. Управляемые процессы диффузионного типа. — М.: Наука, 1977. 400 с.
19. Липцер Р., Ширяев А. Теория мартингалов. — М.: Физматлит, 1986. 512 с.
20. Миллер Б., Миллер Г., Семенихин К. Методы синтеза оптимального управления марковским процессом с конечным множеством состояний при наличии ограничений // Автоматика и телемеханика, 2011. Вып. 2. С. 111–130. doi: 10.1134/S000511791102010X.
21. Миллер Б., Миллер Г., Семенихин К. Регуляризация задачи оптимального управления марковским процессом с конечным числом состояний при наличии ограничений // Автоматика и телемеханика, 2016. Вып. 9. С. 96–123. EDN: WWVXGF.
22. Жакод Ж., Ширяев А. Предельные теоремы для случайных процессов / Пер. с англ. — М.: Физматлит, 1994. Т. 1. 544 с. (Jacod J., Shiryaev A. N. Limit theorems for stochastic processes. — Berlin: Springer, 1987. 600 p.)
23. Ishikawa Y., Kunita H. Malliavin calculus on the Wiener–Poisson space and its application to canonical SDE with jumps // Stoch. Proc. Appl., 2006. Vol. 116. Iss. 12. P. 1743–1769. doi: 10.1016/j.spa.2006.04.013.
24. Wonham W. On the separation theorem of stochastic control // SIAM J. Control, 1968. Vol. 6. Iss. 2. P. 312–326. doi: 10.1137/0306023.
25. Борисов А. Фильтрация состояний и параметров специальных марковских скачкообразных процессов по косвенным наблюдениям без шума // Информатика и её применения, 2025. Т. 19. Вып. 1. С. 25–32. doi: 10.14357/19922264250104. EDN: MZAJVZ.
26. Борисов А. Использование методов оптимальной фильтрации для пассивного мониторинга доступной пропускной способности сетевого канала // Автоматика и телемеханика, 2025. Вып. 6. С. 61–85. doi: 10.31857/S0005231025060048.
27. Kern P., Müller C. A closed form formula for the stochastic exponential of a matrix-valued semimartingale // J. Stochastic Analysis, 2022. Vol. 3. Iss. 2. Art. 3. 19 p. doi: 10.31390/josa.3.2.03. EDN: UGPTFV.
28. Лакишмикантам В., Лиля С., Мартынюк А. Устойчивость движения: метод сравнения. — Киев: Наукова думка, 1991. 248 с.

Поступила в редакцию 10.03.2026

Принята к публикации 15.08.2026

OPTIMAL STOCHASTIC CONTROL OF MARKOV JUMP PROCESSES UNDER DELAYED NOISE-FREE OBSERVATIONS I: UNIVERSAL CANONICAL SPACE AND THE MARTINGALE PROBLEM

A. V. Borisov^{1,2} and Yu. N. Kurinov²

¹Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

²M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation

Abstract: The first part of this series presents the theoretical foundations required for the proper formulation and solution of a finite-horizon stochastic control problem under incomplete information. The controlled system is represented by a class of Markov jump processes (MJPs) with a finite state space. The optimality criterion is defined as the expected value of an integral loss functional. The observations available for control synthesis are functions of the controlled state, measured without external noise but subject to a time delay. The class of admissible controls consists of processes that are predictable with respect to the natural filtration generated by the observations and that satisfy a set of geometric and integral constraints. A universal filtered probability space is constructed to provide a solution to the martingale problem associated with this class of controlled MJPs. In addition, conditions ensuring the continuity of both the MJP state trajectory and the objective functional with respect to the applied control are established.

Keywords: controlled Markov jump process; Wiener–Poisson space; martingale problem; Poisson stochastic measure

DOI: 10.14357/19922264260302

EDN: AZXCMB

Acknowledgments

The research was supported by the Russian Science Foundation, project No. 25-21-00504.

References

1. Dynkin, E. B., and A. A. Yushkevich. 1975. *Upravlyaemye markovskie protsessy i ikh prilozheniya* [Controlled Markov processes and their applications]. Moscow: Nauka. 338 p.
2. Davis, M. H. A. 1993. *Markov models and optimization*. London: Chapman and Hall/CRC. 308 p. doi: 10.1201/9780203748039.
3. Piunovskiy, A., and Y. Zhang. 2020. *Continuous-time Markov decision processes: Borel space models and general control strategies*. Cham: Springer. 583 p. doi: 10.1007/978-3-030-54987-9.
4. Bosov, A. V. 2024. Stabilizatsiya avtonomnogo lineynogo vykhoda markovskoy tsepi po kvadrachnomu kriteriyu na beskonечnom gorizonte [Autonomous linear output of the Markov chain stabilization by square criterion on an infinite horizon]. *Informatika i ee Primeneniya — Inform. Appl.* 18(3):38–44. doi: 10.14357/19922264240305. EDN: XVTFLH.
5. Low, S., F. Paganini, and J. Doyle. 2002. Internet congestion control. *IEEE Contr. Syst. Mag.* 22(1):28–43. doi: 10.1109/37.980245.
6. Altman, E. 2002. Applications of Markov decision processes in communication networks. *Handbook of Markov decision processes*. Eds. E. A. Feinberg and A. Shwartz. International series in operations research and management science. Boston, MA: Springer. 40:489–536. doi: 10.1007/978-1-4615-0805-2_16.
7. Miller, B. M., K. E. Avrachenkov, K. V. Stepanyan, and G. B. Miller. 2005. Flow control as a stochastic optimal control problem with incomplete information. *Probl. Inf. Transm.* 41(2):150–170. doi: 10.1007/s11122-005-0020-8. EDN: LJFPRR.
8. McInnes, D., and B. Miller. 2017. Optimal control of a large dam using time-inhomogeneous Markov chains with an application to flood control. *IFAC PapersOn-Line* 50(1):3499–3504. doi: 10.1016/j.ifacol.2017.08.936. EDN: XPJIEV.
9. Shaldambayeva, S., K. Zhumakhanova, A. Sandygulovala, et al. 2025. Partially observable Markov decision processes in shared autonomy applications: A survey. *IEEE Access* 13:186937–186951. doi: 10.1109/ACCESS.2025.3625601.
10. Fox, A., F. De Pellegrini, E. Altman, et al. 2025. Performing load balancing under constraints. *23rd Symposium (International) on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks Proceedings*. IEEE. 103–110. doi: 10.23919/WiOpt66569.2025.11123242.
11. Rieder, U., and J. Winter. 2009. Optimal control of Markovian jump processes with partial information and applications to a parallel queueing model. *Math. Method. Oper. Res.* 70:567–596. doi: 10.1007/s00186-009-0284-7.

12. Li, Q., J. Ma, R. Fan, and L. Xia. 2019. An overview for Markov decision processes in queues and networks. *Stochastic models in reliability, network security and system safety*. Eds. Q. L. Li, J. Wang, and H. B. Yu. Communications in computer and information science ser. Singapore: Springer. 1102:44–71. doi: 10.1007/978-981-15-0864-6_3.
13. White, D. J. 1996. A survey of applications of Markov decision processes. *J. Oper. Res. Soc.* 44(11):1073–1096. doi: 10.2307/2583870.
14. Shi, P., and F. Li. 2015. A survey on Markovian jump systems: Modeling and design. *Int. J. Control Autom.* 13(1):1–16. doi: 10.1007/s12555-014-0576-4.
15. Borisov, A. 2023. Rynok s markovskoy skachkoobraznoy volatil'nost'yu I: monitoring tseny riska kak zadacha optimal'noy fil'tratsii [Market with Markov jump volatility I: Price of risk monitoring as an optimal filtering problem]. *Informatika i ee Primeneniya — Inform. Appl.* 17(2):27–33. doi: 10.14357/19922264230204. EDN: GAXCHQ.
16. Borisov, A. 2024. Rynok s markovskoy skachkoobraznoy volatil'nost'yu V: popolnenie rynka derivativami [Market with Markov jump volatility V: Market completion with derivatives]. *Informatika i ee Primeneniya — Inform. Appl.* 18(2):9–16. doi: 10.14357/19922264240202. EDN: DQFSDO.
17. Bosov, A. V. 2025. Stabilizatsiya traektorii lineynoy sistemy so skachkoobraznym dreyfom pri tselochislennykh ograniчениyakh na upravlenie [Stabilization of the trajectory of a linear system with jumping drift under integer control constraints]. *Informatika i ee Primeneniya — Inform. Appl.* 19(3):10–18. doi: 10.14357/19922264250302. EDN: YZEHC.
18. Krylov, N. V. 1977. *Upravlyaemye protsessy diffuzionnogo tipa* [Controlled diffusion processes]. Moscow: Nauka. 400 p.
19. Liptser, R. Sh., and A. N. Shiryaev. 1986. *Teoriya martin-galov* [Theory of martingales]. Moscow: Fizmatlit. 512 p.
20. Miller, B. M., G. B. Miller, and K. V. Semenikhin. 2011. Methods to design optimal control of Markov process with finite state set in the presence of constraints. *Automat. Rem. Contr.* 72(2):323–341. doi: 10.1134/S000511791102010X. EDN: OHUBSJ.
21. Miller, B. M., G. B. Miller, and K. V. Semenikhin. 2016. Optimal control problem regularization for the Markov process with finite number of states and constraints. *Automat. Rem. Contr.* 77(9):1589–1611. doi: 10.1134/S0005117916090071. EDN: XFJXFJ.
22. Jacod, J., and A. N. Shiryaev. 1987. *Limit theorems for stochastic processes*. Berlin: Springer. 600 p.
23. Ishikawa, Y., and H. Kunita. 2006. Malliavin calculus on the Wiener–Poisson space and its application to canonical SDE with jumps. *Stoch. Proc. Appl.* 116(12):1743–1769. doi: 10.1016/j.spa.2006.04.013.
24. Wonham, W. M. 1968. On the separation theorem of stochastic control. *SIAM J. Control* 6(2):312–326. doi: 10.1137/0306023.
25. 1 Borisov, A. V. 2025. Fil'tratsiya sostoyaniy i parametrov spetsial'nykh markovskikh skachkoobraznykh protsessov po kosvennym nablyudeniym bez shuma [Filtering of states and parameters of special Markov jump processes via indirect perfect observations]. *Informatika i ee primeneniya — Inform. Appl.* 19(1):25–32. doi: 10.14357/19922264250104. EDN: MZAJVZ.
26. Borisov, A. V. 2025. The use of optimal filtering methods for passive monitoring of available bandwidth of a network channel. *Automat. Rem. Contr.* 86(6):545–563.
27. Kern, P., and C. Müllner. 2022. A closed form formula for the stochastic exponential of a matrix-valued semimartingale. *J. Stochastic Analysis* 3(2):3. 19 p. doi: 10.31390/josa.3.2.03. EDN: UGPTFV.
28. Lakshmikantham, V., S. Leela, and A. A. Martynyuk. 1991. *Ustoichivost' dvizheniya: metod sravneniya* [Motion stability: Comparison method]. Kiev: Naukova Dumka. 248 p.

Received March 10, 2026

Accepted August 15, 2026

Contributors

Borisov Andrey V. (b. 1965) — Doctor of Science in physics and mathematics, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; professor, Department of Mathematical Statistics, Faculty of Computational Mathematics and Cybernetics, M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation; aborisov@frcsc.ru

Kurinov Yuri N. (b. 2002) — master student, Department of Mathematical Statistics, Faculty of Computational Mathematics and Cybernetics, M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation; kurinovurij@gmail.com

УСТОЙЧИВЫЕ АЛГОРИТМЫ АДАПТИВНОГО ОЦЕНИВАНИЯ СОСТОЯНИЙ ДИНАМИЧЕСКИХ СИСТЕМ ПРИ СЛУЧАЙНЫХ ВРЕМЕННЫХ ЗАДЕРЖКАХ НАБЛЮДЕНИЙ*

А. В. Босов¹, С. А. Босов², И. В. Урюпин³

Аннотация: Предложены новые вычислительно устойчивые алгоритмы адаптивной фильтрации состояния движущегося в водной среде объекта по акустическим наблюдениям со случайными временными задержками. Разработанная ранее и адаптированная для модели временных задержек версия расширенного фильтра Калмана (РФК) по методу линейных псевдонаблюдений дополнена двумя адаптивными модификациями фильтра для случая неизвестных ковариаций возмущений динамики и ошибок измерений. Для оценивания ковариаций использованы устойчивые схемы адаптивного фильтра Калмана (АФК), базирующиеся на анализе невязок измерений по оценкам фильтрации. Эти схемы усовершенствованы путем дополнительной оптимизации для учета положительно диагональных структур неизвестных ковариаций, предполагаемых моделью движения и создаваемых линейными псевдонаблюдениями. Выполнен масштабный численный эксперимент, подтвердивший работоспособность предложенных схем адаптации. В расчетах использована та же модель, что и в предыдущих работах, благодаря чему удалось отдельно оценить влияние адаптивной постановки и обозначить возможные направления дальнейшего развития методики.

Ключевые слова: стохастическая фильтрация; стохастическая система со случайными задержками наблюдений; расширенный фильтр Калмана (РФК); РФК по методу линейных псевдонаблюдений; адаптивный фильтр Калмана (АФК)

DOI: 10.14357/19922264260303

EDN: HVLJCG

1 Введение

Для решения многих задач анализа динамических систем используются модели, неопределенность в которых связана с отсутствием априорной информации о значениях части параметров. Существуют различные формальные постановки таких задач и методы их решения. Значимое место среди них занимает адаптивная фильтрация, основанная на идее совместного выполнения двух процедур: фильтрации состояния динамической системы по наблюдениям и оценивания неизвестных параметров. При этом для фильтрации могут использоваться стандартные алгоритмы, в которых неизвестные параметры заменяются их текущими оценками. В свою очередь, параметры могут оцениваться стандартными методами с использованием оценок ненаблюдаемых состояний, полученных на этапе фильтрации. Тем самым оба процесса оказываются взаимосвязанными: уточнение состояния влияет на оценивание параметров, а уточнение параметров — на последующую фильтрацию. Учет

этой взаимной зависимости и составляет основу адаптивного подхода [1, 2]. Распространенный метод этого подхода — адаптивная калмановская фильтрация. Это не только подходы, восходящие к пионерским работам 1960–1970-х гг. и построенные вокруг линейного фильтра Калмана (ЛФК) [3], но и более поздние варианты нелинейных фильтров. Наиболее известным среди них стал РФК [4]. Но много внимания уделяется и другим субоптимальным методам фильтрации, сохраняющим калмановскую структуру. К ним относятся многочисленные модификации РФК, а также различные варианты сигма-точечных фильтров. Для таких алгоритмов часто применяются методы адаптации, первоначально разработанные для ЛФК или близкие к ним по общей идее.

Применительно к адаптивной калмановской фильтрации традиционно наибольшее внимание уделяется постановкам, в которых неизвестными параметрами являются ковариации возмущений динамики и шумов измерений. Впервые подход к адаптивному оцениванию неизвестных ковариаций

* Исследование выполнено за счет гранта Российского научного фонда № 25-21-00550, <https://rscf.ru/project/25-21-00550/>. Работа выполнялась с использованием инфраструктуры Центра коллективного пользования «Высокопроизводительные вычисления и большие данные» (ЦКП «Информатика») ФИЦ ИУ РАН (г. Москва).

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ABosov@frccsc.ru

²Федеральный исследовательский центр «Информатика и управление» Российской академии наук, SBosov@frccsc.ru

³Федеральный исследовательский центр «Информатика и управление» Российской академии наук, uryupin93@yandex.ru

ций с опорой на базовые соотношения ЛФК был предложен в [5, 6], и поэтому он называется алгоритмом (или схемой) Сейджа—Хуса. Другие подходы, включая байесовское оценивание и метод максимального правдоподобия, систематизированы в [7, 8]. Именно в этих работах появился термин «адаптивный фильтр Калмана» и было предложено использовать скользящее окно фиксированного размера вместо рекуррентной оценки Сейджа—Хуса, строящейся по всей совокупности поступающих измерений. Эта схема довольно естественно модифицируется для оценивания коэффициента усиления фильтра, пропуская этап оценивания ковариаций [9]. В дальнейшем предлагались различные варианты усовершенствования суммирования в схеме Сейджа—Хуса [10–14]. Однако качественно иной уровень адаптации обеспечила смена парадигмы. Основу схемы Сейджа—Хуса составляет анализ моментных характеристик невязки, т. е. разности между поступившим измерением и его прогнозируемым значением (когда в функцию наблюдателя подставляются вычисленный на текущем шаге прогноз и нулевые ошибки). В работах [15, 16] вместо этого предлагается базироваться на апостериорной невязке, когда в функцию наблюдателя подставляется вычисленная на текущем шаге оценка фильтрации. Варианты совершенствования формул Сейджа—Хуса в [15] получены с помощью метода максимального правдоподобия; эта работа представляется приоритетной. В статье [16] рассматривается только оценивание ковариации ошибок измерений. Кроме того, полезна работа [17], в которой этот же результат используется и объединяется с приемами робастной калмановской фильтрации на основе ковариаций. Главное достоинство адаптации, основанной на анализе апостериорных невязок [15, 16], — это гораздо более высокая устойчивость схем оценивания по сравнению с вариантами Сейджа—Хуса.

В рамках данной тематики наряду с фундаментальными исследованиями выполнен большой объем прикладных исследований и практических реализаций, который сам по себе заслуживает отдельного обзора. Во-первых, отметим, что все адаптивные схемы почти автоматически переносятся на любые фильтры, имеющие так называемую калмановскую структуру. Это, прежде всего, уже упомянутый РФК со всеми своими модификациями, а также все семейство сигма-точечных фильтров, включая непахнущий (Unscented) и кубатурные (Cubature) фильтры Калмана. Во-вторых, следует упомянуть широкую область приложений, открывающуюся с навигационных задач (начиная с основополагающих статей [15, 16]), но далеко не ограничивающуюся ими. Хорошими примерами

такого разнообразия служат: химико-технологические процессы и управление реакторами [18]; батарейные системы и оценка состояния заряда [19]; океанографические и климатические модели [20]; биомедицинская обработка сигналов [21]. Эти примеры не претендуют на полноту обзора приложений, но показывают, что методика калмановской адаптации востребована не только в навигации, но и в промышленности, химии, энергетике и теории управления. Кроме того, она привлекает внимание исследователей в таких не самых очевидных приложениях фильтрации, как океанография, климатология и даже медицина. В данной статье приложение — это применение автономных подводных аппаратов (ПА), а именно: позиционирование ПА по косвенным наблюдениям со случайными временными запаздываниями [22–25]. Метод фильтрации — РФК с линейными псевдонаблюдениями, предложенный в [26]. Это типичный вариант усовершенствованного РФК, который естественно сочетается с любой схемой адаптации. Трудности, порождаемые прежде всего ключевой особенностью модели, запаздывающими на случайное время наблюдениями, усугубляются общей тенденцией РФК к нестабильному поведению [27]. В этих условиях выбор базовой схемы адаптации на основе апостериорных невязок [15, 16] выглядит вполне естественно. Таким образом, ставится задача адаптировать указанную схему к модели с задержками и проверить работоспособность и эффективность результирующего алгоритма в рамках состоятельного вычислительного эксперимента.

2 Модель системы наблюдения и расширенный фильтр Калмана по методу линейных псевдонаблюдений

Рассмотрим функции состояния $X_t \in \mathbb{R}^{p \times}$ — положение ПА — и наблюдения $y_t \in \mathbb{R}^{q \times}$ — измерения, выполняемые внешним наблюдателем. Будем считать, что $X_t = (X(t), Y(t), Z(t))'$ — вектор декартовых координат, которые требуется оценивать. Дискретные по времени измерения поступают в моменты $1, 2, \dots, t, \dots$, соответствующие равномерно разбиению физического времени с шагом δ с. Первое наблюдение y_0 интерпретируется как сигнал обнаружения ПА. Предполагается, что сигнал от обнаруженного объекта поступает с запаздыванием, величина которого зависит от характеристик среды и расстояния между объектом и наблюдателем, а именно: если наблюдатель находится в точке

с координатами $(X_{\mathcal{M}}, Y_{\mathcal{M}}, Z_{\mathcal{M}})$, то временная задержка τ_t поступления измерений имеет вид:

$$\tau_t = \min \left(\left[\left((X(t) - X_{\mathcal{M}})^2 + (Y(t) - Y_{\mathcal{M}})^2 + (Z(t) - Z_{\mathcal{M}})^2 \right)^{1/2} / (\delta v_s) \right], T \right), \quad (1)$$

где $v_s = 5400$ км/ч (1550 м/с) — скорость звука в воде. Задержка, таким образом, равна времени, затрачиваемому акустическим сигналом на прохождение в воде расстояния между ПА и наблюдателем. Целая часть числа $[\cdot]$ в (1) нужна для формальной записи модели с дискретным временем, а $\min$ и верхнее ограничение T отражают предположение о том, что известна величина максимально возможной задержки: $\tau_t \leq T$. Таким образом, положение ПА, детектируемое измерением y_0 в момент $t = 0$, задается величиной X_{-T_0} , а положение, отвечающее измерению y_t в момент $t > 0$, — величиной $X_{t-\tau_t}$. Так интерпретируются измерения одного наблюдателя. Если их несколько, то в одном наблюдении комбинируются измерения с разными временными задержками.

Для записи формальной модели можно считать, что движение ПА начинается в момент $t = -T - 1$, но положения $X_{-T}, X_{-T+1}, \dots, X_{-T_0}$ не измеряются. Определение начального положения задается в виде $X_{-T_0-1} = \eta$, значения $X_{-T_0-2}, \dots, X_{-T-1}$, считаются неизвестными. Относительно случайного вектора η предполагаются заданными моменты: среднее m_η и ковариация D_η . Далее учтем, что наблюдателей может быть несколько. Для i -го наблюдателя временная задержка $\tau_t^{(i)}$ определяется соотношением (1) и координатами $(X_{\mathcal{M}}^{(i)}, Y_{\mathcal{M}}^{(i)}, Z_{\mathcal{M}}^{(i)})$, $i = \overline{1, q}$. В итоге имеем следующую модель системы наблюдения:

$$\left. \begin{aligned} X_t &= \Phi_t^{(1)}(X_{t-1}) + \Phi_t^{(2)}(X_{t-1})W_t; \\ y_t^{(i)} &= \psi_t^{(i,1)}(X_{t-\tau_t^{(i)}}) + \psi_t^{(i,2)}(X_{t-\tau_t^{(i)}})v_t^{(i)}, \\ i &= \overline{1, q}, \quad t = -T, -T+1, \dots, 0, 1, \dots, \\ X_{-\max_{i=\overline{1, q}} \tau_t^{(i)} - 1} &= \eta, \end{aligned} \right\} \quad (2)$$

где $\Phi_t^{(1)}, \Phi_t^{(2)}, \psi_t^{(i,1)}$ и $\psi_t^{(i,2)}$ — заданные функции; возмущения $W_t \in \mathbb{R}^{p_w}$ и ошибки измерений $v_t^{(i)} \in \mathbb{R}^{q_i^{(i)}}$ — независимые дискретные белые шумы второго порядка; η, W_t и $v_t^{(i)}$ независимы в совокупности, соответствующие математические ожидания и ковариации обозначаются как $m_W(t), D_W(t)$ и $m_v^{(i)}(t), D_v^{(i)}(t)$. Оператор $\max_{i=\overline{1, q}} \tau_t^{(i)}$ в (2) использован для того, чтобы исключить из рассмотрения моменты времени, когда доступны измерения не всех наблюдателей, а части: чтобы не усложнять обозначения, процедура оценки положения начинается в тот момент, когда измерения есть

у всех наблюдателей. До этого момента достаточно иметь грубую оценку положения, например путем геометрического пересчета измерений в декартовы координаты без учета ошибок измерений.

Для оценивания X_t по наблюдениям $y_t^{(i)}$, $i = \overline{1, q}$, будем использовать вариант РФК по методу линейных псевдонаблюдений [23–26]. Суть этого метода состоит в том, что «истинные» наблюдения $y_t^{(i)}$ в модели (2) заменяют специальным образом сформированные псевдонаблюдения:

$$Y_t^{(i)} = \Psi_t^{(i,1)}(y_t^{(i)})X_{t-\tilde{\tau}_t^{(i)}} + \Psi_t^{(i,2)}(X_{t-\tilde{\tau}_t^{(i)}}, y_t^{(i)})V_t^{(i)}. \quad (3)$$

Смысл псевдонаблюдений (3) состоит в их линейной зависимости от оцениваемого состояния X_t . Кроме того, неизвестные случайные временные задержки $\tau_t^{(i)}$ заменены на оценки $\tilde{\tau}_t^{(i)} = \tilde{\tau}_t^{(i)}(y_t)$. При этом (3) не является результатом линеаризации модели наблюдения (2), а учитывает более тонкие зависимости между измеряемыми физическими величинами — ключевыми в подводной навигации измерениями y_φ, y_λ и y_r — пеленга φ , угла возвышения λ и дальности r соответственно. Использование тригонометрических зависимостей между измеряемыми углами и минимаксными свойствами гауссовского распределения подробно описано в [26]. Учитывая, что вектор наблюдений y_t состоит из измерений $y_{\varphi_t}^{(i)}, y_{\lambda_t}^{(i)}$ и $y_{r_t}^{(i)}$, получаем вектор псевдонаблюдений Y_t , который состоит из псевдоизмерений $Y_{\varphi_t}^{(i)}, Y_{\lambda_t}^{(i)}$ и $Y_{r_t}^{(i)}$. Простая оценка задержки через текущее измерение дальности:

$$\tilde{\tau}_t^{(i)} = \min \left\{ T, \left\lceil \frac{y_{r_t}^{(i)}}{\delta v_s} \right\rceil \right\}.$$

Обоснованная в [26] форма псевдонаблюдений $Y_{\varphi_t}^{(i)}, Y_{\lambda_t}^{(i)}$ и $Y_{r_t}^{(i)}$ имеет следующий вид:

$$\left. \begin{aligned} Y_{\varphi_t}^{(i)} &= -Y_{\mathcal{M}}^{(i)}y_{\varphi}^{\cos} + X_{\mathcal{M}}^{(i)}y_{\varphi}^{\sin}; \\ Y_{\lambda_t}^{(i)} &= -y_{\varphi}^{\cos}y_{\lambda}^{\cos}Z_{\mathcal{M}}^{(i)} + y_{\lambda}^{\sin}X_{\mathcal{M}}^{(i)}; \\ Y_{r_t}^{(i)} &= Z_{\mathcal{M}}^{(i)} + y_{r_t}^{(i)}y_{\lambda}^{\sin}, \end{aligned} \right\} \quad (4)$$

где

$$\begin{aligned} y_{\varphi}^{\sin} &= \sin(y_{\varphi_t}^{(i)}); \quad y_{\varphi}^{\cos} = \cos(y_{\varphi_t}^{(i)}); \\ y_{\lambda}^{\sin} &= \sin(y_{\lambda_t}^{(i)}); \quad y_{\lambda}^{\cos} = \cos(y_{\lambda_t}^{(i)}). \end{aligned}$$

Соответствующая таким псевдонаблюдениям модель:

$$\begin{pmatrix} Y_{\varphi_t}^{(i)} \\ Y_{\lambda_t}^{(i)} \\ Y_{r_t}^{(i)} \end{pmatrix} = \begin{pmatrix} y_{\varphi}^{\sin} - y_{\varphi}^{\cos} & 0 \\ y_{\lambda}^{\sin} & 0 & -y_{\varphi}^{\cos} y_{\lambda}^{\cos} \\ 0 & 0 & 1 \end{pmatrix} X_{t-\tilde{\tau}_t^{(i)}} + \begin{pmatrix} X_{\mathcal{M}}^{(i)} - X(t) & Y(t) - Y_{\mathcal{M}}^{(i)} & 0 \\ 0 & (Z(t) - Z_{\mathcal{M}}^{(i)}) y_{\lambda}^{\cos} X_{\mathcal{M}}^{(i)} - X(t) & 0 \\ 0 & 0 & y_{r_t}^{(i)} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ y_{r_t}^{(i)} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ (Z(t) - Z_{\mathcal{M}}^{(i)}) y_{\varphi}^{\cos} & 0 \\ 0 & y_{\lambda}^{\sin} \end{pmatrix} V_t^{(i)}. \quad (5)$$

Здесь явно записаны фигурирующие в (3) матрицы $\Psi_t^{(i,1)}(y_t^{(i)})$ и $\Psi_t^{(i,2)}(X_{t-\tilde{\tau}_t^{(i)}}, y_t^{(i)})$, а ошибки измерений формируются q группами независимых векторов $V_t^{(i)} = (v_{1_t}^{(i)}, v_{2_t}^{(i)}, v_{3_t}^{(i)}, v_{4_t}^{(i)}, v_{5_t}^{(i)})'$, каждая состоит из 5 независимых центрированных гауссовских случайных величин с дисперсиями: $D_{v_{1_t}^{(i)}} = D_{v_{2_t}^{(i)}} = \sigma_{\varphi}^2$; $D_{v_{3_t}^{(i)}} = D_{v_{4_t}^{(i)}} = \sigma_{\lambda}^2$; $D_{v_{5_t}^{(i)}} = \sigma_r^2$. Здесь σ_{φ}^2 , σ_{λ}^2 и σ_r^2 — дисперсии ошибок измерения пеленга, угла возвышения и дальности, которые можно считать одинаковыми у всех наблюдателей. Под заменой модели наблюдения понимается то, что «истинные» наблюдения $y_t^{(i)}$ из (2) используются только для вычисления функций $\Psi_t^{(i,1)}$ и $\Psi_t^{(i,2)}$, а для оценки состояния X_t — только псевдонаблюдения $Y_s^{(i)}$, $s \leq t$, из (4). При этом фильтр «считает», что вычисленные согласно (4) значения $Y_t^{(i)}$ описываются моделью (5), а модель наблюдений для $y_t^{(i)}$ из (2) вообще не используется.

Теперь можно взять классический РФК [4] и только учесть в нем сдвиги из-за временных задержек [23–26]:

$$\left. \begin{aligned} \tilde{X}_t &= \Phi_t^{(1)} (\hat{X}_{t-1}) + \Phi_t^{(2)} (\hat{X}_{t-1}) m_W(t); \\ \tilde{\Phi}_t^{(1)} &= \frac{\partial \Phi_t^{(1)}(X)}{\partial X} \Big|_{X=\tilde{X}_t}; \quad \tilde{\Phi}_t^{(2)} = \Phi_t^{(2)} (\tilde{X}_t); \\ \tilde{K}_t &= \tilde{\Phi}_t^{(1)} \tilde{K}_{t-1} (\tilde{\Phi}_t^{(1)})' + \tilde{\Phi}_t^{(2)} D_W(t) (\tilde{\Phi}_t^{(2)})'; \\ \tilde{X}_t &= \tilde{X}_t + K_t \Delta \tilde{Y}_t; \\ \Delta \tilde{Y}_t &= (Y_t^{(1)} - \Psi_t^{(1,1)}(y_t^{(1)}) \tilde{X}_{t-\tilde{\tau}_t^{(1)}} - \\ &\quad - m_{v_t^{(1)}}(t), \dots, Y_t^{(q)} - \Psi_t^{(q,1)}(y_t^{(q)}) \tilde{X}_{t-\tilde{\tau}_t^{(q)}} - \\ &\quad - m_{v_t^{(q)}}(t)); \\ K_t &= \tilde{K}_t (\Psi_t^{(1)})' \left((\Psi_t^{(1)} \tilde{K}_t (\Psi_t^{(1)})' + \right. \\ &\quad \left. + \tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})' \right)^{-1}; \\ \hat{K}_t &= \tilde{K}_t - K_t \Psi_t^{(1)} \tilde{K}_t, \end{aligned} \right\} \quad (6)$$

где

$$\Psi_t^{(1)} = \begin{pmatrix} \Psi_t^{(1,1)}(y_t^{(1)}) \\ \vdots \\ \Psi_t^{(q,1)}(y_t^{(q)}) \end{pmatrix}; \quad \tilde{\Psi}_t^{(2)} = \text{diag} \left\{ \Psi_t^{(1,2)}(\tilde{X}_{t-\tilde{\tau}_t^{(1)}}, y_t^{(1)}), \dots, \Psi_t^{(q,2)}(\tilde{X}_{t-\tilde{\tau}_t^{(q)}}, y_t^{(q)}) \right\}.$$

Этот фильтр представляет собой комбинацию обычных РФК, примененных к уравнениям состояния (2) и наблюдениям (5), с коррекцией каждого i -го наблюдателя на оценку $\tilde{\tau}_t^{(i)}$ своей временной задержки $\tau_t^{(i)}$. Традиционные для РФК эвристики сохраняют тот же смысл: $\tilde{K}_t$ — эвристическая ковариация ошибки прогноза; $\hat{K}_t$ — эвристическая ковариация ошибки оценки; $\Delta \tilde{Y}_t$ — вектор невязок измерений, аппроксимирующий обновляющий процесс. Такие интерпретации параметров фильтра (6) позволят в следующем разделе получить адаптивные оценки вторых моментов возмущений W_t и ошибок измерений $V_t^{(i)}$, следуя логике АФК.

3 Варианты адаптивных оценок вторых моментов в модели Калмана

Повторим в имеющихся обозначениях (2) и (3) основные положения классического АФК, т. е. начнем с задачи для линейной системы наблюдения:

$$\left. \begin{aligned} X_t &= \Phi_t^{(1)} X_{t-1} + \Phi_t^{(2)} W_t = \Phi_t^{(1)} X_{t-1} + \\ &\quad + Q^{1/2} W_t; \\ Y_t &= \Psi_t^{(1)} X_t + \Psi_t^{(2)} V_t = \Psi_t^{(1)} X_t + R^{1/2} V_t. \end{aligned} \right\} \quad (7)$$

Как и выше, здесь X_t — состояние; Y_t — наблюдения; теми же символами $\Phi_t^{(1)}$ и $\Psi_t^{(1)}$ обозначены матрицы системы и наблюдения. Отличие, связанное с адаптивной постановкой, — только в описании возмущений и ошибок измерений. Предполагается, что они заданы стандартными (центрированными и нормированными) гауссовскими белыми шумами W_t и V_t , так что возмущения в уравнениях динамики и ошибки измерения в уравнениях наблюдений имеют постоянные ковариации Q и R . Такие обозначения на данный момент можно считать стандартными для адаптивной калмановской фильтрации.

Если Q и R известны, то имеется фильтр Калмана [3]:

$$\left. \begin{aligned} \tilde{X}_t &= \Phi_t^{(1)} \hat{X}_{t-1}; \quad \tilde{K}_t = \Phi_t^{(1)} \hat{K}_{t-1} \left(\Phi_t^{(1)} \right)' + Q; \\ \hat{X}_t &= \tilde{X}_t + K_t \Delta \tilde{Y}_t; \quad \Delta \tilde{Y}_t = Y_t - \Psi_t^{(1)} \tilde{X}_t; \\ K_t &= \tilde{K}_t \left(\Psi_t^{(1)} \right)' \left(\Psi_t^{(1)} \tilde{K}_t \left(\Psi_t^{(1)} \right)' + R \right)^{-1}; \\ \hat{K}_t &= \tilde{K}_t - K_t \Psi_t^{(1)} \tilde{K}_t. \end{aligned} \right\} \quad (8)$$

Принципиальное свойство этого фильтра состоит в том, что вычисляемые алгоритмом фильтрации параметры фильтра имеют вполне определенный смысл:

$$\left. \begin{aligned} \tilde{K}_t &= \text{cov} \left(\Delta \tilde{X}_t, \Delta \tilde{X}_t \right), \quad \Delta \tilde{X}_t = X_t - \tilde{X}_t; \\ \hat{K}_t &= \text{cov} \left(\Delta \hat{X}_t, \Delta \hat{X}_t \right), \quad \Delta \hat{X}_t = X_t - \hat{X}_t; \\ \text{cov} \left(\Delta \tilde{Y}_t, \Delta \tilde{Y}_t \right) &= \Psi_t^{(1)} \tilde{K}_t \left(\Psi_t^{(1)} \right)' + R. \end{aligned} \right\} \quad (9)$$

Модель адаптивной фильтрации предполагает, что Q и R неизвестны. Цель адаптивного фильтра может формулироваться как получение оценок $\hat{Q}_t$ и $\hat{R}_t$, что предлагалось в оригинальных работах [5, 6], так и только оценивание коэффициента фильтра K_t , что предложено в [9]. При этом, конечно, нужны какие-то ограничения автономности, хотя бы постоянство $\Phi_t^{(1)}$ и $\Psi_t^{(1)}$. Идея адаптации предполагает использование фильтра (8), точнее его уравнений для решения целевой задачи фильтрации состояния X_t по наблюдениям Y_t . В эти уравнения надо подставить $\hat{Q}_t$ и $\hat{R}_t$. Обоснованием для построения этих оценок служат свойства параметров фильтра Калмана (9):

$$\left. \begin{aligned} \tilde{K}_t &= \Phi_t^{(1)} \hat{K}_{t-1} \left(\Phi_t^{(1)} \right)' + \hat{Q}_t = \\ &= \widehat{\text{cov}} \left(\Delta \tilde{X}_t, \Delta \tilde{X}_t \right); \\ \Psi_t^{(1)} \tilde{K}_t \left(\Psi_t^{(1)} \right)' + \hat{R}_t &= \widehat{\text{cov}} \left(\Delta \tilde{Y}_t, \Delta \tilde{Y}_t \right). \end{aligned} \right\} \quad (10)$$

Обратим внимание, что здесь уже нельзя писать ковариации, они заменены на оценки $\widehat{\text{cov}}$, поскольку точные соотношения ЛФК уже не выполняются из-за замены истинных ковариаций Q и R на оценки $\hat{Q}_t$ и $\hat{R}_t$. Оценивать ковариации в (10) как в схеме Сейджа–Хуса [5, 6], так и в схеме АФК [7, 8] предлагается простыми статистиками. Для $\widehat{\text{cov}}(\Delta \tilde{Y}_t, \Delta \tilde{Y}_t)$ невязок наблюдений — просто вычислять среднее по всем невязкам или по окну заданного размера. Вторую величину $\widehat{\text{cov}}(\Delta \tilde{X}_t, \Delta \tilde{X}_t)$ вычислить также нельзя, поскольку нельзя вычислить точно разность $\Delta \tilde{X}_t = X_t - \tilde{X}_t$. Но ее предлагается аппроксимировать как $\Delta \tilde{X}_t \approx \hat{X}_t - \tilde{X}_t$. В итоге можно записать вот такие варианты адаптивных оценок (с окном размера N):

$$\left. \begin{aligned} \hat{Q}_t &= \frac{1}{N} \sum_{s=t-N+1}^t \left(\hat{X}_s - \tilde{X}_s \right) \left(\hat{X}_s - \tilde{X}_s \right)' - \\ &\quad - \Phi_t^{(1)} \hat{K}_{t-1} \left(\Phi_t^{(1)} \right)'; \\ \hat{R}_t &= \frac{1}{N} \sum_{s=t-N+1}^t \Delta \tilde{Y}_s \left(\Delta \tilde{Y}_s \right)' - \Psi_t^{(1)} \tilde{K}_t \left(\Psi_t^{(1)} \right)'. \end{aligned} \right\} \quad (11)$$

Главные достоинства (11) — простота и сохранение калмановской, а значит, объяснимой структуры фильтра. Но эти достоинства нивелируются существенными недостатками, суть которых заключается в очень жестких условиях устойчивости, необходимых для корректной работы всей схемы. Но даже для хорошо обусловленных стационарных моделей гарантировать в (11) хотя бы неотрицательную определенность матриц $\hat{Q}_t$ и $\hat{R}_t$ нельзя. Уже это становится достаточным основанием для поиска усовершенствований (11). Наиболее успешным, как представляется, было решение, предложенное в [15, 16] почти одновременно. Но, повторим, в [16] оценивалось только значение R , а кроме того, обоснование финального выражения фактически отсутствует. В [15] все проделано корректно, но вывод целевых соотношений получился довольно громоздким из-за использования метода максимального правдоподобия. Это, конечно, вторичные замечания, потому что главное — это альтернативные оценкам (11) выражения, обладающие гораздо большей вычислительной стабильностью.

Начнем с альтернативной оценки $\hat{R}_t$. Она получена за счет идеи перейти от использования невязок $\Delta \tilde{Y}_t = Y_t - \Psi_t^{(1)} \tilde{X}_t$ к величинам $\Delta \hat{Y}_t = Y_t - \Psi_t^{(1)} \hat{X}_t$. Используемый в [15, 16] вариант их названия — инновации или обновления — представляется не слишком удачным, потому что приводит к противоречию с теорией оптимальной стохастической фильтрации на основе обновляющих процессов [28]. В частности, в условиях оптимальности ЛФК обычные невязки $\Delta \tilde{Y}_t$ являются обновляющим процессом. Более корректно называть $\Delta \tilde{Y}_t$ невязками по прогнозу, а $\Delta \hat{Y}_t$ — невязками по оценке, или апостериорными невязками. Использование $\Delta \hat{Y}_t$ дает соотношение (11), а аналогичное соотношение для $\Delta \tilde{Y}_t$ приводит к альтернативной оценке:

$$\hat{R}_t = \frac{1}{N} \sum_{s=t-N+1}^t \Delta \hat{Y}_s \left(\Delta \hat{Y}_s \right)' + \Psi_t^{(1)} \hat{K}_t \left(\Psi_t^{(1)} \right)'. \quad (12)$$

Главное достоинство (12) в сравнении с (11) — это «изменение» корректирующего статистическую оценку ковариации невязки (первое слагаемое) вычитания на сумму (второе слагаемое). Громоздкий вывод из [15] можно сделать проще. Короткий путь

состоит в непосредственном применении свойства гауссовского распределения к калмановской модели (7) и фильтру (8). Рассмотрим вектор $(\xi, \eta)'$:

$$\xi = R^{1/2}V_t = Y_t - \Psi_t^{(1)}X_t; \eta = Y_0^t = (Y_0', \dots, Y_t')'.$$

В калмановской модели эти векторы гауссовские. Условное математическое ожидание $E\{\xi|\eta\}$ даст невязку оценки. Соответственно, представляет интерес соотношение, связывающее ковариацию $E\{\xi|\eta\}$ и ковариацию возмущения R . Имеем

$$\text{cov}(\xi, \xi) = R;$$

$$E\{\xi|\eta\} = E\left\{Y_t - \Psi_t^{(1)}X_t | Y_0^t\right\} = Y_t - \Psi_t^{(1)}\hat{X}_t = \Delta\hat{Y}_t;$$

$$\begin{aligned} \text{cov}(\xi, \xi|\eta) &= \text{cov}\left(Y_t - \Psi_t^{(1)}X_t, Y_t - \Psi_t^{(1)}X_t | Y_0^t\right) = \\ &= \Psi_t^{(1)}\text{cov}(X_t, X_t | Y_0^t) \left(\Psi_t^{(1)}\right)' = \Psi_t^{(1)}\hat{K}_t \left(\Psi_t^{(1)}\right)'. \end{aligned}$$

Далее $\text{cov}(\xi, \eta)$ представим в виде (в статистике это соотношение часто приводят в скалярном виде и называют формулой полной дисперсии, или Law of Total Variance):

$$\begin{aligned} \text{cov}(\xi, \xi) &= E\{(\xi - E\{\xi|\eta\} + E\{\xi|\eta\} - E\{\xi\}) \times \\ &\times (\xi - E\{\xi|\eta\} + E\{\xi|\eta\} - E\{\xi\})'\} = \\ &= E\{(\xi - E\{\xi|\eta\})(\xi - E\{\xi|\eta\})'\} + \\ &+ E\{(E\{\xi|\eta\} - E\{\xi\})(E\{\xi|\eta\} - E\{\xi\})'\} = \\ &= \text{cov}(\xi, \xi|\eta) + \text{cov}(E\{\xi|\eta\}, E\{\xi|\eta\}), \end{aligned}$$

поскольку $\xi - E\{\xi|\eta\}$ и $E\{\xi|\eta\} - E\{\xi\}$ некоррелированы. Теперь, учитывая, что $E\{\xi\} = E\{\Delta\hat{Y}_t\} = 0$, окончательно получаем

$$\begin{aligned} R &= \text{cov}(\xi, \xi) = \\ &= \Psi_t^{(1)}\hat{K}_t \left(\Psi_t^{(1)}\right)' + E\left\{\Delta\hat{Y}_t\Delta\hat{Y}_t'\right\}. \end{aligned} \quad (13)$$

Формула (13) — это и есть то базовое соотношение, которое в [15] доказывается с помощью метода максимального правдоподобия, а в [16] записывается со ссылкой на оценку Гаусса—Маркова и ковариацию остатков в методе наименьших квадратов. Оценка $\hat{R}_t$ в (12) получается обычной заменой точного значения $E\{\Delta\hat{Y}_t, \Delta\hat{Y}_t'\}$ на статистическое среднее с окном длины N , вычисляемое, как и во всех адаптивных оценках, по накапливаемым результатам фильтрации.

Теперь перейдем к альтернативной оценке $\hat{Q}_t$. Она также имеется в [15] и получается из того же базового соотношения ЛФК (8):

$$Q = \tilde{K}_t - \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)'.$$

Его можно уточнить следующим образом:

$$\begin{aligned} Q &= \text{cov}\left(\Delta\tilde{X}_t, \Delta\tilde{X}_t\right) - \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)' = \\ &= \text{cov}\left(X_t - \hat{X}_t + \hat{X}_t - \tilde{X}_t, X_t - \hat{X}_t + \hat{X}_t - \tilde{X}_t\right) - \\ &- \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)' = \text{cov}\left(X_t - \hat{X}_t, X_t - \hat{X}_t\right) + \\ &+ \text{cov}\left(\hat{X}_t - \tilde{X}_t, \hat{X}_t - \tilde{X}_t\right) - \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)' = \\ &= \text{cov}\left(\hat{X}_t - \tilde{X}_t, \hat{X}_t - \tilde{X}_t\right) + \hat{K}_t - \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)', \end{aligned}$$

потому что в калмановской модели $X_t - \hat{X}_t$ и $\hat{X}_t - \tilde{X}_t$ некоррелированы. В итоге получаем адаптивную оценку $\hat{Q}_t$ вида

$$\begin{aligned} \hat{Q}_t &= \frac{1}{N} \sum_{s=t-N+1}^t \left(\hat{X}_s - \tilde{X}_s\right) \left(\hat{X}_s - \tilde{X}_s\right)' + \\ &+ \hat{K}_t - \Phi_t^{(1)}\hat{K}_{t-1} \left(\Phi_t^{(1)}\right)'. \end{aligned} \quad (14)$$

Этот вариант гораздо интереснее, чем (11), в потенциале численной устойчивости, хотя все еще оставляет возможности для нарушения условия неотрицательности $\hat{Q}_t$. Этот недостаток будет учтен при формировании оценки уже для целевой модели (2), (3) и фильтра (6).

4 Адаптивные оценки вторых моментов в модели с временными задержками

Из имеющихся нескольких принципиальных схем оценивания параметров Q и R шумов в калмановской модели (7) предпочтительными выглядят оценка $\hat{Q}_t$ (14) и $\hat{R}_t$ (12). Возьмем их за основу для решения задачи адаптивной фильтрации для (2), (3). Вначале надо сформулировать саму задачу, внеся изменения в модель, соответствующие смыслу адаптивного оценивания ковариаций шумов. Для этого уточним (2), (3):

$$\left. \begin{aligned} X_t &= \Phi_t^{(1)}(X_{t-1}) + Q^{1/2}W_t; \\ y_t^{(1)} &= \psi_t^{(i,1)}\left(X_{t-\tau_t^{(i)}}\right) + R^{1/2}v_t^{(i)}; \\ Y_t^{(i)} &= \Psi_t^{(i,1)}\left(y_t^{(i)}\right)X_{t-\tilde{\tau}_t^{(i)}} + \\ &+ \Psi_t^{(i,1)}\left(X_{t-\tilde{\tau}_t^{(i)}}, y_t^{(i)}\right)V_t^{(i)}, \\ i &= \overline{1, q}, t = -T, -T+1, \dots, 0, 1, \dots, \\ X_{-\min_{i=\overline{1, q}} \tau_t^{(i)}-1} &= \eta. \end{aligned} \right\} \quad (15)$$

С одной стороны, модель (15) устроена ровно в той же логике, что и калмановская модель (7)

в смысле адаптивного оценивания ковариаций шумов. Поэтому и в фильтр (6) надо внести ровно те же уточнения:

- (1) поскольку шумы W_t и $v_t^{(i)}$ теперь стандартные, то $m_W(t) = 0$, $m_{v_t^{(i)}}(t) = 0$ и $D_W(t) = \text{diag}\{1, \dots, 1\}$;
- (2) поскольку $\Phi_t^{(2)}(X_{t-1}) = Q^{1/2}$, то надо заменить $\tilde{\Phi}_t^{(2)} D_W(t) (\tilde{\Phi}_t^{(2)})'$ на $\hat{Q}_{t-1}$;
- (3) из равенства $\psi_t^{(i,2)}(X_{t-\tau_t^{(i)}}) = R^{1/2}$ с учетом псевдонаблюдений вытекает необходимость заменить $\tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})'$ на $\hat{R}_{t-1}$.

Здесь важно обратить внимание на то, что равенство $\psi_t^{(i,2)}(X_{t-\tau_t^{(i)}}) = R^{1/2}$ в модели (15) означает, что все q наблюдателей одинаковы, т.е. имеют одинаковые точностные характеристики. И это используется далее для улучшения оценки (12), так как все наблюдения могут задействоваться наравне для оценивания R . Но второй важный момент состоит в том, что одинаковая ковариация R для «истинных» ошибок измерений $v_t^{(i)}$ не означает, что постоянна и ковариация у шумов в псевдонаблюдениях (3), слагаемое $\Psi_t^{(i,2)}(X_{t-\tilde{\tau}_t^{(i)}}) V_t^{(i)}$ заменить нельзя. Понять это можно, посмотрев на форму псевдонаблюдений (5).

Но есть другое полезное свойство, обеспечиваемое равенством $R = \text{diag}\{\sigma_\varphi^2, \sigma_\lambda^2, \sigma_r^2\}$. Такой вид R , напомним, получается из конкретной модели одного наблюдателя — три независимых канала измерения пеленга, угла возвышения и дальности. Для $D_V(t)$ в фильтре (6) это дает

$$D_V(t) = D_V = \text{diag}\{\sigma_\varphi^2, \sigma_\varphi^2, \sigma_\lambda^2, \sigma_\lambda^2, \sigma_r^2, \dots, \sigma_\varphi^2, \sigma_\varphi^2, \sigma_\lambda^2, \sigma_\lambda^2, \sigma_r^2\}, \quad (16)$$

т.е. диагональную матрицу размерности $5q \times 5q$ с повторяющимися диагональными блоками $\text{diag}\{\sigma_\varphi^2, \sigma_\varphi^2, \sigma_\lambda^2, \sigma_\lambda^2, \sigma_r^2\}$.

Подчеркнем нюанс, возникший в обозначениях в связи с особенностями модели с несколькими наблюдателями и применением псевдонаблюдений. Как и в калмановской модели, переменная R обозначает неизвестную ковариацию шумов. Но, во-первых, в модели (7) нет нескольких наблюдателей, поэтому R в модель (15) входит иначе — через $\text{diag}\{R, \dots, R\}$. Во-вторых, в модель с псевдонаблюдениями R входит только как параметр в определение ковариации $\tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})'$ псевдонаблюдений, используемое в фильтре (6). Важно помнить, что при этом оценка $\hat{R}_t$ относится именно к $\tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})'$, и перейти от нее к оценке R (если

это потребуется) можно только поэтапно: $\hat{R}_t$ оценивает $\tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})'$, отсюда можно попытаться получить оценку D_V , привести эту оценку к блочно-диагональной структуре, из которой получить оценки для σ_φ^2 , σ_λ^2 и σ_r^2 , а из них уже получается оценка R . Для улучшения $\hat{R}_t$ ниже будет пройдена именно эта цепочка.

Выше было сказано, что состояние — это декартовы координаты: $X_t = (X(t), Y(t), Z(t))'$. Поскольку часто при описании движения используются простые модели, в которых возмущения по разным координатам также предполагаются независимыми, то и для Q как частный случай будем рассматривать вариант $Q = \text{diag}\{\sigma_X^2, \sigma_Y^2, \sigma_Z^2\}$. Это позволит так же, как $\hat{R}_t$, улучшить оценку $\hat{Q}_t$.

Адаптировать имеющиеся оценки АФК для модели (15) с запаздывающими временными наблюдениями довольно просто. Первый шаг — это сдвиг на величину максимальной по текущим данным задержки $\tilde{\tau}_t = \max_{i=1,q} \tilde{\tau}_t^{(i)}$, второй — использование тех параметров фильтра (прогнозов, невязок, оценок и эвристических ковариаций), которые отвечают сдвинутому на $\tilde{\tau}_t$ времени. Применительно к оценке (12) сказанное дает:

$$\hat{R}_t = \frac{1}{N} \sum_{s=t-\tilde{\tau}_t-N+1}^{t-\tilde{\tau}_t} \Delta \hat{Y}_s (\Delta \hat{Y}_s)' + \Psi_t^{(1)} \hat{K}_{t-\tilde{\tau}_t} (\Psi_t^{(1)})', \quad (17)$$

а применительно к оценке (14):

$$\hat{Q}_t = \frac{1}{N} \sum_{s=t-\tilde{\tau}_t-N+1}^{t-\tilde{\tau}_t} (\hat{X}_s - \tilde{X}_s) (\hat{X}_s - \tilde{X}_s)' + \hat{K}_{t-\tilde{\tau}_t} - \tilde{\Phi}_{t-\tilde{\tau}_t}^{(1)} \hat{K}_{t-\tilde{\tau}_t-1} (\tilde{\Phi}_{t-\tilde{\tau}_t}^{(1)})'. \quad (18)$$

Наконец, можно говорить об улучшении оценок (17) и (18) за счет учета модели с задержками и метода линейных псевдонаблюдений.

Вычислив $\hat{R}_t$ согласно (17), получим оценку $\tilde{\Psi}_t^{(2)} D_V(t) (\tilde{\Psi}_t^{(2)})'$. Матрица $\tilde{\Psi}_t^{(2)}$ имеет блочно-диагональную структуру, составлена из значений $\Psi_t^{(i,2)}(\tilde{X}_{t-\tilde{\tau}_t^{(i)}}) V_t^{(i)}$ согласно (6) и, таким образом, известна точно. Ее размерность $3q \times 5q$. Матрица $D_V(t) = D_V$ из (16) имеет размерность $5q \times 5q$. Если определить оценку $\hat{D}_V(t)$ как решение уравнения $\hat{R}_t = \tilde{\Psi}_t^{(2)} \hat{D}_V(t) (\tilde{\Psi}_t^{(2)})'$, то таких решений будет бесконечное число. Вместо этого оценку $\hat{D}_V(t)$ предлагается определить как

$$\left. \begin{aligned} \hat{D}_V(t) &= \text{diag} \left\{ \hat{\sigma}_\varphi^2, \hat{\sigma}_\varphi^2, \hat{\sigma}_\lambda^2, \hat{\sigma}_\lambda^2, \hat{\sigma}_r^2, \dots \right. \\ &\quad \left. \dots, \hat{\sigma}_\varphi^2, \hat{\sigma}_\varphi^2, \hat{\sigma}_\lambda^2, \hat{\sigma}_\lambda^2, \hat{\sigma}_r^2 \right\}, \\ (\hat{\sigma}_\varphi^2, \hat{\sigma}_\varphi^2, \hat{\sigma}_r^2) &= \\ &= \arg \min \left\| \hat{R}_t - \tilde{\Psi}_t^{(2)} \hat{D}_V(t) \left(\tilde{\Psi}_t^{(2)} \right)' \right\|, \\ \hat{\sigma}_\varphi^2 \geq 0, \hat{\sigma}_\lambda^2 \geq 0, \hat{\sigma}_r^2 \geq 0, \end{aligned} \right\} \quad (19)$$

где $\|x\|$ — обычная матричная норма Фробениуса, а у оценок $\hat{\sigma}_\varphi^2$, $\hat{\sigma}_\varphi^2$ и $\hat{\sigma}_r^2$ опущена зависимость от t : $\hat{\sigma}_\varphi^2 = \hat{\sigma}_\varphi^2(t)$, $\hat{\sigma}_\lambda^2 = \hat{\sigma}_\lambda^2(t)$, $\hat{\sigma}_r^2 = \hat{\sigma}_r^2(t)$. Поскольку матрица $\hat{R}_t$ по определению (17) неотрицательно определенная, то точное решение (19) обеспечит неотрицательность оценок $\hat{\sigma}_\varphi^2$, $\hat{\sigma}_\varphi^2$ и $\hat{\sigma}_r^2$. Но при реализации решать задачу (19) придется численно, что может нарушить это условие и привести к неустойчивости адаптивного фильтра в целом, поэтому оптимизация в (19) дополнена условиями $\hat{\sigma}_\varphi^2 \geq 0$, $\hat{\sigma}_\lambda^2 \geq 0$ и $\hat{\sigma}_r^2 \geq 0$.

Таким образом, получаем задачу положительных наименьших квадратов, для практической реализации подойдет любой универсальный метод нелинейного программирования, например метод активного множества [29] (именно он использован в численных экспериментах). Соответственно, улучшенная оценка $\hat{R}_t$ получается в виде

$$\hat{R}_t^* = \tilde{\Psi}_t^{(2)} \hat{D}_V(t) \left(\tilde{\Psi}_t^{(2)} \right)'.$$

Аналогично получается улучшение для оценки $\hat{Q}_t$ из (18). Во-первых, сама оценка (18) нуждается в уточнении, поскольку даже ее усовершенствованная по сравнению с исходной схемой Сейджа—Хуса форма не гарантирует этой оценке неотрицательную определенность, а нарушение этого условия для ковариации может привести к неустойчивости всего адаптивного фильтра в целом. Поскольку $\hat{Q}_t$ согласно определению (18) симметричная, то ее можно представить в виде разложения на собственные векторы и собственные значения $\hat{Q}_t = P \Lambda P'$, заменить в диагональной матрице $\Lambda = \text{diag} \{ \lambda_1, \lambda_2, \lambda_3 \}$ отрицательные значения нулями:

$$\Lambda_+ = \text{diag} \{ \max(\lambda_1, 0), \max(\lambda_2, 0), \max(\lambda_3, 0) \}$$

и окончательно считать оценку $\hat{Q}_t = P \Lambda_+ P'$. Подчеркнем, что это необходимо проделывать с оценкой (18) в любом случае, так что можно считать ее значение гарантированно неотрицательно определенной матрицей.

Далее вернемся к сделанному предположению $Q = \text{diag} \{ \sigma_X^2, \sigma_Y^2, \sigma_Z^2 \}$. Поскольку «исправленная» оценка (18) не гарантирует, что $\hat{Q}_t = \text{diag} \{ \hat{\sigma}_X^2, \hat{\sigma}_Y^2, \hat{\sigma}_Z^2 \}$, улучшенную оценку $\hat{Q}_t^*$ предлагается искать как решение задачи

$$\begin{aligned} \hat{Q}_t^* &= \text{diag} \{ \hat{\sigma}_X^2, \hat{\sigma}_Y^2, \hat{\sigma}_Z^2 \}, \\ (\hat{\sigma}_X^2, \hat{\sigma}_Y^2, \hat{\sigma}_Z^2) &= \arg \min \left\| \hat{Q}_t - \text{diag} \{ \sigma_X^2, \sigma_Y^2, \sigma_Z^2 \} \right\|, \\ \hat{\sigma}_X^2 \geq 0, \hat{\sigma}_Y^2 \geq 0, \hat{\sigma}_Z^2 \geq 0. \end{aligned}$$

Это такая же задача положительных наименьших квадратов, как сформулированная для $\hat{R}_t^*$ задача (19), но для ее решения привлекать специализированную оптимизацию не требуется, так как здесь нет таких сложностей со структурой. Здесь можно сразу получить улучшенную оценку ковариации $\hat{Q}_t^* = \text{diag} \{ \hat{Q}_t \}$, т. е. просто как диагональ исправленной оценки (18).

Последним вопросом для всех вариантов предложенных адаптивных оценок остается выбор начальных условий. Как в (17), так и в (18) первый расчет возможен лишь в момент $t = N$, т. е. только после накопления оценок и параметров фильтра (6) в количестве, равном выбранному размеру N окна адаптации. До этого момента должны использоваться заранее заданные значения $\hat{Q}_t = Q_0$ и $\hat{R}_t = R_0$, $t < N$. Во многих случаях выбор Q_0 и R_0 не является принципиально сложной задачей. Достаточно задать грубые, но физически разумные верхние оценки соответствующих дисперсий. Например, если известно, что скорость течения не может превышать 100 км/ч, а ошибка измерения дальности не может превышать 500 м, эти ограничения можно использовать для задания начальных ковариационных матриц. Такой выбор может быть достаточно консервативным, но на начальном участке работы фильтра это предпочтительнее, чем использование заведомо заниженных ковариаций, способных привести к чрезмерному доверию к модели или измерениям. В следующем разделе в численном эксперименте будем следовать этому положению, увеличивая истинные начальные значения среднеквадратичных отклонений в 5 раз.

Между тем этот вопрос дает и вариант альтернативной АФК оценки. Если выбранные верхние границы Q_0 и R_0 использовать не только на начальном этапе, но и для всех t и не заниматься, тем самым, адаптивным оцениванием, то реализованная таким образом оценка будет соответствовать робастному фильтру Калмана [30]. Здесь речь о свойстве ЛФК быть минимаксной оценкой в модели (7) в предположении, что ковариации Q и R не просто неизвестны, но имеют верхние ограничения $Q \leq Q_0$ и $R \leq R_0$. Робастный фильтр Калмана при этом может иметь гораздо более гибкие условия применения, так как никаких условий стационарности, в отличие от АФК, не требует. С другой стороны, достоверные сведения о Q_0 и R_0 могут отсутствовать. В модельных экспериментах такого вопроса нет, поэтому оценку фильтра (6) с заменой Q и R на Q_0 и R_0 вычисляли и сравнивали с оценками

АФК, имея в виду именно ее предполагаемые робастные свойства. Но определение «робастный» применительно к РФК следует ставить в кавычки, поскольку, в отличие от ЛФК, гарантированной минимаксности РФК не имеет, как не имеет никаких других гарантированных статистических свойств.

5 Численный эксперимент

В [23–25] использовалась модель движения с постоянной средней скоростью и двумя типовыми наблюдателями для анализа работы фильтра (6). В соответствии с адаптивной постановкой дополнительно будем предполагать, что вторые моменты возмущений неизвестны. Перечислим основные положения модели. Подводный аппарат обнаруживается в момент $t = 0$ с начальным условием $X_{-t_0-1} = \eta = (\eta_X, \eta_Y, \eta_Z)'$, вектор η состоит из независимых элементов, распределенных равномерно: $\eta_X \sim R[10, 20]$, $\eta_Y \sim R[10, 20]$ и $\eta_Z \sim R[0, 5; 1, 5]$. Два наблюдателя $\mathcal{M}^{(1)}$ и $\mathcal{M}^{(2)}$ расположены на поверхности воды и имеют координаты $(0, -1, 0)$ и $(-2, 0, 0)$, единица измерения — км. Подводный аппарат движется с известной постоянной средней скоростью $s = (s_X, s_Y, s_Z)'$ км/ч, фактическую скорость $S(t) = (S_X, S_Y, S_Z)'$ формируют аддитивные случайные возмущения $W_t = (w_X(t), w_Y(t), w_Z(t))'$. Дискретное время t задается равномерным шагом $\delta = 0,0001$ ч, примерно три такта в секунду. Уравнения движения принимают вид:

$$\begin{aligned} X(t) &= X(t-1) + \delta S_X(t), \quad S_X(t) = s_X + \sigma_{S_X} w_X(t); \\ Y(t) &= Y(t-1) + \delta S_Y(t), \quad S_Y(t) = s_Y + \sigma_{S_Y} w_Y(t); \\ Z(t) &= Z(t-1) + \delta S_Z(t), \quad S_Z(t) = s_Z + \sigma_{S_Z} w_Z(t), \end{aligned}$$

где $w_X(t)$, $w_Y(t)$ и $w_Z(t)$ — независимые стандартные гауссовские белые шумы. Постоянная средняя скорость s моделируется вектором из независимых элементов: $s_X \sim R[-20, -10]$; $s_Y \sim R[-20, -10]$; $s_Z \sim R[-2, 0]$. Отсюда следует, что

$$E\{S(t)\} = E\{s\} = (-15, -15, -1)' = -E\{\eta\},$$

т. е. в среднем ПА движется в сторону начала координат (предполагаемой цели движения). Интенсивности возмущений σ_{S_X} , σ_{S_Y} и σ_{S_Z} составляют диагональ матрицы $Q^{1/2}$ и подлежат адаптивному оцениванию. Их истинные значения сохранены как в [23–25]: $\sigma_{S_X} = 15$; $\sigma_{S_Y} = 15$; $\sigma_{S_Z} = 1$. Верхняя граница и вариант начального условия для $\hat{Q}_t$ и $\hat{Q}_t^*$ выбраны как $Q_0^{1/2} = 5Q^{1/2} = \text{diag}\{\sigma_{S_X}, \sigma_{S_Y}, \sigma_{S_Z}\}$. Для сравнения выполнены расчеты адаптивных фильтров с точным начальным условием $Q^{1/2}$ и фильтра (6) с известной Q .

Наблюдатели $\mathcal{M}^{(1)}$ и $\mathcal{M}^{(2)}$ — одинаковые и типовые, измеряют величины $y_{\varphi_t}^{(i)}$, $y_{\lambda_t}^{(i)}$ и $y_{r_t}^{(i)}$, $i = 1, 2$ (пеленги, углы возвышения и дальности относительно своего положения). Неизвестные ковариации ошибок измерений R задаются отклонениями $\sigma_\varphi = \sigma_\varphi^{(1)} = \sigma_\varphi^{(2)}$, $\sigma_\lambda = \sigma_\lambda^{(1)} = \sigma_\lambda^{(2)}$ и $\sigma_r = \sigma_r^{(1)} = \sigma_r^{(2)}$, так что адаптивному оцениванию подлежат σ_φ , σ_λ и σ_r . Их реальные значения сохранены как в [23–25]: $\sigma_\varphi = \sigma_\lambda = \pi/180$ рад, $\sigma_r = 0,1$ км. Верхняя граница и вариант начального условия для $\hat{R}_t$ и $\hat{R}_t^*$ выбраны как $R_0^{1/2} = 5R^{1/2}$. Для сравнения выполнены расчеты адаптивных фильтров с точным начальным условием $R^{1/2}$ и фильтра (6) с известной R .

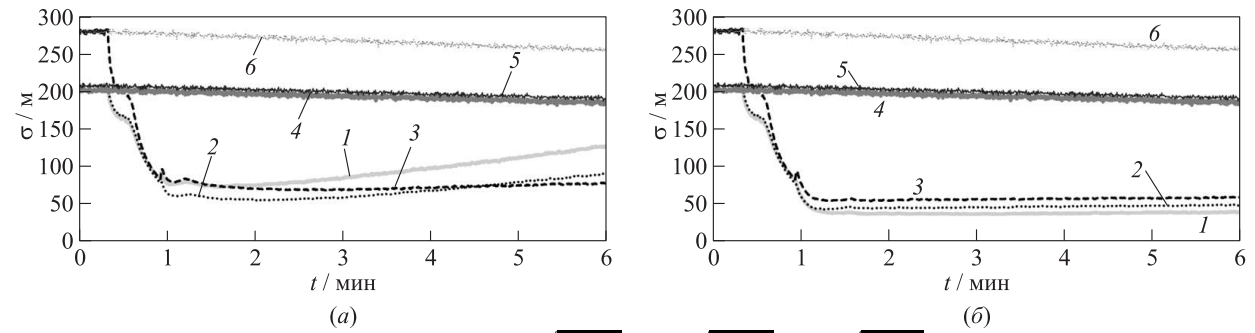
Моделирование выполнялось для моментов $t = 0, \dots, 1000$, т. е. в течение 0,1 ч = 6 мин. Определенная в [23–25] максимальная задержка $T = 56$ составляет около 20 с. До момента $t = 56$ в качестве начального значения фильтра (6) использовалась простая геометрическая оценка положения $\hat{X}_t$ (фильтр прямых измерений): каждая тройка измерений $y_{\varphi_t}^{(i)}$, $y_{\lambda_t}^{(i)}$, $y_{r_t}^{(i)}$ (два угла и расстояние) может быть непосредственно пересчитана в декартовы координаты, учет временной задержки дает слагаемое $s\tau_t^{(i)}$, две геометрические оценки взвешиваются с одинаковыми весами. Точность такого простого фильтра следует рассматривать как верхнюю границу в том смысле, что фильтр, дающий оценку худшего качества, следует считать непригодным (нестабильным). Ясно, что этот фильтр не зависит от адаптивной постановки, на его качество не влияют предположения о возмущениях Q и R , поэтому значения точности для $\hat{X}_t$ — такие же, как в [23–25].

Все расчеты выполнены на одном и том же пучке 10 000 траекторий движения-наблюдения. Дополнительно для сравнения выполнены эксперименты с моделью, предполагающей $T = 0$. Основная цель расчетов — сравнить оценки фильтров, использующих схемы адаптации $\hat{Q}_t$, $\hat{R}_t$ и $\hat{Q}_t^*$, $\hat{R}_t^*$, а также «робастный» фильтр (6) с оценками Q_0 и R_0 .

Точность фильтрации характеризуют стандартные отклонения, например для j -й траектории смоделированного пучка $X_j(t)$ и соответствующих оценок $\hat{X}_j(t)$, $j = \overline{1, 10\,000}$, для координаты $X(t)$ вычислялись функции

$$D_{\hat{X}}(t) = \frac{1}{10\,000} \sum_{j=1}^{10\,000} \left(X_j(t) - \hat{X}_j(t) \right)^2,$$

для иллюстраций — $\sqrt{D_{\hat{X}}(t)}$, $\sqrt{D_{\hat{Y}}(t)}$, $\dots$, $\sqrt{D_{\hat{Z}}(t)}$ и интегрированные показатели



Средние отклонения ошибок оценок АФК (1 – $\sqrt{D_{\hat{x}}(t)}$; 2 – $\sqrt{D_{\hat{y}}(t)}$; 3 – $\sqrt{D_{\hat{z}}(t)}$) и фильтра прямых измерений (4 – $\sqrt{D_{\bar{x}}(t)}$; 5 – $\sqrt{D_{\bar{y}}(t)}$; 6 – $\sqrt{D_{\bar{z}}(t)}$). Схемы адаптации: (а) $\hat{Q}_t, \hat{R}_t$; (б) $\hat{Q}_t^*, \hat{R}_t^*$

Точность фильтрации

Фильтры	$T = 0$			$T = 56$		
	$\hat{\Sigma}_{\hat{x}}/\hat{\sigma}_{\hat{x}}$	$\hat{\Sigma}_{\hat{y}}/\hat{\sigma}_{\hat{y}}$	$\hat{\Sigma}_{\hat{z}}/\hat{\sigma}_{\hat{z}}$	$\hat{\Sigma}_{\hat{x}}/\hat{\sigma}_{\hat{x}}$	$\hat{\Sigma}_{\hat{y}}/\hat{\sigma}_{\hat{y}}$	$\hat{\Sigma}_{\hat{z}}/\hat{\sigma}_{\hat{z}}$
$\hat{Q}_t, \hat{R}_t, Q_0 = Q, R_0 = R$	73,8/116,4	50,3/78,5	52,4/61,9	90,9/120,1	70,5/84,0	85,2/76,6
$\hat{Q}_t, \hat{R}_t, Q_0 = 5Q, R_0 = 5R$	91,7/124,6	66,6/86,0	69,6/68,3	103,8/123,1	81,8/87,0	93,1/76,9
$\hat{Q}_t^*, \hat{R}_t^*, Q_0 = Q, R_0 = R$	27,0/26,9	28,7/28,4	32,0/25,5	56,0/44,7	63,1/54,0	84,3/68,6
$\hat{Q}_t^*, \hat{R}_t^*, Q_0 = 5Q, R_0 = 5R$	36,9/28,9	41,3/33,4	47,6/35,5	57,6/39,3	64,9/48,9	80,1/59,0
«Робастный» РФК $Q_0 = 5Q, R_0 = 5R$	33,5/19,9	30,4/19,3	33,9/16,0	52,2/23,2	49,6/22,8	57,2/18,2
«Точный» РФК $Q_0 = Q, R_0 = R$	23,0/20,0	22,1/19,6	24,7/16,4	38,4/22,4	37,5/21,8	43,5/15,4

$$\hat{\Sigma} = \frac{1}{1000} \sum_{t=1}^{1000} \sqrt{D_{\hat{x}}(t)}; \hat{\sigma}_{\hat{x}} = \frac{1}{100} \sum_{t=901}^{1000} \sqrt{D_{\hat{x}}(t)},$$

т.е. отклонения, усредненные по всему времени и по последним 100 шагам фильтрации. Таким образом, для каждого эксперимента определены величины $\hat{\sigma}_{\hat{x}}, \hat{\sigma}_{\hat{y}}, \dots, \hat{\sigma}_{\hat{z}}, \hat{\Sigma}_{\hat{x}}, \hat{\Sigma}_{\hat{y}}, \dots, \hat{\Sigma}_{\hat{z}}$.

Качественную картину эффективности адаптивных схем и фильтра дают иллюстрации на рисунке. Рассчитанные количественные значения собраны в таблицу.

Поскольку результаты для фильтра прямых измерений не зависят от условий адаптации, укажем их для возможности сравнения с данными, включенными в таблицу:

– $T = 0$:

$$\begin{aligned} \hat{\Sigma}_{\bar{x}} &= 192,5; \hat{\sigma}_{\bar{x}} = 186,5; \\ \hat{\Sigma}_{\bar{y}} &= 198,6; \hat{\sigma}_{\bar{y}} = 192,5; \\ \hat{\Sigma}_{\bar{z}} &= 267,1; \hat{\sigma}_{\bar{z}} = 257,8; \end{aligned}$$

– $T = 56$:

$$\begin{aligned} \hat{\Sigma}_{\bar{x}} &= 193,6; \hat{\sigma}_{\bar{x}} = 187,3; \\ \hat{\Sigma}_{\bar{y}} &= 199,4; \hat{\sigma}_{\bar{y}} = 193,4; \\ \hat{\Sigma}_{\bar{z}} &= 268,2; \hat{\sigma}_{\bar{z}} = 258,8. \end{aligned}$$

Здесь нужно пояснить, что маленькая разница между моделями с временной задержкой ($T = 56$)

и без нее ($T = 0$) объясняется наличием точной информации о значении постоянной средней скорости s , что дает очень точный прогноз, так как хаотические изменения скорости $Q^{1/2}W_t$ независимы и суммируются, теряя влияние. Тот же эффект действует и в РФК (6), так как в нем используется такое же прогнозирование, но большее влияние оказывает сама процедура фильтрации, объединяющая в рамках одной структуры РФК измерения и оценки с разными временными задержками. Эта разница не столь велика, но видна и обнаружила себя во всех ранних экспериментах [23–25].

6 Заключение

В качестве заключения уместно сформулировать некоторые выводы по результатам, полученным в эксперименте. Основной вывод состоит в том, что предложенные схемы адаптации показали свою работоспособность. Использованная модель достаточно сложна, ее нельзя считать простым академическим примером, она существенно нелинейна, что делает применение метода АФК в комбинации с РФК очень проблематичным. Кроме того, имеется определенная экстремальность: слишком хаотическое движение, довольно большие скорости и удаленность. Но как и РФК по методу линейных псевдонаблюдений, так и предложенная в статье

версия, дополненная методом АФК, оказались работоспособными. Формально нужно констатировать общее превосходство схемы $\hat{Q}_t^*$, $\hat{R}_t^*$, т.е. предложенные в статье решения учитывать диагональную структуру оцениваемых параметров сработали.

Вместе с тем есть основания для сдержанного отношения к результату. Обратим внимание на три характерных фрагмента в графиках точности АФК: (1) начальный этап, когда не выполняется адаптация и используются геометрические оценки; (2) используется РФК с начальной оценкой Q_0 и R_0 при накоплении измерений для окна адаптации N ; (3) собственно работа АФК–РФК. Здесь видны проблемы алгоритма РФК в целом: хотя оба варианта адаптации работают и дают реальное улучшение в сравнении с единственно доступным вариантом фильтра прямых измерений, в обоих вариантах видна неприятная тенденция роста погрешности оценивания по всем координатам с течением времени. Эта тенденция противоречит физическому содержанию задачи, так как ПА приближается к наблюдателям, пропадает эффект временной задержки, фактически точнее становятся измерения. Эти тенденции видны у фильтра прямых измерений, но отсутствуют у РФК. Значит, ошибка накапливается самим фильтром, а хорошо известно, что для РФК такая ситуация типична [27]. В рассмотренном примере эти недостатки РФК существенного влияния не оказали, поскольку за время фильтрации ПА успевает достаточно близко приблизиться к цели. Однако повод для продолжения поиска способов совершенствования схем адаптации представляется вполне ясным.

Наконец, нельзя не отметить превосходство «робастного» фильтра: просто подставив вместо адаптивной оценки ковариации достаточно большое значение, удалось получить результат даже лучший, чем любые адаптации. Здесь тоже нужно быть осторожным с оценкой результата, так как на практике, а не в рассмотренном модельном примере, информации о том, какое именно значение служит верхней границей ковариаций, может не оказаться. Но в целом поведение «робастного» варианта РФК заслуживает внимания и тоже может рассматриваться как повод для улучшения способов адаптации.

Литература

1. Фомин В. Н. Рекуррентное оценивание и адаптивная фильтрация. — М.: Наука, 1984. 286 с.
2. Haykin S. Adaptive filter theory. — 5th ed. — Boston, MA, USA: Pearson, 2014. 889 p.

3. Kalman R. E. A new approach to linear filtering and prediction problems // J. Basic Eng. — T. ASME, 1960. Vol. 82. No. 1. P. 35–45. doi: 10.1115/1.3662552.
4. Bernstein I., Friedland B. Estimation of the state of a nonlinear process in the presence of nongaussian noise and disturbances // J. Frankl. Inst., 1966. Vol. 281. No. 6. P. 455–480. doi: 10.1016/0016-0032(66)90434-0.
5. Sage A. P., Husa G. W. Adaptive filtering with unknown prior statistics // Joint Automatic Control Conference Proceedings. — American Automatic Control Council, 1969. P. 760–769. doi: 10.1109/JACC. 1969.4169325.
6. Sage A. P., Husa G. W. Algorithms for sequential adaptive estimation of prior statistics // 8th Symposium on Adaptive Processes Decision and Control Proceedings. — IEEE, 1969. P. 61–61. doi: 10.1109/SAP.1969.269927.
7. Mehra R. On the identification of variances and adaptive Kalman filtering // IEEE T. Automat. Contr., 1970. Vol. 15. No. 2. P. 175–184. doi: 10.1109/TAC. 1970.1099422.
8. Mehra R. Approaches to adaptive filtering // IEEE T. Automat. Contr., 1972. Vol. 17. No. 5. P. 693–698. doi: 10.1109/TAC.1972.1100100.
9. Carew B., Belanger P. Identification of optimum filter steady-state gain for systems with unknown noise covariances // IEEE T. Automat. Contr., 1973. Vol. 18. No. 6. P. 582–587. doi: 10.1109/TAC.1973.1100420.
10. Yang Y., Xu T. An adaptive Kalman filter based on sage windowing weights and variance components // J. Navigation, 2003. Vol. 56. No. 2. P. 231–240. doi: 10.1017/S0373463303002248.
11. Hu C., Chen W., Chen Y., Liu D. Adaptive Kalman filtering for vehicle navigation // J. Global Positioning Systems, 2003. Vol. 2. No. 1. P. 42–47. doi: 10.5081/JGPS.2.1.42.
12. Odelson B. J., Rajamani M. R., Rawlings J. B. A new autocovariance least-squares method for estimating noise covariances // Automatica, 2006. Vol. 42. No. 2. P. 303–308. doi: 10.1016/j.automatica.2005.09.006.
13. Yang Y., Gao W. An optimal adaptive Kalman filter // J. Geodesy, 2006. Vol. 80. P. 177–183. doi: 10.1007/s00190-006-0041-0.
14. Åkesson B. M., Jørgensen J. B., Poulsen N. K., Jørgensen S. B. A generalized autocovariance least-squares method for Kalman filter tuning // J. Process Contr., 2008. Vol. 18. No. 7–8. P. 769–779. doi: 10.1016/j.jprocont.2007.11.003.
15. Mohamed A., Schwarz K. Adaptive Kalman filtering for INS/GPS // J. Geodesy, 1999. Vol. 73. P. 193–203. doi: 10.1007/s001900050236.
16. Wang J. Stochastic modeling for real-time kinematic GPS/GLONASS positioning // Navigation — U.S., 1999. Vol. 46. P. 297–305. doi: 10.1002/j.2161-4296.1999.tb02416.x.
17. Yang Y., He H., Xu G. Adaptively robust filtering for kinematic geodetic positioning // J. Geodesy, 2001. Vol. 75. No. 2–3. P. 109–116. doi: 10.1007/s001900000157.
18. Bavdekar V. A., Deshpande A. P., Patwardhan S. C. Identification of process and measurement noise covariance for state and parameter estimation using extended Kalman

- filter // J. Process Contr., 2011. Vol. 21. No. 4. P. 585–601. doi: 10.1016/j.jprocont.2011.01.001.
19. Sun F., Hu X., Zou Y., Li S. Adaptive unscented Kalman filtering for state of charge estimation of a lithium-ion battery for electric vehicles // Energy, 2011. Vol. 36. No. 5. P. 3531–3540. doi: 10.1016/j.energy.2011.03.059.
20. Blanchet I., Frankignoul C., Cane M.A. A comparison of adaptive Kalman filters for a tropical Pacific Ocean model // Mon. Weather Rev., 1997. Vol. 125. No. 1. P. 40–58. doi: 10.1175/1520-0493(1997)125<0040:ACOAKF>2.0.CO;2.
21. Moradi M. H., Rad M. A., Khezerloo R. B. ECG signal enhancement using adaptive Kalman filter and signal averaging // Int. J. Cardiol., 2014. Vol. 173. Iss. 3. P. 553–555. doi: 10.1016/j.ijcard.2014.03.128.
22. Босов А. В. Оптимальная фильтрация состояния нелинейной динамической системы по наблюдениям со случайными запаздываниями // Информатика и её применения, 2023. Т. 17. Вып. 3. С. 8–17. doi: 10.14357/19922264230302. EDN: CFVYJM.
23. Bosov A. Tracking a maneuvering object by indirect observations with random delays // Drones, 2023. Vol. 7. No. 7. Art. 468. 17 p. doi: 10.3390/drones7070468.
24. Bosov A. Maneuvering object tracking and movement parameters identification by indirect observations with random delays // Axioms, 2024. Vol. 13. No. 10. Art. 668. 17 p. doi: 10.3390/axioms13100668.
25. Босов А. В. Позиционирование и идентификация параметров движения подводного аппарата по наблюдениям со случайными запаздываниями // Автоматика и телемеханика, 2024. № 12. С. 23–48. doi: 10.31857/S0005231024120026. EDN: XUMKVA.
26. Босов А. В., Урюпин И. В. Модифицированный вариант расширенного фильтра Калмана по методу линейных псевдонаблюдений // Информатика и её применения, 2025. Т. 19. Вып. 2. С. 17–26. doi: 10.14357/19922264250203. EDN: ZOVFSQ.
27. Босов А. В., Урюпин И. В. Практическое исследование вопроса неустойчивости расширенного фильтра Калмана // Информатика и её применения, 2025. Т. 19. Вып. 4. С. 12–25. doi: 10.14357/19922264250402. EDN: BMTYSW.
28. Липцер Р. Ш., Ширяев А. Н. Статистика случайных процессов (нелинейная фильтрация и смежные вопросы). — М.: Наука, 1974. 696 с.
29. Lawson C. L., Hanson R. J. Solving least squares problems. — Classics in applied mathematics ser. — Philadelphia, PA, USA: SIAM, 1995. Vol. 15. 337 p.
30. Morris J. The Kalman filter: A robust estimator for some classes of linear quadratic problems // IEEE T. Inform. Theory, 1976. Vol. 22. No. 5. P. 526–534. doi: 10.1109/TIT.1976.1055611.

Поступила в редакцию 04.05.2026

Принята к публикации 15.08.2026

STABLE ALGORITHMS FOR ADAPTIVE STATE ESTIMATION OF DYNAMIC SYSTEMS UNDER RANDOM TIME DELAYS OF OBSERVATIONS

A. V. Bosov, S. A. Bosov, and I. V. Uryupin

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: New computationally stable algorithms are proposed for adaptive filtering of the state of an object moving in an aquatic environment, based on acoustic observations with random time delays. A previously developed version of the extended Kalman filter, adapted to the time-delay model and built upon the method of linear pseudoobservations, is supplemented with two adaptive filter modifications for the case of unknown covariances of dynamic disturbances and measurement errors. To estimate the covariances, stable adaptive Kalman filter schemes are used, derived from the analysis of measurement residuals with respect to the filtering estimates. These schemes are improved by additional optimization in order to account for the positive diagonal structures of the unknown covariances assumed by the motion model and generated by the linear pseudoobservations. A large-scale numerical experiment was carried out, confirming the operability of the proposed adaptation schemes. The calculations employed the same model as in previous works, which made it possible to separately assess the influence of the adaptive formulation and to outline possible directions for further development of the methodology.

Keywords: stochastic filtering; stochastic system with random observation delays; extended Kalman filter (EKF); EKF based on the method of linear pseudoobservations; adaptive Kalman filter (AKF)

DOI: 10.14357/19922264260303

EDN: HVLJCG

Acknowledgments

The research was supported by a grant from the Russian Science Foundation No.25-21-00550, <https://rscf.ru/project/25-21-00550/>. The research was carried out using the infrastructure of the Shared Research Facilities “High Performance Computing and Big Data” (CKP “Informatics”) of FRC CSC RAS (Moscow).

References

- Fomin, V. N. 1984. *Rekurrentnoe otsenivanie i adaptivnaya fil'tratsiya* [Recursive estimation and adaptive filtering]. Moscow: Nauka. 286 p.
- Haykin, S. 2014. *Adaptive filter theory*. 5th ed. Boston, MA: Pearson. 889 p.
- Kalman, R. E. 1960. A new approach to linear filtering and prediction problems. *J. Basic Eng. — T. ASME* 82(1):35–45. doi: 10.1115/1.3662552.
- Bernstein, I., and B. Friedland. 1966. Estimation of the state of a nonlinear process in the presence of nongaussian noise and disturbances. *J. Frankl. Inst.* 281(6):455–480. doi: 10.1016/0016-0032(66)90434-0.
- Sage, A. P., and G. W. Husa. 1969. Adaptive filtering with unknown prior statistics. *Joint Automatic Control Conference Proceedings*. American Automatic Control Council. 760–769. doi: 10.1109/JACC.1969.4169325.
- Sage, A. P., and G. W. Husa. 1969. Algorithms for sequential adaptive estimation of prior statistics. *8th Symposium on Adaptive Processes Decision and Control Proceedings*. IEEE. 61–61. doi: 10.1109/SAP.1969.269927.
- Mehra, R. 1970. On the identification of variances and adaptive Kalman filtering. *IEEE T. Automat. Contr.* 15(2):175–184. doi: 10.1109/TAC.1970.1099422.
- Mehra, R. 1972. Approaches to adaptive filtering. *IEEE T. Automat. Contr.* 17(5):693–698. doi: 10.1109/TAC.1972.1100100.
- Carew, B., and P. Belanger. 1973. Identification of optimum filter steady-state gain for systems with unknown noise covariances. *IEEE T. Automat. Contr.* 18(6):582–587. doi: 10.1109/TAC.1973.1100420.
- Yang, Y., and T. Xu. 2003. An adaptive Kalman filter based on sage windowing weights and variance components. *J. Navigation* 56(2):231–240. doi: 10.1017/S0373463303002248.
- Hu, C., W. Chen, Y. Chen, and D. Liu. 2003. Adaptive Kalman filtering for vehicle navigation. *J. Global Positioning Systems* 2(1):42–47. doi: 10.5081/JGPS.2.1.42.
- Odelson, B. J., M. R. Rajamani, and J. B. Rawlings. 2006. A new autocovariance least-squares method for estimating noise covariances. *Automatica* 42(2):303–308. doi: 10.1016/j.automatica.2005.09.006.
- Yang, Y., and W. Gao. 2006. An optimal adaptive Kalman filter. *J. Geodesy* 80(4):177–183. doi: 10.1007/s00190-006-0041-0.
- Åkesson, B. M., J. B. Jørgensen, N. K. Poulsen, and S. B. Jørgensen. 2008. A generalized autocovariance least-squares method for Kalman filter tuning. *J. Process Contr.* 18(7-8):769–779. doi: 10.1016/j.jprocont.2007.11.003.
- Mohamed, A. H., and K. P. Schwarz. 1999. Adaptive Kalman filtering for INS/GPS. *J. Geodesy* 73(4):193–203. doi: 10.1007/s001900050236.
- Wang, J. 1999. Stochastic modeling for real-time kinematic GPS/GLONASS positioning. *Navigation — U.S.* 46(4):297–305. doi: 10.1002/j.2161-4296.1999.tb02416.x.
- Yang, Y., H. He, and G. Xu. 2001. Adaptively robust filtering for kinematic geodetic positioning. *J. Geodesy* 75(2-3):109–116. doi: 10.1007/s001900000157.
- Bavdekar, V. A., A. P. Deshpande, and S. C. Patwardhan. 2011. Identification of process and measurement noise covariance for state and parameter estimation using extended Kalman filter. *J. Process Contr.* 21(4):585–601. doi: 10.1016/j.jprocont.2011.01.001.
- Sun, F., X. Hu, Y. Zou, and S. Li. 2011. Adaptive unscented Kalman filtering for state of charge estimation of a lithium-ion battery for electric vehicles. *Energy* 36(5):3531–3540. doi: 10.1016/j.energy.2011.03.059.
- Blanchet, I., C. Frankignoul, and M. A. Cane. 1997. A comparison of adaptive Kalman filters for a tropical Pacific Ocean model. *Mon. Weather Rev.* 125(1):40–58. doi: 10.1175/1520-0493(1997)125<0040:ACOKF>2.0.CO;2.
- Moradi, M. H., M. A. Rad, and R. B. Khezerloo. 2014. ECG signal enhancement using adaptive Kalman filter and signal averaging. *Int. J. Cardiol.* 173(3):553–555. doi: 10.1016/j.ijcard.2014.03.128.
- Bosov, A. V. 2023. Optimal'naya fil'tratsiya sostoyaniya nelineynoy dinamicheskoy sistemy po nablyudeniyam so sluchaynymi zapazdyvaniyami [Nonlinear dynamic system state optimal filtering by observations with random delays]. *Informatika i ee Primeneniya — Inform. Appl.* 17(3):8–17. doi: 10.14357/19922264230302. EDN: CFVYJM.
- Bosov, A. 2023. Tracking a maneuvering object by indirect observations with random delays. *Drones* 7(7):468. 17 p. doi: 10.3390/drones7070468.
- Bosov, A. 2024. Maneuvering object tracking and movement parameters identification by indirect observations with random delays. *Axioms* 13(10):668. 17 p. doi: 10.3390/axioms13100668. EDN: AYLLFE.
- Bosov, A. V. 2024. AUV positioning and motion parameter identification based on observations with random delays. *Automat. Rem. Contr.* 85(12):1024–1040. doi: 10.1134/S0005117924700413. EDN: PLPFMZ.
- Bosov, A. V., and I. V. Uryupin. 2025. Modifitsirovanny variant rasshirennogo fil'tra Kalmana po metodu lineynykh psevdonablyudeniy [A modified extended

- Kalman filter by the linear pseudomeasurement method]. *Informatika i ee Primeneniya — Inform. Appl.* 19(2):17–26. doi: 10.14357/19922264250203. EDN: ZOVFSQ.
27. Bosov, A. V., and I. V. Uryupin. 2025. Prakticheskoe issledovanie voprosa nestabil'nosti rasshirennogo fil'tra Kalmana [A practical study of the extended Kalman filter instability]. *Informatika i ee Primeneniya — Inform. Appl.* 19(4):12–25. doi: 10.14357/19922264250402. EDN: BMTYSW.
28. Liptser, R. S., and A. N. Shiryaev. 1977. *Statistics of random processes: I. General theory*. Berlin–Heidelberg: Springer-Verlag. 394 p.
29. Lawson, C. L., and R. J. Hanson. 1995. *Solving least squares problems*. Classics in applied mathematics ser. Philadelphia, PA: SIAM. Vol. 15. 337 p.
30. Morris, J. 1976. The Kalman filter: A robust estimator for some classes of linear quadratic problems. *IEEE T. Inform. Theory* 22(5):526–534. doi: 10.1109/TIT.1976.1055611.

Received May 4, 2026

Accepted August 15, 2026

Contributors

Bosov Alexey V. (b. 1969) — Doctor of Science in technology, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; ABosov@frccsc.ru

Bosov Svjatoslav A. (b. 1992) — engineer, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; sabosov@frccsc.ru

Uryupin Ilya V. (b. 1993) — Candidate of Science (PhD) in physics and mathematics, junior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; uryupin93@yandex.ru

АСИМПТОТИЧЕСКИЙ АНАЛИЗ МЕТОДОВ Пороговой ОБРАБОТКИ В РАЗРЕЖЕННЫХ МОДЕЛЯХ С ПУАССОНОВСКИМ ЧИСЛОМ НАБЛЮДЕНИЙ*

Е. И. Мележников¹, О. В. Шестаков²

Аннотация: Рассматривается задача пороговой обработки разреженного сигнала при наблюдениях, формируемых пуассоновским процессом с заданной интенсивностью. В отличие от классической постановки с фиксированным объемом выборки, число наблюдений случайно и определяется траекторией процесса. Исследуется поведение среднеквадратичного риска и его оценки, построенной по правилу SURE (Stein's unbiased risk estimate). Особое внимание уделяется влиянию случайности объема выборки на точность восстановления сигнала и свойства оценок риска. Получена верхняя оценка риска при оптимальном выборе порога и показано, что его асимптотический порядок совпадает с детерминированным случаем. Кроме того, доказаны центральная предельная теорема и усиленный закон больших чисел для SURE-оценки риска. Тем самым установлена устойчивость асимптотических свойств пороговых процедур при переходе к модели, задаваемой пуассоновским процессом. Полученные результаты применимы в задачах анализа потоковых данных, где наблюдения поступают в случайные моменты времени и объем выборки не фиксирован заранее. Это расширяет область применения пороговых методов в статистических моделях со случайным числом наблюдений.

Ключевые слова: пороговая обработка; среднеквадратичный риск; оценка риска; разреженная модель; пуассоновский процесс; центральная предельная теорема; усиленный закон больших чисел

DOI: 10.14357/19922264260304

EDN: UJQIXC

1 Введение

Пороговые методы — один из базовых инструментов восстановления разреженного сигнала на фоне гауссовского шума. Их эффективность объясняется тем, что удачно выбранный порог позволяет одновременно подавлять шумовые компоненты и сохранять редкие значимые сигналы. По этой причине асимптотический анализ риска пороговых процедур занимает важное место в задачах вейвлет-сжатия, статистического обнаружения редких эффектов и смежных разделах математической статистики [1–3].

В модели с фиксированным числом наблюдений исследовано асимптотическое поведение среднеквадратичного риска и его оценки при различных видах пороговой обработки [1, 2, 4–12]. Например, в работе [12] для разреженной модели исследована асимптотика теоретического риска и доказаны центральная предельная теорема и усиленный закон больших чисел для оценки риска, построенной по методу Стейна (SURE) [13]. Однако во многих

прикладных задачах объем данных случаен. Такая ситуация возникает, например, в астрономии при анализе космического излучения, в задачах сетевого мониторинга, при обработке потоков сообщений или пакетов, а также в других моделях, где наблюдения поступают в случайные моменты времени.

В статье рассматривается разреженная модель с аддитивным гауссовским шумом, в которой число наблюдений за время t задается пуассоновским процессом $\{N_\lambda(t), t \geq 0\}$ с интенсивностью $\lambda > 0$. В качестве асимптотического параметра используется величина $x = \lambda t$, равная среднему числу наблюдений за интервал времени $[0, t]$. Для этой модели изучается поведение минимального риска, доказываются центральная предельная теорема и усиленный закон больших чисел для SURE-оценки риска.

Основной результат первой части работы состоит в том, что рандомизация числа наблюдений не меняет главного порядка роста риска: для порога, минимизирующего математическое ожидание риска, сохраняется оценка порядка $x^{1-\gamma} \ln x$, совпада-

*Статья подготовлена при финансовой поддержке Московского центра фундаментальной и прикладной математики (грант Минобрнауки России № 075-15-2025-345).

¹Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики; Московский центр фундаментальной и прикладной математики, melezhnen@gmail.com

²Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики; Федеральный исследовательский центр «Информатика и управление» Российской академии наук; Московский центр фундаментальной и прикладной математики, oshestakov@cs.msu.ru

ющая по порядку с детерминированным случаем. Далее для SURE-оценки риска в модели, где число наблюдений задается пуассоновским процессом, устанавливается центральная предельная теорема. Кроме того, доказывается усиленный закон больших чисел при $x = \lambda t \rightarrow \infty$. Тем самым показано, что основные асимптотические свойства пороговых процедур, известные для модели с фиксированным объемом выборки, сохраняются и в существенно более общей постановке, когда объем выборки случаен и управляется пуассоновским процессом.

Статья имеет следующую структуру. В разд. 2 формулируется постановка задачи, описывается модель и вводятся основные обозначения. В разд. 3 получена верхняя оценка теоретического риска при оптимальном пороге. Раздел 4 посвящен двум предельным результатам: центральной предельной теореме для SURE-оценки риска и усиленному закону больших чисел для этой оценки. В заключении обсуждаются полученные результаты и возможные направления дальнейших исследований.

2 Постановка задачи и обозначения

Рассматривается задача восстановления разреженного сигнала в условиях, когда число наблюдений за фиксированный промежуток времени случайно. Такая ситуация естественно возникает в задачах, где данные формируются как поток событий: за интервал времени регистрируется случайное число измерений, каждое из которых содержит шумовую и, возможно, сигнальную компоненту.

Данная постановка представляет собой естественное обобщение модели с фиксированным числом наблюдений, исследованной в работе [12], на случай, когда объем выборки носит случайный характер.

В качестве модели числа наблюдений используется пуассоновский процесс $\{N_\lambda(t), t \geq 0\}$ с интенсивностью $\lambda > 0$. Таким образом, за время t регистрируется случайное число наблюдений $N_\lambda(t)$. В качестве асимптотического параметра рассматривается среднее число наблюдений $x = \lambda t$. Наблюдения имеют вид:

$$X_i = \mu_i + \varepsilon_i, \quad i = \overline{1, N_\lambda(t)},$$

где $\varepsilon_i \sim \mathcal{N}(0, \sigma^2)$ — независимые гауссовские случайные величины.

Структура сигнала задается в соответствии с разреженной моделью, рассмотренной в работе [12]:

$$\mu_i = a_i z_i,$$

где $a_i \in \mathbb{R}$ — детерминированные амплитуды сигнальных компонент; $z_i \sim \text{Be}(p_x)$ — независимые индикаторы, принимающие значение 1 с вероятностью p_x и 0 иначе. Случайные величины z_i моделируют наличие редких информативных компонент сигнала. Также подразумевается, что z_i независимы от ε_i .

Таким образом, наблюдаемый вектор представляет собой зашумленную разреженную структуру, в которой значимые компоненты возникают редко и не имеют фиксированного расположения.

Величина

$$N_0 = \sum_{i=1}^{N_\lambda(t)} z_i$$

задает число ненулевых компонент сигнала.

Разреженность модели задается условием

$$xp_x = o(x^{1-\gamma}), \quad 0 < \gamma < 1, \quad x \rightarrow \infty. \quad (1)$$

Это означает, что среднее число ненулевых компонент растет медленнее $x^{1-\gamma}$.

Для краткости при $x \geq 1$ будем использовать обозначения

$$N_x \sim \text{Pois}(x), \quad \pi_{x,k} := \mathbb{P}(N_x = k) = e^{-x} \frac{x^k}{k!}, \quad k = 0, 1, 2, \dots$$

Такие обозначения используются для распределения значения пуассоновского процесса $N_\lambda(t)$ при среднем числе наблюдений $x = \lambda t$.

Для заданного порога $T > 0$ рассматривается общий класс пороговых функций. Пусть функция $h(u, T)$ удовлетворяет следующим условиям:

$$\begin{aligned} h(-u, T) &= -h(u, T), \quad 0 \leq h(u, T) \leq T; \\ u &\geq 0; \\ h(T, T) &= T. \end{aligned}$$

Первое условие означает нечетность функции по переменной u , второе задает ее ограниченность, а третье обеспечивает непрерывность соответствующей пороговой функции в точке $u = T$.

Пороговая функция имеет вид:

$$p(T, u) = \begin{cases} u - h(u, T), & |u| > T; \\ 0, & |u| \leq T. \end{cases}$$

Соответствующая оценка сигнальной компоненты имеет вид:

$$\hat{\mu}_i(T) = p(T, X_i).$$

Таким образом, внутри пороговой области наблюдение обнуляется, а вне ее подвергается корректровке, определяемой функцией h . Кроме того,

далее предполагается, что функция $h(u, T)$ дифференцируема по переменной u вне, возможно, конечного числа точек и для некоторой константы $C > 0$ выполнено

$$\left| \frac{\partial h}{\partial u}(u, T) \right| \leq CT^2.$$

В качестве примера приведем мягкую пороговую обработку:

$$p(T, u) = \begin{cases} u - T, & u > T; \\ u + T, & u < -T; \\ 0, & |u| \leq T. \end{cases}$$

Если число наблюдений фиксировано и равно k , то теоретический риск определяется формулой:

$$R_k(T) = \sum_{i=1}^k \mathbb{E} (\hat{\mu}_i(T) - \mu_i)^2.$$

Классический выбор порога в модели с фиксированным числом наблюдений — универсальный порог

$$T_u(k) = \sigma \sqrt{2 \ln k},$$

который обеспечивает подавление шумовых компонент с высокой вероятностью (см., например, [1, 14]) и среди «разумных» порогов имеет максимальное значение. В модели со случайным числом наблюдений естественно использовать его аналог, в котором число наблюдений заменяется его средним значением:

$$T_u(x) = \sigma \sqrt{2 \ln x}, \quad x \geq 1.$$

Обозначим через

$$T_{k,\min} = \arg \min_{0 < T \leq T_u(k)} R_k(T)$$

теоретически оптимальный порог в модели с фиксированным числом наблюдений k .

Кроме того, для каждого k будем рассматривать несмещенную оценку риска, построенную по методу Стейна (SURE) [13]:

$$\hat{R}_k(T) = \sum_{i=1}^k F_i(T),$$

где

$$F_i(T) = \begin{cases} X_i^2 - \sigma^2, & |X_i| \leq T; \\ h^2(X_i, T) + \sigma^2 - 2\sigma^2 \frac{\partial h}{\partial u}(X_i, T), & |X_i| > T. \end{cases}$$

Соответствующий адаптивный порог определяется как

$$T_{k,S} = \arg \min_{0 < T \leq T_u(k)} \hat{R}_k(T).$$

В модели со случайным числом наблюдений риск определяется как математическое ожидание квадратичной ошибки:

$$R_x(T) := \mathbb{E} \sum_{i=1}^{N_x} (\hat{\mu}_i(T) - \mu_i)^2.$$

Соответственно, оптимальный порог в модели со случайным числом наблюдений определяется как

$$T_{x,\min} = \arg \min_{0 < T \leq T_u(x)} R_x(T),$$

а соответствующий адаптивный порог — как

$$T_{N_x,S} = \arg \min_{0 < T \leq T_u(x)} \hat{R}_{N_x}(T).$$

Ниже исследуются асимптотические свойства величин $R_x(T_{x,\min})$ и $\hat{R}_{N_x}(T_{N_x,S})$ для пуассоновского процесса $\{N_\lambda(t), t \geq 0\}$ при $x = \lambda t \rightarrow \infty$.

Замечание 1. Одной и той же буквой (c , C и т. п.) будут обозначаться некоторые положительные константы c , возможно, разными значениями.

3 Верхняя оценка риска при случайном числе наблюдений

Теорема 1. Пусть выполнено условие разреженности (1). Тогда существует константа $C > 0$ такая, что

$$R_x(T_{x,\min}) \leq Cx^{1-\gamma} \ln x, \quad x \rightarrow \infty. \quad (2)$$

Доказательство.

$$R_x(T_{x,\min}) = \sum_{k=0}^{\infty} \pi_{x,k} \mathbb{E} \left(\|\hat{\mu}(T_{x,\min}) - \mu\|^2 \mid N_x = k \right). \quad (3)$$

Зафиксируем числа c_1 и c_2 так, что

$$0 < c_1 < 3 - e; \quad c_2 > e - 1.$$

Разобьем сумму (3) на три части:

$$R_x(T_{x,\min}) \leq S_1 + S_2 + S_3,$$

где

$$\begin{aligned} S_1 &= \sum_{k=0}^{\lfloor c_1 x \rfloor} \pi_{x,k} \mathbb{E} \left(\|\hat{\mu}(T_{x,\min}) - \mu\|^2 \mid N_x = k \right); \\ S_2 &= \sum_{k=\lfloor c_1 x \rfloor + 1}^{\lfloor c_2 x \rfloor} \pi_{x,k} \mathbb{E} \left(\|\hat{\mu}(T_{x,\min}) - \mu\|^2 \mid N_x = k \right); \\ S_3 &= \sum_{k=\lfloor c_2 x \rfloor + 1}^{\infty} \pi_{x,k} \mathbb{E} \left(\|\hat{\mu}(T_{x,\min}) - \mu\|^2 \mid N_x = k \right). \end{aligned}$$

Оценка суммы S_3 .

Как и в [12], для любого порога $T \leq T_u(x)$ выполняется оценка

$$R_k(T) \leq CkT_u^2(x).$$

Поэтому получаем

$$R_k(T_{x,\min}) \leq CkT_u^2(x).$$

Следовательно,

$$\begin{aligned} S_3 &\leq \\ &\leq CT_u^2(x) \sum_{k=\lfloor c_2 x \rfloor + 1}^{\infty} k\pi_{x,k} = CT_u^2(x) \sum_{k=\lfloor c_2 x \rfloor + 1}^{\infty} k \frac{e^{-x} x^k}{k!} = \\ &= Cx T_u^2(x) \sum_{k=\lfloor c_2 x \rfloor + 1}^{\infty} \frac{e^{-x} x^{k-1}}{(k-1)!} = Cx T_u^2(x) \sum_{k=\lfloor c_2 x \rfloor}^{\infty} \pi_{x,k} = \\ &= CT_u^2(x) x \mathbb{P}(\xi_x \geq c_2 x), \quad (4) \end{aligned}$$

где $\xi_x \sim \text{Pois}(x)$.

Для оценки вероятности применим неравенство Маркова с функцией $g(t) = e^t$:

$$\mathbb{P}(\xi_x \geq c_2 x) = \mathbb{P}(e^{\xi_x} \geq e^{c_2 x}) \leq \frac{\mathbb{E}e^{\xi_x}}{e^{c_2 x}}.$$

Но

$$\begin{aligned} \mathbb{E}e^{\xi_x} &= \sum_{k=0}^{\infty} e^k e^{-x} \frac{x^k}{k!} = e^{-x} \sum_{k=0}^{\infty} \frac{(ex)^k}{k!} = \\ &= e^{-x} e^{ex} = e^{x(e-1)}. \end{aligned}$$

Поэтому

$$\mathbb{P}(\xi_x \geq c_2 x) \leq e^{x(e-1-c_2)}. \quad (5)$$

Так как $c_2 > e - 1$, правая часть экспоненциально стремится к нулю; $T_u^2(x) = 2\sigma^2 \ln x$. Поэтому из (4) получаем

$$S_3 \leq Cx \ln x e^{-cx} \xrightarrow{x \rightarrow \infty} 0. \quad (6)$$

Оценка суммы S_1 .

Аналогично,

$$S_1 \leq CT_u^2(x) \sum_{k=0}^{\lfloor c_1 x \rfloor} k\pi_{x,k} \leq CT_u^2(x) x \mathbb{P}(\xi_x \leq c_1 x).$$

Оценим вероятность. Имеем

$$\mathbb{P}(\xi_x \leq c_1 x) = \mathbb{P}(x - \xi_x \geq (1 - c_1)x) \leq \frac{\mathbb{E}e^{x - \xi_x}}{e^{(1-c_1)x}}.$$

Осталось вычислить $\mathbb{E}e^{x - \xi_x}$. Разобьем сумму на две части:

$$\begin{aligned} \mathbb{E}e^{x - \xi_x} &= \sum_{k=0}^{\lfloor x \rfloor} e^{x-k} e^{-x} \frac{x^k}{k!} + \sum_{k=\lfloor x \rfloor + 1}^{\infty} e^{k-x} e^{-x} \frac{x^k}{k!} = \\ &= \sum_{k=0}^{\lfloor x \rfloor} \frac{(x/e)^k}{k!} + e^{-2x} \sum_{k=\lfloor x \rfloor + 1}^{\infty} \frac{(xe)^k}{k!}. \end{aligned}$$

Первую сумму оценим сверху:

$$\sum_{k=0}^{\lfloor x \rfloor} \frac{(x/e)^k}{k!} \leq \sum_{k=0}^{\infty} \frac{(x/e)^k}{k!} = e^{x/e}.$$

Для второй суммы имеем

$$\begin{aligned} e^{-2x} \sum_{k=\lfloor x \rfloor + 1}^{\infty} \frac{(xe)^k}{k!} &\leq e^{-2x} \sum_{k=0}^{\infty} \frac{(xe)^k}{k!} = \\ &= e^{-2x} e^{xe} = e^{x(e-2)}. \end{aligned}$$

Так как $e - 2 > 1/e$, получаем

$$\mathbb{E}e^{x - \xi_x} \leq C e^{x(e-2)}$$

с некоторой константой $C > 0$. Следовательно,

$$\mathbb{P}(\xi_x \leq c_1 x) \leq C e^{x(e-3+c_1)}. \quad (7)$$

Поскольку $c_1 < 3 - e$, правая часть экспоненциально убывает, и потому

$$S_1 \leq Cx \ln x e^{-cx} \xrightarrow{x \rightarrow \infty} 0. \quad (8)$$

Оценка суммы S_2 .

Для k из промежутка $[c_1 x, c_2 x]$ условная квадратичная ошибка имеет тот же порядок, что и в модели с неслучайным числом наблюдений. Действительно, из результатов [12] следует, что оптимальный порог в детерминированной модели удовлетворяет соотношению

$$T_{k,\min} = \sigma \sqrt{2\gamma \ln k + O(1)}, \quad k \rightarrow \infty.$$

Если $c_1 x \leq k \leq c_2 x$, то

$$\ln k = \ln x + O(1).$$

Следовательно,

$$T_{k,\min} = \sigma \sqrt{2\gamma \ln k + O(1)} = \sigma \sqrt{2\gamma \ln x + O(1)}$$

и, в частности, порог имеет порядок $\sqrt{\ln x}$.

Доказательство оценки риска в [12, теорема 1] использует только порядок k , степень разреженности и тот факт, что порог имеет порядок $\sqrt{\ln k}$.

Поэтому те же самые выкладки, проведенные при $c_1x \leq k \leq c_2x$, дают равномерно по $k \in [c_1x, c_2x]$ оценку

$$\mathbb{E} \left(\|\hat{\mu}(T_{x,\min}) - \mu\|^2 \mid N_x = k \right) \leq Cx^{1-\gamma} \ln x.$$

Отсюда

$$S_2 \leq Cx^{1-\gamma} \ln x \sum_{k=\lfloor c_1x \rfloor + 1}^{\lfloor c_2x \rfloor} \pi_{x,k} \leq Cx^{1-\gamma} \ln x. \quad (9)$$

Теперь из (6), (8) и (9) следует, что

$$R_x(T_{x,\min}) \leq Cx^{1-\gamma} \ln x.$$

Теорема доказана.

4 Центральная предельная теорема и усиленный закон больших чисел для оценки риска

В данном разделе устанавливаются асимптотические свойства оценки риска в модели, где число наблюдений задается пуассоновским процессом. В частности, для этой оценки доказывается центральная предельная теорема, а также усиленный закон больших чисел.

Теорема 2. Пусть выполнено условие (1) и $1/2 < \gamma < 1$. Тогда

$$\frac{\hat{R}_{N_x}(T_{N_x,S}) - R_x(T_{x,\min})}{\sigma^2 \sqrt{2x}} \Rightarrow \mathcal{N}(0, 1), \quad x \rightarrow \infty. \quad (10)$$

Доказательство. Обозначим через $h_x(t)$ характеристическую функцию случайной величины $(\hat{R}_{N_x}(T_{N_x,S}) - R_x(T_{x,\min})) / (\sigma^2 \sqrt{2x})$. Тогда по формуле полной вероятности

$$\begin{aligned} h_x(t) &= \sum_{k=0}^{\infty} \pi_{x,k} \mathbb{E} \left[\exp \left\{ \frac{it}{\sigma^2 \sqrt{2x}} \left(\hat{R}_k(T_{k,S}) - R_x(T_{x,\min}) \right) \right\} \right] = \\ &= \sum_{k=0}^{\infty} \pi_{x,k} \exp \left\{ \frac{it}{\sigma^2 \sqrt{2x}} (R_k(T_{k,\min}) - R_x(T_{x,\min})) \right\} \varphi_k \left(t \sqrt{\frac{k}{x}} \right), \quad (11) \end{aligned}$$

где φ_k — характеристическая функция случайной величины $(\hat{R}_k(T_{k,S}) - R_k(T_{k,\min})) / (\sigma^2 \sqrt{2k})$.

Пусть $\varphi(t) = e^{-t^2/2}$ — характеристическая функция стандартного нормального закона. Положим

$$g_x(t) = \sum_{k=0}^{\infty} \pi_{x,k} \exp \left\{ \frac{it}{\sigma^2 \sqrt{2x}} (R_k(T_{k,\min}) - R_x(T_{x,\min})) \right\} \varphi \left(t \sqrt{\frac{k}{x}} \right). \quad (12)$$

Покажем сначала, что

$$|h_x(t) - g_x(t)| \rightarrow 0 \quad \text{при каждом фиксированном } t \in \mathbb{R}. \quad (13)$$

Из (11) и (12) следует

$$|h_x(t) - g_x(t)| \leq \sum_{k=0}^{\infty} \pi_{x,k} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right|.$$

Разобьем эту сумму так же, как в теореме 1:

$$|h_x(t) - g_x(t)| \leq A_1(x, t) + A_2(x, t) + A_3(x, t),$$

где

$$\begin{aligned} A_1(x, t) &= \sum_{k=0}^{\lfloor c_1x \rfloor} \pi_{x,k} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right|; \\ A_2(x, t) &= \sum_{k=\lfloor c_1x \rfloor + 1}^{\lfloor c_2x \rfloor} \pi_{x,k} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right|; \\ A_3(x, t) &= \sum_{k=\lfloor c_2x \rfloor + 1}^{\infty} \pi_{x,k} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right|. \end{aligned}$$

Так как $|\varphi_k(s)| \leq 1$ и $|\varphi(s)| \leq 1$, то

$$A_1(x, t) \leq 2\mathbb{P}(N_x \leq c_1x), \quad A_3(x, t) \leq 2\mathbb{P}(N_x \geq c_2x).$$

Используя уже полученные оценки (5) и (7), получаем, что обе вероятности стремятся к нулю экспоненциально.

Для $A_2(x, t)$ замечаем, что при $c_1x \leq k \leq c_2x$ аргумент $t\sqrt{k/x}$ лежит в фиксированном отрезке. Из доказательства центральной предельной теоремы для случая с фиксированным числом наблюдений в [12] следует, что характеристические функции φ_k сходятся к φ равномерно на любом отрезке. Поэтому

$$\sup_{c_1x \leq k \leq c_2x} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right| \rightarrow 0.$$

Следовательно,

$$A_2(x, t) \leq \sup_{c_1 x \leq k \leq c_2 x} \left| \varphi_k \left(t \sqrt{\frac{k}{x}} \right) - \varphi \left(t \sqrt{\frac{k}{x}} \right) \right| \times \\ \times \sum_{k=\lfloor c_1 x \rfloor + 1}^{\lfloor c_2 x \rfloor} \pi_{x,k} \rightarrow 0.$$

Тем самым (13) доказано.

Теперь перепишем $g_x(t)$ в более удобном виде. Положим

$$U_x = \frac{N_x}{x}, \quad V_x = \frac{R_{N_x}(T_{N_x, \min}) - R_x(T_{x, \min})}{\sigma^2 \sqrt{2x}}.$$

Тогда из (12) имеем

$$g_x(t) = \mathbb{E} \left[\varphi \left(t \sqrt{U_x} \right) e^{itV_x} \right].$$

Покажем, что при $x \rightarrow \infty$

$$U_x \xrightarrow{\mathbb{P}} 1; \quad V_x \xrightarrow{\mathbb{P}} 0.$$

Для U_x это очевидно, поскольку $N_x/x \xrightarrow{\text{п. н.}} 1$ по усиленному закону больших чисел для пуассоновского процесса [15].

Для V_x возьмем произвольное $\varepsilon > 0$ и снова разложим вероятность по трем областям:

$$\mathbb{P}(|V_x| > \varepsilon) = B_1(x, \varepsilon) + B_2(x, \varepsilon) + B_3(x, \varepsilon),$$

где

$$B_1(x, \varepsilon) = \sum_{k=0}^{\lfloor c_1 x \rfloor} \pi_{x,k} \mathbb{P} \left(\frac{|R_k(T_{k, \min}) - R_x(T_{x, \min})|}{\sigma^2 \sqrt{2x}} > \varepsilon \right); \\ B_2(x, \varepsilon) = \sum_{k=\lfloor c_1 x \rfloor + 1}^{\lfloor c_2 x \rfloor} \pi_{x,k} \mathbb{P} \left(\frac{|R_k(T_{k, \min}) - R_x(T_{x, \min})|}{\sigma^2 \sqrt{2x}} > \varepsilon \right); \\ B_3(x, \varepsilon) = \sum_{k=\lfloor c_2 x \rfloor + 1}^{\infty} \pi_{x,k} \mathbb{P} \left(\frac{|R_k(T_{k, \min}) - R_x(T_{x, \min})|}{\sigma^2 \sqrt{2x}} > \varepsilon \right).$$

Очевидно,

$$B_1(x, \varepsilon) \leq \mathbb{P}(N_x \leq c_1 x); \quad B_3(x, \varepsilon) \leq \mathbb{P}(N_x \geq c_2 x),$$

и эти величины стремятся к нулю экспоненциально аналогично предыдущим рассуждениям. Для $B_2(x, \varepsilon)$ используем оценку риска из [12] и (2):

$$\sup_{c_1 x \leq k \leq c_2 x} \frac{|R_k(T_{k, \min}) - R_x(T_{x, \min})|}{\sigma^2 \sqrt{2x}} \leq \\ \leq C \frac{x^{1-\gamma} \ln x}{\sqrt{x}} = C x^{1/2-\gamma} \ln x \rightarrow 0,$$

поскольку $\gamma > 1/2$. Значит, начиная с некоторого $x_0(\varepsilon)$, все вероятности в определении $B_2(x, \varepsilon)$ равны нулю. Следовательно, $V_x \rightarrow 0$ по вероятности.

Из сходимости $(U_x, V_x) \rightarrow (1, 0)$ по вероятности и ограниченности функции

$$(u, v) \mapsto \varphi(t\sqrt{u})e^{itv}$$

следует сходимость

$$g_x(t) \rightarrow \varphi(t).$$

Вместе с (13) это дает

$$h_x(t) \rightarrow \varphi(t) \quad \text{при каждом } t \in \mathbb{R}.$$

Это и означает (10). Теорема доказана.

Теорема 3. Пусть выполнено условие (1). Тогда для любого $0 < \gamma < 1$

$$\frac{\hat{R}_{N_x}(T_{N_x, S}) - R_x(T_{x, \min})}{x} \xrightarrow[\text{п. н.}]{x \rightarrow \infty} 0.$$

Доказательство: Сначала рассмотрим натуральные значения x , т. е. $x = n$. Тогда

$$\mathbb{P} \left(\left| \frac{\hat{R}_{N_n}(T_{N_n, S}) - R_n(T_{n, \min})}{n} \right| > \varepsilon \right) = \\ = \mathbb{P} \left(\left| \frac{\hat{R}_{N_n}(T_{N_n, S}) - R_n(T_{n, \min})}{n} \right| > \varepsilon, \right. \\ \left. c_1 n < N_n < c_2 n \right) + \\ + \mathbb{P} \left(\left| \frac{\hat{R}_{N_n}(T_{N_n, S}) - R_n(T_{n, \min})}{n} \right| > \varepsilon, N_n \leq c_1 n \right) + \\ + \mathbb{P} \left(\left| \frac{\hat{R}_{N_n}(T_{N_n, S}) - R_n(T_{n, \min})}{n} \right| > \varepsilon, c_2 n \leq N_n \right) \equiv \\ \equiv p_n + q_n + r_n.$$

Далее, оценивая q_n и r_n так же, как в теореме 1, получаем

$$\sum_{n=1}^{\infty} (q_n + r_n) < \infty.$$

Для оценки p_n воспользуемся результатами работы [8]. Согласно лемме 3 и теореме 2 из [8], можно

выбрать такое α : $0 < \alpha < \min(1, 2\gamma)$, что найдутся константы $C, c > 0$, для которых

$$\begin{aligned} p_n &\leq \sum_{k=[c_1 n]}^{[c_2 n]} \mathbb{P}(N_n = k) \times \\ &\times \mathbb{P}\left(\left|\frac{\widehat{R}_k(T_{k,S}) - R_n(T_{n,\min})}{n}\right| > \varepsilon \mid N_n = k\right) \leq \\ &\leq \max_{[c_1 n] \leq k \leq [c_2 n]} \mathbb{P}\left(\left|\frac{\widehat{R}_k(T_{k,S}) - R_n(T_{n,\min})}{n}\right| > \varepsilon\right) \leq \\ &\leq C \ln n \exp\left\{-\frac{c n^{1-\alpha}}{(\ln n)^3}\right\}, \end{aligned}$$

и потому

$$\sum_{n=1}^{\infty} p_n < \infty.$$

Следовательно, по лемме Бореля–Кантелли

$$\frac{\widehat{R}_{N_n}(T_{N_n,S}) - R_n(T_{n,\min})}{n} \rightarrow 0 \text{ п. н. при } n \rightarrow \infty.$$

Теперь перейдем к произвольным $x \geq 1$. Пусть $n \leq x \leq n+1$, где $n = \lfloor x \rfloor$. Положим

$$\begin{aligned} \bar{Z}_x &:= \widehat{R}_{N_x}(T_{N_x,S}) - R_x(T_{x,\min}); \\ W_x &:= \bar{Z}_x - \bar{Z}_n. \end{aligned}$$

Тогда

$$\begin{aligned} W_x &= \sum_{i=1}^{N_n} (F_i(T_{N_x,S}) - F_i(T_{N_n,S})) - \\ &- (R_x(T_{x,\min}) - R_n(T_{n,\min})) + \\ &+ \sum_{i=N_n+1}^{N_x} F_i(T_{N_x,S}) =: A_1(x) + A_2(x) + A_3(x). \end{aligned}$$

Оценка $A_3(x)$.

Из условий на $h(u, T)$ и определения $F_i(T)$ следует, что при любом T и любом i

$$|F_i(T)| \leq CT^2.$$

Поскольку $T_{N_x,S} \leq T_u(x)$ и при $x \in [n, n+1]$ выполнено $N_x \leq N_{n+1}$, получаем

$$\sup_{n \leq x \leq n+1} |A_3(x)| \leq CT_u^2(n+1)(N_{n+1} - N_n).$$

Здесь

$$T_u^2(n+1) = 2\sigma^2 \ln(n+1) = O(\ln n).$$

Кроме того, $N_{n+1} - N_n \sim \text{Pois}(1)$. Поэтому для любого $\delta > 0$

$$\sum_{n=1}^{\infty} \mathbb{P}\left(\frac{(N_{n+1} - N_n) \ln n}{n} > \delta\right) < \infty.$$

По лемме Бореля–Кантелли отсюда следует, что

$$\frac{1}{x} \sup_{n \leq x \leq n+1} |A_3(x)| \rightarrow 0 \text{ п. н.}$$

Оценка $A_2(x)$.

По теореме 1 имеем

$$R_x(T_{x,\min}) \leq Cx^{1-\gamma} \ln x.$$

Следовательно,

$$\begin{aligned} \frac{1}{x} \sup_{n \leq x \leq n+1} |A_2(x)| &\leq \frac{1}{x} \sup_{n \leq x \leq n+1} R_x(T_{x,\min}) + \\ &+ \frac{R_n(T_{n,\min})}{n} \leq Cn^{-\gamma} \ln n \rightarrow 0, \end{aligned}$$

т. е.

$$\frac{1}{x} \sup_{n \leq x \leq n+1} |A_2(x)| \rightarrow 0 \text{ п. н.}$$

Оценка $A_1(x)$.

Положим

$$V_n := \sup_{n \leq x \leq n+1} \left| \sum_{i=1}^{N_n} (F_i(T_{N_x,S}) - F_i(T_{N_n,S})) \right|.$$

Покажем, что

$$\frac{V_n}{n} \rightarrow 0 \text{ п. н.}$$

Зафиксируем $\varepsilon > 0$. По формуле полной вероятности

$$\begin{aligned} \mathbb{P}\left(\frac{V_n}{n} > \varepsilon\right) &= \sum_{k=0}^{\infty} \pi_{n,k} \times \\ &\times \mathbb{P}\left(\sup_{n \leq x \leq n+1} \left| \frac{1}{n} \sum_{i=1}^{N_n} (F_i(T_{N_x,S}) - F_i(T_{N_n,S})) \right| > \right. \\ &\quad \left. > \varepsilon \mid N_n = k\right) =: \\ &=: J_1(n) + J_2(n) + J_3(n), \end{aligned}$$

где $J_1(n)$, $J_2(n)$ и $J_3(n)$ отвечают областям $k \leq c_1 n$, $c_1 n < k \leq c_2 n$ и $k > c_2 n$ соответственно (c_1 и c_2 такие же, как в теореме 1).

Так как условные вероятности не превосходят 1, то

$$J_1(n) \leq \mathbb{P}(N_n \leq c_1 n); \quad J_3(n) \leq \mathbb{P}(N_n \geq c_2 n).$$

По оценкам (7) и (5) обе эти величины стремятся к нулю экспоненциально.

Остается центральная часть $J_2(n)$. Зафиксируем k , где $c_1 n < k \leq c_2 n$, и положим

$$p_{k,m}^* := \mathbb{P} \left(\left| \frac{1}{n} \sum_{i=1}^k (F_i(T_{m,S}) - F_i(T_{k,S})) \right| > \varepsilon \right), \quad m \geq 0.$$

Тогда

$$\begin{aligned} & \mathbb{P} \left(\sup_{n \leq x \leq n+1} \left| \frac{1}{n} \sum_{i=1}^{N_n} (F_i(T_{N_x,S}) - F_i(T_{N_n,S})) \right| > \varepsilon \mid N_n = k \right) = \\ &= \sum_{m=0}^{\infty} \mathbb{P} \left(\sup_{n \leq x \leq n+1} \left| \frac{1}{n} \sum_{i=1}^k (F_i(T_{N_x,S}) - F_i(T_{k,S})) \right| > \varepsilon \mid N_n = k, N_x = m \right) \times \\ & \quad \times \mathbb{P}(N_x = m \mid N_n = k) = \\ &= \sum_{m=0}^{\infty} \mathbb{P}(N_x = m \mid N_n = k) p_{k,m}^* = \\ &= \sum_{m=0}^{\infty} \mathbb{P}(N_x - N_n = m - k \mid N_n = k) p_{k,m}^* = \\ &= \sum_{m=0}^{\infty} \mathbb{P}(N_x - N_n = m - k) =: \\ & \quad =: I_1(k, n) + I_2(k, n) + I_3(k, n), \end{aligned}$$

где $I_1(k, n)$, $I_2(k, n)$ и $I_3(k, n)$ отвечают областям

$$0 \leq m < \lfloor c_1 n \rfloor, \quad \lfloor c_1 n \rfloor \leq m \leq \lfloor c'_2 n \rfloor, \quad m \geq \lfloor c'_2 n \rfloor + 1, \quad c'_2 > c_2,$$

а $I_1(k, n) = 0$, поскольку для всех слагаемых в этой сумме $m - k < 0$. Так как $c'_2 > c_2$, используя рассуждения, аналогичные теореме 1, получаем, что $I_3(k, n) < C e^{-cn}$.

Далее,

$$I_2(k, n) \leq \max_{\lfloor c_1 n \rfloor \leq m \leq \lfloor c'_2 n \rfloor} p_{k,m}^*.$$

Следовательно,

$$J_2(n) \leq \max_{\lfloor c_1 n \rfloor + 1 \leq k \leq \lfloor c_2 n \rfloor} \max_{\lfloor c_1 n \rfloor \leq m \leq \lfloor c'_2 n \rfloor} p_{k,m}^* + C e^{-cn}.$$

Теперь снова используем результаты работы [8]. Аналогично можно выбрать такое α из диапазона $(0, \min(1, 2\gamma))$, что существуют константы $C, c > 0$ такие, что равномерно по $\lfloor c_1 n \rfloor + 1 \leq k \leq \lfloor c_2 n \rfloor$, $\lfloor c_1 n \rfloor \leq m \leq \lfloor c'_2 n \rfloor$ выполнено

$$p_{k,m}^* \leq C \ln n \exp \left\{ -\frac{c n^{1-\alpha}}{(\ln n)^3} \right\}.$$

Поэтому

$$J_2(n) \leq C \ln n \exp \left\{ -\frac{c n^{1-\alpha}}{(\ln n)^3} \right\} + C e^{-cn}.$$

С учетом оценок для $J_1(n)$ и $J_3(n)$ получаем

$$\mathbb{P} \left(\frac{V_n}{n} > \varepsilon \right) \leq C \ln n \exp \left\{ -\frac{c n^{1-\alpha}}{(\ln n)^3} \right\} + C e^{-cn}.$$

Правая часть суммируема по n , поэтому по лемме Бореля–Кантелли

$$\frac{V_n}{n} \rightarrow 0 \text{ п. н.}$$

Завершение доказательства.

Положим

$$U_n := V_n + \sup_{n \leq x \leq n+1} |A_2(x)| + \sup_{n \leq x \leq n+1} |A_3(x)|.$$

Тогда из полученных выше оценок следует, что

$$\frac{U_n}{n} \rightarrow 0 \text{ п. н.}$$

Кроме того, для $n \leq x \leq n+1$ имеем

$$|\bar{Z}_x - \bar{Z}_n| \leq U_n,$$

т. е.

$$\bar{Z}_n - U_n \leq \bar{Z}_x \leq \bar{Z}_n + U_n.$$

Так как $n \leq x \leq n+1$, то

$$\frac{\bar{Z}_n - U_n}{n+1} \leq \frac{\bar{Z}_x}{x} \leq \frac{\bar{Z}_n + U_n}{n}.$$

Поскольку $\bar{Z}_n/n \rightarrow 0$ п. н. и $U_n/n \rightarrow 0$ п. н., получаем

$$\frac{\bar{Z}_x}{x} \rightarrow 0 \text{ п. н. при } x \rightarrow \infty.$$

Теорема доказана.

5 Заключение

В работе исследована задача пороговой обработки в разреженной модели с аддитивным гауссовским шумом в случае, когда число наблюдений за фиксированный промежуток времени задается пуассоновским процессом. В этой постановке риск определяется как математическое ожидание квадратичной ошибки с учетом случайности числа наблюдений.

Показано, что переход к модели, в которой число наблюдений задается пуассоновским процессом, не меняет главного порядка роста риска: для оптимального выбора порога сохраняется оценка порядка $x^{1-\gamma} \ln x$, где $x = \lambda t$ есть среднее число наблюдений. Тем самым установлено, что в рассматриваемой модели рандомизация числа наблюдений не нарушает основной асимптотики, известной для случая фиксированного объема выборки.

Кроме того, для SURE-оценки риска в модели, порождаемой пуассоновским процессом, доказаны центральная предельная теорема и усиленный закон больших чисел. Таким образом, основные предельные свойства, установленные ранее в постановке с фиксированным числом наблюдений, сохраняются и в более общей модели.

Полученные результаты показывают, что асимптотическая теория пороговых процедур устойчива по отношению к рандомизации объема выборки. Это делает естественным дальнейшее развитие данного подхода для более общих моделей случайного числа наблюдений, а также для более сложных схем шума и зависимостей.

Литература

1. Donoho D., Johnstone I. M. Ideal spatial adaptation via wavelet shrinkage // *Biometrika*, 1994. Vol. 81. No. 3. P. 425–455. doi: 10.1093/biomet/81.3.425.
2. Donoho D., Johnstone I. M. Adapting to unknown smoothness via wavelet shrinkage // *J. Am. Stat. Assoc.*, 1995. Vol. 90. No. 432. P. 1200–1224. doi: 10.1080/01621459.1995.10476626.
3. Donoho D., Jin J. Higher criticism for detecting sparse heterogeneous mixtures // *Ann. Stat.*, 2004. Vol. 32. No. 3. P. 962–994. doi: 10.1214/009053604000000265.
4. Lin Y., Cai J. A new threshold function for signal denoising based on wavelet transform // *Conference (International) on Measuring Technology and Mechatronics Automation Proceedings*. — Piscataway, NJ, USA: IEEE, 2010. P. 200–203. doi: 10.1109/ICMTMA.2010.347.
5. Huang H.-C., Lee T. C. M. Stabilized thresholding with generalized sure for image denoising // *IEEE Conference (International) on Image Processing*. — Piscataway, NJ, USA: IEEE, 2010. P. 1881–1884. doi: 10.1109/ICIP.2010.5652353.
6. He C., Xing J., Li J., Yang Q., Wang R. A new wavelet thresholding function based on hyperbolic tangent function // *Math. Probl. Eng.*, 2015. Vol. 2015. Art. 528656. 10 p. doi: 10.1155/2015/528656.
7. Шестаков О. В. Несмещенная оценка риска пороговой обработки с двумя пороговыми значениями // *Информатика и её применения*, 2022. Т. 16. Вып. 4. С. 14–19. doi: 10.14357/19922264220403. EDN: DZBVL.
8. Kudryavtsev A. A., Shestakov O. V. Properties of the SURE estimates when using continuous thresholding functions for wavelet shrinkage // *Mathematics*, 2024. Vol. 12. No. 23. Art. 3646. 14 p. doi: 10.3390/math12233646. EDN: AETFBD.
9. Воронцов М. О., Шестаков О. В. Асимптотическая нормальность и сильная состоятельность оценки риска при использовании FDR-порога в условиях слабой зависимости // *Информатика и её применения*, 2024. Т. 18. Вып. 3. С. 69–79. doi: 10.14357/19922264240309. EDN: ZOQVTO.
10. Шестаков О. В. Статистические свойства оценки среднеквадратичного риска метода блочной пороговой обработки в задачах непараметрической регрессии со случайной сеткой // *Информатика и её применения*, 2024. Т. 18. Вып. 4. С. 26–38. doi: 10.14357/19922264240404. EDN: WHZQPX.
11. Шестаков О. В. Решение обратных статистических задач с помощью методов пороговой обработки, допускающих построение несмещенной оценки среднеквадратичного риска // *Информатика и её применения*, 2025. Т. 19. Вып. 1. С. 74–81. doi: 10.14357/19922264250110. EDN: ZSIBDL.
12. Melezhnikov E. I., Shestakov O. V., Stepanov E. S. Asymptotic analysis of a thresholding method for sparse models with application to network delay detection // *Mathematics*, 2026. Vol. 14. No. 1. Art. 148. 13 p. doi: 10.3390/math14010148. EDN: RRBORZ.
13. Stein C. Estimation of the mean of a multivariate normal distribution // *Ann. Stat.*, 1981. Vol. 9. No. 6. P. 1135–1151.
14. Mallat S. A wavelet tour of signal processing. — New York, NY, USA: Academic Press, 1999. 857 p.
15. Кингман Дж. Пуассоновские процессы / Пер. с англ. — М: Изд-во МЦНМО, 2007. 136 с. (Kingman J. F. C. Poisson processes. — Oxford: Clarendon Press, 1992. 112 p.)

Поступила в редакцию 05.05.2026

Принята к публикации 15.08.2026

ASYMPTOTIC ANALYSIS OF THRESHOLD PROCESSING METHODS IN SPARSE MODELS WITH A POISSON NUMBER OF OBSERVATIONS

E. I. Melezhnikov^{1,2} and O. V. Shestakov^{1,2,3}

¹Department of Mathematical Statistics, Faculty of Computational Mathematics and Cybernetics, M. V. Lomonosov Moscow State University, 1-52 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation

²Moscow Center for Fundamental and Applied Mathematics, M. V. Lomonosov Moscow State University, 1 Leninskie Gory, GSP-1, Moscow 119991, Russian Federation

³Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: The problem of threshold processing of a sparse signal with noisy observations is considered. The number of observations is assumed to be random and generated by a Poisson process with a given intensity. The behavior of the mean-square risk and its estimate based on Stein’s unbiased risk estimate (SURE) is investigated. Special attention is paid to the effect of randomness in the sample size on signal recovery accuracy and on the properties of risk estimation. An upper bound for the risk under optimal threshold selection is obtained and it is shown that its asymptotic order coincides with that in the deterministic case. In addition, a central limit theorem and a strong law of large numbers for the SURE risk estimate are proved. Thus, the stability of the asymptotic properties of thresholding procedures is established when passing to a model defined by a Poisson process. The obtained results are applicable to problems of streaming data analysis, where observations arrive at random time moments and the sample size is not fixed in advance. This extends the applicability of thresholding methods to statistical models with a random number of observations.

Keywords: thresholding; mean square risk; risk estimate; sparse model; Poisson process; central limit theorem; strong law of large numbers

DOI: 10.14357/19922264260304

EDN: UJQIXC

Acknowledgments

The work was supported by the Ministry of Education and Science of the Russian Federation as part of the program of the Moscow Center for Fundamental and Applied Mathematics under the Agreement No. 075-15-2025-345.

References

- Donoho, D., and I. M. Johnstone. 1994. Ideal spatial adaptation via wavelet shrinkage. *Biometrika* 81(3):425–455. doi: 10.1093/biomet/81.3.425.
- Donoho, D., and I. M. Johnstone. 1995. Adapting to unknown smoothness via wavelet shrinkage. *J. Am. Stat. Assoc.* 90(432):1200–1224. doi: 10.1080/01621459.1995.10476626.
- Donoho, D., and J. Jin. 2004. Higher criticism for detecting sparse heterogeneous mixtures. *Ann. Stat.* 32(3):962–994. doi: 10.1214/009053604000000265.
- Lin, Y., and J. Cai. 2010. A new threshold function for signal denoising based on wavelet transform. *Conference (International) on Measuring Technology and Mechatronics Automation Proceedings*. Piscataway, NJ: IEEE. 200–203. doi: 10.1109/ICMTMA.2010.347.
- Huang, H.-C., and T. C. M. Lee. 2010. Stabilized thresholding with generalized sure for image denoising. *17th Conference (International) on Image Processing Proceedings*. Piscataway, NJ: IEEE. 1881–1884. doi: 10.1109/ICIP.2010.5652353.
- He, C., J. Xing, J. Li, Q. Yang, and R. Wang. 2015. A new wavelet thresholding function based on hyperbolic tangent function. *Math. Probl. Eng.* 2015:528656. 10 p. doi: 10.1155/2015/528656.
- Shestakov, O. V. 2022. Nesmeshchennaya otsenka riska porogovoy obrabotki s dvumya porogovymi znacheniyami [Unbiased thresholding risk estimate with two threshold values]. *Informatika i ee Primeneniya — Inform. Appl.* 16(4):14–19. doi: 10.14357/19922264220403. EDN: DZBVLG.
- Kudryavtsev, A. A., and O. V. Shestakov. 2024. Properties of the SURE estimates when using continuous thresholding functions for wavelet shrinkage. *Mathematics* 12(23):3646. 14 p. doi: 10.3390/math12233646. EDN: AETFBG.
- Vorontsov, M. O., and O. V. Shestakov. 2024. Asimptoticheskaya normal’nost’ i sil’naya sostoyatel’nost’ otsenki riska pri ispol’zovanii FDR-poroga v usloviyakh slaboy zavisimosti [Asymptotic normality and strong consistency of risk estimate when using the FDR threshold under weak dependence condition]. *Informatika i ee Primeneniya — Inform. Appl.* 18(3):69–79. doi: 10.14357/19922264240309. EDN: ZOQVTO.
- Shestakov, O. V. 2024. Statisticheskie svoystva otsenki srednekvadrachnogo riska metoda blochnoy porogovoy

- obrabotki v zadachakh neparametricheskoy regressii so sluchaynoy setkoy [Statistical properties of the mean-square risk estimate for the block threshold processing method in nonparametric regression problems with a random grid]. *Informatika i ee Primeneniya — Inform. Appl.* 18(4):26–33. doi: 10.14357/19922264240404. EDN: WHZQPX.
11. Shestakov, O. V. 2025. Reshenie obratnykh statisticheskikh zadach s pomoshch'yu metodov porogovoy obrabotki, dopuskayushchikh postroenie nesmeshchennoy otsenki srednekvadrachnogo riska [Solving inverse statistical problems using threshold processing methods that allow the construction of an unbiased estimate of the mean-square risk]. *Informatika i ee Primeneniya — Inform. Appl.* 19(1):74–81. doi: 10.14357/19922264250110. EDN: ZSIBDL.
 12. Melezhnikov, E. I., O. V. Shestakov, and E. S. Stepanov. 2026. Asymptotic analysis of a thresholding method for sparse models with application to network delay detection. *Mathematics* 14(1):148. 13 p. doi: 10.3390/math14010148. EDN: RRBORZ.
 13. Stein, C. 1981. Estimation of the mean of a multivariate normal distribution. *Ann. Stat.* 9(6):1135–1151. doi: 10.1214/aos/1176345632.
 14. Mallat, S. 1999. *A wavelet tour of signal processing*. New York, NY: Academic Press. 857 p.
 15. Kingman, J. F. C. 1992. *Poisson processes*. Oxford: Clarendon Press. 112 p.

Received May 5, 2026

Accepted August 15, 2026

Contributors

Melezhnikov Evgeniy I. (b. 1998) — PhD student, Department of Mathematical Statistics, Faculty of Computational Mathematics and Cybernetics, M.V. Lomonosov Moscow State University, 1-52 Leninskiye Gory, GSP-1, Moscow 119991, Russian Federation; junior scientist, Moscow Center for Fundamental and Applied Mathematics, M. V. Lomonosov Moscow State University, 1 Leninskiye Gory, GSP-1, Moscow 119991, Russian Federation; melezhn@gmail.com

Shestakov Oleg V. (b. 1976) — Doctor of Sciences in physics and mathematics, professor, Department of Mathematical Statistics, Faculty of Computational Mathematics and Cybernetics, M.V. Lomonosov Moscow State University, 1-52 Leninskiye Gory, GSP-1, Moscow 119991, Russian Federation; senior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; leading scientist, Moscow Center for Fundamental and Applied Mathematics, M.V. Lomonosov Moscow State University, 1 Leninskiye Gory, GSP-1, Moscow 119991, Russian Federation; oshestakov@cs.msu.su

АНАЛИЗ ЗАГРУЗКИ МНОГОПОЛЬЗОВАТЕЛЬСКОЙ СЕТИ ПРИ СМЕШАННЫХ СТРАТЕГИЯХ МАРШРУТИЗАЦИИ

Ю. Е. Малащенко¹, И. А. Назарова², М. В. Козлов³

Аннотация: В рамках вычислительных экспериментов изучаются монопольные и смешанные стратегии управления исходящими узловыми мультипоточками. Анализируются две монопольные схемы диспетчеризации межузловых потоков — по кратчайшим маршрутам и по путям следования максимального потока. Для указанных способов управления формируются нормированные векторы исходящих мультипоточек, передаваемых в монопольном режиме всем узлам-адресатам. Определяются характеристические векторы загрузки ребер при прохождении по сети нормированных мультипоточек из вершин-источников. Для оценки загрузки сети при использовании смешанных методов диспетчеризации строятся выпуклые комбинации построенных характеристических векторов. Для всех характеристических векторов вычисляются среднеквадратичные отклонения значений компонент, относительные коэффициенты вариации и величина максимального превышения среднего уровня загрузки ребер. Проводится сравнительный анализ агрегированных функциональных показателей для каждого узла и предложенных способов маршрутизации. Изучается влияние узловых мультипоточек на общую загрузку сети. Определяются возможные точки перегрузки и узкие места сети. Результаты экспериментов проиллюстрированы специальными диаграммами.

Ключевые слова: многопродуктовая модель; исходящий узловой мультипоток; распределение загрузки сети

DOI: 10.14357/19922264260305

EDN: OIVGUK

1 Введение

В рамках формализма математической модели передачи многопродуктового потока изучаются различные стратегии маршрутизации для многопользовательской сетевой системы. Для оценки функциональных характеристик сети вводится понятие мультипотока [1] как совокупности межузловых потоков, исходящих одновременно из узла-источника всем узлам-приемниками. В рамках вычислительного эксперимента формируются характеристические векторы загрузки ребер сети и другие показатели работоспособности системы [2]. Полученные массивы данных дают возможность количественно анализировать распределение нагрузки для нормированных межузловых мультипоточек. Рассматриваются две схемы диспетчеризации в монопольном режиме [3] — по кратчайшим маршрутам и по пути следования максимального потока.

В настоящей работе исследуется смешанная стратегия управления исходящими мультипоточками: для каждого узла сети характеристический вектор строится как выпуклая комбинация нормированных межузловых мультипоточек, передаваемых в монопольном режиме как по кратчайшим путям, так и по пути транспортировки

максимального потока. Для оценки нагрузки на сеть для всех характеристических векторов вычисляются среднеквадратичные отклонения значений компонент, коэффициенты вариации, величины максимального превышения среднего уровня загрузки ребер и пр. Полученные результаты позволяют сравнивать функциональные возможности сети для различных сценариев маршрутизации мультипотока. Вычислительные эксперименты проводились методами потокового программирования [4, 5] на сетях с различными структурными особенностями и одинаковой суммарной пропускной способностью ребер. Алгоритмы поиска кратчайших путей, маршрутов максимальных потоков для всех пар узлов, а также построение векторных многопараметрических характеристик имеют полиномиальную сложность [6].

2 Математическая модель

Для описания многопользовательской сетевой системы связи воспользуемся следующей математической записью модели передачи многопродуктового потока (далее — М-модель). Сеть G задается множествами $\langle V, R, U, P \rangle$: узлов (вершин) сети $V = \{v_1, v_2, \dots, v_n, \dots, v_N\}$; неориентированных ре-

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, malash09@ccas.ru

²Федеральный исследовательский центр «Информатика и управление» Российской академии наук, irina-nazar@yandex.ru

³Федеральный исследовательский центр «Информатика и управление» Российской академии наук, kztmp2@ccas.ru

бер $R = \{r_1, r_2, \dots, r_k, \dots, r_E\}$; ориентированных дуг $U = \{u_1, u_2, \dots, u_k, \dots, u_{2E}\}$; пар узлов-корреспондентов $P = \{p_1, p_2, \dots, p_M\}$. Предполагается, что в сети отсутствуют петли и двоянные ребра.

Ребро $r_k \in R$ соединяет *смежные* вершины v_{n_k} и v_{j_k} . Каждому ребру r_k ставятся в соответствие две ориентированные дуги u_k и u_{k+E} из множества U . Дуги $\{u_k, u_{k+E}\}$ определяют прямое и обратное направление передачи потока по ребру r_k между концевыми вершинами v_{n_k} и v_{j_k} . Для каждой вершины v_n формируется список $K(n)$ номеров инцидентных ей ребер: $K(n) = \{k_1, k_2, \dots, k_{a(n)}\}$, где $a(n)$ — число инцидентных ребер для v_n .

В многопользовательской сети G рассматривается $M = N(N-1)$ независимых, неважимоменяемых и равноправных межузловых потоков различных видов. Каждой паре узлов-корреспондентов p_m из множества P соответствуют: вершина-источник с номером s_m , из s_m входной поток m -го вида поступает в сеть; вершина-приемник с номером t_m , из t_m поток m -го вида покидает сеть.

Обозначим через z_m величину *межузлового* потока m -го вида, поступающего в сеть через узел с номером s_m и покидающего сеть из узла с номером t_m ; $x_{mk}, x_{m(k+E)}$ — поток m -го вида, который передается по дугам u_k и u_{k+E} согласно направлению передачи, $x_{mk} \geq 0, x_{m(k+E)} \geq 0, m = \overline{1, M}, k = \overline{1, E}$; $S(v_n)$ — множество номеров исходящих дуг, по ним поток покидает узел v_n ; $T(v_n)$ — множество номеров входящих дуг, по ним поток поступает в узел v_n . Состав множеств $S(v_n)$ и $T(v_n)$ однозначно определяется в ходе выполнения следующей процедуры. Пусть некоторое ребро $r_k \in R$ соединяет вершины с номерами n и j , такими что $n < j$. Тогда ориентированная дуга $u_k = (v_n, v_j)$, направленная из вершины v_n в v_j , считается *исходящей* из вершины v_n и ее номер k заносится в множество $S(v_n)$, а дуга u_{k+E} , направленная из v_j в v_n , — *входящей* для v_n и ее номер $k+E$ помещается в список $T(v_n)$. Дуга u_k является *входящей* для v_j , и ее номер k попадает в $T(v_j)$, а дуга u_{k+E} — *исходящей*, и номер $k+E$ вносится в список исходящих дуг $S(v_j)$.

Во всех узлах сети $v_n \in V, n = \overline{1, N}$, для каждого вида потока должны выполняться условия сохранения потоков:

$$\begin{aligned} \sum_{i \in S(v_n)} x_{mi} - \sum_{i \in T(v_n)} x_{mi} &= \\ &= \begin{cases} z_m, & \text{если } v_n = v_{s_m}; \\ -z_m, & \text{если } v_n = v_{t_m}; \\ 0 & \text{в остальных случаях,} \end{cases} \\ n = \overline{1, N}, m = \overline{1, M}, x_{mi} \geq 0, z_m \geq 0. \end{aligned} \quad (1)$$

Величина z_m равна входному межузловому потоку m -го вида, проходящему от источника s_m к приемнику t_m пары p_m при распределении потоков $\{x_{mi}\} = \mathbf{x}$ по дугам сети.

Каждому ребру $r_k \in R$ приписывается неотрицательное число d_k — суммарный предельно допустимый поток, который можно передать по ребру r_k в обоих направлениях. В исходной сети компоненты вектора пропускных способностей $\mathbf{d} = (d_1, d_2, \dots, d_k, \dots, d_E)$ — положительные числа d_k . Вектор $\mathbf{d}$ ограничивает сумму потоков всех видов, передаваемых по ребру r_k одновременно:

$$\begin{aligned} \sum_{m=1}^M (x_{mk} + x_{m(k+E)}) &\leq d_k, \quad x_{mk} \geq 0, \\ x_{m(k+E)} &\geq 0, \quad k = \overline{1, E}. \end{aligned} \quad (2)$$

Вектор $\mathbf{y} = (y_1, y_2, \dots, y_k, \dots, y_E)$ с компонентами

$$y_k = \sum_{m=1}^M (x_{mk} + x_{m(k+E)}), \quad x_{mk} \geq 0,$$

$$x_{m(k+E)} \geq 0, \quad k = \overline{1, E},$$

характеризует *загрузку* ребра и определяет требования к пропускной способности — *ресурсам* — сети при передаче межузловых потоков $z_m, m = \overline{1, M}$.

Условия (1) и (2) задают множество допустимых значений вектора межузловых потоков $\mathbf{z} = (z_1, z_2, \dots, z_m, \dots, z_M)$:

$$\begin{aligned} \mathcal{Z}(\mathbf{d}) &= \{\mathbf{z} \geq 0 \mid \exists \mathbf{x} \geq 0 : (\mathbf{z}, \mathbf{x}) \\ &\text{удовлетворяют (1), (2)}\}. \end{aligned}$$

Для каждой вершины $v_n \in V, n = \overline{1, N}$, вводится подмножество $P(v_n)$ пар-корреспондентов, для которых v_n служит узлом-источником: $P(v_n) = \{p_m \mid s_m = n, t_m \neq n, t_m = \overline{1, N}\}$, и определяется список номеров $M(n)$ пар p_m , входящих в подмножество $P(v_n)$: $M(n) = \{m \mid p_m \in P(v_n)\}$. Для каждого $n, n = \overline{1, N}$, список $M(n)$ содержит $N-1$ элемент. Для каждой вершины v_n формируется вектор исходящих межузловых потоков (далее — VMS-вектор, от английского vertex-multistream), или вектор мультипотока

$$\vec{z}(n) = \{z_m \mid p_m \in P(v_n)\}.$$

3 Загрузка сети при маршрутизации по пути передачи максимального потока

Сравнительный анализ способов маршрутизации передачи потоков проводится в рамках вычис-

лительных экспериментов. При подготовке расчетных данных для каждой пары узлов-корреспондентов независимо определяется величина максимального потока и путь его передачи в монопольном режиме. Задается исходная сеть $G(0)$, пропускные способности $d_k(0)$, $k = \overline{1, E}$, и предполагается, что между парой узлов $p_m \in P$ передается поток m -го вида. В исходной сети $G(0)$ для каждой фиксированной пары p_m независимо и последовательно подсчитывается максимальный поток z_m , передаваемый в монопольном режиме из s_m в t_m .

Задача 1. Для некоторого $p_m \in P$ найти

$$z_m^0(0) = \max_{Z(d), x} z_m$$

при условиях (1), (2), $z_i = 0$ для $i \neq m$, $p_i \in P$.

Решение задачи 1 — величина максимального потока $z_m^0(0)$ для выделенной пары узлов-корреспондентов p_m и соответствующие значения дуговых потоков:

$$x_{mk}^0(0) \geq 0, \quad k = \overline{1, 2E}.$$

Определяются реберные загрузки $y_k^0(0)$ и список номеров ребер, для которых при передаче междуузлов потока $z_m^0(0)$ величина загрузки $y_k^0(0)$ положительна:

$$L(m) = \{k | y_k^0(0) = x_{mk}^0(0) + x_{m(k+E)}^0(0) > 0, \quad k = \overline{1, E}\}.$$

Для каждой фиксированной пары p_m рассматривается набор ребер R_m , образующих маршруты передачи максимального потока $z_m^0(0)$ (далее — MFT-маршрут, от английского maximum flow transmission) из узла s_m в узел t_m : $R_m = \{r_k | k \in L(m)\}$. После решения последовательности задач 1 для всех $p_m \in P$ устанавливаются нормирующие коэффициенты

$$\omega_m^0(0) = \frac{1}{z_m^0(0)}, \quad z_m^0(0) \neq 0, \quad m = \overline{1, M}, \quad (3)$$

и вычисляются нормированные дуговые потоки:

$$x_{mk}^0 = \omega_m^0(0) x_{mk}^0(0), \quad m = \overline{1, M}, \quad k = \overline{1, 2E}. \quad (4)$$

Согласно условиям *нормировки* для дуговых потоков (3), при передаче соответствующих x_{mk}^0 по ребрам сети междуузловой поток z_m^0 из узла s_m в узел t_m равен единице для всех $p_m \in P$.

На основании решения задачи 1 для каждой вершины v_n строится нормированный вектор исходящего мультипотока, т. е.

$$\bar{z}^0(n) = \{z_m^0(n) | z_m^0(n) = 1, \quad p_m \in P(v_n)\}. \quad (5)$$

Для нормированных дуговых потоков (4) и каждого нормированного VMS-вектора $\bar{z}^0(n)$ (5) вычисляется *загрузка* k -го ребра сети:

$$y_k^0(n) = \sum_{m \in M(n)} (x_{mk}^0 + x_{m(k+E)}^0), \quad n = \overline{1, N}. \quad (6)$$

Формируются характеристические MFT-векторы загрузок:

$$\bar{y}^0(n) = (y_1^0(n), \dots, y_k^0(n), \dots, y_E^0(n)), \quad n = \overline{1, N}. \quad (7)$$

4 Загрузка сети при передаче мультипотока по кратчайшим маршрутам

Для оценки загрузки ребер в сети $G(0)$ для некоторой пары узлов $p_m = (s_m, t_m)$, $p_m \in P$, при передаче междуузлов потока z_m находятся все пути, содержащие минимальное число ребер (далее — SPT-маршруты, от английского shortest path transmission). Определяется множество наборов номеров дуг $H_m(0)$, которые входят в SPT-маршруты для m -го вида потока:

$$H_m(0) = \{h_m^1(0), h_m^2(0), \dots, h_m^j(0), \dots, h_m^{J_m(0)}(0)\},$$

где $h_m^j(0)$ — список номеров дуг в j -м пути в сети $G(0)$ между узлами s_m и t_m ; $J_m(0)$ — число SPT-маршрутов для m -й пары.

Для пары p_m , $p_m \in P$, по всем маршрутам из списка $H_m(0)$ передается междуузловой поток, равный единице, и для каждой k -й дуги, $k = \overline{1, 2E}$, подсчитывается значение индикаторной функции

$$\eta_k^j(m) = \begin{cases} 1, & \text{если } k \in h_m^j(0); \\ 0 & \text{в остальных случаях.} \end{cases}$$

Для пары p_m подсчитываются дуговые потоки

$$x_{mk}^*(0) = \sum_{j=1}^{J_m(0)} \eta_k^j(m), \quad m = \overline{1, M}, \quad k = \overline{1, 2E}. \quad (8)$$

Межузловой поток $z_m^*(0)$ по SPT-маршрутам между узлами s_m и t_m вычисляется по формулам (1) и (8). Рассчитывается нормирующий коэффициент

$$\omega_m^*(0) = \frac{1}{z_m^*(0)}, \quad z_m^*(0) \neq 0, \quad m = \overline{1, M},$$

и дуговые потоки

$$x_{mk}^* = \omega_m^*(0) x_{mk}^*(0), \quad m = \overline{1, M}, \quad k = \overline{1, 2E}. \quad (9)$$

При передаче всех потоков x_{mk}^* по ребрам сети из узла s_m в узел t_m поступает равный единице меж-узловой поток z_m^* для всех $p_m \in P$. Распределение межузловых потоков z_m^* определяется с помощью дуговых потоков x_{mk}^* вдоль SPT-маршрутов.

На основании дуговых потоков x_{mk}^* для каждой вершины v_n формируется нормированный вектор исходящего мультипотока:

$$\bar{\mathbf{z}}^*(n) = \{z_m^*(n) | z_m^*(n) = 1, p_m \in P(v_n)\}. \quad (10)$$

Для дуговых потоков (9) и каждого VMS-вектора $\bar{\mathbf{z}}^*(n)$ (10) вычисляется *загрузка* k -го ребра сети:

$$y_k^*(n) = \sum_{m \in M(n)} (x_{mk}^* + x_{m(k+E)}^*), \quad n = \overline{1, N}. \quad (11)$$

Характеристический SPT-вектор загрузок

$$\bar{\mathbf{y}}^*(n) = (y_1^*(n), \dots, y_k^*(n), \dots, y_E^*(n)), \quad n = \overline{1, N}, \quad (12)$$

определяет распределение загрузки ребер сети при одновременной передаче из узла v_n всех исходящих межузловых VMS-потоков $z_m^* = 1, m \in M(n)$.

5 Анализ распределения реберных загрузок

Вычислительные эксперименты проводились на моделях сетевых систем, представленных на рис. 1. В каждой сети имеются 69 узлов. Пропускные способности ребер $d_k(0)$ равномерно распределены на отрезке $[900, 999]$. В ходе исследования была сделана нормировка, и потому суммарная пропускная способность в обеих сетях одинакова:

$$\sum_{k=1}^E d_k(0) = D(0) = 68\,256.$$

Для характеристических векторов $y^*(n)$ и $y^0(n)$ оценивалось распределение загрузки ребер сети при

передаче в монопольных режимах нормированных VMS-векторов потоков $\bar{\mathbf{z}}^*(n)$ и $\bar{\mathbf{z}}^0(n)$. Согласно (6) и (11), для каждого $n = \overline{1, N}$ подсчитываются значения компонент $y_k^*(n)$ и $y_k^0(n)$, $k = \overline{1, E}$, и длина (норма) векторов $\bar{\mathbf{y}}^*(n)$ и $\bar{\mathbf{y}}^0(n)$:

$$|\bar{\mathbf{y}}^{(\cdot)}(n)| = \left[\sum_{k=1}^E (y_k^{(\cdot)}(n))^2 \right]^{1/2}, \quad n = \overline{1, N}.$$

Вычисляется средняя загрузка ребра при передаче потока $\bar{\mathbf{z}}^{(\cdot)}(n)$:

$$\tilde{y}^{(\cdot)}(n) = \frac{1}{E} \sum_{k=1}^E y_k^{(\cdot)}(n), \quad n = \overline{1, N}.$$

Величина $\tilde{y}^{(\cdot)}(n)$ — среднее значение загрузки ребра при одновременной передаче из узла v_n нормированного вектора мультипотока $\bar{\mathbf{z}}^{(\cdot)}(n)$ всем адресатам в монопольном режиме по SPT- или MFT-маршрутам соответственно. Определяется среднеквадратичное отклонение

$$\sigma^{(\cdot)}(n) = \left[\frac{1}{E} \sum_{k=1}^E (y_k^{(\cdot)}(n) - \tilde{y}^{(\cdot)}(n))^2 \right]^{1/2}, \quad n = \overline{1, N}.$$

Диаграммы на рис. 2 характеризуют норму векторов загрузок в базовой и кольцевой сетях. По вертикальной оси откладываются значения $|\bar{\mathbf{y}}^*(n)|$, а по горизонтальной — $|\bar{\mathbf{y}}^0(n)|$ для узла v_n . Точки на диаграмме соответствуют вершинам. На рис. 2, *а* для базовой сети точки лежат ниже биссектрисы первого ортанта, поскольку при передаче максимального потока используются обходные пути с большим числом ребер. В кольцевой сети 2, *б* присутствует больше ребер, меньше разброс в длине маршрутов передачи потоков, поэтому по сравнению с рис. 2, *а* точки на рис. 2, *б* располагаются ближе к биссектрисе и началу координат.

Диаграммы на рис. 3 дают возможность сравнивать SPT- и MFT-стратегии для базовой и коль-

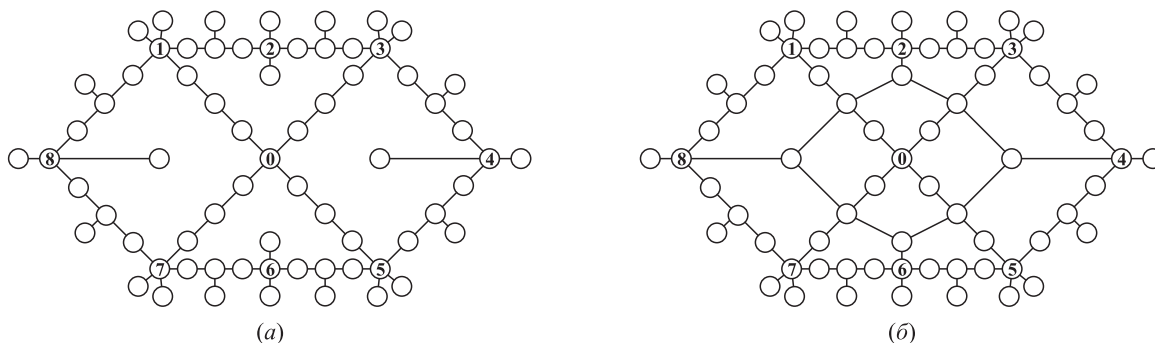


Рис. 1 Базовая (а) и кольцевая (б) сети

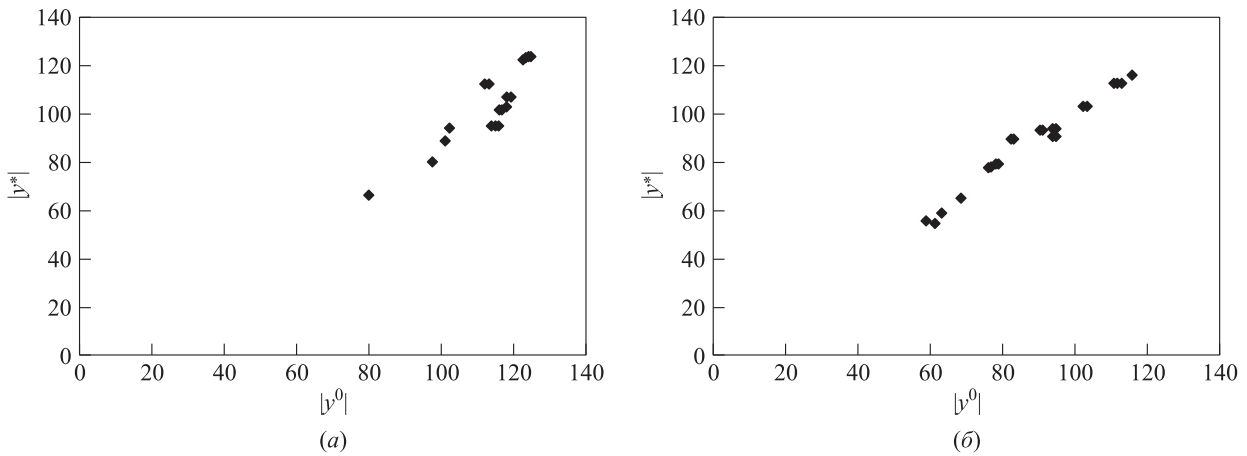


Рис. 2 Норма векторов нагрузок в базовой (а) и кольцевой (б) сетях

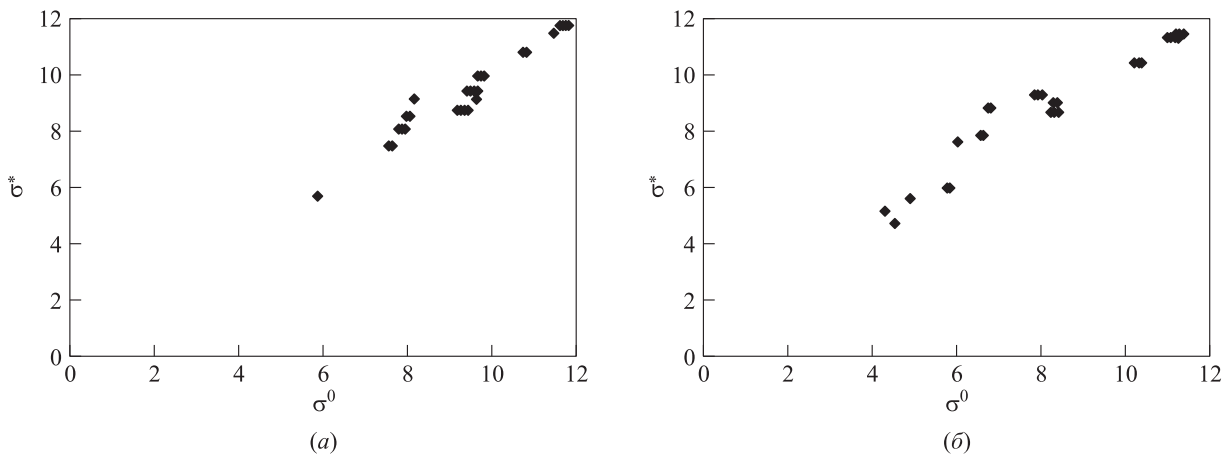


Рис. 3 Среднеквадратичное отклонение загрузки при различных способах маршрутизации в базовой (а) и кольцевой (б) сетях

цевой сетей. По вертикальной оси откладываются значения $\sigma^*(n)$ при передаче нормированного вектора потоков $\vec{z}^*(n)$ из узла v_n при SPT-маршрутизации, по горизонтальной — $\sigma^0(n)$ при MFT-маршрутизации. Точки на диаграммах отвечают вершинам сети. На рис. 3, а для базовой сети точки расположены вблизи биссектрисы, и нельзя говорить о доминировании одного из способов маршрутизации. На рис. 3, б для кольцевой сети можно увидеть, что SPT-маршрутизация приводит к большему разбросу значений загрузки.

Для оценки возможных нагрузок при смешанных стратегиях маршрутизации используется выпуклая комбинация характеристических векторов $\vec{y}^0(n)$ и $\vec{y}^*(n)$:

$$\begin{aligned}\vec{y}(\gamma(n)) &= \gamma(n)\vec{y}^0(n) + (1 - \gamma(n))\vec{y}^*(n) = \\ &= \vec{y}^*(n) + \gamma(n)(\vec{y}^0(n) - \vec{y}^*(n)), \\ 0 &\leq \gamma(n) \leq 1, \quad n = \overline{1, N}.\end{aligned}$$

Вектор $\vec{y}(\gamma(n))$ характеризует нагрузки при использовании смешанной стратегии маршрутизации (далее — MIXT-вектор нагрузок, от английского mixed transmission).

Для смешанной стратегии маршрутизации — MIXT-вектора нагрузок — вычисляется значение $\gamma^+(n)$, при котором достигается минимальная величина оценки среднеквадратичного отклонения.

Задача 2. Для каждого n найти $\gamma^+(n)$, при котором достигается

$$\sigma(\gamma^+(n)) = \min_{0 \leq \gamma(n) \leq 1} \sigma(\gamma(n)), \quad n = \overline{1, N}.$$

Значения $\gamma^+(n)$, $n = \overline{1, N}$, упорядочиваются по величине от большего к меньшему и перенумеровываются согласно порядку: $\{\gamma^+(i)\}$: $\gamma^+(i) \geq \gamma^+(i+1)$, $i = \overline{1, N-1}$. На рис. 4 представлены диаграммы для базовой и кольцевой сетей. По горизонтальной

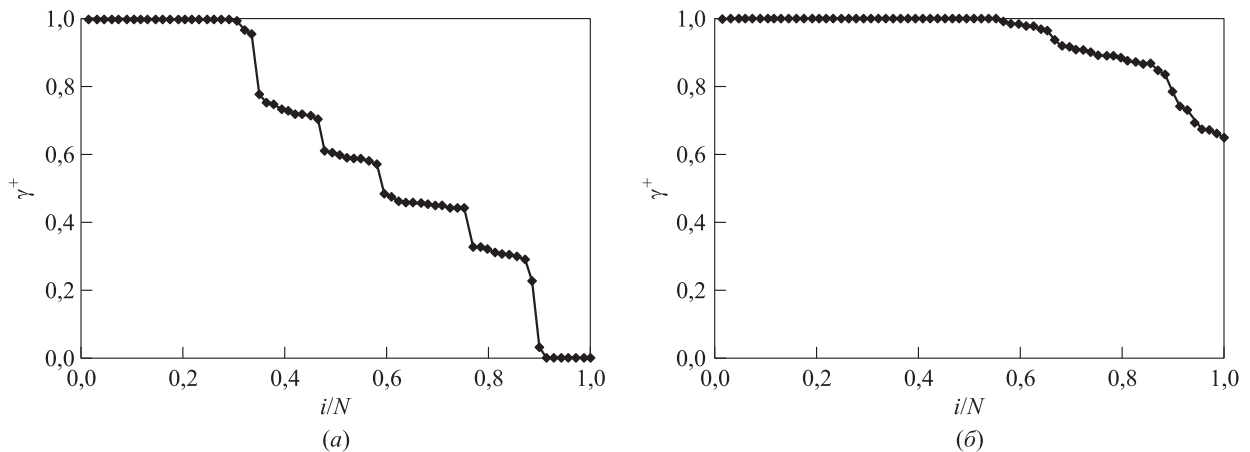


Рис. 4 Значения $\gamma^+(n)$, при которых достигается минимальная величина оценки среднеквадратичного отклонения в базовой (а) и кольцевой (б) сетях

оси откладываются относительные номера i/N , по вертикальной — значения $\gamma^+(i)$.

На рис. 4, а для базовой сети минимальное значение $\sigma(\gamma)$ достигается для 35% узлов при использовании монопольной MFT-стратегии и для 20% при выборе SPT-стратегии. Для 45% вершин минимальное значение $\sigma(\gamma)$ реализуется для $0 < \gamma^+(n) < 1$, что соответствует смешанной стратегии.

На рис. 4, б для кольцевой сети для почти 60% узлов использование монопольной MFT-стратегии приводит к минимальному разбросу реберной загрузки. Кроме того, в кольцевой сети значение γ^+ превосходит 0,6 для всех узлов. Таким образом, вклад SPT-стратегии при формировании смешанной стратегии невелик. Как следует из рис. 3, разброс $\sigma(n)$ для кольцевой сети достаточно мал, анализ значений γ^+ дает возможность отследить эту разницу и сравнить стратегии.

Для каждого узла определяется коэффициент вариации при передаче нормированного мультипотока $\bar{z}^{(\cdot)}(n)$:

$$\mu^{(\cdot)}(n) = \frac{\sigma^{(\cdot)}(n)}{\bar{y}^{(\cdot)}(n)}, \quad n = \overline{1, N}.$$

На рис. 5 представлены диаграммы коэффициента вариации для базовой и кольцевой сетей. По горизонтальной оси откладываются значения $\mu^0(n)$, по вертикальной — $\mu^*(n)$. Точки на диаграммах соответствуют узлам сети.

Из диаграмм рис. 5 как для базовой, так и для кольцевой сетей видно, что отклонения при SPT-стратегии значительно больше, чем при MFT-стратегии. Маршрутизация SPT использует меньше ребер, вследствие чего суммарная нагрузка также оказывается меньше. На диаграммах большинство точек-узлов лежит выше биссектрисы, хотя среднеквадратичные значения почти совпадают.

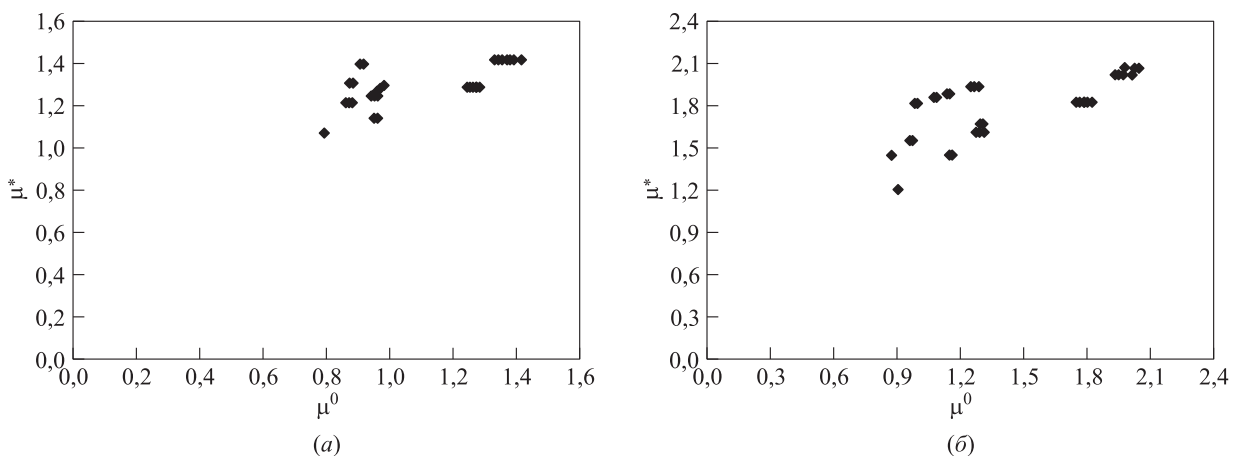


Рис. 5 Коэффициент вариации для базовой (а) и кольцевой (б) сетей

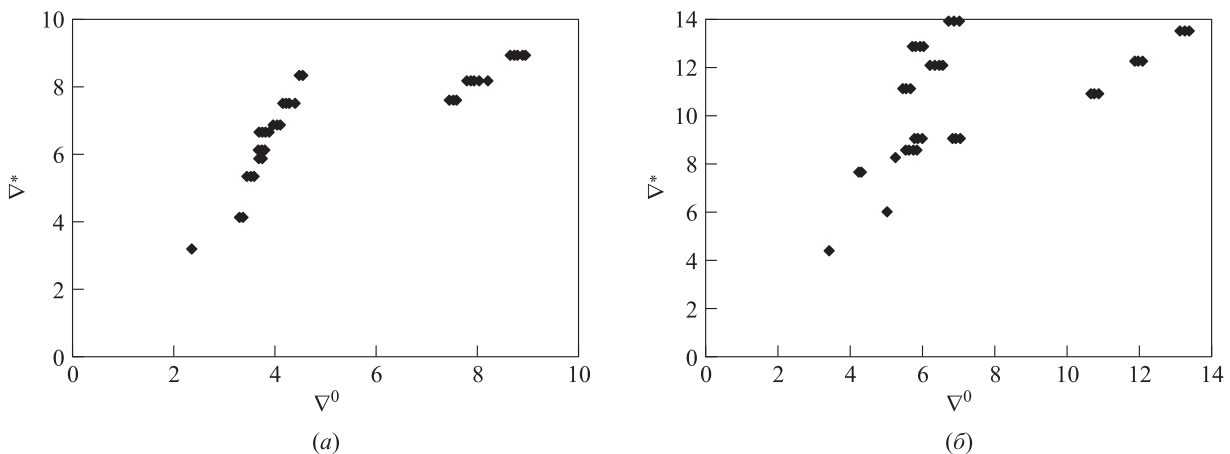


Рис. 6 Максимальные превышения загрузки ребер в базовой (а) и кольцевой (б) сетях

Для каждого характеристического вектора $\vec{y}^*(n)$ и $\vec{y}^0(n)$ ((7), (12)) для каждого узла определяется коэффициент максимального превышения загрузки ребер (далее — МЕХ-превышение, от английского *max excess*) при передаче нормированного мультипотока $\vec{z}^{(\cdot)}(n)$:

$$\nabla^{(\cdot)}(n) = \max_{k=1, E} \left[\frac{y_k^{(\cdot)}(n)}{\tilde{y}^{(\cdot)}(n)} \right], \quad n = \overline{1, N}.$$

Безразмерная относительная величина МЕХ-превышения показывает, во сколько раз максимальная реберная нагрузка превышает среднее значение характеристического вектора для данного узла при различных стратегиях.

На рис. 6 представлены диаграммы МЕХ-превышений для базовой и кольцевой сетей. По горизонтальной оси откладываются значения $\nabla^0(n)$, по вертикальной — значения $\nabla^*(n)$. Точки на диаграммах соответствуют узлам сети. Приведенные диаграммы позволяют проследить, как меняются перегрузки при различных стратегиях маршрутизации. Из диаграмм рис. 6 следует, что как для базовой, так и для кольцевой сети существует большое число узлов, для которых значения $\nabla^*(n)$ значительно превышают $\nabla^0(n)$. При передаче нормированного мультипотока с единичными компонентами из таких узлов существуют ребра с большой нагрузкой. На рис. 6, б для кольцевой сети точки-узлы значительно удалены от биссектрисы, поскольку средние значения меньше, а кратчайшие пути содержат меньше ребер. На рис. 6, а для базовой сети разброс точек-узлов не так велик, но все же значителен.

позволили осуществить детальный сравнительный анализ распределения реберных нагрузок. Результаты показали, что для некоторых групп узлов более эффективны монопольные стратегии, а для других наилучшие показатели удается получить с помощью смешанных схем маршрутизации. Характеристические векторы — нагрузка ребер — заметно отличаются при различных способах маршрутизации. Использовались различные параметры оценки разброса величины компонент каждого характеристического вектора. Разброс численных значений коэффициента вариации дает возможность точнее разделить узлы на отдельные группы по нагрузке на сеть, особенно при SPT-стратегиях. При вычислении максимального превышения для компонент характеристических векторов были найдены ребра с нагрузкой, на порядок большей, чем средний показатель по сети. На практике такие ребра можно рассматривать как «узкое место» при передаче соответствующего потока.

Полученные агрегированные значения параметров для разных характеристических векторов позволяют анализировать сетевую систему при передаче всех нормированных единичных мультипотоков из всех узлов всем адресатам одновременно. Представленные результаты лежат в русле работ [7–12], предлагаются различные модели распределения потоков и подходы к анализу пропускной способности.

Литература

1. Малашенко Ю.Е., Назарова И.А. Сравнительный анализ узловых мультипотоков в многопользовательской сетевой системе // Информатика и её применения, 2024. Т. 18. Вып. 1. С. 40–45. doi: 10.14357/19922264240106. EDN: AKCMCQ.

6 Заключение

Вычислительные эксперименты, проведенные на основе нормированных узловых мультипотоков,

2. Малащенко Ю. Е., Назарова И. А. Агрегированные характеристики монопольных режимов управления узловыми мультипотоками в многопользовательской сетевой системе // Известия РАН. Теория и системы управления, 2026. № 3. С. 102–111.
3. Малащенко Ю. Е., Назарова И. А. Анализ загрузки многопользовательской сети при расщеплении потоков по кратчайшим маршрутам // Информатика и её применения, 2023. Т. 17. Вып. 3. С. 33–38. doi: 10.14357/19922264230305. EDN: NLUSQJ.
4. Йенсен П., Барнес Д. Потокное программирование / Пер. с англ. — М.: Радио и связь, 1984. 392 с. (Jensen P. A., Barnes J. W. Network flow programming. — New York, NY, USA: Wiley, 1980. 408 p.)
5. Salimifard K., Bigharaz S. The multicommodity network flow problem: State of the art classification, applications, and solution methods // Operational Research, 2022. Vol. 22. P. 1–47. doi: 10.1007/s12351-020-00564-8. EDN: MPJHZO.
6. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ / Пер. с англ. — 3-е изд. — М.: Вильямс, 2013. 1328 с. (Cormen T. H., Leiserson C. I., Rivest R. L., Stein C. Introduction to algorithms. — 3rd ed. — Cambridge, MA, USA: The MIT Press, 2009. 1313 p.)
7. Аду К. И. Б., Маркова Е. В., Гайдамака Ю. В., Шоргин С. Я. Анализ схемы доступа с прерыванием при нарезке радиоресурсов сети пятого поколения // Информатика и её применения, 2023. Т. 17. Вып. 1. С. 96–106. doi: 10.14357/19922264230113. EDN: TNKSWK.
8. Самуйлов А. К., Платонова А. А., Шоргин В. С., Гайдамака Ю. В. К моделированию эффектов обслуживания многоадресного трафика в сетях 5G NR // Информатика и её применения, 2023. Т. 17. Вып. 2. С. 71–77. doi: 10.14357/19922264230210. EDN: SLMGZU.
9. Острикова Д. Ю., Голос Е. С., Бесчастный В. А., Мачнев Е. А., Шоргин В. С., Гайдамака Ю. В. Метод оценки характеристик систем 5G/6G «новое радио» с учетом макро- и микромобильности пользователей // Информатика и её применения, 2024. Т. 18. Вып. 2. С. 32–39. doi: 10.14357/19922264240205. EDN: JCUFHS.
10. Голосов П. Е. Об управлении задачами с ограничениями в условиях неопределенности // Автоматизация процессов управления, 2024. № 3. С. 102–110. doi: 10.35752/1991-2927_2024_3_77_102. EDN: LOBIYO.
11. Gostev I. M., Golosov P. E. Efficiency Analysis of a simulation model of cloud computing in the case of multiple server failures // Program. Comput. Soft., 2024. Vol. 50. Iss. S2. P. S128–S133. doi: 10.1134/S0361768824700518. EDN: DOXODF.
12. Сопин Э. С., Назарьин А. И., Шоргин С. Я. Разработка модели для расчета производительности планирования передач в сетях 5G NR с учетом сигнального трафика // Информатика и её применения, 2025. Т. 19. Вып. 3. С. 46–54. doi: 10.14357/19922264250306. EDN: EMAQVK.

Поступила в редакцию 10.04.2026

Принята к публикации 15.08.2026

MULTIUSER NETWORK LOAD ANALYSIS UNDER MIXED ROUTING STRATEGIES

Yu. E. Malashenko, I. A. Nazarova, and M. V. Kozlov

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: Within computational experiments, monopolistic and mixed routing strategies for outgoing nodal multiflows in multiuser network systems are studied. Two basic monopolistic dispatching schemes for internodal flows are analyzed: routing along shortest paths and routing along maximum flow transmission paths. For each strategy, normalized vectors of outgoing multiflows — transmitted in a monopolistic mode from every source node to all destination nodes — are formulated. The characteristic vectors of edge loading are determined when normalized multiflows from source vertices pass through the network. To evaluate network performance under mixed dispatching strategies, convex combinations of these characteristic vectors are constructed. For all characteristic vectors, the standard deviations of component values, the relative coefficients of variation, and the magnitude of the maximum excess of the average edge loading level are calculated. A comparative analysis of the aggregated functional indicators for each node and the proposed routing methods is carried out. The impact of nodal multiflows on overall network load is investigated and potential overload points and bottlenecks are identified. The experimental results are illustrated using specialized diagrams.

Keywords: multicommodity flow model; outgoing nodal multiflow; network load distribution

DOI: 10.14357/19922264260305

EDN: OIVGUK

References

1. Malashenko, Yu. E., and I. A. Nazarova. 2024. Sravnitel'nyy analiz uzlovykh mul'tipotokov v mnogopol'zovatel'skoy setevoy sisteme [Analysis of node multiflows in a multiuser network system]. *Informatika i ee Primeneniya — Inform. Appl.* 18(1):40–45. doi: 10.14357/19922264240106. EDN: AKCMCQ.
2. Malashenko, Yu. E., and I. A. Nazarova. 2026. Aggregated characteristics of monopoly control modes for nodal multiflows in a multiuser network system. *J. Comput. Sys. Sc. Int.* 65(3).
3. Malashenko, Yu. E., and I. A. Nazarova. 2023. Analiz zagruzki mnogopol'zovatel'skoy seti pri rasshcheplenii potokov po kratchayshim marshrutam [Multiuser network load analysis by splitting flows along the shortest routes]. *Informatika i ee Primeneniya — Inform. Appl.* 17(3):33–38. doi: 10.14357/19922264230305. EDN: NLUSQJ.
4. Jensen, P. A., and J. W. Barnes. 1980. *Network flow programming*. New York, NY: Wiley. 408 p.
5. Salimifard, K., and S. Bigharaz. 2020. The multicommodity network flow problem: State of the art classification, applications, and solution methods. *Operational Research* 22(1):1–47. doi: 10.1007/s12351-020-00564-8. EDN: MPJHZO.
6. Cormen, T. H., C. I. Leiserson, R. L. Rivest, and C. Stein. 2009. *Introduction to algorithms*. 3rd ed. Cambridge, MA: The MIT Press. 1313 p.
7. Adou, K. Y. B., E. V. Markova, Yu. V. Gaidamaka, and S. Ya. Shorgin. 2023. Analiz skhemy dostupa s preryvaniem pri narezke radioresursov seti pyatogo pokoleniya [Preemption-based prioritization scheme for network resources slicing in 5G systems]. *Informatika i ee Primeneniya — Inform. Appl.* 17(1):96–106. doi: 10.14357/19922264230113. EDN: TNKSWK.
8. Samoylov, A. K., A. A. Platonova, V. S. Shorgin, and Yu. V. Gaidamaka. 2023. K modelirovaniyu effektivov ob-sluzhivaniya mnogoadresnogo trafika v setyakh 5G NR [On modeling the effects of multicast traffic servicing in 5G NR networks]. *Informatika i ee Primeneniya — Inform. Appl.* 17(2):71–77. doi: 10.14357/19922264230210. EDN: SLMGZU.
9. Ostrikova, D. Yu., E. S. Golos, V. A. Beschastnyi, E. A. Machnev, V. S. Shorgin, and Yu. V. Gaidamaka. 2024. Metod otsenki kharakteristik sistem 5G/6G “novoe radio” s uchetom makro- i mikromobil'nosti pol'zovateley [Assessing the characteristics of 5G/6G “new radio” systems with user's macro- and micromobility]. *Informatika i ee Primeneniya — Inform. Appl.* 18(2):32–39. doi: 10.14357/19922264240205. EDN: JCUFHS.
10. Golosov, P. E. 2024. Ob upravlenii zadachami s ogranicheniyami v usloviyakh neopredelennosti [The management of constrained tasks under uncertainty]. *Avtomatizatsiya protsessov upravleniya* [Automation of Control Processes] 3(77):102–110. doi: 10.35752/1991-2927_2024_3_77_102. EDN: LOBIYO.
11. Gostev, I. M., and P. E. Golosov. 2024. Efficiency analysis of a simulation model of cloud computing in the case of multiple server failures. *Program. Comput. Soft.* 50(S2):S128–S133. doi: 10.1134/S0361768824700518. EDN: DOXODE.
12. Sopin, E. S., A. I. Nazarin, and S. Ya. Shorgin. 2025. Razrabotka modeli dlya rascheta proizvoditel'nosti planirovaniya peredach v setyakh 5G NR s uchetom signal'nogo trafika [Model development for performance of transmission scheduling in 5G New Radio networks under signaling and user traffic constraints]. *Informatika i ee Primeneniya — Inform. Appl.* 19(3):46–54. doi: 10.14357/19922264250306. EDN: EMAQVK.

Received April 10, 2026

Accepted August 15, 2026

Contributors

Malashenko Yuri E. (b. 1946) — Doctor of Science in physics and mathematics, senior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; malash09@ccas.ru

Nazarova Irina A. (b. 1966) — Candidate of Science (PhD) in physics and mathematics, scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; irina-nazar@yandex.ru

Kozlov Mihail V. (b. 1958) — senior mathematician, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; kztm2@ccas.ru

ИНТЕРПРЕТАЦИЯ КЛАСТЕРНОЙ СТРУКТУРЫ ДАННЫХ НА ОСНОВЕ ЭЛЛИПСОИДОВ

М. П. Кривенко¹

Аннотация: Рассматриваются эквивалентные определения эллипсоидов, а также постановки задач аналитической геометрии, нацеленные на интерпретацию кластерной структуры данных. Дается обоснование алгоритмов их решения. Обсуждаются два примера из области анализа данных. В их основе лежит модель смеси нормальных распределений. Для интерпретации кластеров данных, соответствующих элементам смеси, привлекаются эллипсоиды. Первый пример посвящен моделированию референсных значений путем описания эмпирического распределения многомерных данных о пациентах, включающих возраст и измерения биомаркеров PSA (Prostate-Specific Antigen). Предложенные решения на базе смеси демонстрируют отчетливые преимущества, а также позволяют напрямую использовать методы визуализации на основе эллипсов для выявления специфических особенностей объекта исследований. Во втором примере рассматривается консолидирующий метод анализа лонгитюдных данных, когда серия многомерных характеристик некоторого объекта составляет единый вектор наблюдаемых значений. Для демонстрации появляющихся возможностей анализа данных решается задача ранней диагностики рака с использованием биомаркеров PSA. Преимущество консолидирующего метода подтверждается с помощью высокой степени отделимости наборов кластеров-элементов смеси, измеренной числом попарных пересечений соответствующих эллипсоидов. Анализ степени пересеченности наборов эллипсоидов для различных классов диагнозов может также стать источником для выявления вклада отдельных кластеров данных в ошибки классификации.

Ключевые слова: смесь нормальных распределений; представление эллипсоидов; алгоритмы обработки эллипсоидов; референсные значения; классификация серийных данных; лонгитюдный анализ; консолидирующий подход

DOI: 10.14357/19922264260306

EDN: YSZTCG

1 Введение

При классификации данных и аппроксимации их распределений важную роль играет модель конечной смеси распределений, когда n -мерная плотность распределения представима в виде

$$f(\mathbf{x}) = \sum_{j=1}^k p_j g(\mathbf{x}, \boldsymbol{\vartheta}_j).$$

В этой модели неизвестными могут быть все или часть следующих характеристик (параметров смеси): число k элементов смеси, а также вероятности p_j появления и параметры $\boldsymbol{\vartheta}_j$ распределений элементов смеси. В ходе исследовательского (разведочного) этапа анализа n -мерных данных, как правило, в качестве $g(\mathbf{x}, \boldsymbol{\vartheta}_j)$ принимается нормальная плотность, т. е.

$$g(\mathbf{x}, \boldsymbol{\vartheta}_j) = \varphi(\mathbf{x}, \boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j).$$

Общие вопросы построения и применения модели смеси, описание подходов к оцениванию ее параметров, изложение алгоритмов обработки данных представлены в ряде источников. Данная работа

нацелена на формирование первоначального представления о структуре совокупности выявленных групп данных — кластеров, отвечающих отдельным элементам смеси, и посвящена приемам интерпретации получающихся результатов анализа данных. Поэтому ключевыми из имеющихся публикаций оказываются [1–5].

Для характеристики отдельного j -го кластера предлагается использовать поверхность с равными для ее точек значениями плотности распределения вида

$$\frac{1}{(2\pi)^{n/2} |\boldsymbol{\Sigma}_j|^{1/2}} \exp \left(-(\mathbf{x} - \boldsymbol{\mu}_j)^T \boldsymbol{\Sigma}_j^{-1} \frac{\mathbf{x} - \boldsymbol{\mu}_j}{2} \right) = \text{const}$$

или, что то же самое, при некотором ρ

$$(\mathbf{x} - \boldsymbol{\mu}_j)^T \boldsymbol{\Sigma}_j^{-1} (\mathbf{x} - \boldsymbol{\mu}_j) = \rho, \quad \rho > 0. \quad (1)$$

Если для нормального распределения задаться вероятностью $P \in (0, 1)$ попадания в область, ограниченную поверхностью (1), то параметр ρ находится из уравнения

$$\Pr \{ \chi_n^2 \leq \rho \} = P,$$

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, mkkrivenko@ipiran.ru

где χ_n^2 — случайная величина, имеющая хи-квадрат-распределение с n степенями свободы. Поверхность вида (1) носит название эллипсоида равной плотности распределения (или просто эллипсоида равной вероятности).

2 Эквивалентные определения эллипсоида

В качестве основы удобнее принять определение n -мерного эллипсоида $\mathbb{E}$ в виде

$$\mathbb{E} \equiv (\mathbf{x} - \mathbf{c})^T \mathbf{A} (\mathbf{x} - \mathbf{c}) \leq 1,$$

где $\mathbf{A} \succ 0$, т. е. положительно определена. Если при этом $\mathbf{A}$ — несимметричная матрица, то, рассмотрев симметричную матрицу $(1/2)(\mathbf{A} + \mathbf{A}^T)$, которая также положительно определена, получим, что левая часть останется без изменений после замены $\mathbf{A}$ на $(1/2)(\mathbf{A} + \mathbf{A}^T)$. Таким образом, можно считать, что в определениях эллипсоида матрица $\mathbf{A}$ не только положительно определенная, но и симметричная.

В случае нормального распределения j -го элемента смеси для совокупности внутренних точек эллипсоида равной вероятности примем обозначение:

$$\mathbb{E}_\rho \equiv (\mathbf{x} - \mathbf{c})^T \mathbf{A} (\mathbf{x} - \mathbf{c}) \leq \rho,$$

где $\mathbf{A} = \Sigma_j^{-1}$, $\mathbf{c} = \mu_j$. Такое определение $\mathbb{E}_\rho$ эквивалентно $\mathbb{E}$ и указывает на связь с нормальным распределением, уточняя область его использования.

Приведем другие эквивалентные формы записи эллипсоидов. Интересные сами по себе, они играют важную роль при получении теоретических результатов и выработке рекомендаций вычислительного характера, позволяют корректно интерпретировать совокупности эллипсоидов равной вероятности.

Для симметричной положительно определенной матрицы $\mathbf{A}$ существует спектральное разложение

$$\mathbf{A} = \mathbf{Q} \Sigma^2 \mathbf{Q}^T,$$

где $\mathbf{Q} \mathbf{Q}^T = \mathbf{I}$; $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_n)$ при $\sigma_i > 0 \forall i$. Тогда после подстановки разложения $\mathbf{A}$ имеем:

$$\mathbb{E} \equiv \{\mathbf{x} | (\mathbf{x} - \mathbf{c})^T \mathbf{Q} \Sigma^2 \mathbf{Q}^T (\mathbf{x} - \mathbf{c}) \leq 1\} \quad (2)$$

или

$$\mathbb{E} \equiv \{\mathbf{x} | \|\Sigma \mathbf{U}^T (\mathbf{x} - \mathbf{c})\| \leq 1\}.$$

Обозначив $\mathbf{w} = \Sigma \mathbf{Q}^T (\mathbf{x} - \mathbf{c})$, получаем

$$\mathbb{E} \equiv \{\mathbf{x} | \mathbf{x} = \mathbf{c} + \mathbf{Q} \Sigma^{-1} \mathbf{w}, \|\mathbf{w}\| \leq 1\}. \quad (3)$$

В более общем виде: если $\mathbf{A}$ представима с помощью невырожденной квадратной матрицы $\mathbf{B}$ в виде

$$\mathbf{A} = \mathbf{B} \mathbf{B}^T,$$

а сингулярное разложение $\mathbf{B}$ есть

$$\mathbf{B} = \mathbf{Q} \Sigma \mathbf{V}^T,$$

то

$$\mathbf{A} = \mathbf{Q} \Sigma^2 \mathbf{Q}^T,$$

Тогда в терминах матрицы $\mathbf{B}$ с учетом обозначения $\mathbf{B}^{-T} = (\mathbf{B}^{-1})^T = (\mathbf{B}^T)^{-1}$ соотношения (2) и (3) принимают вид:

$$\left. \begin{aligned} \mathbb{E} &\equiv \{\mathbf{x} | (\mathbf{x} - \mathbf{c})^T \mathbf{B} \mathbf{B}^T (\mathbf{x} - \mathbf{c}) \leq 1\}; \\ \mathbb{E} &\equiv \{\mathbf{x} | \|\mathbf{B}^T (\mathbf{x} - \mathbf{c})\| \leq 1\}; \\ \mathbb{E} &\equiv \{\mathbf{x} | \mathbf{x} = \mathbf{c} + \mathbf{B}^{-T} \mathbf{w}, \|\mathbf{w}\| \leq 1\} \end{aligned} \right\} \quad (4)$$

после замены $\mathbf{w} = \mathbf{B}^T (\mathbf{x} - \mathbf{c})$.

Матрица $\mathbf{B}$ может быть факторизована как

$$\mathbf{B} = \mathbf{L} \mathbf{Q},$$

где $\mathbf{L}$ — нижняя треугольная матрица с положительными диагональными элементами, а $\mathbf{Q}$ — ортогональная. Тогда

$$\mathbf{A} = \mathbf{B} \mathbf{B}^T = \mathbf{L} \mathbf{L}^T,$$

что дает факторизацию Холецкого. Соответственно, действуют эквивалентные определения эллипсоидов:

$$\mathbb{E} \equiv \{\mathbf{x} | (\mathbf{x} - \mathbf{c})^T \mathbf{L} \mathbf{L}^T (\mathbf{x} - \mathbf{c}) \leq 1\};$$

$$\mathbb{E} \equiv \{\mathbf{x} | \|\mathbf{L}^T (\mathbf{x} - \mathbf{c})\| \leq 1\};$$

$$\mathbb{E} \equiv \{\mathbf{x} | \mathbf{x} = \mathbf{c} + \mathbf{L}^{-T} \mathbf{w}, \|\mathbf{w}\| \leq 1\}$$

после замены $\mathbf{w} = \mathbf{B}^T (\mathbf{x} - \mathbf{c})$.

Смысл приведенных вариаций в том, что с вычислительной точки зрения более эффективно использовать представление эллипсоида с помощью представления Холецкого в терминах $\mathbf{c}$ и $\mathbf{L}$, а также хранить $\mathbf{L}$ в упакованном формате. Если эллипсоид $\mathbb{E}_1$, заданный с помощью $\mathbf{c}_1$ и $\mathbf{L}_1$, модифицируется так, чтобы получить эллипсоид $\mathbb{E}_2$, определяемый через $\mathbf{c}_2$ и $\mathbf{B}_2$ (т. е. полную матрицу), то представление в терминах $\mathbf{L}_2$ эффективно и точно вычисляется с помощью LQ-алгоритма. Оказывается, что гораздо точнее получать $\mathbf{L}_2$ по LQ-алгоритму, чем с помощью представления Холецкого для $\mathbf{A} = \mathbf{B}_2 \mathbf{B}_2^T$. Описанные в [6] процедуры используют LQ-алгоритмы и избегают формирования $\mathbf{A}$.

Рассмотрим линейное преобразование данных вида

$$\mathbf{y} = \mathbf{M}^T (\mathbf{x} - \mathbf{b}),$$

где вектор $\mathbf{b}$ и невырожденная квадратная матрица $\mathbf{M}$ заданы. Оно переводит эллипсоид также в эллипсоид. Действительно, если использовать представление (4) и вид обратного преобразования

$$\mathbf{x} = \mathbf{b} + \mathbf{M}^T \mathbf{y},$$

то для получения нужного образа

$$\tilde{\mathbb{E}} \equiv \left\{ \mathbf{y} \mid \|\tilde{\mathbf{B}}^T(\tilde{\mathbf{y}} - \tilde{\mathbf{c}})\| \leq 1 \right\}$$

достаточно в исходное представление внести следующие изменения:

$$\begin{aligned} \mathbf{B}^T(\mathbf{x} - \mathbf{c}) &= \mathbf{B}^T\mathbf{x} - \mathbf{B}^T\mathbf{b} - \mathbf{B}^T\mathbf{c} + \mathbf{B}^T\mathbf{b} = \\ &= \mathbf{B}^T\mathbf{M}^{-T}\mathbf{M}^T(\mathbf{x} - \mathbf{b}) - \mathbf{B}^T\mathbf{M}^{-T}\mathbf{M}^T(\mathbf{c} - \mathbf{b}) = \\ &= \mathbf{B}^T\mathbf{M}^{-T}\mathbf{M}^T(\mathbf{x} - \mathbf{b}) - \mathbf{B}^T\mathbf{M}^{-T}\mathbf{M}^T(\mathbf{c} - \mathbf{b}) = \\ &= (\mathbf{M}^{-1}\mathbf{B})^T (\mathbf{M}^T(\mathbf{x} - \mathbf{b}) - \mathbf{M}^T(\mathbf{c} - \mathbf{b})) \end{aligned}$$

и положить

$$\tilde{\mathbf{B}} \equiv \mathbf{M}^{-1}\mathbf{B}; \quad \tilde{\mathbf{c}} \equiv \mathbf{M}^T(\mathbf{c} - \mathbf{b}).$$

3 Задачи на эллипсоиды

3.1 Экстремальные значения координат эллипсоида

Сначала определим их, решив более общую задачу ортогональной проекции эллипсоида на прямую $\mathbf{L} \equiv \{\mathbf{x} \mid \mathbf{x} = \mathbf{x}_0 + s\mathbf{v}\}$, заданную точкой $\mathbf{x}_0$, направляющим вектором $\mathbf{v}$ и параметром s . Для произвольной точки $\mathbf{x}$ ее ортогональной проекции на прямую $\mathbf{L}$ соответствует параметр

$$s = \frac{\mathbf{v}^T(\mathbf{x} - \mathbf{x}_0)}{\mathbf{v}^T\mathbf{v}}.$$

Если $\mathbf{x}$ принадлежит эллипсоиду

$$\mathbb{E} \equiv \{\mathbf{x} \mid \mathbf{x} = \mathbf{c} + \mathbf{L}^{-T}\mathbf{y}, \|\mathbf{y}\| \leq 1\},$$

то для $\|\mathbf{y}\| \leq 1$

$$s = \frac{\mathbf{v}^T(\mathbf{L}^{-T}\mathbf{y} + \mathbf{c} - \mathbf{x}_0)}{\mathbf{v}^T\mathbf{v}} = s_0 + \mathbf{w}^T\mathbf{y},$$

где $s_0 = \mathbf{v}^T(\mathbf{c} - \mathbf{x}_0)/(\mathbf{v}^T\mathbf{v})$; $\mathbf{w} = \mathbf{L}^{-1}\mathbf{v}/(\mathbf{v}^T\mathbf{v})$. Отсюда следует, что ортогональные проекции соответствуют интервалу

$$[s_-, s_+] = [s_0 - \|\mathbf{w}\|, s_0 + \|\mathbf{w}\|].$$

Полученные результаты позволяют найти ортогональные проекции на оси координат, что дает

границы области, в которую вписан заданный эллипсоид. Эти рамки также можно получить путем прямого решения набора оптимизационных задач. Для этого рассмотрим эллипсоид в виде

$$\mathbb{E}_\rho \equiv (\mathbf{x} - \mathbf{c})^T \mathbf{A}(\mathbf{x} - \mathbf{c}) \leq \rho$$

или

$$\mathbf{u}^T \mathbf{A} \mathbf{u} \leq \rho,$$

где $\mathbf{u} = \mathbf{x} - \mathbf{c}$. Необходимо решить n оптимизационных задач вида $\min_{\mathbf{u}^T \mathbf{A} \mathbf{u} \leq \rho} u_l$. Согласно теореме [7, гл. 1, § 3.2.1] для функции Лагранжа

$$\phi(\mathbf{u}, r, s) = ru_l + s(\mathbf{u}^T \mathbf{A} \mathbf{u} - \rho)$$

существует такой вектор множителей Лагранжа $(r, s) \neq 0$, что для $\phi(\mathbf{u}, r, s)$ и точки локального экстремума $\hat{\mathbf{u}}$ выполняются условия:

— стационарности

$$\left. \frac{\partial \phi}{\partial u_i} \right|_{\hat{\mathbf{u}}} = 0 \text{ или } 2s\mathbf{A}\hat{\mathbf{u}} = -r\mathbf{e}^{(l)}, i = \overline{1, n}, \quad (5)$$

где

$$e_i^{(l)} = \begin{cases} 1, & i = l; \\ 0, & i = \overline{1, l-1}, i = \overline{l+1, n}; \end{cases}$$

— дополняющей нежесткости

$$s(\hat{\mathbf{u}}^T \mathbf{A} \hat{\mathbf{u}} - \rho) = 0; \quad (6)$$

— неотрицательности

$$s \geq 0.$$

Если $r = 0$, то согласно (5) и $s = 0$, что противоречит условию $(r, s) \neq 0$. Следовательно, $r \neq 0$ и можно положить $r = 1$. Пусть $s = 0$ при $r = 1$; это приходит опять же в противоречие с (5) для координаты $e_l^{(l)}$. Таким образом, $r = 1$ и $s \neq 0$. Тогда из (5) следует:

$$\hat{\mathbf{u}} = -\frac{1}{2s} \mathbf{A}^{-1} \mathbf{e}^{(l)}. \quad (7)$$

Найдем значение s , подставив (7) в (6):

$$\frac{1}{4s^2} \left(\mathbf{e}^{(l)} \right)^T (\mathbf{A}^{-1})^T \mathbf{A} \mathbf{A}^{-1} \mathbf{e}^{(l)} - \rho = 0,$$

откуда с учетом того, что $(\mathbf{A}^{-1})^T = \mathbf{A}^{-1}$, следует, что

$$s = \sqrt{\frac{\left(\mathbf{e}^{(l)} \right)^T \mathbf{A}^{-1} \mathbf{e}^{(l)}}{4\rho}} = \sqrt{\frac{\mathbf{A}_{ll}^{-1}}{4\rho}},$$

где $\mathbf{A}_{ll}^{-1}$ — элемент матрицы $\mathbf{A}^{-1}$ с индексами (l, l) . В результате из (7) получаем:

$$\hat{\mathbf{u}} = \frac{\mathbf{A}^{-1} \mathbf{e}^{(l)} \sqrt{\rho}}{\sqrt{\mathbf{A}_{ll}^{-1}}}.$$

В векторе $\hat{\mathbf{u}}$ представляет интерес l -я координата, поэтому имеем:

$$\hat{u}_l = -\frac{\mathbf{A}_{ll}^{-1} \sqrt{\rho}}{\sqrt{\mathbf{A}_{ll}^{-1}}} = -\sqrt{\mathbf{A}_{ll}^{-1} \rho}$$

или

$$x_l = c_l - \sqrt{\mathbf{A}_{ll}^{-1} \rho}.$$

Аналогично получается максимальная координата. Таким образом, интервал значений l -й координаты, ограниченный экстремальными значениями, принимает простой вид:

$$|x_l - c_l| \leq \sqrt{\mathbf{A}_{ll}^{-1} \rho}.$$

3.2 Анализ взаимного расположения эллипсоидов

Для двух эллипсоидов $\mathbb{E}_1$ и $\mathbb{E}_2$ требуется определить, пересекаются ли они. Частная двумерная задача о проведении из некоторой точки к эллипсу самого короткого и самого длинного отрезка известна как задача Аполлония (III–II вв. до н. э.) [7, гл. 1, § 2.5].

Воспользуемся тем, что линейное преобразование эллипсоида изоморфно, и переведем исходную задачу в задачу о пересечении опять же двух эллипсоидов, один из которых — единичный шар с центром в точке 0, после чего останется только найти расстояние от точки 0 до ближайшей точки эллипсоида.

Напомним, что для некоторого эллипсоида $\mathbb{E}$ матрица $\mathbf{A}$ — симметричная положительно определенная матрица и для нее имеет место спектральное разложение вида $\mathbf{A} = \mathbf{Q} \mathbf{\Lambda} \mathbf{Q}^T$, где $\mathbf{\Lambda}$ — диагональная матрица с положительными элементами, а $\mathbf{Q}^T \mathbf{Q} = \mathbf{I}$ и, в частности, $\mathbf{Q}^{-T} = \mathbf{Q}$, $\mathbf{Q}^{-1} = \mathbf{Q}^T$.

Для первого эллипсоида $\mathbb{E}_1$ вводится замена переменных $\mathbf{y} = \mathbf{x} - \mathbf{c}_1$, что сводит исследование к задаче о пересечении множеств

$$\mathbf{y}^T \mathbf{A}_1 \mathbf{y} \leq 1$$

и

$$(\mathbf{y} - (\mathbf{c}_2 - \mathbf{c}_1))^T \mathbf{A}_2 (\mathbf{y} - (\mathbf{c}_2 - \mathbf{c}_1)) \leq 1.$$

Для $\mathbf{A}_1$ действует спектральное разложение $\mathbf{A}_1 = \mathbf{Q}_1 \mathbf{\Lambda}_1 \mathbf{Q}_1^T$. Обозначим $\mathbf{B}_1 = \mathbf{\Lambda}_1^{1/2} \mathbf{Q}_1^T$, тогда

$\mathbf{B}_1^{-1} = \mathbf{Q}_1^{-T} \mathbf{\Lambda}_1^{-1/2} = \mathbf{Q}_1 \mathbf{\Lambda}_1^{-1/2}$ и $\mathbf{A}_1 = \mathbf{B}_1^T \mathbf{B}_1$. Сделаем замену $\mathbf{z} = \mathbf{B}_1 \mathbf{y}$ или $\mathbf{y} = \mathbf{B}_1^{-1} \mathbf{z}$. При этом

$$\mathbf{x} - \mathbf{c}_1 = \mathbf{y} = \mathbf{B}_1^{-1} \mathbf{z} = \mathbf{Q}_1^{-T} \mathbf{\Lambda}_1^{-1/2} \mathbf{z} = \mathbf{Q}_1 \mathbf{\Lambda}_1^{-1/2} \mathbf{z}.$$

Здесь если $\mathbf{\Lambda}_1 = \text{diag}(\lambda_1, \dots, \lambda_n)$, то $\mathbf{\Lambda}_1^{-1/2} = (1/\sqrt{\lambda_1}, \dots, 1/\sqrt{\lambda_n})$. Тогда получаем последовательность задач о пересечении:

$$(\mathbf{B}_1^{-1} \mathbf{z})^T \mathbf{A}_1 \mathbf{B}_1^{-1} \mathbf{z} \leq 1$$

и

$$(\mathbf{B}_1^{-1} \mathbf{z} - (\mathbf{c}_2 - \mathbf{c}_1))^T \mathbf{A}_2 (\mathbf{B}_1^{-1} \mathbf{z} - (\mathbf{c}_2 - \mathbf{c}_1)) \leq 1;$$

$$\mathbf{z}^T \mathbf{B}_1^{-T} \mathbf{A}_1 \mathbf{B}_1^{-1} \mathbf{z} \leq 1$$

и

$$(\mathbf{z} - \mathbf{B}_1(\mathbf{c}_2 - \mathbf{c}_1))^T \mathbf{B}_1^{-T} \mathbf{A}_2 \mathbf{B}_1^{-1} (\mathbf{z} - \mathbf{B}_1(\mathbf{c}_2 - \mathbf{c}_1)) \leq 1;$$

$$\mathbf{z}^T \mathbf{z} \leq 1$$

и

$$(\mathbf{z} - \mathbf{c}_{21})^T \mathbf{A}_{21} (\mathbf{z} - \mathbf{c}_{21}) \leq 1,$$

где

$$\mathbf{c}_{21} = \mathbf{B}_1(\mathbf{c}_2 - \mathbf{c}_1),$$

$$\begin{aligned} \mathbf{A}_{21} &= \mathbf{B}_1^{-T} \mathbf{A}_2 \mathbf{B}_1^{-1} = \\ &= (\mathbf{Q}_1^{-T} \mathbf{\Lambda}_1^{-1/2})^T \mathbf{A}_2 \mathbf{Q}_1^{-T} \mathbf{\Lambda}_1^{-1/2} = \\ &= \mathbf{\Lambda}_1^{-1/2} \mathbf{Q}_1^{-1} \mathbf{A}_2 \mathbf{Q}_1^{-T} \mathbf{\Lambda}_1^{-1/2} = \\ &= \mathbf{\Lambda}_1^{-1/2} \mathbf{Q}_1^T \mathbf{A}_2 \mathbf{Q}_1 \mathbf{\Lambda}_1^{-1/2}. \end{aligned}$$

Проверим свойства матрицы

$$\mathbf{A}_{21} = (\mathbf{B}_1^{-1})^T \mathbf{A}_2 \mathbf{B}_1^{-1}.$$

Из следующих равенств:

$$\begin{aligned} \mathbf{A}_{21}^T &= ((\mathbf{B}_1^{-1})^T \mathbf{A}_2 \mathbf{B}_1^{-1})^T = \\ &= (\mathbf{B}_1^{-1})^T \mathbf{A}_2^T \mathbf{B}_1^{-1} = (\mathbf{B}_1^{-1})^T \mathbf{A}_2 \mathbf{B}_1^{-1} = \mathbf{A}_{21} \end{aligned}$$

получаем, что $\mathbf{A}_{21}$ — симметричная матрица. Далее, для произвольного $\mathbf{x}$ имеем:

$$\begin{aligned} \mathbf{x}^T \mathbf{A}_{21} \mathbf{x} &= \mathbf{x}^T (\mathbf{B}_1^{-1})^T \mathbf{A}_2 \mathbf{B}_1^{-1} \mathbf{x} = \\ &= (\mathbf{B}_1^{-1} \mathbf{x})^T \mathbf{A}_2 (\mathbf{B}_1^{-1} \mathbf{x}) \geq 0, \end{aligned}$$

так как $\mathbf{A}_2$ — положительно определенная матрица, а $\mathbf{B}_1$ — невырожденная. Таким образом, $\mathbf{A}_{21}$ — симметричная и положительно определенная матрица. Следовательно, для нее существует спектральное разложение $\mathbf{A}_{21} = \mathbf{Q}_{21} \mathbf{\Lambda}_{21} \mathbf{Q}_{21}^T$.

Сделаем замену $z = Q_{21}u$. При этом

$$\begin{aligned} x = y + c_1 &= B_1^{-1}z + c_1 = B_1^{-1}Q_{21}u + c_1 = \\ &= Q_1\Lambda_1^{-1/2}Q_{21}u + c_1. \end{aligned}$$

Тогда получаем последовательность задач о пересечении двух эллипсоидов:

$$u^T Q_{21}^T Q_{21} u \leq 1$$

и

$$\begin{aligned} (Q_{21}u - c_{21})^T A_{21} (Q_{21}u - c_{21}) &\leq 1; \\ u^T u &\leq 1 \end{aligned}$$

и

$$\begin{aligned} (u - Q_{21}^T c_{21})^T Q_{21}^T A_{21} Q_{21} (u - Q_{21}^T c_{21}) &\leq 1; \\ u^T u &\leq 1 \end{aligned}$$

и

$$\begin{aligned} (u - Q_{21}^T c_{21})^T A_{21} (u - Q_{21}^T c_{21}) &\leq 1; \\ u^T u &\leq 1 \end{aligned}$$

и

$$(u - c_{22})^T A_{21} (u - c_{22}) \leq 1,$$

где $c_{22} = Q_{21}^T c_{21}$. Последняя задача о пересечении шара и эллипсоида решается последовательно:

- найдем точку $\hat{u}$ эллипсоида, ближайшую к точке 0 и отстоящую от нее на расстояние R^2 ;
- сравним значение R с единицей и примем решение о пересечении исходных эллипсоидов.

Возникла самостоятельная оптимизационная задача:

$$\min_{(u-b)^T L(u-b) - 1 \leq 0} \sum_{i=1}^n u_i^2,$$

где $b = c_{22}$; $L = \text{diag}(l_1, \dots, l_n) = \Lambda_{21}$.

Согласно теореме [7, гл. 1, § 3.2.1] для функции Лагранжа

$$\phi(u, r, s) = r \sum_{i=1}^n u_i^2 + s \left[\sum_{i=1}^n l_i (u_i - b_i)^2 - 1 \right]$$

существует такой вектор множителей Лагранжа $(r, s) \neq 0$, что для $\phi(u, r, s)$ и точки локального экстремума $\hat{u}$ выполняются так называемые условия стационарности, дополняющей условия нежесткости и неотрицательности:

$$\left. \frac{\partial \phi}{\partial u_i} \right|_{\hat{u}} = 0 \text{ или } r\hat{u}_i + sl_i(\hat{u}_i - b_i) = 0, \quad i = \overline{1, n}; \quad (8)$$

$$s \left[\sum_{i=1}^n l_i (\hat{u}_i - b_i)^2 - 1 \right] = 0, \quad s \geq 0. \quad (9)$$

Пусть $r = 0$ и $\hat{u}_i - b_i = 0$ для любого i . Тогда из условия (9) следует, что $s = 0$, что противоречит условию $(r, s) \neq 0$. Пусть теперь $r = 0$ и $\hat{u}_i - b_i \neq 0$ для некоторого i . Тогда условие (8) для этого значения i говорит о том, что $sl_i(\hat{u}_i - b_i) = 0$, где $l_i \neq 0$; следовательно, $s = 0$, что опять же противоречит условию $(r, s) \neq 0$. Таким образом, $r \neq 0$ и можно положить $r = 1$.

Пусть $s = 0$. Тогда из условия (8) следует, что $\hat{u}_i = 0, i = \overline{1, n}$. В силу того что точка $\hat{u}$ принадлежит эллипсоиду, должно выполняться неравенство

$$\sum_{i=1}^n l_i b_i^2 - 1 \leq 0.$$

Выделим случай $\hat{u}_i = 0, i = \overline{1, n}$, и $\sum_{i=1}^n l_i b_i^2 - 1 \leq 0$ в отдельный и будем его выявлять сразу же перед решением исходной задачи; он означает, что центр первого эллипсоида принадлежит второму эллипсоиду и, следовательно, имеет место пересечение. Это позволяет далее предполагать, что $s \neq 0$ и $\sum_{i=1}^n l_i b_i^2 - 1 > 0$.

Из условия (8) при $r = 1$ следует:

$$\hat{u}_i + sl_i(\hat{u}_i - b_i) = 0,$$

или

$$\hat{u}_i(1 + sl_i) = sl_i b_i.$$

Но $l_i > 0, s > 0$. Следовательно, $1 + sl_i \neq 0$ и

$$\hat{u}_i = \frac{l_i b_i s}{1 + l_i s}, \quad i = \overline{1, n}.$$

Подставляя полученные выражения в условие (9), получаем:

$$\sum_{i=1}^n l_i \left(\frac{l_i b_i s}{1 + l_i s} - b_i \right)^2 - 1 = 0,$$

или

$$\sum_{i=1}^n \frac{l_i b_i^2}{(1 + l_i s)^2} - 1 = 0. \quad (10)$$

Введем функцию

$$\psi(s) = \sum_{i=1}^n \frac{l_i b_i^2}{(1 + l_i s)^2} - 1, \quad s > 0.$$

Исследуем свойства производных этой функции. С учетом того что $l_i > 0$ для $i = \overline{1, n}$, имеем:

$$\psi'(s) = -2 \sum_{i=1}^n \frac{l_i^2 b_i^2}{(1 + l_i s)^3} < 0;$$

$$\psi'' = 6 \sum_{i=1}^n \frac{l_i^3 b_i^2}{(1 + l_i s)^4} > 0.$$

Используя рассматриваемое ограничение

$$\sum_{i=1}^n l_i b_i^2 - 1 > 0,$$

получаем

$$\psi(0) = \sum_{i=1}^n l_i b_i^2 - 1 > 0.$$

Используя свойства первой производной, получаем, что при $s > 0$ функция $\psi(s)$ убывающая. При этом

$$\lim_{s \rightarrow \infty} \psi(s) = -1 < 0.$$

В результате получаем, что уравнение (10) имеет корень. Его нахождение будем осуществлять с помощью итерационного метода Ньютона по формулам:

$$s_0 = 0, \\ s_k = s_{k-1} - \frac{\psi(s_{k-1})}{\psi'(s_{k-1})}, \quad k = 1, 2, \dots$$

Если решение $\hat{s}$ уравнения (10) найдено, то

$$\hat{u}_i = \frac{l_i b_i \hat{s}}{1 + l_i \hat{s}}, \quad i = \overline{1, n}, \\ R^2 = \hat{s}^2 \sum_{i=1}^n \frac{l_i^2 b_i^2}{(1 + l_i \hat{s})^2}.$$

Координаты точки второго эллипсоида, ближе всего расположенной к центру первого, находятся из соотношения

$$x = Q_1 \Lambda_1^{-1/2} Q_{21} \hat{u} + c_1.$$

4 Применения для анализа данных

В [8] рассматривалась задача моделирования референсных значений — результатов наблюдения величин определенного типа, полученных от одного лица или группы лиц в соответствии с заявленным описанием. Для этих целей использовалась модель смеси нормальных распределений. За счет усложнения она позволяет точнее описывать реальные распределения данных, но, оставаясь параметрической, обеспечивает значительное сжатие информации об объекте анализа. При этом сохраняется преимущество относительно простых аналитических решений типовых вероятностных задач, поскольку основой по-прежнему служит нормальное распределение.

Объектом статистического анализа были выбраны данные для 363 мужчин, включающие их возраст и измерения биомаркеров PSA, опубликованные в приложении 5.1 гл. 5 в [9]. Подбор числа элементов смеси с помощью графических методов и информационных критериев не дал четких результатов, множественная проверка гипотез на основе критерия отношения правдоподобия привела к оценке $\hat{k} = 4$. Таким образом, совместное распределение показателей «возраст» (соответствует u_1) и «PSA» (соответствует u_2) может быть описано с помощью смеси четырех нормальных распределений $\varphi(u_1, u_2, (\mu_{j1}, \mu_{j2}, \sigma_{j1}^2, \sigma_{j2}^2, \rho_j))$, а именно:

$$f(u) = 0,446\varphi(u_1, u_2, (55,800, 0,591, 83,600, 0,068, 0,147)) + \\ + 0,345\varphi(u_1, u_2, (60,400, 1,410, 89,600, 0,286, 0,126)) + \\ + 0,187\varphi(u_1, u_2, (63,400, 3,750, 68,900, 2,370, 0,211)) + \\ + 0,022\varphi(u_1, u_2, (72,400, 5,520, 25,000, 12,100, -0,989)). \quad (11)$$

Отсюда находятся условные распределения, с помощью которых можно определять референсные интервалы для конкретных значений возраста. Предложенные решения на базе смеси демонстрируют явные преимущества: высокая детализация по возрастам; сглаживание результатов наблюдений для различных по объему возрастным групп; возможность формировать предположения о характере зависимости между возрастом и уровнем PSA. В дополнение к последнему двухмерный характер данных позволяет напрямую использовать методы визуализации: на рис. 1 изображены эллипсы равной вероятности, полученные при одинаковых значениях $P = 0,5$ для всех элементов смеси (порядок

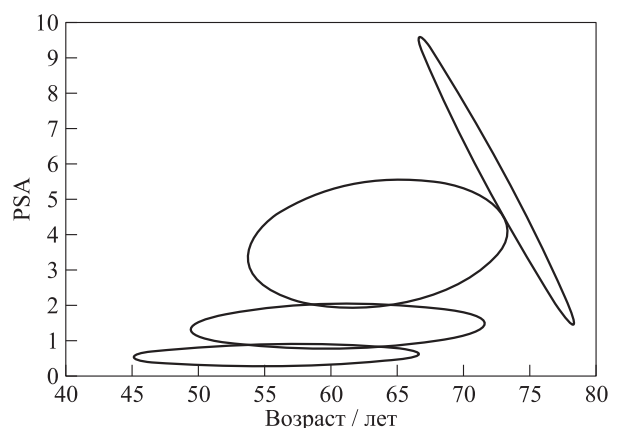


Рис. 1 Эллипсы равной вероятности, соответствующие элементам найденной оценки смеси нормальных распределений

включения элементов в смесь согласно (11) соответствует следованию эллипсов на рис. 1 снизу вверх). В частности, благодаря рис. 1 обнаруживается важная особенность объекта исследований: более возрастным кластерам пациентов соответствуют значения PSA со все большим разбросом, что ярче всего проявляется для верхнего справа эллипса с центром в точке (72,4, 5,52).

Для демонстрации возможностей построенных средств манипулирования эллипсоидами в случае, когда из-за многомерности не получается обращаться к простым методам визуализации, рассмотрим задачу оценки качества подгонки модели при классификации лонгитюдных данных.

В [10] рассматривалась задача байесовской классификации результатов наблюдения группы объектов в течение некоторого промежутка времени; соответствующие методы известны как лонгитюдные (продольные, протяженные во времени). Предлагалось представлять серии многомерных характеристик некоторого объекта как единый вектор, что позволило за счет увеличения размерности данных получить единую картину описания объектов, а также формализовать построение модели данных. Для демонстрации сути предлагаемого консолидирующего подхода и иллюстрации появляющихся возможностей анализа данных изучалась проблема ранней диагностики рака с использованием биомаркера PSA. Было выявлено, что многомерный подход при обработке серий наблюдений приводит к повышению точности диагностики.

Для экспериментов использовался набор данных, сформированный на основе [11]. Он содержал результаты наблюдений в 71 случае рака простаты (далее — диагноз $D = 1$) и для 70 пациентов из контрольной группы ($D = 0$). Рассматривались два типа маркеров: общий PSA (tPSA, total PSA) и свободный PSA (fPSA, free PSA). Всего имелись 683 наблюдения, каждое из которых включало идентификатор пациента, диагноз, промежуток времени до установления окончательного диагноза, уровни tPSA и fPSA, возраст пациента. Данные распадалась на серии наблюдений для отдельных пациентов; длина L серии менялась от одного пациента к другому.

При фиксированном наборе маркеров (tPSA и fPSA, или только tPSA, или только fPSA) и определенном значении L использовался обучаемый байесовский классификатор. Для описания данных каждого из двух классов принималась вероятностная модель смеси анализаторов главных компонент, включая выбор ее эффективной размерности [12], т.е. значений параметров числа элементов смеси для каждого класса и значений эффективной размерности для каждого элемента смеси нор-

мальных распределений и определенного диагноза. Качество классификации характеризовалось ее точностью и оценивалось методом перепроверки. Основной вывод из полученных результатов состоял в том, что предложенный консолидирующий метод анализа серий наблюдений на основе подобранной модели смеси позволяет эффективно исследовать произвольное число признаков, измеряемых в течение временного промежутка.

Объединение данных, фрагментированных по времени и по характеристикам, в единое целое естественным образом подключает преимущества обработки многомерных данных, а также позволяет избежать потери общей эффективности статистического вывода из-за декомпозиции общей задачи анализа данных, характерной для обычного лонгитюдного подхода.

Подтвердить преимущество консолидирующего метода можно с помощью степени делимости представлений данных для двух диагнозов сразу же после оценивания их характеристик. Модель смеси распределений описывает совокупность данных для каждого диагноза как набор кластеров-элементов смеси. Если соответствующие эллипсоиды попарно из различных классов преимущественно не пересекаются, т.е. делимы друг от друга, то ошибки классификации ожидаемо малы и точность классификации высока. Теперь сравним число пересечений эллипсоидов в двух ситуациях:

- обработка векторов данных, компоненты которых соответствуют временной последовательности их поступления;
- обработка векторов данных без привязки к последовательности моментов времени их фиксации; маскирование лонгитюдности данных реализуется путем многократной случайной перестановки наблюдаемых значений маркера fPSA.

Выбор параметров анализа данных опирался на выводы [10] и пал на значения: $L = 4$; $n = 5$; $k = 3$; кратность перестановок 100. Полученные результаты представлены на рис. 2 и демонстрируют, что замена комплексной обработки последовательности наблюдений с учетом течения времени на анализ совокупности тех же, но неупорядоченных во времени наблюдений приводит к «сближению» двух классов данных, что влечет за собой рост ошибок классификации. Последнее полностью подтверждается, но после проведения трудоемкого бутстреп-анализа [10].

Анализ степени пересеченности наборов эллипсоидов для различных классов объектов может также стать источником для выявления вклада отдельных кластеров данных в ошибки классификации.

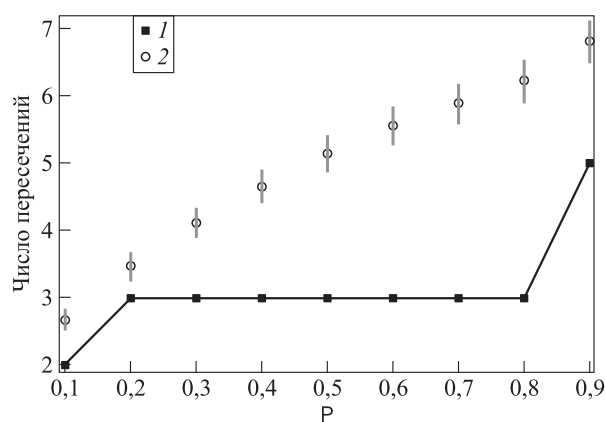


Рис. 2 Зависимость числа $N(\text{IS})$ (1) и среднего числа $N(\text{IS}|\text{rand})$ (2) попарных пересечений эллипсоидов от вероятности P попадания в них соответственно для исходных данных и полученных путем случайных перестановок значений fPSA. Вертикальные отрезки для точек $N(\text{IS}|\text{rand})$ отражают 95%-ный доверительный интервал для среднего на основе нормальной аппроксимации

Так, для всех значений $P = \overline{0,2; 0,8}$ только один второй элемент оценки смеси (второй кластер) для $D = 1$ имеет пересечение со всеми остальными эллипсоидами для $D = 0$, тогда как для всех остальных шести пересечения отсутствуют. Напомним, что применение смеси нормальных многомерных распределений в задаче построения эмпирического байесовского классификатора позволяет после оценивания параметров модели провести классификацию данных и установить не только общие характеристики некоторого кластера, но и перечислить объекты, наиболее вероятно входящие в него. Таким образом, специалист в предметной области получает возможность прояснить природу потерь при классификации, получив заранее совокупность прецедентов (здесь это второй кластер для $D = 1$).

5 Заключение

Рассмотренный набор постановок задач представления и обработки эллипсоидов применительно к задачам анализа данных, а также соответствующих алгоритмов их решения может быть дополнен вопросами измерения «невыврожденности» распределения на основе эллипсоидов рассеяния [13, разд. 22.7], сечения эллипсоидов [3, разд. 5.2.2], рядом других алгоритмов [6]. Подобное расширение становится особенно ценным, если сопровождается раскрытием прикладных задач, где оно действительно актуально.

Если принять во внимание многомерность данных, то важным моментом для практики становятся

ся вычислительные проблемы: уточнение условий, при которых решаются задачи анализа данных (например, речь идет об одноразовой или систематической обработке); выбор форм представления данных (например, принятие за основу конкретных определений эллипсоида); выделение критических алгоритмов обработки (например, сравнительный анализ вычислительной эффективности матричных операций).

Литература

1. *McLachlan G., Peel D.* Finite mixture models. — New York, NY, USA: Wiley & Sons, 2000. 419 p. doi: 10.1002/0471721182.
2. *Королев В. Ю.* EM-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. Теоретический обзор. — М.: ИПИ РАН, 2007. 94 с.
3. *Кривенко М. П.* Прикладные методы оценивания распределения многомерных данных малой выборки. — М.: ИПИ РАН, 2011. 146 с. EDN: QJZIID.
4. *Yao W., Xiang S., Raton B.* Mixture models: Parametric, semiparametric, and new directions. — Boca Raton, CA, USA: Chapman & Hall/CRC Press, 2024. 397 p. doi: 10.1201/9781003038511.
5. *Кривенко М. П.* Оценивание параметров смеси нормальных многомерных распределений с ограничениями на ковариационные матрицы // Информатика и её применения, 2025. Т. 19. Вып. 2. С. 2–8. doi: 10.14357/19922264250201. EDN: YJOPVN.
6. *Pope S. B.* Algorithms for ellipsoid. — Ithaca, NY, USA: Sibley School of Mechanical & Aerospace Engineering Cornell University, 2008. Report FDA-08-01. 49 p. https://tcg.mae.cornell.edu/pubs/Pope_FDA_08.pdf.
7. *Галеев Э. М., Тихомиров В. М.* Оптимизация: теория, примеры, задачи. — М.: Эдиториал УРСС, 2000. 320 с.
8. *Кривенко М. П.* Модели для представления и обработки референсных значений // Информатика и её применения, 2015. Т. 9. Вып. 2. С. 63–74. doi: 10.14357/19922264150208. EDN: TZBVTJ.
9. *Harris E. K., Boyd J. C.* Statistical bases of reference values in laboratory medicine. — New York, NY, USA: Marcel Dekker, 1995. 384 p. doi: 10.1201/9781482273151.
10. *Кривенко М. П.* Байесовская классификация серий многомерных данных // Системы и средства информатики, 2020. Т. 30. № 1. С. 34–45. doi: 10.14357/08696527200103. EDN: DSSUBO.
11. *Thornquist M. D., Omenn G. S., Goodman G. E., et al.* Statistical design and monitoring of the carotene and retinol efficacy trial (CARET) // Control. Clin. Trials, 1993. Vol. 14. Iss. 4. P. 308–324. doi: 10.1016/0197-2456(93)90228-6.
12. *Кривенко М. П.* Снижение размерности для смесей вероятностных анализаторов главных компонент

применительно к задачам медицинской диагностики // Системы и средства информатики, 2019. Т. 29. № 4. С. 4–13. doi: 10.14357/08696527190401. EDN: AHIZZR.

13. Крамер Г. Математические методы статистики / Пер. с англ. — М.: Мир, 1975. 648 с. (*Cramer H. Mathematical methods of statistics. — Princeton, NJ, USA: Princeton University Press, 1946. 575 p.*)

Поступила в редакцию 15.05.2026

Принята к публикации 15.08.2026

INTERPRETATION OF ELLIPSOID-BASED CLUSTER DATA STRUCTURE

M. P. Krivenko

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: Equivalent definitions of ellipsoids are considered as well as formulations of analytic geometry problems aimed at interpreting the cluster structure of data. The corresponding solution algorithms are mathematically substantiated. Two examples from the field of data analysis are discussed based on a Gaussian mixture model. Ellipsoids are used to interpret the data clusters corresponding to the elements of the mixture. The first example focuses on modeling reference values by describing the empirical distribution of multivariate patient data, including age and PSA (Prostate-Specific Antigen) biomarker measurements. The proposed mixture-based solutions demonstrate clear advantages and enable the direct application of ellipse-based visualization methods to identify specific features of the object under study. The second example considers a consolidated approach for analyzing longitudinal data when a series of multidimensional object characteristics is represented as a single vector of observed values. To demonstrate the emerging capabilities of data analysis, the problem of early diagnosis of cancer using PSA biomarkers is investigated. The advantage of the consolidating method is confirmed by a high degree of separability of sets of cluster elements of the mixture measured by the number of pairwise intersections of the corresponding ellipsoids. Analysis of the degree of intersection of sets of ellipsoids for different classes of diagnoses can further help identify the contribution of individual data clusters to classification errors.

Keywords: mixture of normal distributions; representation of ellipsoids; ellipsoid processing algorithms; reference values; serial data classification; longitudinal analysis; consolidation approach

DOI: 10.14357/19922264260306

EDN: YSZTCG

References

1. McLachlan, G., and D. Peel. 2000. *Finite mixture models*. New York, NY: Wiley & Sons. 419 p. doi: 10.1002/0471721182.
2. Korolev, V. Yu. 2007. *EM-algorithm, ego modifikatsii i ikh primeneniye k zadache razdeleniya smesey veroyatnostnykh raspredeleniy. Teoreticheskiy obzor* [EM-algorithm modifications and their application to the separation of mixtures of probability distributions. Theoretical review]. Moscow: IPI RAN. 94 p.
3. Krivenko, M. P. 2011. *Prikladnye metody otsenivaniya raspredeleniya mnogomernykh dannykh maloy vyborki* [Applied methods for estimating the distribution of small sample multidimensional data]. Moscow: IPI RAN. 146 p. EDN: QJZIHD.
4. Yao, W., S. Xiang, and B. Raton. 2024. *Mixture models: Parametric, semiparametric, and new directions*. New York, NY: Chapman & Hall/CRC Press. 397 p. doi: 10.1201/9781003038511.
5. Krivenko, M. P. 2025. Otsenivaniye parametrov smesi normal'nykh mnogomernykh raspredeleniy s ogranicheniya-mi na kovariatsionnye matritsy [Estimation of parameters of a mixture of normal multivariate distributions with constraints on covariance matrices]. *Informatika i ee Primeniya — Inform. Appl.* 19(2):2–8. doi: 10.14357/19922264250201. EDN: YJOPVN.
6. Pope, S. B. 2008. Algorithms for ellipsoid. Ithaca, NY: Sibley School of Mechanical & Aerospace Engineering Cornell University. Report FDA-08-01. 49 p. Available at: https://tcg.mae.cornell.edu/pubs/Pope_FDA_08.pdf (accessed July 30, 2026).
7. Galeev, E. M., and V. M. Tikhomirov. 2000. *Optimizatsiya: teoriya, primery, zadachi* [Optimization: Theory, examples, problems]. Moscow: Editorial URSS. 320 p.
8. Krivenko, M. P. 2015. Modeli dlya predstavleniya i obrabotki referensnykh znacheniy [Models for representation and treatment of reference values]. *Informatika i ee Primeniya — Inform. Appl.* 9(2):63–74. doi: 10.14357/19922264150208. EDN: TZBVTJ.
9. Harris, E. K., and J. C. Boyd. 1995. *Statistical bases of reference values in laboratory medicine*. New York, NY: Marcel Dekker. 384 p. doi: 10.1201/9781482273151.

10. Krivenko, M. P. 2020. Bayesovskaya klassifikatsiya seriynogomernykh dannyykh [Bayesian classification of serial multivariate data]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 30(1):34–45. doi: 10.14357/08696527200103. EDN: DSSUBO.
11. Thornquist, M. D., G. S. Omenn, G. E. Goodman, *et al.* 1993. Statistical design and monitoring of the carotene and retinol efficacy trial (CARET). *Control. Clin. Trials* 14(4):308–324. doi: 10.1016/0197-2456(93)90228-6.
12. Krivenko, M. P. 2019. Snizhenie razmernosti dlya smesi veroyatnostnykh analizatorov glavnykh komponent primenitel'no k zadacham meditsinskoy diagnostiki [Dimensionality reduction for mixture of probabilistic principal component analyzers in relation to the tasks of medical diagnostics]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 29(4):4–13. doi: 10.14357/08696527190401. EDN: AHIZZR.
13. Cramer, H. 1946. *Mathematical methods of statistics*. Princeton, NJ: Princeton University Press. 575 p.

Received May 15, 2026

Accepted August 15, 2026

Contributor

Krivenko Michail P. (b. 1946) — Doctor of Science in technology, professor, leading scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; mkrivenko@ipiran.ru

САМООБУЧАЕМОЕ ИНКРЕМЕНТАЛЬНОЕ ОБНАРУЖЕНИЕ КЛАССОВ НА ОСНОВЕ ВЕРОЯТНОСТНО-ИНФОРМИРОВАННОГО НЕПРЕРЫВНОГО ОБУЧЕНИЯ*

А. М. Достовалова¹, А. К. Горшенин²

Аннотация: Предложен метод решения задачи непрерывной инкрементальной классификации, состоящей в выявлении данных новых классов в условиях отсутствия разметки для малых наборов временных рядов и табличных данных. Для формирования точных псевдометок новых данных, дополняющих выявленные ранее закономерности, разработана специализированная нейросеть (НС), информированная на уровне архитектуры моделью глубокой смеси гауссовских распределений с реализацией обучения на основе функционала контрастных потерь. Метод протестирован на открытых наборах для различных архитектур сети-дискриминатора, в том числе трансформерной. Проведено сравнение эффективности метода с неинформированными сетями и методами машинного обучения для формирования псевдометок. Информированная сеть демонстрирует преимущество по точности в сравнении с рассмотренными альтернативными подходами при обнаружении в неразмеченных данных новых классов в условиях ограниченных по числу элементов обучающих датасетов. Прирост значений гармонического среднего для F_1 -меры (F_1^H , балансирует точность распознавания объектов старых и новых классов) достигает 66,32% (в среднем 15,28%), а по макроусредненной F_1 -мере (F_1^{avg} , отражает точность классификации по всем классам без учета их размера) — 52,86% (в среднем 11,8%).

Ключевые слова: инкрементальное обучение; вероятностное информирование; обнаружение новых классов; неразмеченные данные; глубокие гауссовские смеси

DOI: 10.14357/19922264260307

EDN: ZDDABJ

1 Введение

Прикладные задачи медицинской диагностики [1] или обнаружения аномалий [2] требуют от НС способности к непрерывному обучению. Это значит, что если обучающие данные поступают непрерывно, то сеть-дискриминатор должна эффективно обучаться на новых примерах, не поддаваясь эффекту «катастрофического забывания» закономерностей предшествующих данных. Наибольшую сложность представляет инкрементальная (поточная) классификация. В этой задаче каждая новая порция данных содержит новые классы [3], причем объекты могут быть как частично размеченными [4–6], так и даже полностью неразмеченными. В таких случаях для неразмеченных данных формируют псевдометки, например с помощью предобученных сетей, техник контрастного обучения, предварительной кластеризации или промптов [7, 8].

Однако техники инкрементального обучения слабо развиты для обработки временных рядов

и табличных данных. В этой области, в отличие от изображений, на сегодняшний день встречаются только методы для работы с размеченными данными [9]: существующие подходы предполагают, что все передающиеся на вход сети порции данных имеют метки классов. Реальные наборы временных и табличных данных часто оказываются малыми по числу элементов и обладают выраженной специфичностью. Эти факторы сильно ограничивают использование предобученных моделей [10], на основе которых строится большинство известных техник инкрементального обучения, и нередко не позволяют напрямую применять для обработки таких данных методы, созданные для работы с изображениями.

В работе предложен метод информированного самообучаемого обнаружения классов Self-Supervised Class Discovery Informed Network (SSCDiN) для решения задачи инкрементальной классификации с выявлением в неразмеченных данных новых классов для малых датасетов временных рядов и последовательностей. Для дан-

* Исследование выполнено за счет гранта Российского научного фонда № 25-21-00448, <https://rscf.ru/project/25-21-00448/>. Работа выполнялась с использованием инфраструктуры Центра коллективного пользования «Высокопроизводительные вычисления и большие данные» (ЦКП «Информатика») ФИЦ ИУ РАН (г. Москва).

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, adostovalova@frccsc.ru

²Федеральный исследовательский центр «Информатика и управление» Российской академии наук, agorshenin@frccsc.ru

ных временных рядов и таблиц такая постановка задачи рассматривается впервые. В методе для формирования точных псевдометок используется НС, информированная моделью глубокой смеси гауссовских распределений [11]. Подход вероятностного информирования, развивающий направление физически информированных НС [12], заключается в использовании сетью вероятностных моделей и их характеристик в качестве дополнительной информации об обрабатываемых данных [13–15], повышающие интерпретируемость результатов [16]. Он продемонстрировал высокую эффективность при решении классических задач обработки изображений и временных рядов при ограниченных обучающих данных [17–19].

Метод SSCDiN был протестирован на шести открытых наборах данных из репозитория UCI, на которых было проведено сравнение эффективности альтернативных неинформированных и статистических методов формирования псевдометок.

2 Постановка задачи

Пусть задан малый набор $T = \{T_i\}_{i=1,2}$ данных таблиц или временных рядов. Данные в подмножестве исходного набора T_1 размечены, а в T_2 — нет, при этом число новых классов M_1 и M_2 в каждом из них известно. Сеть-дискриминатор $f(\cdot)$ последовательно учится классифицировать элементы из T_1 и T_2 . Требуется разработать такую нейросетевую архитектуру $D(\cdot)$ для формирования псевдометок элементов из множества T_2 , чтобы максимизировать вероятность правильной классификации элементов набора T сетью $f(\cdot)$:

$$\mathbb{P} \left(f(T) = Y \mid y_{(2)}^* = D(T_2) \right) \rightarrow \max,$$

где Y — реальные метки классов объектов из T , а $y_{(2)}^*$ — псевдометки, сформированные для множества T_2 .

3 Инкрементальное обучение с выявлением новых классов

На рис. 1 представлена схема метода SSCDiN, который представляет собой адаптацию известного в инкрементальном обучении подхода повторения опыта (*англ.* Experience Replay, ER) [20] для выявления новых классов в неразмеченных данных. На первом шаге сеть-дискриминатор $f(\cdot)$ обучается на размеченном множестве T_1 . Одновременно, как в классическом методе ER, формируется вспомогательное множество (буфер) B_{label} заданного размера, в который случайным образом без повторения выбираются элементы из T_1 .

Чтобы минимизировать забывание ранее выученных закономерностей сетью $f(\cdot)$ при обучении на данных T_2 помимо использования буфера B_{label} необходимо генерировать для T_2 высокоточные псевдометки, исключаящие пересечение с исходной выборкой T_1 . Это реализуется с помощью сети Deep Gaussian Mixture Discriminator (DGMD), которая информирована на уровне архитектуры глубокой гауссовской смесью и использует данные из B_{label} для контрастного обучения [21], максимизирующего отличие меток B_{label} от меток T_2 . Выбор модели для информирования обусловлен необходимостью взаимодействия со сложными, нелинейно зависимыми данными, при моделировании которых глубокая смесь демонстрирует более высокую эффективность в сравнении с классическими методами кластеризации [22].

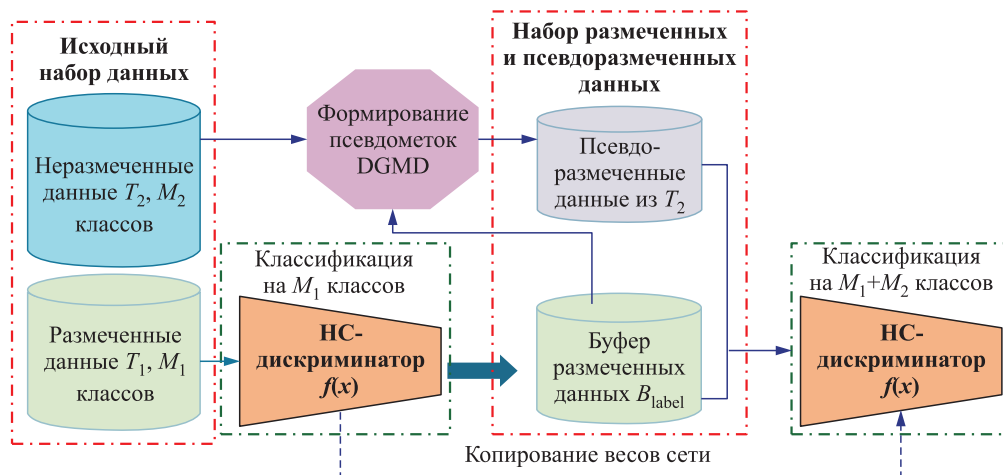


Рис. 1 Схема метода SSCDiN для обнаружения новых классов при инкрементальном обучении

Псевдоразмеченные данные объединяются с множеством B_{label} , и сеть $f(\cdot)$ дообучается на них с использованием функции потерь $\text{Loss}_{\text{incr}}$ вида

$$\text{Loss}_{\text{incr}} = L_{\text{CE}}(B_{\text{label}}) + \gamma L_{\text{pseudo}}(T_2),$$

$$L_{\text{pseudo}}(T_2) = - \sum_{t_j \in T_2} \sum_{i=1}^K D_i(t_j) \log(f(t_j)),$$

где L_{CE} — кросс-энтропия; $\gamma \in [0, 1]$ — весовой коэффициент; $K = M_1 + M_2$; $D_i(t_j)$ — вероятность принадлежности элемента t_j классу i при псевдоразметке.

4 Информированная сеть для псевдоразметки

Глубокая смесь гауссовских распределений (DGMM) [11] из h слоев, которой информирована сеть DGMD, задается следующими выражениями:

$$(1) \quad x_i = \eta_{s_1}^{(1)} + \Lambda_{s_1}^{(1)} z_i^{(1)} + u_i^{(1)}$$

с вероятностью $\pi_{s_1}^{(1)}$, $s_1 = \overline{1, k_1}$;

$$\vdots$$

$$(h) \quad z_i^{(h-1)} = \eta_{s_h}^{(h)} + \Lambda_{s_h}^{(h)} z_i^{(h)} + u_i^{(h)}$$

с вероятностью $\pi_{s_h}^{(h)}$, $s_h = \overline{1, k_h}$,

где $\mathbf{x} \in \mathbb{R}^{q \times p}$ — вектор входных данных (нулевой слой модели); $\mathbf{z}^{(h)} \sim N(0, I_p)$ — скрытые переменные (I_p — единичная матрица размерности $p \times p$); $\mathbf{u}^{(l)} \sim N(0, \Psi_{s_l}^{(l)})$, $l = \overline{1, h}$, — случайные ошибки с диагональной матрицей ковариаций размера $p \times p$ ($\mathbf{u}^{(l)}$ и $\mathbf{z}^{(h)}$ независимы); $\eta_{s_i}^{(i)}$ — векторы математических ожиданий; $\Lambda_{s_i}^{(i)}$ — матрицы факторных нагрузок, $i = \overline{1, h}$. Согласно [11], на каждом слое DGMM представляет собой многомерную смесь нормальных распределений. Пусть $h = 2$, число компонент

в первом слое равно H , а во втором — K . Тогда распределение выходного слоя имеет вид:

$$f_{z^{(h-1)}}(y) = \sum_{s_1=1}^H \sum_{s_2=1}^K \pi_{s_1, s_2} N(y, \mu_{s_1, s_2}, \Sigma_{s_1, s_2}),$$

$$\pi_{s_1, s_2} = \pi_{s_1} \pi_{s_2}, \quad \mu_{s_1, s_2} = \eta_{s_1}^{(1)} + \sum_{l=1}^h \prod_{m=1}^{l-1} \Lambda_{s_m}^{(m)} \eta_{s_l}^{(l)};$$

$$\Sigma_{s_1, s_2} = \Psi_{s_1}^{(1)} + \sum_{l=2}^h \prod_{m=1}^{l-1} \Lambda_{s_m}^{(1)} \Psi_{s_l}^{(l)} \prod_{m=1}^{l-1} \Lambda_{s_m}^{(1)}. \quad (1)$$

Формулы (1) легли в основу реализации архитектурного информирования в сети DGMD, представленной на рис. 2. Эта архитектура состоит из кодировщика D-Enc и информированного классификатора, в котором DGMM из двух слоев, заданная обучаемыми параметрами $\eta_{s_m}^{(m)}$ и $\Lambda_{s_m}^{(m)}$, моделирует пространство скрытых признаков сети. Упрощения исходной модели, такие как фиксированное число слоев и выполнение условий $\Psi_{s_2}^{(2)} = I_p$ и $\Psi_{s_1}^{(1)} = 0$, позволяли уменьшить склонность сети к переобучению в задачах обработки малых данных.

В сети DGMD признаки, сформированные кодировщиком, вначале сжимаются в PAR раз с помощью полносвязного слоя (или умножаются на единичную матрицу), после чего из них формируются стохастические эмбединги. Это реализовано с помощью разложения на компоненты DGMM за счет вычитания и умножения на группированные параметры μ_{s_1, s_2} и Σ_{s_1, s_2} , сформированные по формулам (1) из $\eta_{s_m}^{(m)}$ и $\Lambda_{s_m}^{(m)}$. Такое разложение позволяло придать линейную структуру пространству скрытых признаков модели. После эмбединги нормализовывались, объединялись в общий вектор, из которого с помощью двух полносвязных слоев формировалась выходная метка класса.

Сеть DGMD (обозначается как $D(\cdot)$) обучалась на множестве T_2 и буфере размеченных дан-

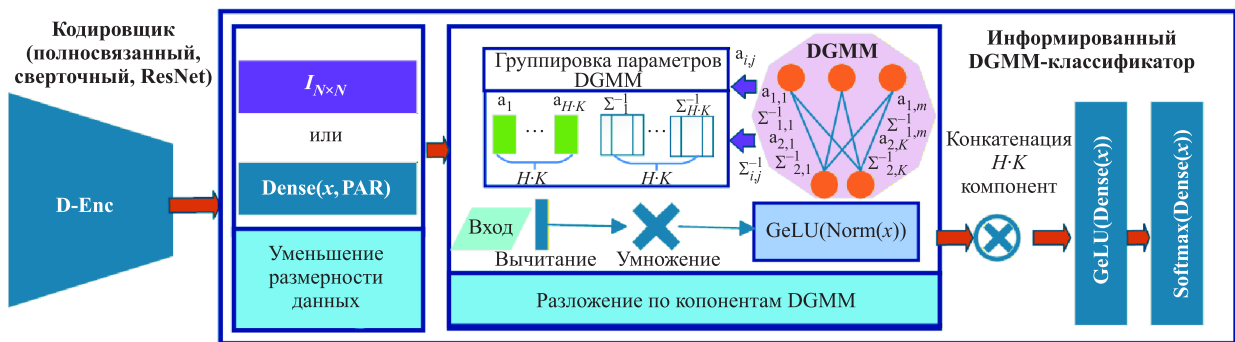


Рис. 2 Архитектура DGMD

ных B_{label} с использованием специальной функции потерь вида

$$\begin{aligned} \text{Loss}_D = L_{\text{CE}}(B_{\text{label}}) + \\ + \alpha \sum_{t_j \in T_2} \left(\sum_{b_i \in B_{\text{label}}} \log(\|b_i - t_j\|_2 + 1) (D(b_i)D(t_j)^T) + \right. \\ \left. + \sum_{t_i \in T_2} \log(\|t_i - t_j\|_2 + 1) (D(t_i)D(t_j)^T) \right). \quad (2) \end{aligned}$$

Формула (2) состоит из двух слагаемых: кросс-энтропии для размеченных данных B_{label} и мягкой контрастной потери между неразмеченными и размеченными данными с весовым коэффициентом $\alpha \in [0, 2]$. Если элементы похожи и евклидово расстояние между ними под знаком логарифма мало, то косинус угла между формируемыми DGMD нормализованными метками $(D(b_i)D(t_j)^T)$ может быть велик, что означает их сходство. Иначе большее расстояние между элементами должно повлечь уменьшение косинуса угла между метками и усилению разницы между ними. Две суммы в контрастной потере учитывают разницу между элементами T_2 и B_{label} , а также разницу между разными классами в множестве T_2 .

5 Тестирование метода информированного самообучаемого обнаружения классов на данных последовательностей и временных рядов

5.1 Тестовые данные

Для тестирования SSCDiN были рассмотрены 6 наборов табличных данных и временных рядов из репозитория UCI, описание которых представлено в табл. 1. Перечисленные наборы относятся к категории малых данных за исключением Abalone, содержащего более четырех тысяч элементов. Наборы были сложными для классификации из-за выраженного дисбаланса классов в наборе: разница между числом элементов мажоритарных и миноритарных классов могла достигать 10–20 раз. Каждый из датасетов разделялся на два множества T_1 и T_2 , при этом $M_2 = \{2; 3\}$.

Для оценки точности классификации использовались метрики ($i = 1; 2$):

Таблица 1 Описание тестируемых наборов из репозитория UCI

Набор UCI	Размер	Классы
Ecoli	336	8
Daily Demand (DD)	60	5
Abalone	4180	5
Heart Disease (HD)	303	5
Yeast	1484	10
Glass	214	6

$$\begin{aligned} F_1^{\text{avg}} &= \frac{1}{K} \sum_{i=1}^2 \sum_{j=1}^{M_i} F_1^{(i,j)}; \\ F_1^H &= \frac{2F_1^{T_1} \cdot F_1^{T_2}}{F_1^{T_1} + F_1^{T_2}}; \\ F_1^{T_i} &= \frac{1}{M_i} \sum_{j=1}^{M_i} F_1^{(i,j)}, \end{aligned}$$

где $F_1^{(i,j)}$ — значение F_1 -меры, вычисленное для класса j из множества T_i . Макроусредненная метрика F_1^{avg} описывает среднюю точность распознавания элементов из множеств T_1 и T_2 , а среднее геометрическое F_1^H показывает, насколько точно сеть $f(\cdot)$ обнаруживает новые классы (следует из метрики $F_1^{T_2}$) и одновременно классифицирует ранее уже встречавшиеся классы (следует из $F_1^{T_1}$). Высокие значения обеих метрик показывают, что сеть $f(\cdot)$ выучила закономерности в новых данных, но при этом не забыла старые классы.

В качестве сети $f(\cdot)$ в SSCDiN рассматривались четырехслойная полносвязная сеть, трансформер и сеть с рекуррентным блоком. Рассмотрены сети с относительно небольшим числом параметров (например, ResNet18 содержала порядка 152 тыс. параметров), поскольку тестируемые наборы были малыми и более сложные архитектуры на таких данных бы не обучились. Гиперпараметры сети $f(\cdot)$ и сети DGMD перечислены в табл. 2. Выбор лучшей комбинации параметров осуществлялся методом Grid Search [23].

При использовании в качестве кодировщика D-Enc сверточных архитектур (четырёхслойная сеть CNN и ResNet18, предобученная на Imagenet) исходные данные, имевшие вид одномерного вектора, преобразовывались в угловое поле Грамиана [24].

Была проведена оценка влияния выбора способа формирования псевдометок в методе SSCDiN на результат классификации. Сеть DGMD сравнивалась с методами машинного обучения (ML-методами) для формирования псевдометок [22], такими как классическая (GMM — Gaussian Mixture Model)

Таблица 2 Гиперпараметры метода SSCDiN и их описание

Название	Описание	Значения
hid	Число элементов в слоях полносвязной сети $f(\cdot)$	5–15
batch	Размер батча обучающих данных	5–32
optim	Алгоритм оптимизации	Adam, AdamW
lr	Шаг обучения	10^{-4} – 10^{-3}
features	Число признаков при позиционном кодировании в энкодере трансформера	20–60
heads	Число голов внимания в энкодере трансформера	2–10
D-Enc	Кодировщик, используемый в DGMD: полносвязный (Dense), сверточный (CNN) и ResNet18	Dense, CNN, ResNet18
H	Число параметров в скрытом слое DGMD	1–6
PAR	Фактор снижения размерности в DGMD	2–5

и глубокая смеси гауссовских распределений и метод k -средних (k -means). Эти методы определяли положение центров M_2 кластеров для неразмеченных данных. Затем эта информация объединялась данными о центрах классов размеченных элементов, полученных на основе процедур статистического вывода.

Помимо аналитических методов также рассматривались и неинформированные архитектуры. От схемы, представленной на рис. 2, они отличались тем, что в них информированный блок заменялся на последовательность из трех полносвязных слоев с активацией GeLU (далее обозначается Lin), которая не была информирована глубокой смесью. Другие, более сложные, в том числе предобученные нейросетевые архитектуры для сравнения не привлекались. В условиях когда обучающий набор мал по размеру и сильно специфичен, использование таких сетей часто оказывается неэффективным из-за переобучения. Простые линейные модели и классические подходы показывают аналогичные

или лучшие результаты, требуя в сотни раз меньше данных для настройки [25, 26].

5.2 Результаты тестирования

В табл. 3 представлены результаты классификации методом SSCDiN наборов из репозитория UCI при $M_2 = 2$, полученные полносвязной сетью-дискриминатором $f(\cdot)$ при разных методах формирования псевдометок. Значения метрик F_1^{avg} и F_1^H приведены через символ «;». Наибольшие величины F_1^H выделены жирным шрифтом. Представленные в разделе результаты были лучшими и отбирались не менее чем по 20 запускам.

Для всех рассмотренных наборов точность выявления новых классов полносвязной сетью $f(\cdot)$ выше при использовании DGMD для нанесения псевдометок в сравнении со ML-методами и неинформированными методами. Прирост относительно лучших по метрикам F_1^{avg} и F_1^H результатов при использовании ML-методов достигает 45,09%

Таблица 3 Значения метрик F_1^{avg} и F_1^H ($\times 100\%$), полученные полносвязным дискриминатором $f(\cdot)$ при разных методах формирования псевдометок

Метод	Набор UCI					
	Ecoli	DD	Abalone	HD	Yeast	Glass
ML-методы						
GMM	16,05; 0,0	0,0; 0,0	33,14; 0,0	23,76; 0,0	16,13; 7,27	28,32; 0,0
k -means	12,56; 0,0	8,0; 0,0	37,99; 0,0	10,21; 0,0	9,62; 0,0	25,43; 0,0
DGMM	28,85; 27,88	4,0; 0,0	36,44; 0,0	23,63; 22,71	8,91; 9,86	39,46; 37,26
Нейросети без информирования						
ResNet18	36,95; 33,0	33,03; 32,43	38,57; 0,0	31,65; 33,10	27,79; 0,0	37,06; 27,8
ResNet18+Lin	20,70; 0,0	38,63; 37,90	36,17; 0,0	33,11; 34,72	25,01; 0,0	33,23; 26,63
Dense + Lin	43,47; 48,30	44,66; 39,77	22,46; 18,02	37,59; 0,0	16,20; 17,29	27,00; 29,80
Варианты архитектуры DGMD						
Dense DGMD	48,11; 53,45	46,66; 47,05	37,23; 20,28	34,06; 35,79	21,6; 22,44	38,38; 41,45
ResNet18 DGMD	46,73; 39,93	53,35; 50,23	29,16; 28,17	36,64; 37,17	13,63; 14,67	41,34; 30,85
CNN DGMD	59,69; 56,32	53,09; 53,04	34,12; 29,08	40,57; 41,88	26,10; 28,58	49,64; 55,12

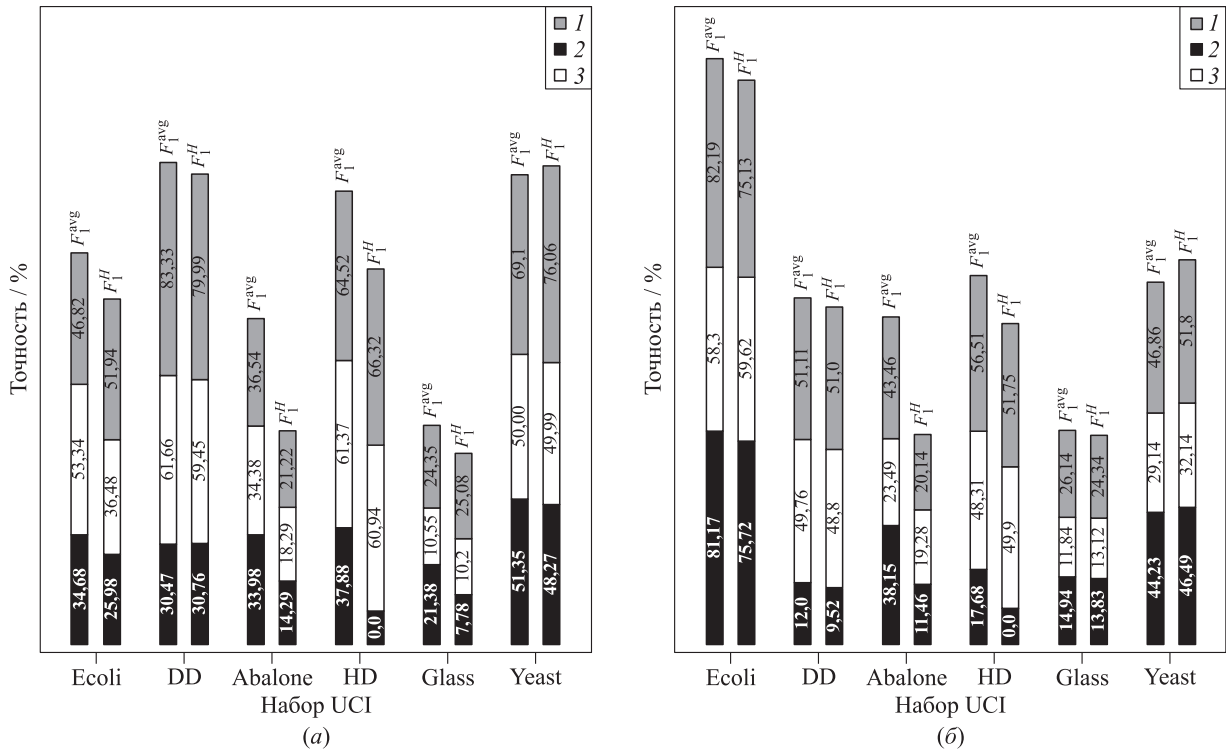


Рис. 3 Лучшие оценки точности классификации наборов UCI ($M_2 = 2$) трансформерной (а) и рекуррентной (б) сетью-дискриминатором $f(\cdot)$ при использовании DGMD (1), ML (2) и неинформированных методов (3) для формирования псевдометок

и 53,04% (средние приросты — 19,39% и 27,72% соответственно). Прирост относительно лучших результатов при использовании неинформированных архитектур достигает 16,11% и 27,32% по метрикам F_1^{avg} и F_1^H соответственно (средние приросты составляют 11,04% и 13,02%).

Лучшие оценки точности выявления новых классов ($M_2 = 2$) трансформерной и рекуррентной сетями $f(\cdot)$ для разных методов формирования псевдометок представлены на рис. 3. Для всех рассмотренных наборов точность выявления новых классов выше при использовании DGMD для нанесения псевдометок. Прирост относительно лучших по метрикам F_1^{avg} и F_1^H результатов при использовании ML-методов достигает 52,86% и 66,32% для трансформерного дискриминатора (в среднем 19,15% и 32,25% соответственно), а для рекуррентного — 39,11% и 51,75% (19,37% и 19,52% в среднем). Прирост относительно лучших результатов, полученных при использовании неинформированных архитектур, достигает 21,67% и 26,07% по метрикам F_1^{avg} и F_1^H соответственно для трансформерного дискриминатора (в среднем 8,89% и 14,21%), а для рекуррентного — 23,89% и 19,66% (14,24% и 8,55% в среднем).

Для подтверждения общности полученных результатов и независимости от выбора удачного разбиения набора был рассмотрен другой способ разбиения датасетов на множества T_1 и T_2 : рассмотрен случай, когда $M_2 = 3$. Согласно полученным результатам, все рассмотренные сети-дискриминаторы демонстрируют более высокую точность выявления новых классов при использовании DGMD для нанесения псевдометок. Для полносвязного дискриминатора прирост метрик F_1^{avg} и F_1^H при разметке с помощью DGMD составляет 0,0%–12,01% и 0,14%–7,24% при средних показателях неинформированных методов на уровне 40,66% и 38,73% соответственно. Для трансформерного дискриминатора прирост F_1^{avg} и F_1^H составляет 0,8%–12,59% и 0,0%–11,93% с уровня 53,47% и 49,65% соответственно, а для рекуррентного — 0,0%–4,51% и 0,8%–59,46% с уровня 49,06% и 36,10%.

Сеть DGMD демонстрирует более высокое качество формирования псевдометок при представлении входных данных в виде углового поля Грамиана. При $M_2 = 2$ в 12 из 18 тестов лучшие результаты были получены при использовании в качестве кодировщика D-Enc сверточной сети CNN, в четырех тестах — при использовании ResNet18 и в двух — для полносвязного кодировщика. При $M_2 = 3$

в семи из 18 тестов лучшие результаты были получены при использовании в качестве кодировщика D-Enc сверточной сети CNN, в четырех тестах — при использовании ResNet18 и в семи — для полносвязного кодировщика. Сверточный кодировщик использует более богатое, чем у полносвязной сети, пространство признаков, полученное из представлений данных в виде поля Грамиана, но при этом менее склонен к переобучению, чем ResNet 18.

6 Заключение

В работе представлен вероятностно-информированный метод SSCDiN для решения задачи обнаружения новых классов в неразмеченных данных для таблиц и временных рядов. Для данных такого типа подобная постановка задачи является новой и ранее не рассматривалась в литературе. Результаты обработки открытых наборов UCI, в том числе малых, продемонстрировали, что использование при инкрементальном обучении в методе SSCDiN информированной моделью глубокой гауссовской смеси сети DGMD позволяет более эффективно бороться с эффектом катастрофического забывания за счет формирования псевдометок более высокого качества в сравнении с неинформированными подходами, в том числе известными ML-методами. Прирост по метрике F_1^H , балансирующей точность обнаружения объектов старых и новых классов, достигает 66,32% (в среднем 15,28%) по сравнению с использованием альтернативных неинформированных и ML-методов. Прирост средней точности классификации по метрике F_1^{avg} при этом достигает 52,86% (в среднем 11,8%). Приросты метрик тем выше, чем меньше классов и, следовательно, элементов в множестве неразмеченных данных. Эти результаты демонстрируют перспективность применения подходов информирования в области инкрементального обучения, особенно при обработке малых наборов данных.

Перспективными представляются следующие направления исследований. Прежде всего, это разработка вероятностно-информированного подхода к выявлению новых классов для случая, когда их число в неразмеченных данных неизвестно. Наиболее простым методом в этом случае представляется предварительная кластеризация неразмеченных данных, однако возможны и иные решения. Другое направление связано с рассмотрением возможности создания адаптаций для различных подходов инкрементального обучения на размеченных данных для обнаружения в неразмеченном датасете новых классов. В настоящей статье предложен метод, основанный на использовании вспомогательного

буфера, однако видится возможным использование в этой задаче подхода переноса обучения и генеративных моделей.

Планируется продолжить исследования применения информированных подходов для противодействия эффекту катастрофического забывания при решении иных задач инкрементального обучения, в том числе для полностью размеченных данных на основе глубоких гауссовских моделей. Интерес представляет и исследование эффективности информирования в случае отказа от условия малости данных.

Литература

1. Hofmanninger J., Perkonigg M., Brink J. A., et al. Dynamic memory to alleviate catastrophic forgetting in continuous learning settings // *Medical image computing and computer assisted intervention* / Eds. A. L. Martel, P. Abolmaesumi, D. Stoyanov, D. Mateus, M. A. Zuluaiga, S. K. Zhou, D. Racocanu, L. Joskowicz. — Lecture notes in computer science ser. — Cham: Springer, 2020. Vol. 12262. P. 359–368. doi: 10.1007/978-3-030-59713-9_35.
2. Ribeiro A. G., Vilaça L., Costa C., et al. Automatic visual inspection for industrial application // *J. Imaging*, 2025. Vol. 11. Iss. 10. Art. 350. 30 p. doi: 10.3390/jimaging11100350.
3. Harman F. Incremental learning in medical imaging: A comprehensive survey of deep neural network advances and challenges // *IEEE Access*, 2026. Vol. 14. P.15812–15840. doi: 10.1109/ACCESS.2026.3659025.
4. Wang L., Yang K., Li C., Hong L., Li Z., Zhu J. ORDisCo: Effective and efficient usage of incremental unlabeled data for semi-supervised continual learning // *IEEE/CVF Conference on Computer Vision and Pattern Recognition Proceedings*. — IEEE: 2021. P. 5379–5388. doi: 10.1109/CVPR46437.2021.00534.
5. Lechat A., Herbin S., Jurie F. Pseudo-labeling for class incremental learning // *32nd British Machine Vision Conference Proceedings*. — British Machine Vision Association, 2021. Art. 332. 14 p. doi: 10.5244/C.35.363.
6. Wang Q., Xu K., Feng D., et al. Memory replay with unlabeled data for semi-supervised class-incremental learning via temporal consistency // *Front. Comput. Sci.* — Chi., 2025. Vol. 19. Art. 1912370. 4 p. doi: 10.1007/s11704-025-40828-0.
7. Roy S., Liu M., Zhong Z., Sebe N., Ricci E. Class-incremental novel class discovery // *Computer vision* / Eds. S. Avidan, G. Brostow, M. Cissé, G. M. Farinella, T. Hassner. — Lecture notes in computer science ser. — Cham: Springer, 2022. Vol. 13693. P. 317–333. doi: 10.1007/978-3-031-19827-4_19.
8. An J., Du Z., Zhang H., Wu D. TSPT: Two-Step prompt tuning for class-incremental novel class discovery // *Knowl.-Based Syst.*, 2025. Vol. 319. Art. 113603. 10 p. doi: 10.1016/j.knosys.2025.113603.

9. *Besnard Q., Ragot N.* Continual learning for time series forecasting: A first survey // *Engineering Proceedings*, 2024. Vol. 68. Iss. 1. Art. 49. 10 p. doi: 10.3390/eng-proc2024068049.
10. *Qiao Z., Pham Q., Cao Z., et al.* Class-incremental learning for time series: Benchmark and evaluation // *30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining Proceedings*. — New York, NY, USA: ACM, 2024. P. 5613–5624. doi: 10.1145/3637528.3671581.
11. *Viroli C., McLachlan G. J.* Deep Gaussian mixture models // *Stat. Comput.*, 2019. Vol. 29. P. 43–51. doi: 10.1007/s11222-017-9793-z.
12. *Karniadakis G. E., Kevrekidis I. G., Lu L., Perdikaris P., Wang S., Yang L.* Physics-informed machine learning // *Nature Reviews Physics*, 2021. Vol. 3. No. 6. P. 422–440. doi: 10.1038/s42254-021-00314-5.
13. *Горшенин А. К., Кузьмин В. Ю.* Анализ конфигураций LSTM-сетей для построения среднесрочных векторных прогнозов // *Информатика и её применения*, 2020. Т. 14. Вып. 1. С. 10–16. doi: 10.14357/19922264200102. EDN: SZNTXE.
14. *Горшенин А. К., Кузьмин В. Ю.* Метод повышения точности нейросетевых прогнозов с использованием смешанных вероятностных моделей и его реализация в виде цифрового сервиса // *Информатика и её применения*, 2021. Т. 15. Вып. 3. С. 63–74. doi: 10.14357/19922264210309. EDN: FDRKZX.
15. *Gorshenin A. K., Kuzmin V. Yu.* Statistical feature construction for forecasting accuracy increase and its applications in neural network based analysis // *Mathematics*, 2022. Vol. 10. No. 4. Art. 589. 21 p. doi: 10.3390/math10040589. EDN: PQFGHU.
16. *Грушо А. А., Грушо Н. А., Забейжайло М. И., Писковский В. О., Тимонина Е. Е.* Машинное обучение и доверие к результатам классификации // *Информатика и её применения*, 2025. Т. 19. Вып. 2. С. 63–68. doi: 10.14357/19922264250208. EDN: CXRNK.
17. *Горшенин А. К., Горбунов С. А., Волканов Д. Ю.* О классификации объектов сетевой вычислительной инфраструктуры на основе анализа статистических аномалий в трафике // *Информатика и её применения*, 2023. Т. 17. Вып. 3. С. 76–87. doi: 10.14357/19922264230311. EDN: XHTMVI.
18. *Достовалова А. М.* Нейросетевое квадродерево и его применение для сегментирования спутниковых изображений // *Информатика и её применения*, 2024. Т. 18. Вып. 4. С. 77–85. doi: 10.14357/19922264240410. EDN: LCGQQC.
19. *Грушо А. А., Грушо Н. А., Забейжайло М. И., Кульченков В. В., Тимонина Е. Е.* Классификация малых наборов данных большой размерности // *Информатика и её применения*, 2025. Т. 19. Вып. 3. С. 67–72. doi: 10.14357/19922264250308. EDN: SUSRRC.
20. *Hao J., Phung S. L., Di Y., et al.* Enhanced experience replay for class incremental continual learning // *Conference (International) on Digital Image Computing: Techniques and Applications Proceedings*. — IEEE, 2023. P. 258–264. doi: 10.1109/DICTA60407.2023.00043.
21. *Chen T., Kornblith S., Norouzi M., Hinton G.* A simple framework for contrastive learning of visual representations // *Machine learning / Eds. H. Daumé, A. Singh*. — *Proceedings of machine learning research ser.* — PMLR, 2020. Vol. 119. P. 1597–1607. doi: 10.5555/3524938.3525087.
22. *Gorshenin A. K., Dostovalova A. M.* Small sample classification and regression for time series and tabular data based on deep Gaussian mixture models // *Pattern Recognition Image Analysis*, 2025. Vol. 35. Iss. 2. P. 83–93. doi: 10.1134/S1054661825700014. EDN: AUJMF.
23. *Bergstra J., Bengio Y.* Random search for hyper-parameter optimization // *J. Mach. Learn. Res.*, 2012. Vol. 13. Iss. 10. P. 281–305.
24. *Hakim A., Zubak I., Marx C., et al.* Feasibility of using Gramian angular field for preprocessing MR spectroscopy data in AI classification tasks: Differentiating glioblastoma from lymphoma // *Eur. J. Radiol.*, 2025. Vol. 184. Art. 111957. 8 p. doi: 10.1016/j.ejrad.2025.111957.
25. *Toner W., Lee T. L., Joosen A., Singh R., Asenov M.* Performance of zero-shot time series foundation models on cloud data. — *Cornell University*, 2025. arXiv.2502.12944 [cs.LG]. 12 p.
26. *Tan M., Merrill M. A., Gupta V., Althoff T., Hartvigsen T.* Are language models actually useful for time series forecasting? // *38th Annual Conference on Neural Information Processing Systems Proceedings*. — *Curran Associates Inc.*, 2024. Vol. 37. P. 60162–60191. doi: 10.5555/3737916.3739838.

Поступила в редакцию 14.04.2026

Принята к публикации 15.08.2026

SELF-SUPERVISED INCREMENTAL CLASS DISCOVERY VIA PROBABILITY-INFORMED CONTINUAL LEARNING

A. M. Dostovalova and A. K. Gorshenin

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: The paper proposes a method for solving the continuous incremental classification problem, which consists in discovering new classes in data streams under the condition of absent labeling for limited time series and tabular data. To generate accurate pseudolabels for new data that complement previously identified patterns, a specialized neural network was developed whose architecture is informed by a deep mixture of Gaussian distributions and which implements learning based on a contrastive loss function. The method was tested on publicly available datasets using various discriminator architectures, including the Transformer. The performance of the proposed method was compared against uninformed networks and machine learning methods for pseudo-labeling. The informed network demonstrates superior generalization capabilities in detecting new classes within unlabeled data, particularly under conditions of small-scale training datasets. The gain in the harmonic F_1^H metric, which balances the recognition accuracy for objects of old and new classes, reaches 66.32% (with an average value of 15.28%), while the macroaveraged classification accuracy for the dataset based on the F_1^{avg} metric increases by 52.86% (with an average value of 11.8%).

Keywords: incremental learning; probability informing; new classes discovery; unlabeled data; deep Gaussian mixture models

DOI: 10.14357/19922264260307

EDN: ZDDABJ

Acknowledgments

The research was supported by the Russian Science Foundation, project No. 25-21-00448 (<https://rscf.ru/project/25-21-00448/>). The research was carried out using the infrastructure of the Shared Research Facilities “High Performance Computing and Big Data” (CKP “Informatics”) of FRC CSC RAS (Moscow).

References

- Hofmanninger, J., M. Perkonigg, J. A. Brink, *et al.* 2020. Dynamic memory to alleviate catastrophic forgetting in continuous learning settings. *Medical image computing and computer assisted intervention*. Eds. A. L. Martel, P. Abolmaesumi, D. Stoyanov, D. Mateus, M. A. Zuluaga, S. K. Zhou, D. Racocanu, and L. Joskowicz. Lecture notes in computer science. Cham: Springer. 12262:359–368. doi: 10.1007/978-3-030-59713-9_35.
- Ribeiro, A. G., L. Vilça, C. Costa, *et al.* 2025. Automatic visual inspection for industrial application. *J. Imaging* 11(10):350. 30 p. doi: 10.3390/jimaging11100350.
- Harman, F. 2026. Incremental learning in medical imaging: A comprehensive survey of deep neural network advances and challenges. *IEEE Access* 14:15812–15840. doi: 10.1109/ACCESS.2026.3659025.
- Wang, L., K. Yang, C. Li, L. Hong, Z. Li, and J. Zhu. 2021. ORDisCo: Effective and efficient usage of incremental unlabeled data for semi-supervised continual learning. *IEEE/CVF Conference on Computer Vision and Pattern Recognition Proceedings*. IEEE. 5379–5388. doi: 10.1109/CVPR46437.2021.00534.
- Lechat, A., S. Herbin, and F. Jurie. 2021. Pseudo-labeling for class incremental learning. *32nd British Machine Vision Conference Proceedings*. British Machine Vision Association. Art. 332. 14 p. doi: 10.5244/C.35.363.
- Wang, Q., K. Xu, D. Feng, *et al.* 2025. Memory replay with unlabeled data for semi-supervised class-incremental learning via temporal consistency. *Front. Comput. Sci. — Chi.* 19(12):1912370. 4 p. doi: 10.1007/s11704-025-40828-0.
- Roy, S., M. Liu, Z. Zhong, N. Sebe, and E. Ricci. 2022. Class-incremental novel class discovery. *Computer vision*. Eds. S. Avidan, G. Brostow, M. Cissé, G. M. Farinella, and T. Hassner. Lecture notes in computer science. Springer. 13693:317–333. doi: 10.1007/978-3-031-19827-4_19.
- An, J., Z. Du, H. Zhang, and D. Wu. 2025. TSPT: Two-step prompt tuning for class-incremental novel class discovery. *Knowl.-Based Syst.* 319:113603. 10 p. doi: 10.1016/j.knsys.2025.113603.
- Besnard, Q., and N. Ragot. 2024. Continual learning for time series forecasting: A first survey. *Engineering Proceedings* 68(1):49. 10 p. doi: 10.3390/engproc2024068049.
- Qiao, Z., Q. Pham, Z. Cao, *et al.* 2024. Class-incremental learning for time series: Benchmark and evaluation. *30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining Proceedings*. New York, NY: ACM. 5613–5624. doi: 10.1145/3637528.3671581.

11. Viroli, C., and G.J. McLachlan. 2019. Deep Gaussian mixture models. *Stat. Comput.* 29(1):43–51. doi: 10.1007/s11222-017-9793-z.
12. Karniadakis, G. E., I. G. Kevrekidis, L. Lu, P. Perdikaris, S. Wang, and L. Yang. 2021. Physics-informed machine learning. *Nature Reviews Physics* 3(6):422–440. doi: 10.1038/s42254-021-00314-5.
13. Gorshenin, A. K., and V. Yu. Kuzmin. 2020. Analiz konfiguratsiy LSTM-setey dlya postroeniya srednesrochnykh vektornykh prognozov [Analysis of configurations of LSTM networks for medium-term vector forecasting]. *Informatika i ee primeneniya — Inform. Appl.* 14(1):10–16. doi: 10.14357/19922264200102. EDN: SZNTXE.
14. Gorshenin, A. K., and V. Yu. Kuzmin. 2021. Metod povysheniya tochnosti neyrosetevykh prognozov s ispol'zovaniem smeshannykh veroyatnostnykh modeley i ego realizatsiya v vide tsifrovogo servisa [Method for improving accuracy of neural network forecasts based on probability mixture models and its implementation as a digital service]. *Informatika i ee primeneniya — Inform. Appl.* 15(3):63–74. doi: 10.14357/19922264210309. EDN: FDRKZX.
15. Gorshenin, A. K., and V. Yu. Kuzmin. 2022. Statistical feature construction for forecasting accuracy increase and its applications in neural network based analysis. *Mathematics* 10(4):589. 21 p. doi: 10.3390/math10040589. EDN: PQFGHU.
16. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, V. O. Piskovski, and E. E. Timonina. 2025. Mashinnoe obuchenie i doverie k rezul'tatam klassifikatsii [Machine learning and trust in classification results]. *Informatika i ee Primeneniya — Inform. Appl.* 19(2):63–68. doi: 10.14357/19922264250208. EDN: CXRNNK.
17. Gorshenin, A. K., S. A. Gorbunov, and D. Yu. Volkanov. 2023. O klasterizatsii ob'ektov setevoy vychislitel'noy infrastruktury na osnove analiza statisticheskikh anomalii v trafike [Toward clustering of network computing infrastructure objects based on analysis of statistical anomalies in network traffic]. *Informatika i ee primeneniya — Inform. Appl.* 17(3):76–87. doi: 10.14357/19922264230311. EDN: XHTMVI.
18. Dostovalova, A. M. 2024. Neyrosetevoe kvadroderevo i ego primeneniye dlya segmentirovaniya sputnikovyykh izobrazheniy [Neural quadtree and its applications for SAR imagery segmentation]. *Informatika i ee primeneniya — Inform. Appl.* 18(4):77–85. doi: 10.14357/19922264240410. EDN: LCGQQC.
19. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, V. V. Kulchenkov, and E. E. Timonina. 2025. Klassifikatsiya malykh naborov dannykh bol'shoy razmernosti [Classification of small sets of data of large dimension]. *Informatika i ee Primeneniya — Inform. Appl.* 19(3):67–72. doi: 10.14357/19922264250308. EDN: SUSRRC.
20. Hao, J., S. L. Phung, Y. Di, H. T. Le, and A. Bouzerdoum. 2023. Enhanced experience replay for class incremental continual learning. *Conference (International) on Digital Image Computing: Techniques and Applications Proceedings*. IEEE. 258–264. doi: 10.1109/DICTA60407.2023.00043.
21. Chen, T., S. Kornblith, M. Norouzi, and G. Hinton. 2020. A simple framework for contrastive learning of visual representations. *Machine learning*. Eds. H. Daumé and A. Singh. Proceedings of machine learning research ser. PMLR. 149:1597–1607. doi: 10.5555/3524938.3525087.
22. Gorshenin, A. K., and A. M. Dostovalova. 2025. Small sample classification and regression for time series and tabular data based on deep Gaussian mixture models. *Pattern Recognition Image Analysis* 35(2):83–93. doi: 10.1134/S1054661825700014. EDN: AUJMFC.
23. Bergstra, J., and Y. Bengio. 2012. Random search for hyper-parameter optimization. *J. Mach. Learn. Res.* 13(10):281–305.
24. Hakim, A., I. Zubak, C. Marx, et al. 2025. Feasibility of using Gramian angular field for preprocessing MR spectroscopy data in AI classification tasks: Differentiating glioblastoma from lymphoma. *Eur. J. Radiol.* 184:111957. 8 p. doi: 10.1016/j.ejrad.2025.111957.
25. Toner, W., T. L. Lee, A. Joosen, R. Singh, and M. Asenov. 2025. Performance of zero-shot time series foundation models on cloud data. Cornell University. 12 p. Available at: <https://arxiv.org/pdf/2502.12944> (accessed August 10, 2026).
26. Tan, M., M. A. Merrill, V. Gupta, T. Althoff, and T. Hartvigsen. 2024. Are language models actually useful for time series forecasting? *38th Annual Conference on Neural Information Processing Systems Proceedings*. Curran Associates Inc. 37:60162–60191. doi: 10.5555/3737916.3739838.

Received April 14, 2026

Accepted August 15, 2026

Contributors

Dostovalova Anastasia M. (b. 1999) — junior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; adostovalova@frccsc.ru

Gorshenin Andrey K. (b. 1986) — Doctor of Science in physics and mathematics, associate professor, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; agorshenin@frccsc.ru

МЕТОДЫ ПОРОЖДЕНИЯ МЕТРИК НА МНОЖЕСТВАХ ОБЪЕКТОВ В КОНТЕКСТЕ ТОПОЛОГИЧЕСКОЙ ТЕОРИИ АНАЛИЗА ДАННЫХ.

ЧАСТЬ 2. ЭКСПЕРИМЕНТАЛЬНОЕ ПОРОЖДЕНИЕ МЕТРИК НА ОБЪЕКТАХ В КОНТЕКСТЕ МЕТРИЧЕСКИХ АЛГОРИТМОВ ЧИСЛОВОГО ПРОГНОЗИРОВАНИЯ

И. Ю. Торшин¹

Аннотация: В первой части работы систематизированы основные теоретические направления для порождения проблемно-ориентированных метрик на множествах объектов (ρ_Q -метрик) на базе метрик на признаках (ρ_L -метрик). В данной статье на основе анализа понятий компактности получены критерии настройки ρ_Q -метрик. Проведены вычислительные эксперименты на 1000 независимых выборках данных с использованием 5000 ρ_Q -метрик, синтезированных в соответствии с предлагаемыми 20 подходами, для числового прогнозирования алгоритмами k -ближайших соседей. Вычислительные эксперименты показали, что в 95% случаев эффективными оказались ρ_Q -метрики трех типов: на основе синтетических числовых признаков (61%), с попарным сопоставлением на основе векторов (22%) и некоммутативные метрики на основе массивов ρ_L -расстояний (12%). Важно отметить, что ρ_Q -метрики на основе синтетических числовых признаков могут обеспечить одни из наилучших результатов для 83% выборок данных, что делает данный подход наиболее перспективным.

Ключевые слова: топологический анализ данных; функции расстояния на объектах; алгебраический подход; теория анализа значений признаков

DOI: 10.14357/19922264260308

EDN: ZZTDAQ

1 Введение

Алгоритмы кластеризации, классификации, распознавания и числового прогнозирования используют метрические функции расстояния на множествах исследуемых объектов (ρ_Q -метрики). Представленное в первой части настоящей статьи описание проблемы порождения ρ_Q -метрик в контексте современных методов анализа данных указало на наличие обширного массива эмпирических способов введения метрик на множествах объектов и на отсутствие сколько-нибудь теоретически обоснованных способов решения этой важной вспомогательной задачи.

Необходимость систематизации способов определения ρ_Q -метрик обусловила применение методов топологической теории анализа данных научной школы академиков Ю.И. Журавлёва и К.В. Рудакова [1–3] в первой части исследования [4]. В данной, второй, части представлены результаты практического применения теоретического аппарата, разработанного в первой части статьи.

В первой части были систематизированы теоретические направления порождения ρ_Q -метрик с акцентом на направление, связанное с использова-

нием метрик на множествах объектов $\Gamma_k^{-1}(\Gamma_k(x_i))$ (ρ_L -метрик) [4]. Множества $\Gamma_k^{-1}(\Gamma_k(x_i))$ соответствуют значениям элементарных признаков $\Gamma_k(x_i)$ объектов $x_i \in \mathbf{X}$ в пространстве $(\mathbf{X}, T(\mathbf{X}))$, образованном топологией $T(\mathbf{X})$ над множеством исходных описаний объектов $\mathbf{X}$. Систематизация способов порождения ρ_Q -метрик была осуществлена на основе фундаментальных различий в методах учета элементарных признаков Γ_k и сопоставления множеств $\Gamma_k^{-1}(\Gamma_k(x_i))$ [4]:

- (1) коммутативный учет элементарных признаков с поэлементным сопоставлением множеств $\Gamma_k^{-1}(\Gamma_k(x_i))$, включая расстояния на основе синтетических числовых признаков;
- (2) коммутативный учет Γ_k с попарным сопоставлением множеств $\Gamma_k^{-1}(\Gamma_k(x_i))$,
- (3) некоммутативный учет Γ_k с поэлементным сопоставлением $\Gamma_k^{-1}(\Gamma_k(x_i))$;
- (4) некоммутативный учет Γ_k с попарным сопоставлением $\Gamma_k^{-1}(\Gamma_k(x_i))$.

В табл. 1 суммированы сформулированные в настоящей работе подходы.

Подходы, перечисленные в табл. 1, служат базой для проведения вычислительных экспериментов по

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, itorshin@frccsc.ru

Таблица 1 Предлагаемые способы определения ρ_Q -метрик между объектами x_i и x_j посредством ρ_L -метрик

Обозначение	Название	Примечание
Коммутативный учет Γ_k с поэлементным сопоставлением множеств из $\Gamma(x_i), \Gamma(x_j)$		
$\rho_{Q\bar{w}\otimes}(x_i, x_j)$	Метрика Хэмминга с весами и корректором	Булевы Γ_k
$\rho_{Q\bar{w}\Sigma}(x_i, x_j)$	Квазилинейные модели	Небулевы Γ_k
$\rho_{Q\bar{w}\Phi\otimes}(x_i, x_j)$	ЭФР-метрики	Булевы Γ_k
$\rho_{Q\bar{w}\Phi\Phi}(x_i, x_j)$	ЭФР-метрики	Небулевы Γ_k
$\rho_{Q\bar{w}\Gamma_{k'}}(x_i, x_j)$	Расстояния на синтетических числовых признаках	Любые Γ_k
Коммутативный учет Γ_k с попарным сопоставлением множеств из $\Gamma(x_i), \Gamma(x_j)$		
$\rho_{Q\bar{w}\Sigma_{12}}(x_i, x_j)$	Квазилинейные модели	Любые Γ_k
$\rho_{Q\bar{w}\Phi_{12}}(x_i, x_j)$	ЭФР-метрики	Любые Γ_k
$\rho_{Q\bar{w}\Sigma_{12}\min}(x_i, x_j)$	Квазилинейные модели над списком минимальных расстояний	Любые Γ_k
$\rho_{Q\bar{w}\Phi_{12}\min}(x_i, x_j)$	ЭФР-метрики над списком минимальных расстояний	Любые Γ_k
$\rho_{Q\bar{w}v_{12}}(x_i, x_j)$	«Векторные» метрики между $\rho_{L_{12}}(x_i)$ и $\rho_{L_{12}}(x_j)$	Любые Γ_k
$\rho_{Q\bar{w}\Phi_{12}}(x_i, x_j)$	ЭФР-метрики между $\rho_{L_{12}}(x_i)$ и $\rho_{L_{12}}(x_j)$	Любые Γ_k
$\hat{\Phi}(x)\rho_{L_{12}}(x_i)$	Метрики на основе синтетических ЭФР-признаков	Любые Γ_k
Некоммутативный учет Γ_k с поэлементным/попарным сопоставлением $\Gamma(x_i), \Gamma(x_j)$		
$\rho_{Q\theta\otimes}(x_i, x_j)$	На основе массива булевых расстояний	Булевы Γ_k
$\rho_{Q\theta}(x_i, x_j)$	На основе массива расстояний $\rho_{L_{12}}(x_i, x_j)$	Небулевы Γ_k
$\rho_{Q\theta_{12}}(x_i, x_j)$	На основе массива расстояний $\rho_{L_{12}}(x_i, x_j)$	Любые Γ_k
$\rho_{Q\theta_{121}}(x_i, x_j)$	На основе массивов расстояний $\rho_{L_{12}}(x_i)$ и $\rho_{L_{12}}(x_j)$	Любые Γ_k
ρ_{Qa} -метрики типа «объект–класс» и соответствующие ρ_Q -метрики		
$\rho_{Qa\bar{w}\Sigma}(x_i, x_j)$	Квазилинейные модели ρ_{Qa} -метрик	Любые Γ_k
$\rho_{Qa\bar{w}\Phi}(x_i, x_j)$	ЭФР ρ_{Qa} -метрики	Любые Γ_k
$\rho_{Q\bar{w}v_{12a}}(x_i, x_j)$	«Векторные» ρ_Q -метрики между $\rho_{La}(x_i)$ и $\rho_{La}(x_j)$	Любые Γ_k
$\rho_{Q\bar{w}\Phi_{12a}}(x_i, x_j)$	ЭФР ρ_Q -метрики между $\rho_{La}(x_i)$ и $\rho_{La}(x_j)$	Любые Γ_k

Примечания: $\rho_{Q\bar{w}}$ — параметризованная метрика с весами $\bar{w}$; ЭФР — эмпирические функции распределения.

оценке их применимости к решению соответствующих задач. Для практического использования этих определений ρ_Q -метрик необходимо разработать методы введения экспертных метрик на основе множества прецедентов $Q = \varphi(\mathbf{X})$, по которым будут настраиваться предлагаемые в табл. 1 метрики. С этой целью далее приведены результаты анализа математических понятий компактности и получен критерий настройки ρ_Q -метрик, делающий возможным проведение соответствующих вычислительных экспериментов. Затем представлены результаты проведения соответствующих вычислительных экспериментов.

2 О проблематике введения экспертных метрик на пространствах объектов на основе информации в множестве прецедентов

В общем случае ρ_Q -метрики, вводимые по любому из предлагаемых выше подходов, содержат

те или иные параметры, значения которых неизвестны. Обозначим такие параметризованные ρ_Q -метрики как $\rho_{Q\bar{w}}$. Для получения $\rho_{Q\bar{w}}$ -метрик, наиболее адекватных конкретной прикладной задаче, необходимо настроить вектор весов $\bar{w}$. Для настройки вектора весов методами локальной или глобальной оптимизации необходим некоторый функционал, оценивающий качество метрики, соответствующей тому или иному значению $\bar{w}$. Если используемая форма такого функционала включает оценку отличий в значениях $\rho_{Q\bar{w}}$ -метрики для всех пар объектов от значений некоторой эталонной («экспертной») метрики (значения которой известны на основании информации, задаваемой множеством прецедентов Q), то это обуславливает необходимость введения тех или иных «экспертных» метрик.

С математической точки зрения подходы к определению экспертных метрик целесообразно основывать на понятиях компактности изучаемых множеств и пространств объектов. В функциональном анализе термин «компактность» указывает на свойство множества/пространства содержать в бесконечном покрытии конечное подпокрытие [5]. Произвольное метрическое пространство компактно

тогда и только тогда, когда оно «вполне ограничено» или «предкомпактно» (для произвольного $\varepsilon > 0$ существует конечная ε -сеть) и «полно» (для каждой точки есть центрированная система окрестностей с непустым пересечением).

Очевидно, что в функциональном анализе свойства «вполне ограничено» и «полно» подразумевают операции с бесконечно малыми величинами (произвольное $\varepsilon > 0$), использование предельного перехода и, таким образом, пространства мощности континуума. В то же время множество исходных описаний объектов $\mathbf{X}$, индуцированное над $\mathbf{X}$ топологическое пространство $(\mathbf{X}, T(\mathbf{X}))$, решетка $L(T(\mathbf{X}))$ и метрическое пространство значений признаков $M_L(L(T(\mathbf{X})), \rho_L)$ конечны.

Доказанная в работе [6] теорема о регулярности и нормальности дискретных топологических и метрических пространств показала, что выполнение условия регулярности $\mathbf{X}$ одновременно гарантирует и существование «дискретных» ε -сетей, и существование центрированной системы окрестностей для любой точки, соответствующей атому решетки $L(T(\mathbf{X}))$ (т.е. объекту q_i , так что «точкой прикосновения» такой системы окрестностей служит по крайней мере сам объект q_i). Таким образом, пространство $(\mathbf{X}, T(\mathbf{X}))$ при условии регулярности множества $\mathbf{X}$ компактно по построению, равно как и его подмножества. Однако при сопоставлении пространству $(\mathbf{X}, T(\mathbf{X}))$ метрического пространства объектов $M_Q(\mathbf{X}, \rho_Q)$ (посредством введения ρ_L и затем ρ_Q -метрик) свойства компактности произвольных множеств точек в $M_Q(\mathbf{X}, \rho_Q)$ будут зависеть от свойств ρ_L и ρ_Q .

Взаимосвязь приведенных выше определений компактности из функционального анализа и интуитивного понимания «кластера» как своего рода «компактного» множества точек («точки кластера K в пространстве M ближе друг к другу, чем к остальным точкам M ») была подробно исследована ранее [7]. Следствия из соответствующих теорем позволяют определить « ε_0 -отделимость кластера», которая описывается метрикой специального вида, применимой в качестве экспертной.

В применении к задачам классификации и числового прогнозирования простейшим способом оценки компактности множества в $M_Q(\mathbf{X}, \rho_Q)$ служит непараметрическая метрика разреза $\rho_A(x_i, x_j)$, вычисляемая на основании множества прецедентов Q . Например, если t -я целевая переменная Γ_t соответствует многоклассовой задаче с $|\mathbf{I}_t|$ классами A_{tr} , $r = \overline{1, |\mathbf{I}_t|}$, проводится суммирование по классам и нормировка на интервал $[0, 1]$:

$$\rho_A(x_i, x_j) = \frac{1}{2} \sum_{r=1}^{|\mathbf{I}_t|} ((x_i \in A_r) - (x_j \in A_r))^2.$$

Тогда комбинаторный показатель качества настройки ρ_Q -метрики с весами $\vec{w}$, $\rho_{Q\vec{w}}$, относительно экспертной ρ_A записывается как

$$d\rho(\rho_A, \rho_{Q\vec{w}}, \mathbf{X}) = \frac{2}{N(N-1)} \sum_{i=1}^N \sum_{j=i+1}^N (\rho_A(x_i, x_j) - \rho_{Q\vec{w}}(x_i, x_j))^2, \\ x_i, x_j \in \mathbf{X}, N = |\mathbf{X}|,$$

а критерием настройки $\rho_{Q\vec{w}}$ служит минимум $d\rho(\rho_A, \rho_{Q\vec{w}}, \mathbf{X})$:

$$\vec{w} = \arg \min d\rho(\rho_A, \rho_{Q\vec{w}}, \mathbf{X}).$$

3 Вычислительные процедуры для экспериментального тестирования предлагаемых способов порождения ρ_Q -метрик

Эксперименты проведены на модельных данных для задачи числового прогнозирования с признаковыми описаниями объектов в виде векторов $\vec{x} = (x_i)$ булевых признаков ($n = 50$, $i = \overline{1, n}$). Числовые значения целевой переменной вычислялись с помощью булева полинома

$$B(\vec{x}) = \sum_{i=0}^n \sum_{j=0}^n \sum_{l=0}^n w_{ijl} x_i x_j x_l, \quad x_0 = 1,$$

с корректирующим преобразованием $\text{corr}(B(\vec{s}))$ и стохастическим компонентом, абсолютная величина которого составляла $0,05 \text{random}(\cdot) \text{corr}(B(\vec{x}))$. Было сгенерировано 1000 выборок модельных данных по 100 объектов со случайными весами и с корректирующими преобразованиями, выбранными случайным образом из списка элементарных алгебраических функций.

Для порождения ρ_Q -метрик были использованы 13 подходов, перечисленных в табл. 1, которые позволяют оперировать элементарными булевыми признаками Γ_k (т.е. подходы $\rho_{Q\emptyset}$, $\rho_{Q\vec{w}\Phi}$ и $\rho_{Q\vec{w}\Sigma}$ и ρ_{qa} -метрики были исключены). В качестве ρ_L -метрик были использованы 93 метрики из справочника [8]. При порождении синтетических числовых признаков и метрик типа $\rho_{Q\vec{w}\Gamma_k}$, в качестве опорных функций были использованы различные фильтры на основе Фурье-разложения, вейвлетов и др. (всего 11 методов), как и ранее [6]. Для каждой из 1000 выборок данных были порождены и настроены 4997 (~ 5000) ρ_Q -метрик.

В качестве алгоритмов прогнозирования числовых таргетных переменных использовались:

- (1) алгоритмы k -ближайших соседей (k -Nearest Neighbor, kNN) в различных конфигурациях (всего 16 алгоритмов);
- (2) алгоритмы на основе синтетических числовых признаков с корректорами в виде «нейронных сетей» с несколькими слоями (от 2 до 10) с функцией активации softmax;
- (3) алгоритмы на основе синтетических числовых признаков с корректорами в виде полиномов различных конструкций (более 20 формул, включая квазиполиномиальные модели с элементарными функциями).

Оператор семплирования $\hat{\zeta}$ был реализован как десятикратная кросс-валидация с делением каждой выборки объектов на обучение (50%) и контроль (50%).

При заданной ρ_Q -метрике конфигурации kNN-алгоритмов формировались для различных значений k (3, 5, 10 и 20; индивидуальные алгоритмы обозначены как 3NN, 5NN и т. д.); для того же набора значений k с поправками на квартиль (класс) значений таргетной переменной (3NNc, 5NNc и т. д.); алгоритмы с ядром Епанечникова для различных значений параметра λ (0,1, 0,3, 0,5 и 1,0; обозначены как E0,1, E0,3 и т. д.) и алгоритмы с ядром Гаусса [9] для того же набора значений λ (G0,1, G0,3 и т. д.) — таким образом, всего 16 алгоритмов.

4 Результаты экспериментального тестирования

Основная серия экспериментов включала генерацию, настройку и применение ~ 5000 ρ_Q -метрик в 16 алгоритмах kNN (т. е. $16 \cdot 5000 = 80\,000$ конкретных kNN-алгоритмов) для описанных выше выборок модельных данных ($n = 1000$). Анализ показателей качества результатов, производимых изученными алгоритмами числового прогнозирования, был проведен по значениям ранговой корреляции на контроле. В среднем по всем выборкам данных (табл. 2) лучший kNN-алгоритм (выбранный из 80 000 алгоритмов) давал результаты ($r_c = 0,80 \pm 0,07$), сопоставимые с применением метода синтетических числовых признаков с полиномиальными корректорами ($r_c = 0,84 \pm 0,05$) или с нейросетевыми корректорами ($r_c = 0,83 \pm 0,06$), описанными в работе [6]. В то же время kNN-алгоритмы показали худшие показатели переобучения (переобученность $|r - r_c| = 0,14$), чем алгоритмы на основе синтетических признаков (переобученность 0,09).

Более детальный анализ позволил оценить перспективность дальнейшего использования тех или иных способов определения ρ_Q (табл. 3), способов определения ρ_L -метрик и различных алгоритмов kNN. Для каждой из 1000 выборок данных, наилучший из 80 000 изученных алгоритмов kNN выбирался на основе лексикографического упорядочения результатов применения алгоритмов по убыванию значений r_c , r , SD_c и SD .

Таблица 2 Показатели качества использованных алгоритмов числового прогнозирования. Усреднение проведено по 1000 выборок данных

Алгоритм/показатель	kNN (лучший)	$\Gamma_{k'}$ (полиномы)	$\Gamma_{k'}$ (нейросеть)
k	50 ± 294	$1,0 \pm 0,1$	$1,2 \pm 22$
b	-24 ± 142	$0,0 \pm 0,01$	$-0,14 \pm 11$
r	$0,94 \pm 0,04$	$0,93 \pm 0,04$	$0,92 \pm 0,06$
r_c	$0,8 \pm 0,07$	$0,84 \pm 0,05$	$0,83 \pm 0,06$
k_c	$47,5 \pm 280$	$0,93 \pm 0,1$	$0,98 \pm 0,17$
b_c	-23 ± 135	$0,02 \pm 0,1$	$0,00 \pm 0,11$
SD	$0,11 \pm 0,06$	$0,10 \pm 0,03$	$0,01 \pm 0,01$
SD_c	$0,2 \pm 0,04$	$0,16 \pm 0,02$	$0,03 \pm 0,01$

Примечания: k и b — параметры линейной аппроксимации в координатах «известное значение» — «прогноз алгоритма»; r — коэффициент ранговой корреляции; SD — стандартное отклонение рангов на обучающих выборках; k_c , b_c , r_c и SD_c — значения вышеуказанных показателей качества алгоритмов на контрольных выборках; kNN(лучший) — наилучший результат метода k -ближайших соседей (16 алгоритмов kNN, для каждого изучено около 5000 ρ_Q -метрик); $\Gamma_{k'}$ (полиномы) — синтетические числовые признаки с полиномиальным корректором; $\Gamma_{k'}$ (нейросеть) — синтетические числовые признаки с нейросетевым корректором.

Таблица 3 Частоты встречаемости различных способов определения ρ_Q -метрик в лучших алгоритмах kNN, полученных перебором 16 алгоритмов по 5000 ρ_Q -метрикам в 1000 модельных выборок

ρ_Q	Доля лучших kNN	r	r_c	SD	SD _c	sum%
$\rho_{Q\bar{w}\Gamma_{k'}}$	61,1%	0,93	0,81	0,10	0,18	61,1%
$\rho_{Q\bar{w}v12}$	22,0%	0,97	0,76	0,09	0,22	83,1%
$\rho_{Q\theta121}$	11,5%	0,96	0,81	0,18	0,22	94,6%
$\rho_{Q\theta12}$	2,9%	0,94	0,80	0,22	0,25	97,5%
$\rho_{Q\bar{w}\Phi12}$	1,8%	0,91	0,76	0,14	0,20	99,3%

Примечания: r — коэффициент ранговой корреляции; sum% — суммарное покрытие всех выборок данных kNN-алгоритмами на основе перечисленных выше метрик.

Наиболее важным результатом всей серии экспериментов стал тот факт, что из 13 использованных подходов к порождению метрик только 5 подходов входили в наилучшие алгоритмы числового прогнозирования на основании kNN (см. табл. 3). При этом для 94,6% выборок лучшие алгоритмы kNN включали использование всего трех подходов к определению ρ_Q : $\rho_{Q\bar{w}\Gamma_{k'}}$ (входил в наилучшие kNN-алгоритмы для 61% выборок данных); $\rho_{Q\bar{w}v12}$ (22%); $\rho_{Q\theta121}$ (12%). В случае если выбирать в качестве лучших не 1 из 80 000, а 10 наилучших из 80 000 kNN-алгоритмов, то ρ_Q -метрики типа $\rho_{Q\bar{w}\Gamma_{k'}}$ обеспечивали наилучший результат уже для 83,1% выборок данных, причем без снижения средних значений ранговых коэффициентов корреляции на контроле.

Анализ различных ρ_L -метрик в лучших алгоритмах kNN, вне зависимости от используемого способа определения ρ_Q , показал, что наиболее часто лучшие kNN-алгоритмы формировались на основе следующих ρ_L -метрик над множествами функций: метрики Колмогорова (6,2% выборок), инженерной (5,5%), фон Мизеса (5,2%), Кульбака–Лейблера (3,1%), Реньи (2,7%), Lp-метрики (2%) и χ^2 -метрики (2%).

Анализ частот вхождения различных kNN-алгоритмов в наилучшие решения при переборе 16 алгоритмов по 5000 ρ_Q -метрик в 1000 модельных выборок показал, что для 53,4% выборок наилучшим оказался 3NN-алгоритм, а для 23% выборок — один из алгоритмов G0,5, G1,0 или G0,1.

5 Обсуждение результатов

Метрики расстояния на объектах используются прежде всего в алгоритмах типа k -ближайших соседей и, конечно же, в алгоритмах кластеризации. Алгоритмы kNN, предложенные еще в 1951 г., по-прежнему остаются одним из ключевых инстру-

ментов современного интеллектуального анализа данных для предобработки пропусков в данных, рекомендательных систем, решениях задач из области финансов и экономики (оценка кредитных рисков, прогнозирование фондового рынка и др.), в биомедицине [10] и распознавании образов [11]. Преимущества kNN включают простоту реализации и адаптации к новым данным, минимум гиперпараметров [12].

Выбор метрики для алгоритмов kNN остается острой исследовательской проблемой — ведь ρ_Q -метрика, неоптимальная для конкретной задачи, значительно снижает показатели качества работы алгоритма [13]. В задачах, которые могут быть описаны с использованием многомерных пространств (особенно в случае разнородных признаков описаний), часто используемые метрики (евклидова и др.) неэффективны без тех или иных преобразований признаков, так как неподходящее ρ_Q -расстояние приводит к сильному искажению выбора окрестностей объектов (феномен «проклятия размерности»). Современные подходы к преодолению этой проблемы включают, почти без исключений, использование настраиваемых метрик (чаще всего — варианты метрики Махаланобиса) [14].

Настоящая работа заполняет существенные теоретические пробелы в области определения метрик для алгоритмов kNN. В имеющейся литературе теоретические методы порождения функций расстояния для kNN ограничены исключительно линейными пространствами (включая метрику Махаланобиса). Известны попытки применения топологического анализа данных в линейных пространствах (симплициальные комплексы, персистентные гомологии, мозаики Делоне) [15, 16], комбинирования биномиальной функции с евклидовым расстоянием [17]. Как ни странно, основной упор делается на скорость вычислений, а вовсе не на теоретические оценки релевантности получаемых метрик [18]. Поэтому суммированные в табл. 1

фундаментальные категории метрик важны для теоретического осознания проблем введения метрик на объектах.

Результаты проведенных в работе экспериментов также представляют существенный вклад в экспериментальное решение вопроса о выборе ρ_Q -метрики для алгоритмов kNN. Очевидно, что ответ на этот важный вопрос может быть получен посредством сравнительных экспериментальных исследований эффективности различных функций расстояния. По литературным данным, такие исследования ограничены использованием только лишь десятков метрик, тестируемых на десятках выборок достаточно простых реальных данных (в том числе из репозитория UCI). В этих исследованиях рассматриваются давно известные метрики (евклидово расстояние, Махаланобиса, манхэттенское, Минковского, Чебышёва, косинусов, корреляционное, Хэмминга, Жаккарда) и не предлагаются новые способы определения функций расстояния для алгоритмов kNN [10]. Если принять во внимание тот факт, что многие метрики содержат настраиваемые параметры, то опубликованные ранее экспериментальные оценки релевантности различных метрик носят фрагментарный характер.

Тем не менее важными результатами опубликованных ранее экспериментальных исследований стали выводы о том, что

- (1) производительность классификаторов kNN принципиально зависит от используемой метрики;
- (2) не существует оптимальной метрики, которую можно было бы использовать для произвольного набора данных;
- (3) важной характеристикой метрик служит устойчивость к шумовым факторам (в том числе к ошибкам в данных) [10, 19].

Интересно отметить, что, как и в случае порождения синтетических признаков на основе опорных цепей [20] в контексте фундаментальной проблемы метризации дискретных топологических пространств признаков [6], наиболее часто используемыми в наилучших kNN-алгоритмах оказались также ρ_L -метрики над множествами функций (Колмогорова, инженерная, фон Мизеса и др.), а не векторные метрики или метрики над множествами объектов. Теоретическая интерпретация этого факта составляет предмет дальнейших исследований.

Полученные в настоящей работе результаты экспериментального тестирования новых метрик подтверждают выводы работ [10, 19], при этом существенно превосходя ранее полученные результаты по объему проведенных вычислений: проведено

тестирование 16 типов алгоритмов kNN на 1000 выборок существенно нелинейных данных с использованием 5000 метрик (фундаментальные типы суммированы в табл. 1). Важно, что результаты настоящего исследования позволяют рекомендовать ρ_Q -метрики типа $\rho_{Q\bar{w}\Gamma_{k'}}$ как наиболее перспективный способ порождения метрик на объектах. Достоинство метрик $\rho_{Q\bar{w}\Gamma_{k'}}$ заключается в линейной зависимости времени вычислений от числа объектов и признаков. Этот результат позволяет существенно повысить вычислительную эффективность алгоритма числового прогнозирования: ведь для вычисления $\rho_{Q\bar{w}\Gamma_{k'}}$ требуется единственный синтетический признак с наибольшей информативностью и не требуется анализ остальных признаков (что становится существенным фактором устранения так называемого «проклятия размерности»).

6 Заключение

В рамках топологической теории распознавания метрики на множествах значений признаков (ρ_L -метрики) естественным образом вводятся как функционалы, оценивающие расстояние между элементами решетки $L(T(\mathbf{X}))$. В предыдущих работах были систематизированы подходы к порождению ρ_L -метрик, поэтому вполне естественно изучить возможности определения ρ_Q -метрик посредством ρ_L -метрик. Проведение вычислительных экспериментов показало, что из сформулированных в настоящей работе подходов в 95% случаев наиболее эффективными оказались метрики трех типов: коммутативные метрики на основе синтетических числовых признаков или на основе векторов и одна некоммутирующая метрика. Перспективы дальнейших исследований включают устойчивость ρ_Q -метрик к шумовым факторам, введение более сложных ρ_Q -метрик, основанных на использовании не единственного наиболее информативного синтетического признака, а нескольких. Последнее подразумевает использование многомерного пространства, в котором вводятся ρ_Q -метрики.

Литература

1. Журавлев Ю.И. Корректные алгебры над множествами некорректных (эвристических) алгоритмов, часть I // Кибернетика, 1977. № 4. С. 5–17.
2. Журавлев Ю.И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики, 1978. Вып. 33. С. 5–68.

3. Рудаков К. В. О симметрических и функциональных ограничениях для алгоритмов классификации // Докл. Акад. наук, 1987. Т. 297. Вып. 1. С. 43–46.
4. Торшин И. Ю. Методы порождения метрик на множествах объектов в контексте топологической теории анализа данных. Часть 1. Метрики на основе расстояний между значениями признаков // Информатика и её применения, 2026. Т. 20. Вып. 1. С. 39–44. doi: 10.14357/19922264260105. EDN: ZTDPJO.
5. Колмогоров А. Н., Фомин С. В. Элементы теории функций и функционального анализа. — 6-е изд. — М.: Наука, 1989. 624 с.
6. Торшин И. Ю. Метризация дискретных топологических пространств в контексте теории решеток. Часть 1. О нормальности пространств // Информатика и её применения, 2025. Т. 19. Вып. 1. С. 82–88. doi: 10.14357/19922264250111. EDN: CAWKMO.
7. Torshin I. Y., Rudakov K. V. On metric spaces arising during formalization of recognition and classification problems. Part 1: Properties of compactness // Pattern Recognition Image Analysis, 2016. Vol. 26. No. 2. P. 274–284. doi: 10.1134/S1054661816020255. EDN: WAMFRD.
8. Деца Е. И., Деца М. М. Энциклопедический словарь расстояний / Пер. с англ. — М.: Наука, 2008. 444 с. (Deza E. I., Deza M. M. Dictionary of distances. — Amsterdam, Netherlands: North-Holland, Elsevier, 2006. 412 p. doi: 10.1016/B978-0-44452087-6.X5000-8.)
9. Hastie T., Tibshirani R., Friedman J. H. The elements of statistical learning: Data mining, inference, and prediction. — New York, NY, USA: Springer, 2009. 745 p. doi: 10.1007/978-0-387-84858-7.
10. Hu L., Huang M., Ke S. The distance function effect on k -nearest neighbor classification for medical datasets // SpringerPlus, 2016. Vol. 5. No. 1. Art. 1304. 9 p. doi: 10.1186/s40064-016-2941-7.
11. Adeniyi D., Wei Z., Yongquan Y. Automated web usage data mining and recommendation system using K-Nearest Neighbor (kNN) classification method // Applied Computing Informatics, 2015. Vol. 12. Iss. 1. P. 90–108. doi: 10.1016/j.aci.2014.10.001.
12. Cover T., Hart P. Nearest neighbor pattern classification // IEEE T. Inform. Theory, 1967. Vol. 13. No. 1. P. 21–27. doi: 10.1109/TIT.1967.1053964.
13. Lopes N., Ribeiro B. On the impact of distance metrics in instance-based learning algorithms // Pattern recognition and image analysis / Eds. R. Paredes, J. Cardoso, and X. Pardo. — Lecture notes in computer science ser. — Cham: Springer, 2015. Vol. 9117. P. 48–56. doi: 10.1007/978-3-319-19390-8_6.
14. Mulak P., Talhar N. Analysis of distance measures using k -nearest neighbor algorithm on KDD dataset // Int. J. Science Research, 2015. Vol. 4. No. 7. P. 2101–2104.
15. Edelsbrunner H., Osang G. The multi-cover persistence of euclidean balls // Discrete Comput. Geom., 2021. Vol. 65. No. 4. P. 1296–1313. doi: 10.1007/s00454-021-00281-9.
16. Reani Y., Bobrowski O. Morse theory for the kNN distance function // Discrete Comput. Geom., 2026. Vol. 75. No. 2. P. 491–510. doi: 10.1007/s00454-025-00795-6.
17. Zou J., Li H. Precise marketing of e-commerce products based on KNN algorithm // Comput. Intel. Neurosc., 2022. Vol. 2022. Art. 4966439. 12 p. doi: 10.1155/2022/4966439.
18. Halder R. K., Uddin M. N., Uddin M. A. Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications // Big Data, 2024. Vol. 11. Art. 113. 55 p. doi: 10.1186/s40537-024-00973-y.
19. Abu Alfeilat H., Hassanat A., Lasassmeh O., Tarawneh A., Alhasanat M., Eyal Salman H., Prasath V. Effects of distance measure choice on K-nearest neighbor classifier performance: A review // Big Data, 2019. Vol. 7. No. 4. P. 221–248. doi: 10.1089/big.2018.0175.
20. Торшин И. Ю. О порождении синтетических признаков на основе опорных цепей и произвольных метрик в рамках топологического подхода к анализу данных. Часть 1. Включение в формализм эмпирических функций расстояния // Информатика и её применения, 2024. Т. 18. Вып. 1. С. 71–77. doi: 10.14357/19922264240110. EDN: RIVOXR.

Поступила в редакцию 12.03.2026

Принята к публикации 15.08.2026

METHODS FOR GENERATING METRICS ON OBJECT SETS IN THE CONTEXT OF TOPOLOGICAL DATA ANALYSIS THEORY. PART 2. EXPERIMENTAL GENERATION OF METRICS ON OBJECTS IN THE CONTEXT OF METRIC ALGORITHMS FOR NUMERICAL FORECASTING

I. Yu. Torshin

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: In the first part of this work, the main theoretical directions for generating problem-oriented metrics on sets of objects (ρ_Q -metrics) using metrics on features (ρ_L -metrics) were systematized. In this paper, criteria for tuning ρ_Q -metrics are obtained using concepts of compactness. Computational experiments were conducted on 1000 independent data samples with 5000 ρ_Q -metrics synthesized according to 20 proposed approaches for numerical forecasting by k -nearest neighbor algorithms. Computational experiments demonstrated that in 95% cases, ρ_Q -metrics of three types were effective: (i) those based on synthetic numerical features (61%); (ii) vector-based with pairwise matching (22%); and (iii) noncommutative metrics based on ρ_L -distance arrays (12%). Importantly, ρ_Q -metrics based on synthetic numerical features provided the best result for 83% of the datasets, which makes this approach the most promising.

Keywords: topological data analysis; distance functions on objects; algebraic approach; feature value analysis theory

DOI: 10.14357/19922264260308

EDN: ZZTDAQ

References

1. Zhuravlev, Yu. I. 1977. Correct algebras over sets of incorrect (heuristic) algorithms. I. *Cybernetics* 13(4):483–494.
2. Zhuravlev, Yu. I. 1978. Ob algebraicheskom podkhode k resheniyu zadach raspoznavaniya i klassifikatsii [On the algebraic approach to solving recognition and classification tasks]. *Problemy kibernetiki* [Problems of Cybernetics] 33:5–68.
3. Rudakov, K. V. 1988. Symmetric and functional constraints for classification algorithms. *Soviet Mathematics Doklady* 36(3):428–431.
4. Torshin, I. Yu. 2026. Metody porozhdeniya metrik na mnozhestvakh ob"ektov v kontekste topologicheskoy teorii analiza dannykh. Chast' 1. Metriki na osnove rasstoyaniy mezhdu znacheniyami priznakov [Methods for generating metrics on object sets in the context of theory of topological data analysis. Part 1. Metrics based on distances between feature values]. *Informatika i ee primeneniya — Inform. Appl.* 20(1):39–44. doi: 10.14357/19922264260105. EDN: ZTDPJO.
5. Kolmogorov, A. N., and S. V. Fomin. 1999. *Elements of the theory of functions and functional analysis*. New York, NY: Dover Publications. 448 p.
6. Torshin, I. Yu. 2025. Metrizatsiya diskretnykh topologicheskikh prostranstv v kontekste teorii reshetok. Chast' 1. O normal'nosti prostranstv [Metritization of discrete topological spaces in the context of lattice theory. Part 1. On the normality of spaces]. *Informatika i ee primeneniya — Inform. Appl.* 19(1):82–88. doi: 10.14357/19922264250111. EDN: CAWKMO.
7. Torshin, I. Yu., and K. V. Rudakov. 2016. On metric spaces arising during formalization of recognition and classification problems. Part 1: Properties of compactness. *Pattern Recognition Image Analysis* 26(2):274–284. doi: 10.1134/S1054661816020255. EDN: WAMFRD.
8. Deza, E. I., and M. M. Deza. 2006. *Dictionary of distances*. Amsterdam, Netherlands: North-Holland, Elsevier. 412 p. doi: 10.1016/B978-0-44452087-6.X5000-8.
9. Hastie, T., R. Tibshirani, and J. H. Friedman. 2009. *The elements of statistical learning: Data mining, inference, and prediction*. New York, NY: Springer. 745 p. doi: 10.1007/978-0-387-84858-7.
10. Hu, L., M. Huang, and S. Ke. 2016. The distance function effect on k -nearest neighbor classification for medical datasets. *SpringerPlus* 5(1):1304. 9 p. doi: 10.1186/s40064-016-2941-7.
11. Adeniyi, D., Z. Wei, and Y. Yongquan. 2015. Automated web usage data mining and recommendation system using K-Nearest Neighbor (kNN) classification method. *Applied Computing Informatics* 12(1):90–108. doi: 10.1016/j.aci.2014.10.001.
12. Cover, T., and P. Hart. 1967. Nearest neighbor pattern classification. *IEEE T. Inform. Theory* 13(1):21–27. doi: 10.1109/TIT.1967.1053964.
13. Lopes, N., and B. Ribeiro. 2015. On the impact of distance metrics in instance-based learning algorithms. *Pattern recognition and image analysis*. Eds. R. Paredes, J. Car-

- doso, and X. Pardo. Lecture notes in computer science ser. Cham: Springer. 9117:48–56. doi: 10.1007/978-3-319-19390-8_6.
14. Mulak, P., and N. Talhar. 2015. Analysis of distance measures using k -nearest neighbor algorithm on KDD dataset. *Int. J. Science Research* 4(7):2101–2104.
 15. Edelsbrunner, H., and G. Osang. 2021. The multi-cover persistence of Euclidean balls. *Discrete Comput. Geom.* 65(4):1296–1313. doi: 10.1007/s00454-021-00281-9.
 16. Reani, Y., and O. Bobrowski. 2026. Morse theory for the kNN distance function. *Discrete Comput. Geom.* 75(2):491–510. doi: 10.1007/s00454-025-00795-6.
 17. Zou, J., and H. Li. 2022. Precise marketing of e-commerce products based on KNN algorithm. *Comput. Intel. Neurosc.* 2022:4966439. 12 p. doi: 10.1155/2022/4966439.
 18. Halder, R. K., M. N. Uddin, and M. A. Uddin. 2024. Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications. *Big Data* 11:113. 55 p. doi: 10.1186/s40537-024-00973-y.
 19. Abu Alfeilat, H. A., A. B. A. Hassanat, O. Lasassmeh, A. Tarawneh, M. Alhasanat, H. Eyal Salman, and V. Prasath. 2019. Effects of distance measure choice on K-nearest neighbor classifier performance: A review. *Big Data* 7(4):221–248. doi: 10.1089/big.2018.0175.
 20. Torshin, I. Yu. 2024. O porozhdenii sinteticheskikh priznakov na osnove opornykh tsepey i proizvol'nykh metrik v ramkakh topologicheskogo podkhoda k analizu dannykh. Chast' 1. Vkluyuchenie v formalizm empiricheskikh funktsiy rasstoyaniya [On the generation of synthetic features based on support chains and arbitrary metrics within a topological approach to data analysis. Part 1. Inclusion of empirical distance functions into the formalism]. *Informatika i ee Primeneniya — Inform. Appl.* 18(1):71–77. doi: 10.14357/19922264240110. EDN: RIVOXR.

Received March 12, 2026

Accepted August 15, 2026

Contributor

Torshin Ivan Y. (b. 1972) — Candidate of Science (PhD) in physics and mathematics, Candidate of Science (PhD) in chemistry, leading scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str, Moscow 119333, Russian Federation; itorshin@frcsc.ru

МОДЕЛИРОВАНИЕ АВТОМАТИЧЕСКОЙ МНОГОАСПЕКТНОЙ ИДЕНТИФИКАЦИИ ПРОБЛЕМЫ В ГИБРИДНЫХ ИНТЕЛЛЕКТУАЛЬНЫХ МНОГОАГЕНТНЫХ СИСТЕМАХ

С. В. Листопад¹

Аннотация: Разрабатываются концептуальные основы многоаспектной идентификации структуры практических проблем с целью построения автоматических методов их решения на основе гибридных интеллектуальных многоагентных систем (ГиИМАС). Актуальность исследования обусловлена слабой формализацией, неоднородностью и комплексностью практических проблем, требующих высоких трудозатрат со стороны разработчиков систем искусственного интеллекта. В работе обобщены наиболее известные основания декомпозиции проблем, показана необходимость их совместного применения, а также предложена формализованная модель автоматической многоаспектной идентификации проблемы, обеспечивающая выбор оснований декомпозиции в соответствии с типами характерной для нее неопределенности.

Ключевые слова: проблема; концептуальная модель; декомпозиция; редукция; коллектив специалистов; гибридная интеллектуальная многоагентная система

DOI: 10.14357/19922264260309

EDN: MLRDHY

1 Введение

Исследования традиционных подходов к решению практических проблем с привлечением коллективов специалистов [1], а также особенностей проектирования систем искусственного интеллекта [2, 3], моделирующих эту деятельность на основе гибридных интеллектуальных и гибридных интеллектуальных многоагентных систем, продемонстрировали недоопределенность, слабую формализацию, динамичность, существенную непрозрачность и неоднородность проблем как с точки зрения необходимых методов решения, так и целей заинтересованных сторон. В этой связи проектируемые средства автоматического решения проблем должны обеспечивать выработку их формулировки, идентификацию (в общем случае итеративную, формирующую иерархию подпроблем), поиск или выработку методов их решения, а также синтез методов решения частных подпроблем в новый единый, интегрированный метод, релевантный исходной проблеме. Вопросы идентификации проблем в ГиИМАС на основе информационно-управляющих связей рассмотрены в работах [4, 5]. Данные модели формируют основу для конструирования новых методов идентификации проблем в рамках как классических популяционных алгоритмов [6], подходов на основе линейного программирования [7, 8], децентрализованных многоагентных систем [9], так и современных технологий больших языковых моделей [10, 11] и генеративных

агентов [12]. При этом ограничивается учет таких видов неопределенности проблемы, как субъективность, полителичность, динамичность и др. В данной статье предлагается модель автоматической многоаспектной идентификации, обеспечивающей учет типов неопределенности рассматриваемой проблемы и синтез релевантного метода ее идентификации.

2 Особенности идентификации практических проблем

Согласно [4, с. 69], проблема — «затруднение, обуславливающее негативное восприятие субъектом текущей ситуации, характеризующееся такими особенностями, как недоопределенность, комплексность, многослойность, полителичность, непрозрачность, динамичность, субъективность, межпредметное содержание», что согласуется с работами [13–16]. Кроме того, первоначально проблема может быть не определена, как и требования к привлекаемым специалистам, поэтому процесс решения проблемы начинается с выработки ее формулировки и определения проблематики, т. е. комплекса проблем, связанных с рассматриваемой [17]. Актуальность определения проблематики обусловлена комплексностью практической проблемы и существованием ее в контексте определенной системы (технической, экономической, социальной и др.), включающей множество подсистем

¹ Федеральный исследовательский центр «Информатика и управление» Российской академии наук, slistopad@frccsc.ru

тем, одновременно выступающей элементом надсистем более высокого порядка, а также связанной с другими системами одного уровня иерархии (системами-элементами надсистемы).

Системные связи включают иерархические (отношения соподчинения и вложенности), причинно-следственные (каузальные сети и циклы), темпоральные (динамика системы), аксиолого-когнитивные (отношения конфликта, синергии), информационные (зависимость по данным), ресурсные (конкуренция за общий ресурс) и др. [15, 18–21]. Выработка и выбор решения проблемы без учета этих иерархических и одноранговых взаимосвязей может привести к непредусмотренным изменениям в смежных системах, характер которых не ограничивается позитивными эффектами. Для минимизации нежелательных последствий решения проблемы необходима многоаспектная идентификация ее структуры, обеспечивающая разработку множества декомпозиций с учетом многообразия отношений между ней и элементами системы, в которой она возникла.

На основе анализа работ [21–29] в области системного анализа, теории поддержки принятия решений и проектирования интеллектуальных систем для решения практических проблем выделены обобщенные (в рамках каждого возможны дополнительные деления с учетом разнообразия метрик, необходимой степени формализации проблемы и подходов к определению подпроблем) основания декомпозиции практических проблем (см. таблицу).

Как видно из таблицы, ни одно из рассмотренных оснований декомпозиции не перекрывает все типы неопределенности практических проблем, поэтому возникает необходимость в формальном аппарате, который позволит объединить все или несколько из выделенных оснований при идентификации проблемы для формирования ее обобщенной многоаспектной модели.

3 Модель метода автоматической многоаспектной идентификации проблемы

В [4] предложена модель проблемы, поддерживающая ее идентификацию и анализ с учетом комплексности и системного характера. Данная модель — двухуровневое описание проблемы

$$\text{prb} = \langle \overline{\text{prb}}, \text{prb} \rangle, \quad (1)$$

в котором на макроуровне $\overline{\text{prb}}$ (2) она описывается как «черный ящик», фиксирующий основные

элементы затруднения, а на микроуровне prb (3) строится их формализованное описание в виде концептуальных моделей [21].

Макроуровневая модель проблемы представляется кортежем

$$\overline{\text{prb}} = \langle \text{id}, \text{sit}, \text{sbj}, \text{est} \rangle, \quad (2)$$

где id — идентификатор или наименование, позволяющее однозначно различать проблемы между собой; sit — описание ситуации субъектом, столкнувшимся с проблемой; sbj — наименование субъекта; est — оценка, описывающая ситуацию sit как негативную для субъекта sbj .

При построении микроуровневой модели на основе макроуровневого описания разрабатываются модели ситуации sitm , субъекта sbjm , выполняется перечисление и строятся модели стейкхолдеров STHM , с использованием метода pfmt (4) формируется проблемное поле prbfld (5), а также путем синтеза методов решения частных подпроблем генерируется модель metm метода решения [30]. Формально микроуровневая модель описывается кортежем

$$\text{prb} = \langle \text{sitm}, \text{sbjm}, \text{STHM}, \text{pfmt}, \text{metm} \rangle. \quad (3)$$

В случае многоаспектной идентификации проблемы в составе метода pfmt формирования проблемного поля из (3) могут быть выделены три части в зависимости от специфицируемой области поля:

$$\text{pfmt} = \langle \text{sppimt}, \text{slpimt}, \text{sbpimt}^{\text{ma}} \rangle, \quad (4)$$

где sppimt — метод выявления надпроблемы $\overline{\text{prb}}^{\text{sup}}$; slpimt — метод, анализирующий надпроблему и выявляющий проблемы одного уровня иерархии с идентифицируемой; $\text{sbpimt}^{\text{ma}}$ — метод многоаспектной идентификации структуры проблемы.

Проблемное поле, формируемое методом pfmt (4), представляется кортежем

$$\text{prbfld} = \langle \text{PRB}, R_1^{\text{prb-prb}}(\text{PRB}, \text{PRB}), R_2^{\text{prb-prb}}(\text{PRB}, \text{PRB}) \rangle, \quad (5)$$

где PRB — множество проблем, включающее идентифицируемую проблему, ее подпроблемы, надпроблему, проблемы одного уровня иерархии с идентифицируемой, описываемых выражением (1); $R_1^{\text{prb-prb}}$ — множество вертикальных отношений класса «целое—часть» между надпроблемой и идентифицируемой проблемой, надпроблемой и проблемами одного уровня с идентифицируемой проблемой, а также между идентифицируемой проблемой и ее подпроблемами; $R_2^{\text{prb-prb}}$ — множество горизонтальных отношений, например

Обобщенные основания декомпозиции практических проблем

Основание	Характеристика	Снимаемый тип неопределенности	Преимущества	Недостатки
Процессное (по фазам управления в терминах [21])	Выделение подпроблем по фазам управления (прогнозирование, планирование, организация, учет, контроль, анализ, регулирование) [21, 24]	Недоопределенность, динамичность	Опирается на стандартные управленческие циклы, обеспечивает четкую последовательность этапов	Не учитывает содержательные и иерархические связи между подпроблемами, а также субъективность проблемы, жестко фиксирует порядок фаз
Онтогенетическое (по этапам жизненного цикла)	Декомпозиция по этапам жизненного цикла проблемы (от обнаружения до полного разрешения), фазы могут выделяться произвольно, проследить жизненный цикл: начало, середина, конец [24, 26]	Недоопределенность, динамичность	Разворачивает проблему во времени согласно характерным для нее стадиям	Сложность выделения этапов, игнорирование структурных и иерархических связей, междисциплинарности и субъективности проблемы
Структурное (информационно-управляющее в терминах [21])	Декомпозиция на основе анализа информационно-управляющих отношений между задачами с последующей кластеризацией [21, 26, 28, 29]	Непрозрачность, комплексность	Учитывает реальные зависимости (обратные, координирующие), выделяет тесно связанные кластеры	Требуется формализация всех связей, чувствительно к выбору метрик кластеризации, игнорирует субъективность проблемы
Ценностно-целевое (по стратам в терминах [21])	Выделение подпроблем в соответствии с целями и ценностными ориентациями заинтересованных сторон (стейкхолдеров) [21, 23, 27]	Политичность, субъективность, межпредметное содержание	Ориентирует решение на удовлетворение реальных потребностей, учитывает конфликты и синергию интересов	Субъективность оценок, сложность формализации ценностей, игнорирует структурные и иерархические связи, а также динамику проблемы
Абстрактно-уровневое (по стратам в терминах [22])	Декомпозиция по уровням абстракции (стратегический, тактический, операционный) [22, 25]	Многослойность, недоопределенность	Позволяет разделить ответственность и временные горизонты, облегчает координацию между уровнями	Требуется четкого определения границ между уровнями, игнорирует структурные связи, а также динамику и субъективность проблемы
Послойное	Декомпозиция по слоям в соответствии со сложностью принимаемого решения и учитываемой неопределенностью: верхние слои описывают подпроблемы самоорганизации, адаптации и обучения, а нижние — детерминированные задачи [22, 25]	Многослойность, недоопределенность	Позволяет управлять неопределенностью, последовательно снижая ее при движении вниз	Сложность определения границ слоев, игнорирует структурные связи, а также динамику и субъективность проблемы
Смешанное	Последовательное применение процессного и либо структурного, либо ценностно-целевого основания, чтобы отсечь задачи пассивных фаз (учет, контроль) и сосредоточиться на подпроблемах активных фаз [21]	Неопределенности, снимаемые процессным и либо структурным, либо ценностно-целевым основанием	Компенсирует недостатки каждого из используемых оснований	Жестко фиксирует порядок фаз, предполагает применение не более двух оснований декомпозиции, чувствительно к выбору метрик кластеризации, игнорирует иерархические связи

информационно-управляющие и темпоральные отношения между проблемами одного ранга в рамках иерархической структуры, порожденной $R_1^{\text{prb-prb}}$.

Модель $\text{sbpimd}^{\text{ma}}$ метода $\text{sbpimt}^{\text{ma}}$ из (4) предполагает формирование пространства релевантных природе проблемы оснований декомпозиции, разделение ее на части в соответствии с этими основаниями, а также выработку обобщенной декомпозиции проблемы. Предлагаемая модель описывается выражением

$$\text{sbpimd}^{\text{ma}} = \langle \text{DB}, \text{FML}, \text{DFM}, \text{fdbc}, \text{fmad}, \text{DS}, \text{dsim} \rangle, \quad (6)$$

где $\text{DB} = \{\text{db}^{\text{prc}}, \text{db}^{\text{lc}}, \text{db}^{\text{str}}, \text{db}^{\text{vgl}}, \text{db}^{\text{hst}}, \text{db}^{\text{hl}}\}$ — множество оснований декомпозиции, включающее процессное db^{prc} , онтогенетическое db^{lc} , структурное db^{str} , ценностно-целевое db^{vgl} , абстрактно-уровневое db^{hst} , послойное db^{hl} , данное множество может быть расширено при необходимости, в частности различными конфигурациями смешанных оснований; FML — множество прототипных фреймовых моделей [4], описывающих проблему как набор отношений между частично заполненными моделями подпроблем (1); $\text{DBM} \subseteq \text{DB} \otimes \text{FML}$ — соответствие между основаниями декомпозиции и релевантными им прототипными фреймовыми моделями; fdbc — метод построения пространства оснований декомпозиции (7); fmad — метод интерпретации пространства оснований декомпозиции и последовательной инициализации процесса идентификации проблемы в соответствии с выделенными основаниями (8); DS — первоначально пустое множество декомпозиций проблемы, описываемых выражением (9); dsim — метод выработки обобщенной многоаспектной декомпозиции проблемы (10).

Метод построения пространства оснований декомпозиции fdbc из (6) предназначен для формирования упорядоченного подмножества DBO возможных классификационных признаков из множества DB , релевантных конкретной проблеме, исходя из природы ее сложности (непрозрачность, полнотичность, межпредметное содержание и др.). Формально этот метод описывается кортежем

$$\text{fdbc} = \langle \text{DBCT}, \text{dbsel}, \text{dbord} \rangle, \quad (7)$$

где DBCT — соответствие между основаниями декомпозиции DB и расширяемым при необходимости множеством типов неопределенности проблем $\text{CT} = \{\text{ct}^{\text{amb}}, \text{ct}^{\text{cmp}}, \text{ct}^{\text{mlr}}, \text{ct}^{\text{plt}}, \text{ct}^{\text{ntr}}, \text{ct}^{\text{dyn}}, \text{ct}^{\text{sbj}}, \text{ct}^{\text{ids}}\}$, включающим недоопределенность ct^{amb} , комплексность ct^{cmp} , многослойность ct^{mlr} , полнотичность ct^{plt} , непрозрачность ct^{ntr} ,

динамичность ct^{dyn} , субъективность ct^{sbj} , межпредметное содержание ct^{ids} ; dbsel — метод формирования из DBCT рабочего набора $\text{DB}^* \subseteq \text{DB}$ оснований декомпозиции, релевантных рассматриваемой проблеме, путем анализа присущей ей неопределенности $\text{CT}^* \subseteq \text{CT}$; dbord — метод формирования отношения порядка $\prec^{\text{dbp}}$ и упорядоченного множества $\text{DBO} = (\text{DB}^*, \prec^{\text{dbp}})$, описывающего приоритет применения оснований декомпозиции с учетом доминирования типов сложности проблемы и зависимостей между основаниями, если они имеются.

Метод fmad из (6) представляется выражением

$$\text{fmad} = \langle \text{dbit}, \text{sbpimt}(\text{FML}^{\text{ch}}), \text{dcl} \rangle, \quad (8)$$

где dbit — метод отбора фреймовых моделей, который последовательно перебирает элементы множества DBO , формируя для каждого элемента db_i подмножество $\text{FML}_i^{\text{ch}} \subseteq \text{FML}$ релевантных ему прототипов, т.е. $\text{FML}_i^{\text{ch}} = \{\text{fml}_j | \langle \text{db}_i, \text{fml}_j \rangle \in \text{DFM}\}$, $i, j \in \bullet$, $i \leq |\text{DB}|$, $j \leq |\text{FML}|$, после чего вызывает метод $\text{sbpimt}(\text{FML}_i^{\text{ch}})$, передавая ему подмножество FML_i^{ch} , а также метод кластеризации dcl , если это предусмотрено текущим основанием декомпозиции db_i ; $\text{sbpimt}(\text{FML}^{\text{ch}})$ — метод автоматической идентификации структуры проблемы, разработанный в соответствии с моделью sbpimd из [4], предполагающий декомпозицию проблемы с использованием имеющегося в его распоряжении множества FML^{ch} прототипов, а также оценку релевантности декомпозиции идентифицируемой проблеме; dcl — метод кластеризации декомпозиции, обеспечивающий выявление областей однородности на множестве подпроблем и формирование на их основе укрупненных подпроблем.

Множество декомпозиций проблемы DS наполняется декомпозициями ds проблемы по мере выполнения метода fmad . В результате его работы формируется не менее одной декомпозиции для каждого выделенного релевантного проблеме основания из множества DBO . Декомпозиция ds — часть проблемного поля (5) и в общем виде представляется кортежем

$$\text{ds} = \langle \{\text{prb}\} \cup \text{PRB}^*, R_1^{\text{prb-prb}}(\text{prb}, \text{PRB}^*), R_1^{\text{prb-prb}}(\text{PRB}^*, \text{PRB}^*), R_2^{\text{prb-prb}}(\text{PRB}^*, \text{PRB}^*) \rangle, \quad (9)$$

где $\text{PRB}^* \subseteq \text{PRB}$ — множество подпроблем идентифицируемой проблемы prb , т.е. проблем, для которых имеет место $R_1^{\text{prb-prb}}(\text{prb}, \text{PRB}^*)$.

Метод dsim синтеза обобщенной многоаспектной декомпозиции из (6) описывается кортежем

$$\text{dsim} = \langle \text{dsel}, \text{DS}^*, \text{dsyn} \rangle, \quad (10)$$

где $dsel$ — метод оценки и отбора релевантных декомпозиций в множество DS^* ; $DS^* \subseteq DS$ — подмножество декомпозиций отобранных по набору критериев, например однородность выделенных подпроблем, минимизация связей между подпроблемами и другие; $dsyn$ — метод синтеза итоговой обобщенной многоаспектной декомпозиции проблемы на основе множества DS^* , который либо выбирает единственную декомпозицию из DS^* , если $|DS^*| = 1$, либо выполняет построение обобщенной многоаспектной декомпозиции, когда в рамках модели проблемы используется несколько оснований, если $|DS^*| > 1$, либо при $DS^* = \emptyset$ выдает сообщение о невозможности автоматической идентификации проблемы.

Таким образом, результатом работы метода автоматической многоаспектной идентификации проблемы должна быть ее модель, в которой сочетаются разные срезы проблемы (темпоральные, ценностные, функциональные и др.). Модель метода предполагает построение пространства оснований декомпозиции на основе оценки их релевантности каждой очередной проблеме, а также синтез многомерной декомпозиции, отражающей выделенные типы неопределенности проблемы.

4 Заключение

В работе рассмотрены особенности идентификации практических проблем, выполнен анализ основных подходов к декомпозиции проблем и обоснована необходимость многоаспектной идентификации структуры проблемы, позволяющей формировать множество взаимодополняющих декомпозиций.

Разработана модель многоаспектной идентификации проблемы, обеспечивающая формирование пространства оснований декомпозиции, релевантного конкретной проблеме, последующую интерпретацию этого пространства для построения множества декомпозиций, а также их синтез с учетом системных связей подпроблем. Предложенная модель закладывает основу для автоматизации процессов идентификации проблем в системах поддержки принятия решений и интеллектуальных агентных средах. Перспективной представляется разработка методов многоаспектной идентификации структуры проблемы в соответствии с данной моделью на основе больших языковых моделей и технологии генеративных агентов, которые могут использоваться для извлечения оснований декомпозиции из неформализованных описаний и генерации взаимодополняющих декомпозиций проблемы.

Литература

1. Румовская С. Б. Подходы к подбору специалистов при организации коллективного решения проблем // Информатика и её применения, 2023. Т. 17. Вып. 2. С. 96–103. doi: 10.14357/19922264230214. EDN: VJWNOE.
2. Колесников А. В., Листопад С. В. Протокол гетерогенного мышления гибридной интеллектуальной многоагентной системы для решения проблемы восстановления распределительной электросети // Информатика и её применения, 2019. Т. 13. Вып. 2. С. 76–82. doi: 10.14357/19922264190211. EDN: MDLXEF.
3. Румовская С. Б., Колесников А. В., Литвин А. А. Визуальный метаязык описания решения диагностических проблем // Системы и средства информатики, 2019. Т. 29. № 4. С. 39–49. doi: 10.14357/08696527190404. EDN: XVDQLJ.
4. Листопад С. В., Кириков И. А. Концептуальная модель идентификации структуры проблемы в гибридных интеллектуальных многоагентных системах // Информатика и её применения, 2025. Т. 19. Вып. 2. С. 69–75. doi: 10.14357/19922264250209. EDN: EFHCPM.
5. Listopad S. V., Kirikov I. Bottom-up problem structure identification in hybrid intelligent multi-agent systems // 7th Conference (International) on Control Systems, Mathematical Modeling, Automation and Energy Efficiency Proceedings. — IEEE, 2025. P. 744–747. doi: 10.1109/SUMMA68668.2025.11302307.
6. El-Abd M. A cooperative approach to the artificial bee colony algorithm // Congress on Evolutionary Computation Proceedings. — IEEE, 2010. Art. 5586007. 5 p. doi: 10.1109/CEC.2010.5586007.
7. Bonami P., Salvagnin D., Tramontani A. Implementing automatic benders decomposition in a modern MIP solver // Integer programming and combinatorial optimization / Eds. D. Bienstock, G. Zambelli. — Lecture notes in computer science ser. — Cham: Springer, 2020. Vol. 12125. P. 78–90. doi: 10.1007/978-3-030-45771-6_7.
8. Барашов Е. Б., Егоркин А. В., Лемтюжникова Д. В., Посыпкин М. А. Анализ эффективности алгоритма редукции в решении задачи об упаковке в контейнеры // Системы и средства информатики, 2023. Т. 33. № 3. С. 61–75. doi: 10.14357/08696527230305. EDN: QDUAMY.
9. Фишов А. Г., Осинцев А. А., Какоша Ю. В., Одинабеков М. З. Активные распределительные электрические сети с децентрализованным мультиагентным управлением режимом. Ч. 1 // Электричество, 2022. № 10. С. 14–24. doi: 10.24160/0013-5380-2022-10-14-24. EDN: HXXXZS.
10. Егорова А. Ю., Зацман И. М., Романенко В. О. Машинный перевод с помощью ChatGPT: мониторинг воспроизводимости результатов // Системы и средства информатики, 2023. Т. 33. № 3. С. 117–128. doi: 10.14357/08696527230310. EDN: LTOWWN.
11. Босов А. В., Иванов А. В. О применении генеративных моделей в системе электронного обучения математическим дисциплинам // Информатика и её применения, 2024. Т. 18. Вып. 2. С. 72–81. doi: 10.14357/19922264240210. EDN: UWKQLN.

12. *Park J. S., O'Brien J., Cai C. J., Morris M. R., Liang P., Bernstein M. S.* Generative agents: Interactive simulacra of human behavior // 36th Annual Symposium on User Interface Software and Technology Proceedings. — New York, NY, USA: ACM, 2023. Art. 2. 22 p.
13. *Ивин А. А.* Искусство правильно мыслить. — М.: Просвещение, 1990. 240 с. EDN: TJMMWP.
14. *Спиридонов В. Ф.* Психология мышления: решение задач и проблем. — М.: Генезис, 2006. 319 с. EDN: RYZQP.
15. *Тарасенко Ф. П.* Прикладной системный анализ. — М.: Кнорус, 2010. 224 с. EDN: QMUKWJ.
16. *Rumovskaya S.* Revisiting the “Problem” and its structure // 4th Conference (International) on Technology Enhanced Learning in Higher Education Proceedings. — IEEE, 2024. P. 219–223. doi: 10.1109/tele62556.2024.10605656.
17. *Новиков А. М., Новиков Д. А.* Методология. — М.: Синтер, 2007. 668 с.
18. *Steward D. V.* Systems analysis and management: Structure, strategy and design. — New York, NY, USA: Petrocelli Books, 1981. 287 p.
19. *Поспелов Д. А.* Ситуационное управление: теория и практика. — М.: Наука, 1986. 288 с.
20. *Саймон Г.* Науки об искусственном / Пер. с англ. — М.: Едиториал УРСС, 2004. 142 с. (*Simon H. A.* The sciences of the artificial. — 3rd ed. — Cambridge, MA, USA: MIT Press, 1996. 231 p.)
21. *Колесников А. В., Кириков И. А.* Методология и технология решения сложных задач методами функциональных гибридных интеллектуальных систем. — М.: ИПИ РАН, 2007. 387 с.
22. *Месарович М., Мако Д., Такахара И.* Теория иерархических многоуровневых систем / Пер. с англ. — М.: Мир, 1973. 344 с. (*Mesarovic M. D., Macko D., Takahara Y.* Theory of hierarchical, multilevel systems. — New York, NY, USA: Academic Press, 1970. 294 p.)
23. *Checkland P. B.* Systems thinking, systems practice. — Chichester, U.K.: John Wiley & Sons, 1981. 330 p.
24. *Перегудов Ф. И., Тарасенко Ф. П.* Основы системного анализа. — Томск: НТЛ, 1997. 396 с.
25. *Волкова В. Н., Денисов А. А.* Основы теории систем и системного анализа. — СПб.: СПбГТУ, 2001. 512 с.
26. *Анфилатов В. С., Емельянов А. А., Кукушкин А. А.* Системный анализ в управлении. — М.: Финансы и статистика, 2002. 368 с.
27. *Saaty T. L.* Decision making with the analytic hierarchy process // Int. J. Services Sciences, 2008. Vol. 1. Iss. 1. P. 83–98. doi: 10.1504/IJSSCI.2008.017590.
28. *Otero R. E.* Problem decomposition by mutual information and force-based clustering: PhD Thesis. — Atlanta, GA, USA: Georgia Institute of Technology, 2012. 267 p.
29. *Zou Z., Che W., Wang S., Bai Y., Fan C.* Role-based approaches for operational tasks modeling and flexible decomposition // J. Syst. Eng. Electron., 2016. Vol. 27. Iss. 6. P. 1191–1206. doi: 10.21629/JSEE.2016.06.08.
30. *Листопад С. В., Кириков И. А.* Анализ подходов к идентификации структуры проблемы в гибридных интеллектуальных многоагентных системах // Системы и средства информатики, 2024. Т. 34. № 3. С. 35–47. doi: 10.14357/08696527240304. EDN: RSLMXC.

Поступила в редакцию 29.05.2026

Принята к публикации 15.08.2026

MODELING AUTOMATIC MULTIASPECT PROBLEM IDENTIFICATION IN HYBRID INTELLIGENT MULTIAGENT SYSTEMS

S. V. Listopad

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: The article develops a conceptual framework for the multiaspect identification of problem structures with the aim of constructing automated problem-solving methods based on hybrid intelligent multiagent systems. The topic is relevant due to the weak formalization, heterogeneity, and complexity of practical problems, which require significant effort from developers of artificial intelligence systems. The paper summarizes the most well-known bases for problem decomposition, demonstrates the need for their combined application, and proposes a formalized model for automatic multiaspect problem identification, ensuring the selection of decomposition bases in accordance with the types of uncertainty characteristic of the task.

Keywords: problem; conceptual model; decomposition; reduction; team of specialists; hybrid intelligent multiagent system

DOI: 10.14357/19922264260309

EDN: MLRDHY

References

1. Rumovskaya, S. B. 2023. Podkhody k podboru spetsialistov pri organizatsii kollektivnogo resheniya problem [Selection of specialists in the organization of collective solving problems]. *Informatika i ee Primeneniya — Inform. Appl.* 17(2):96–103. doi: 10.14357/19922264230214. EDN: VJWNOE.
2. Kolesnikov, A. V., and S. V. Listopad. 2019. Protokol geterogennogo myshleniya gibridnoy intellektual'noy mnogoagentnoy sistemy dlya resheniya problemy vosstanovleniya raspredelitel'noy elektroseti [Heterogeneous thinking protocol of hybrid intelligent multiagent system for solving distributional power grid recovery problem]. *Informatika i ee Primeneniya — Inform. Appl.* 13(2):76–82. doi: 10.14357/19922264190211. EDN: MDLXEF.
3. Rumovskaya, S. B., A. V. Kolesnikov, and A. A. Litvin. 2019. Vizual'nyy metayazyk opisaniya resheniya diagnosticheskikh problem [Visual metalanguage for description of solution of diagnostic problems]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 29(4):39–49. doi: 10.14357/08696527190404. EDN: XVDQLJ.
4. Listopad, S. V., and I. A. Kirikov. 2025. Kontseptual'naya model' identifikatsii struktury problemy v gibridnykh intellektual'nykh mnogoagentnykh sistemakh [Conceptual model for problem structure identification in hybrid intelligent multiagent systems]. *Informatika i ee Primeneniya — Inform. Appl.* 19(2):69–75. doi: 10.14357/19922264250209. EDN: EFHCPM.
5. Listopad, S., and I. Kirikov. 2025. Bottom-up problem structure identification in hybrid intelligent multi-agent systems. *7th Conference (International) on Control Systems, Mathematical Modeling, Automation and Energy Efficiency Proceedings*. IEEE. 744–747. doi: 10.1109/SUM-MA68668.2025.11302307.
6. El-Abd, M. 2010. A cooperative approach to the artificial bee colony algorithm. *Congress on Evolutionary Computation Proceedings*. IEEE. Art. 5586007. 5 p. doi: 10.1109/CEC.2010.5586007.
7. Bonami, P., D. Salvagnin, and A. Tramontani. 2020. Implementing automatic benders decomposition in a modern MIP solver. *Integer programming and combinatorial optimization*. Eds. D. Bienstock and G. Zambelli. Lecture notes in computer science ser. Cham: Springer. 12125:78–90. doi: 10.1007/978-3-030-45771-6_7.
8. Barashov, E. B., A. V. Egorkin, D. V. Lemtyuzhnikova, and M. A. Posypkin. 2023. Analiz effektivnosti algoritma reduksii v reshenii zadachi ob upakovke v konteynery [Efficiency of the reduction algorithms in the bin packing problem]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 33(3):61–75. doi: 10.14357/08696527230305. EDN: QDUAMY.
9. Fishov, A. G., A. A. Osintsev, Yu. V. Kakosha, and M. Z. Odinabekov. 2022. Aktivnye raspredelitel'nye elektricheskie seti s detsentralizovannym mul'tiagentnym upravleniem rezhimom. Ch. 1 [Active power distribution networks with decentralized multi-agent control mode. Part 1]. *Elektricheskoye* [Electricity] 10:14–24. doi: 10.24160/0013-5380-2022-10-14-24. EDN: HYXXZS.
10. Egorova, A. Yu., I. M. Zatsman, and V. O. Romanenko. 2023. Mashinnyy perevod s pomoshch'yu ChatGPT: monitoring vosproizvodimosti rezul'tatov [Machine translation by ChatGPT: Monitoring of outcome reproducibility]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 33(3):117–128. doi: 10.14357/08696527230310. EDN: LTOWWN.
11. Bosov, A. V., and A. V. Ivanov. 2024. O primenении generativnykh modeley v sisteme elektronnoy obucheniya matematicheskimi distsiplinami [On the application of generative models in the e-learning system of mathematical disciplines]. *Informatika i ee Primeneniya — Inform. Appl.* 18(2):72–81. doi: 10.14357/19922264240210. EDN: UWKQLN.
12. Park, J. S., J. O'Brien, C. J. Cai, M. R. Morris, P. Liang, and M. S. Bernstein. 2023. Generative agents: Interactive simulacra of human behavior. *36th Annual Symposium on User Interface Software and Technology Proceedings*. New York, NY: ACM. Art. 2. 22 p.
13. Ivin, A. A. 1990. *Iskusstvo pravil'no myslit'* [The art of thinking right]. Moscow: Prosveshchenie Publ. 240 p. EDN: TJMMWP.
14. Spiridonov, V. F. 2006. *Psikhologiya myshleniya: reshenie zadach i problem* [The psychology of mind: Solving of tasks and problems]. Moscow: Genesis. 319 p. EDN: RYRZQP.
15. Tarasenko, F. P. 2010. *Prikladnoy sistemnyy analiz* [Applied systems analysis]. Moscow: Knorus. 224 p. EDN: QMUKWJ.
16. Rumovskaya, S. 2024. Revisiting the “Problem” and its structure. *4th Conference (International) on Technology Enhanced Learning in Higher Education Proceedings*. IEEE. 219–223. doi: 10.1109/TELE62556.2024.10605656.
17. Novikov, A. M., and D. A. Novikov. 2007. *Metodologiya* [Methodology]. Moscow: Sinteg. 668 p.
18. Steward, D. V. 1981. *Systems analysis and management: Structure, strategy and design*. New York, NY: Petrocelli Books. 287 p.
19. Pospelov, D. A. 1986. *Situatsionnoye upravlenie: teoriya i praktika* [Situational management: Theory and practice]. Moscow: Nauka. 288 p.
20. Simon, H. A. 1996. *The sciences of the artificial*. 3rd ed. Cambridge, MA: MIT Press. 231 p.
21. Kolesnikov, A. V., and I. A. Kirikov. 2007. *Metodologiya i tekhnologiya resheniya slozhnykh zadach metodami funktsional'nykh gibridnykh intellektual'nykh sistem* [Methodology and technology for solving complex problems using the methods of functional hybrid intelligent systems]. Moscow: IPI RAN. 387 p.
22. Mesarovic, M. D., D. Macko, and Y. Takahara. 1970. *Theory of hierarchical, multilevel systems*. New York, NY: Academic Press. 294 p.
23. Checkland, P. B. 1981. *Systems thinking, systems practice*. Chichester, U.K.: John Wiley & Sons Ltd. 330 p.
24. Peregudov, F. I., and F. P. Tarasenko. 1997. *Osnovy sistemnogo analiza* [Fundamentals of systems analysis]. Tomsk: NTL. 396 p.
25. Volkova, V. N., and A. A. Denisov. 2001. *Osnovy teorii sistem i sistemnogo analiza* [Fundamentals of systems theory

- and systems analysis]. St. Petersburg: SPbGTU Publs. 512 p.
26. Anfilatov, V. C., A. A. Emelyanov, and A. A. Kukushkin. 2002. *Sistemnyy analiz v upravlenii* [Systems analysis in management]. Moscow: Finansy i statistika. 368 p.
 27. Saaty, T. L. 2008. Decision making with the analytic hierarchy process. *Int J. Services Sciences* 1(1):83–98. doi: 10.1504/IJSSCI.2008.017590.
 28. Otero, R. E. 2012. Problem decomposition by mutual information and force-based clustering. Atlanta, GA: Georgia Institute of Technology. PhD Thesis. 267 p.
 29. Zou, Z., W. Che, S. Wang, Y. Bai, and C. Fan. 2016. Role-based approaches for operational tasks modeling and flexible decomposition. *J. Syst. Eng. Electron.* 27(6):1191–1206. doi: 10.21629/JSEE.2016.06.08.
 30. Listopad, S. V., and I. A. Kirikov. 2024. Analiz podkhodov k identifikatsii struktury problemy v gibridnykh intellektual'nykh mnogoagentnykh sistemakh [Analysis of approaches to problem structure identification in hybrid intelligent multiagent systems]. *Sistemy i sredstva informatiki — Systems and Means of Informatics* 34(3):35–47. doi: 10.14357/08696527240304. EDN: RSLMXC.

Received May 29, 2026

Accepted August 15, 2026

Contributor

Listopad Sergey V. (b. 1984) — Candidate of Science (PhD) in technology, director, Kaliningrad Branch of the Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation; slistopad@frcsc.ru

АТАКИ НА УПРАВЛЯЮЩИЕ СЕТЕЦЕНТРИЧЕСКИЕ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ОБМАНА

А. А. Грушо¹, Н. А. Грушо², М. И. Забейло³, А. А. Зацаринный⁴, В. О. Писковский⁵

Аннотация: Применение сетевых технологий в системах управления и поддержки принятия решений определяется концепцией развития контроля периферийных узлов сетевых систем (СЦС), а также требованиями к обеспечению информационной безопасности. Работа посвящена исследованию класса атак на подобные системы, основанного на скрытом искажении свойств информации, необходимой для правильного управления. Главная цель управляющей системы (Центра) в СЦС представляется как ключевая управляющая причина, состоящая из свойств, которые в конечном итоге порождают управляющие воздействия во всей СЦС. Математическая модель распространения управляющих воздействий в СЦС строится с использованием направленных ациклических графов. Рассматриваются примеры атак на СЦС, возможности их идентификации, а также противодействия подобным атакам. Демонстрируется, как предупреждение развития атаки может быть обеспечено идентификацией отсутствующих следствий правильного свойства, а также внедрением обманных свойств.

Ключевые слова: информационная безопасность; сетевые системы; атаки, основанные на обмане; выявление и предупреждение атак

DOI: 10.14357/19922264260310

EDN: WAGKXY

1 Введение

Возможность противника использовать специально подобранные ложные данные и обман для организации атак на управляющие системы, построенные на компьютерах, — одно из важных направлений при анализе и построении безопасных систем. Простейшим примером обмана в этой области служит замена чипа в управляющем компьютере, который честно выполняет функции правильного чипа, но имеет «троянца», перехватывающего и передающего противнику проходящую через чип информацию. Вредоносные воздействия такого типа активно использовались в эпоху холодной войны (см., например, [1, 2]). Разработка мер противодействия современным вариантам подобных технологических решений — актуальная и значимая задача (см., например, [3–5]).

Для нарушения безопасности СЦС имеется целый ряд возможностей использовать методы и технологии обмана. Заметим также, что в работах по программно-целевому методу планирования и управления [6] вопросы безопасности фактически не поднимались, хотя они имеют ту же природу, что и в сетевых системах управления. Поскольку СЦС относится к управляющим системам, то в подчиненные ветви ее архитектурной иерархии передаются такие задания для каждого периферий-

ного узла, которые в совокупности реализуют главную идею, разработанную в управляющей системе (Центре).

Механизм управления в СЦС может быть описан в терминах причинно-следственных взаимосвязей, разработанных в Центре в форме главной идеи (основная причина) с заданиями (производные причины), которые следует исполнять вдоль всей иерархии периферийных узлов сетевой управляющей системы [7]. При этом задачи, требующие решения при движении вниз по этой управленческой иерархии, можно рассматривать как последовательно возникающие следствия из задач, актуальных для предыдущих узлов. В работе рассматривается класс атак на такие управляющие системы с помощью скрытого искажения управляющих воздействий. Предложен метод борьбы с подобными технологиями обмана в управляющих системах, использующий косвенные признаки, которые порождают идентификационную информацию, компрометирующую обман. Например, в случае с заменой чипа достаточно контролировать объем информации из зараженного чипа, который должен быть большим, даже если используется скрытый канал для передачи украденной информации. Далее подробнее рассматривается пример борьбы с методами и технологиями обмана в сетевой управляющей системе.

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, grusho@yandex.ru

²Федеральный исследовательский центр «Информатика и управление» Российской академии наук, info@itake.ru

³Федеральный исследовательский центр «Информатика и управление» Российской академии наук, m.zabeylo@yandex.ru

⁴Федеральный исследовательский центр «Информатика и управление» Российской академии наук, AZatsarinny@frccsc.ru

⁵Федеральный исследовательский центр «Информатика и управление» Российской академии наук, vvp80@yandex.ru

2 Математическая модель

Определим конечное множество характеристик D , из которых строятся конечные множества, называемые свойствами. Часть характеристик, образующих определенную комбинацию, составляет идентификатор свойства. Другие характеристики свойств не видны и труднодоступны. Множество свойств системы будем обозначать через M . Описание СЦС удобно вести на языке свойств и причинно-следственных связей. Простейшие причинно-следственные связи на множествах свойств определяются так, что причина детерминированно порождает следствие, если существует физическая связь причины и следствия. Главную управляющую идею Центра можно описать как управляющую причину, состоящую из свойств, которые в конечном итоге порождают производные причины и действия во всей системе. В свою очередь, свойства могут порождать действия, причиной которых они стали. Действия можно рассматривать как ориентированный ациклический граф (DAG, directed acyclic graph). Вершинами этого графа служат свойства, которые стали следствиями ранее порожденных причин и которые порождают последующие свойства действия в соответствии с дугами графа (см. подробные работы [8–11] и др.). Листьями DAG служат свойства, порождаемые производными причинами. Последние в свою очередь, порождаются из главной причины и, при необходимости, из свойств узлов, которые могут не быть причинами в иерархии причинно-следственных связей Центра в СЦС. Целью действия выступает набор свойств, которые порождаются одним или несколькими DAG описанным выше способом.

Управляющая причина состоит из множества отдельных свойств, которые сами послужили причинами множеств свойств подчиненных узлов СЦС, выступающих одновременно производными причинами. Таким образом, подчиненными узлами управляют производные причины, которые вместе с главной причиной образуют транзитивные причины [12, 13]. Следовательно, свойства производных причин можно считать также следствиями главной причины.

3 Атака

Предположим наличие противника на узле, где готовится действие. Также допустим, что противник смог подменить одно или несколько свойств, участвующих в порождении действия. Математически это означает, что часть листьев DAG не может начать действовать в порождении действия, иници-

рованного Центром. При этом каждое подмененное свойство имеет идентификатор правильного свойства, поэтому контроль наименований порождающих свойств ничего не дал. Участие свойства в порождении действия не может быть проконтролировано иначе, так как частично действие может уже развиваться и выявить отсутствующий фрагмент сложно из-за отсутствия времени на анализ.

Схема причинно-следственных связей, представленная в виде DAG, разрушается при замене любого листа обманным листом. В самом деле, исчезновение любой дуги или вершины нарушает систему построения результирующих свойств, так как разрыв любой причинно-следственной связи ведет к невозможности достраивать цепочку связей до целевого свойства по определению правил построения действия. Любой путь от листа к целевой вершине определяется последовательностью причинно-следственных связей, которая по определению не должна быть избыточной.

Если имеются два DAG, которые пересекаются (без образования циклов), то существует лист, обманная замена которого разрушает, по крайней мере частично, конечные свойства в обоих DAG. Результат можно сформулировать в форме следующего утверждения.

Утверждение. Замена любого листа из порождающих действие приводит к нарушению цели действия.

4 Предупреждение развития атаки

Пусть каждое свойство, участвующее в порождении действия, участвует в причине не только создания следующих свойств действия, но и порождает несколько видимых свойств, которые не участвуют в порождении действия, но при этом реализуемый обман не порождает такие следствия. Тогда поиск обмана сводится к обнаружению отсутствующих следствий правильного свойства. Однако порожденные обманом свойства заранее неизвестны. Поэтому необходимо искать свойства, не породившие своих неинформативных следствий.

5 Алгоритм поиска свойства с отсутствующими видимыми следствиями

Предположим, что подмены произошли на уровне листьев DAG. Тогда в базе данных Центра должны находиться не только следствия производных причин, но также следствия этих следствий.

Часть из них участвует в организации действия, а часть служит информацией, характеризующей конкретный лист. Поскольку листья известны и определяют следующий слой DAG размера m , то поиск надо вести в этом множестве. Простой переборный алгоритм сравнения свойств этого множества и свойств, хранящихся в базе данных Центра, позволяет решить задачу поиска одного из отсутствующих t свойств за среднее время m/t .

Если предположить, что противник заменил k листьев в анализируемом DAG, то математическое ожидание поиска всех обманов не превосходит суммы математических ожиданий одного обмана, т. е. km/t .

6 Планирование действий с помощью цифровых двойников

С учетом описанных угроз необходимо рассмотреть вопросы планирования действий. Опираясь на компьютерные технологии, разработку действий необходимо проводить на языке свойств. Таким образом можно построить причинно-следственную модель будущего действия.

На следующем этапе необходимо расширить такую модель с учетом носителей свойств и ресурсов.

Далее необходимо разработать механизмы защиты действий от потенциальных атак с помощью обмана.

Для построения причинно-следственной модели необходимо определить цели действия и свойства, которые порождают свойства цели. Далее задача построения причинно-следственной модели решается в обратном порядке: исходя из цели действия. Необходимо определить, какие свойства порождают свойства цели действия. Затем установить, каким образом построить свойства, порождающие уже свойства текущего уровня. Таким образом постепенно строится DAG причинно-следственных связей свойств достижения цели. На каждом этапе исследуется возможность выделения листьев DAG, используя свойства порожденных причин или возможность использования свойств, имеющихся на узле. Модель считается построенной, если все пути к цели заканчиваются листьями. Разумеется, построение причинно-следственной модели носит итеративный характер, расширяя свойства главной причины или расширяя возможности узла. Уже на этом этапе выявляются возможности внедрения обманных свойств, для борьбы с которыми необходимо вносить избыточность в множество свойств,

которые можно использовать для идентификации обманов.

Поскольку разрушение действия начинается с уровня листьев, то можно предложить следующий способ защиты от подлога какого-то листа. Предположим, что противник может заменить произвольный лист ложным с правильным идентификатором. Создадим для каждого листа дубликат с другим произвольным именем. Таким образом, в отсутствие противника действие будет стартовать в каждом листе дважды. Поскольку это будет действовать одна причина для одного следствия, то с точки зрения развития действия одновременное порождение дважды одного свойства одной причиной ничему не мешает. Если противник испортил свойство, порождавшее следствие, то идентичная причина породит нужное свойство, и действие будет развиваться, несмотря на подмену свойства. Отметим, что причина порождает следствие, если существует путь к следствию. Чтобы порождение следствия при таком дубле было возможно, необходимо кроме открытого идентификатора иметь единый скрытый идентификатор, позволяющий работать причинам в дубле. Предложенный метод не позволит противнику исключить сразу два варианта одной причины. Вероятность случайного полного исключения порождающего свойства равна $1/(2m - 1)$, где m — число всех листьев.

Технологически трудно представить программно-аппаратное представление одного свойства. Поэтому для построения функциональной модели любого свойства-причины, участвующего в действии, можно использовать программно-аппаратное покрытие причин [14]. Для защиты от модификаций в этом случае используются стандартные методы контроля доступа.

7 Примеры

1. Сетевая коммуникационная система, которая предоставляет сервисы населению. В одном из узлов вышел из строя сервис, но система в целом осталась в рабочем состоянии. Информация о неработающем сервисе доходит до Центра через жалобы пользователей, т. е. по косвенным признакам [15–18]. Сбой стал следствием одной из причин большой системы предоставления услуг населению (цель).
2. Рассмотрим сетевую систему управления, которая передает управляющую информацию для действий сразу для нескольких узлов. При изменении информации о параметрах связи возник узел, который не принял эту информацию и остался без эффективного взаи-

модействия с Центром и связанными узлами. При этом работоспособность программно-аппаратной части не ухудшилась. Причины сбоя могут быть в подмене свойства, необходимого для раскрытия и установки изменений в организации связи. Согласно предложенному методу поиска отсутствующих вспомогательных свойств выявляется подложное свойство и восстанавливается полное необходимое взаимодействие Центра и связанных узлов.

3. Действие — компьютерная модернизация функций периферийного управления населенным пунктом. Качественное оборудование было заменено на дешевую подделку с помощью подмены этикеток. В результате система управления вышла из строя через месяц работы, что привело к большому ущербу. Выход из строя можно было предотвратить, если предварительно исследовать слабые стороны нового оборудования.

8 Заключение

В работе рассмотрена проблема нарушения безопасности управляющей системы с помощью специально подобранных ложных данных и обмана. Построен удобный и универсальный язык описания систем, которые могут подвергаться атакам с помощью обмана различных типов. Основные компоненты такого языка — это свойства систем и причинно-следственные связи. Описание угроз основано на идентификации нарушения причинно-следственных связей при замене образующих актуальную причинно-следственную управленческую иерархию связей свойств на обманные. Для противодействия таким угрозам может использоваться любая дополнительная информация, связанная с содержательной информацией чисто формально, цифровые аналоги систем или система избыточных свойств, специально введенная для контроля действий. Поскольку эти средства и другие косвенные признаки, как правило, не используются для контроля организации действий, то возникают сбои или достигнутые цели не удовлетворяют исходным требованиям. Приведены примеры из различных областей аналогичных угроз и методы противодействия этим угрозам, которые легко интерпретируются с помощью рассмотренных в статье методов.

Литература

1. *Lázňovský M.* Dá se „apíchnout“ psací stroj? KGB to dokázala // *Idnes*, 2015. <https://www.idnes.cz/>

2. *Мелтон К., Алексеенко В.* Шпионские игры: как США внедряли жучки в копировальные аппараты СССР // *TechInsider*, 04.12.2022. <https://www.techinsider.ru/technologies/164236-est-li-v-vashem-printere-zhuchok/>.
3. *Попов И.* Война будущего: взгляд из-за океана. Военные теории и концепции современных США. — М.: АСТ; Астрель, 2004. 444 с. <https://pub.wikireading.ru/84049>.
4. *Макарчук И.Л., Троценко К.А.* Характер операций современных армий. Мультиразумные сетевые военные системы и тактика их действий // *Военная мысль*, 2022. № 11. С. 13–31. EDN: IYRMEF.
5. *Тонкошуров В.П.* Новые тенденции «новых» войн и их влияние на программы вооружений технологически развитых государств мира // *Проблемы военной безопасности России: взгляд в будущее: Мат-лы 11-й Междунар. межведомственной научн.-практич. конф. РАРАН*. — М.: МГТУ им. Н.Э. Баумана, 2026. Т. 1. С. 59–78.
6. *Поспелов Г.С., Ириков В.А.* Программно-целевое планирование и управление. — М.: Советское радио, 1976. 440 с.
7. *Грушо А.А., Грушо Н.А., Забейжайло М.И., Зацаринный А.А., Писковский В.О.* Поиск аномалий в сетевых системах управления // *Информатика и её применения*, 2026. Т. 20. Вып. 2. С. 82–88. doi: 10.14357/19922264260207. EDN: PPXIOI.
8. *Balke A., Pearl J.* Probabilistic evaluation of counterfactual queries // *12th National Conference on Artificial Intelligence Proceedings / Eds. B. Hayes-Roth, R. Korf*. — Menlo Park, CA, USA: MIT Press, 1994. Vol. 1. P. 230–237.
9. *Pearl J.* Causal diagrams for empirical research // *Biometrika*, 1995. Vol. 82. Iss. 4. P. 669–688. doi: 10.2307/2337329.
10. *Pearl J.* Structural and probabilistic causality // *Psychol. Learn. Motiv.*, 1996. Vol. 34. P. 393–435. doi: 10.1016/S0079-7421(08)60566-6.
11. *Pearl J.* The seven tools of causal inference, with reflections on machine learning // *Commun. ACM*, 2019. Vol. 62. Iss. 3. P. 54–60. doi: 10.1145/3241036.
12. *Abel S., Tang Y., Singh J., Paek P.* Applications of causal modeling in cybersecurity: An exploratory approach // *Advances Science Technology Engineering Systems J.*, 2020. Vol. 5. Iss. 3. P. 380–387. doi: 10.25046/aj050349.
13. *Vivek Y., Ravi V., Mane A.A., Naidu L.R.* Explainable artificial intelligence and causal inference based ATM fraud detection. — Cornell University, 2022. 34 p. arXiv:2211.10595 [cs.LG].
14. *Грушо А.А., Грушо Н.А., Забейжайло М.И., Кульченков В.В., Тимонина Е.Е.* Выявление причинно-следственных связей при покрытии причин // *Информатика и её применения*, 2024. Т. 18. Вып. 2. С. 54–59. doi: 10.14357/19922264240208. EDN: MKXMZY.

15. DOWNDetector Ookla: Real-time problem & outage monitoring. <https://downdetector.com>.
16. Sun H., Wang Z., Wang J., Huang Z., Carrington N., Liao J. Data-driven power outage detection by social sensors // IEEE T. Smart Grid, 2016. Vol. 7. No. 5. P. 2516–2524. doi: 10.1109/TSG.2016.2546181.
17. Грушо А. А., Грушо Н. А., Левыкин М. В., Тимонина Е. Е. Методы идентификации захвата хоста в распределенной информационно-вычислительной системе, защищенной с помощью метаданных // Информатика и её применения, 2018. Т. 12. Вып. 4. С. 39–43. doi: 10.14357/19922264180406. EDN: VOGJQB.
18. Смирнов Д. В., Грушо А. А., Забейжайло М. И. К задаче идентификации сбоев в информационно-технологической инфраструктуре путем мониторинга и анализа косвенных данных // Системы и средства информатики, 2024. Т. 34. № 3. С. 14–22. doi: 10.14357/08696527240302. EDN: QZYOGK.

Поступила в редакцию 29.05.2026

Принята к публикации 15.08.2026

ATTACKS ON NETWORK-CENTRIC CONTROL SYSTEMS USING DECEPTION

A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, A. A. Zatsarinny, and V. O. Piskovski

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation

Abstract: The application of network-centric technologies in control and decision support systems is determined by the concept of development of monitoring of peripheral nodes of the network-centric system (NCS) as well as the conditions for ensuring information security. The work is devoted to one class of attacks on such systems, which uses hidden distortion of the properties of information necessary for proper monitoring and control. The main goal of the Center in the NCS is described as the main controlling cause, consisting of properties that ultimately generate controlling effects throughout the NCS. A mathematical model of the control actions in the NCS is constructed using directed acyclic graphs. Examples of attacks on the NCS, the possibility of their identification, and countering such attacks are considered. It is demonstrated how the prevention of the development of an attack can be provided by identifying the missing consequences of the correct property as well as the use of deceptive properties.

Keywords: information security; network-centric systems; anomalies; detection of anomalies

DOI: 10.14357/19922264260310

EDN: WAGKXY

References

1. Láznovský, M. 2015. Dá se „napíchnout“ psací stroj? KGB to dokázala. *Idnes*. Available at: https://www.idnes.cz/technet/vojenstvi/rusove-americanum-odposlouchavali-psaci-stroje.A151027_235308_vojenstvi_mla (accessed August 11, 2026).
2. Melton, K., and V. Alekseenko. 2022. Shpionskie igry: kak SSHa vnedryali zhuchki v kopiroval'nye apparaty SSSR [Spy games: How the USA embedded bugs in Soviet copy machines]. *TechInsider*. Available at: <https://www.techinsider.ru/technologies/164236-est-li-v-vashem-printere-zhuchok/> (accessed August 11, 2026).
3. Popov, I. 2004. Voyna budushchego: vzglyad iz-za okeana. Voennye teorii i kontseptsii sovremennykh SSHa [The war of the future: A view from across the ocean. Military theories and concepts of the modern USA]. Moscow: AST; Astrel. 444 p. Available at: <https://pub.wikireading.ru/84049> (accessed August 11, 2026).
4. Makarchuk, I. L., and K. A. Trotsenko. 2022. Kharakter operatsiy sovremennykh armiy. Mul'tirazumnye setevye voennye sistemy i taktika ikh deystviy [The nature of operations by modern armies. Multiintelligent network military systems and their action tactics]. *Voyennaya mysl'* [Military Thought] 11:13–31. EDN: IYRMEF.
5. Tonkoshkurov, V. P. 2026. Novye tendentsii “novykh” voyn i ikh vliyanie na programmy voozruzheniy tekhnologicheskikh razvitykh gosudarstv mira [New trends in “new” wars and their impact on the arms programs of technologically advanced countries]. *Problemy voyennoy bezopasnosti Rossii: vzglyad v budushchee: Mat-ly 11-y Mezhdunarodnoy mezhdvostvennoy nauchn.-praktich. konf. RARAN* [Russia's military security issues: A look into the future: 11th Interdepartmental Scientific and Practical Conference (International) of the Russian Academy of Sciences Proceedings]. Moscow: MGTU im. N. E. Bauman. 1:59–78.
6. Pospelov, G., and V. A. Irikov. 1976. *Programmno-tselevoye planirovaniye i upravleniye* [Program and target planning and management]. Moscow: Sovetskoye radio. 440 p.
7. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, A. A. Zatsarinny, and V. O. Piskovskii. 2026. Poisk anomalii v setetsentricheskikh sistemakh upravleniya [Search for anomalies in network-centric control systems]. *Informati-*

- ka i ee Primeneniya — Inform. Appl.* 20(2):82–88. doi: 10.14357/19922264260207. EDN: PPXIOI.
8. Balke, A., and J. Pearl. 1994. Probabilistic evaluation of counterfactual queries. *12th National Conference on Artificial Intelligence Proceedings*. Eds. B. Hayes-Roth and R. Korf. Menlo Park, CA: MIT Press. 1:230–237.
 9. Pearl, J. 1995. Causal diagrams for empirical research. *Biometrika* 82(4):669–688. doi: 10.2307/2337329.
 10. Pearl, J. 1996. Structural and probabilistic causality. *Psychol. Learn. Motiv.* 34:393–435. doi: 10.1016/S0079-7421(08)60566-6.
 11. Pearl, J. 2019. The seven tools of causal inference, with reflections on machine learning. *Commun. ACM* 62(3):54–60. doi: 10.1145/3241036.
 12. Abel, S., Y. Tang, J. Singh, and P. Paek. 2020. Applications of causal modeling in cybersecurity: An exploratory approach. *Advances Science Technology Engineering Systems J.* 5(3):380–387. doi: 10.25046/aj050349.
 13. Vivek, Y., V. Ravi, A. A. Mane, and L. R. Naidu. 2022. Explainable artificial intelligence and causal inference based ATM fraud detection. Cornell University. 34 p. Available at: <https://arxiv.org/pdf/2211.10595> (accessed August 11, 2026).
 14. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, V. V. Kulchenkov, and E. E. Timonina. 2024. Vyyavlenie prichinno-sledstvennykh svyazey pri pokrytii prichin [Identification of cause-and-effect relationships when covering causes]. *Informatika i ee Primeneniya — Inform. Appl.* 18(2):54–59. doi: 10.14357/19922264240208. EDN: MKXMZY.
 15. DownteDetector Ookla. Real-time problem & outage monitoring. Available at: <https://downtedetector.com> (accessed August 11, 2026).
 16. Sun, H., Z. Wang, J. Wang, Z. Huang, N. Carrington, and J. Liao. 2016. Data-driven power outage detection by social sensors. *IEEE T. Smart Grid* 7(5):2516–2524. doi: 10.1109/TSG.2016.2546181.
 17. Grusho, A. A., N. A. Grusho, M. V. Levykin, and E. E. Timonina. 2018. Metody identifikatsii zakhvata khosta v raspredelennoy informatsionno-vychislitel'noy sisteme, zashchishchennoy s pomoshch'yu metadannykh [Methods of identification of host capture in a distributed information system which is protected on the basis of meta data]. *Informatika i ee Primeneniya — Inform. Appl.* 12(4):39–43. doi: 10.14357/19922264180406. EDN: VOGJQB.
 18. Smirnov, D. V., A. A. Grusho, and M. I. Zabezhailo. 2024. K zadache identifikatsii sboev v informatsionno-tekhnologicheskoy infrastrukture putem monitoringa i analiza kosvennykh dannyykh [To the problem of identifying failures in the information technology infrastructure by monitoring and analyzing indirect data]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 34(3):14–22. doi: 10.14357/08696527240302. EDN: QZYOGK.

Received May 29, 2026

Accepted August 15, 2026

Contributors

Grusho Alexander A. (b. 1946) — Doctor of Science in physics and mathematics, professor, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; grusho@yandex.ru

Grusho Nikolai A. (b. 1982) — Candidate of Science (PhD) in physics and mathematics, senior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation; info@itake.ru

Zabezhailo Michael I. (b. 1956) — Doctor of Science in physics and mathematics, professor, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119333, Russian Federation; m.zabezhailo@yandex.ru

Zatsarinny Alexander A. (b. 1951) — Doctor of Science in technology, professor, principal scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences; 44-2 Vavilov Str., Moscow 119333, Russian Federation; AZatsarinny@frccsc.ru

Piskovski Viktor O. (b. 1963) — Candidate of Science (PhD) in physics and mathematics, senior scientist, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences; 44-2 Vavilov Str., Moscow 119133, Russian Federation; vpvp80@yandex.ru

Борисов Андрей Владимирович (р. 1965) — доктор физико-математических наук, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук; профессор кафедры математической статистики факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова

Босов Алексей Вячеславович (р. 1969) — доктор технических наук, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Босов Святослав Алексеевич (р. 1992) — инженер Федерального исследовательского центра «Информатика и управление» Российской академии наук

Горшенин Андрей Константинович (р. 1986) — доктор физико-математических наук, доцент, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Грушо Александр Александрович (р. 1946) — доктор физико-математических наук, профессор, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Грушо Николай Александрович (р. 1982) — кандидат физико-математических наук, старший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Достовалова Анастасия Михайловна (р. 1999) — младший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Забейхайло Михаил Иванович (р. 1956) — доктор физико-математических наук, профессор, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Зацаринный Александр Алексеевич (р. 1951) — доктор технических наук, профессор, главный научный сотрудник Федерального исследовательского

центра «Информатика и управление» Российской академии наук

Козлов Михаил Васильевич (р. 1958) — ведущий математик Федерального исследовательского центра «Информатика и управление» Российской академии наук

Кривенко Михаил Петрович (р. 1946) — доктор технических наук, профессор, ведущий научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Куринов Юрий Николаевич (р. 2002) — студент магистратуры факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова

Листопад Сергей Викторович (р. 1984) — кандидат технических наук, директор Калининградского филиала Федерального исследовательского центра «Информатика и управление» Российской академии наук

Малашенко Юрий Евгеньевич (р. 1946) — доктор физико-математических наук, старший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Мележников Евгений Игоревич (р. 1998) — аспирант кафедры математической статистики факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова; младший научный сотрудник Московского центра фундаментальной и прикладной математики

Назарова Ирина Александровна (р. 1966) — кандидат физико-математических наук, научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Писковский Виктор Олегович (р. 1963) — кандидат физико-математических наук, старший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Торшин Иван Юрьевич (р. 1972) — кандидат физико-математических наук, кандидат химических наук, ведущий научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Урюпин Илья Вадимович (р. 1993) — кандидат физико-математических наук, младший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Чижов Иван Владимирович (р. 1984) — кандидат физико-математических наук, доцент кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского

государственного университета имени М. В. Ломоносова; старший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук

Шестаков Олег Владимирович (р. 1976) — доктор физико-математических наук, профессор кафедры математической статистики факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова; старший научный сотрудник Федерального исследовательского центра «Информатика и управление» Российской академии наук; ведущий научный сотрудник Московского центра фундаментальной и прикладной математики

Правила подготовки рукописей для публикации в журнале «Информатика и её применения»

Журнал «Информатика и её применения» публикует теоретические, обзорные и дискуссионные статьи, посвященные научным исследованиям и разработкам в области информатики и ее приложений.

Журнал издается на русском языке. По специальному решению редколлегии отдельные статьи могут печататься на английском языке.

Тематика журнала охватывает следующие направления:

- теоретические основы информатики;
- математические методы исследования сложных систем и процессов;
- информационные системы и сети;
- информационные технологии;
- архитектура и программное обеспечение вычислительных комплексов и сетей.

1. В журнале печатаются статьи, содержащие результаты, ранее не опубликованные и не предназначенные к одновременной публикации в других изданиях.

Публикация предоставленной автором(ами) рукописи не должна нарушать положений глав 69, 70 раздела VII части IV Гражданского кодекса, которые определяют права на результаты интеллектуальной деятельности и средства индивидуализации, в том числе авторские права, в РФ.

Ответственность за нарушение авторских прав, в случае предъявления претензий к редакции журнала, несут авторы статей.

Направляя рукопись в редакцию, авторы сохраняют свои права на данную рукопись и при этом передают учредителям и редколлегии журнала неисключительные права на издание статьи на русском языке (или на языке статьи, если он отличен от русского) и на перевод ее на английский язык, а также на ее распространение в России и за рубежом. Каждый автор должен представить в редакцию подписанный с его стороны «Лицензионный договор о передаче неисключительных прав на использование произведения», текст которого размещен по адресу <http://www.ipiran.ru/publications/licence.doc>. Этот договор может быть представлен в бумажном (в 2-х экз.) или в электронном виде (отсканированная копия заполненного и подписанного документа).

Если при подготовке статьи авторы использовали инструменты на основе искусственного интеллекта, они обязаны включить эту информацию в текст статьи.

Редколлегия вправе запросить у авторов экспертное заключение о возможности публикации предоставленной статьи в открытой печати.

2. К статье прилагаются данные автора (авторов) (см. п. 8). При наличии нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией.
3. Редакция журнала осуществляет экспертизу присланных статей в соответствии с принятой в журнале процедурой рецензирования.

Возвращение рукописи на доработку не означает ее принятия к печати.

Доработанный вариант с ответом на замечания рецензента необходимо прислать в редакцию.

4. Решение редколлегии о публикации статьи или ее отклонении сообщается авторам.
Редколлегия может также направить авторам текст рецензии на их статью. Дискуссия по поводу отклоненных статей не ведется.
5. Редактура статей высылается авторам для просмотра. Замечания к редакции должны быть присланы авторами в кратчайшие сроки.
6. Рукопись предоставляется в электронном виде в форматах MS WORD (.doc или .docx) или L^AT_EX (.tex), дополнительно — в формате .pdf, на дискете, лазерном диске или электронной почтой. Предоставление бумажной рукописи обязательно.

7. При подготовке рукописи в MS Word рекомендуется использовать следующие настройки.

Параметры страницы: формат — A4; ориентация — книжная; поля (см): внутри — 2,5, снаружи — 1,5, сверху — 2, снизу — 2, от края до нижнего колонтитула — 1,3.

Основной текст: стиль — «Обычный», шрифт — Times New Roman, размер — 14 пунктов, абзацный отступ — 0,5 см, 1,5 интервала, выравнивание — по ширине.

Рекомендуемый объем рукописи — не свыше 10 страниц указанного формата. При превышении указанного объема редколлегия вправе потребовать от автора сокращения объема рукописи.

Сокращения слов, помимо стандартных, не допускаются. Допускается минимальное количество аббревиатур.

Все страницы рукописи нумеруются.

Шаблоны оформления представлены в интернете:

http://www.ipiran.ru/journal/template_jiep_ssi_2024.zip

8. Статья должна содержать следующую информацию на *русском и английском языках*:

- название статьи;
- Ф.И.О. авторов, на английском можно только имя и фамилию;
- место работы, с указанием почтового адреса организации и электронного адреса каждого автора;
- сведения об авторах, в соответствии с форматом, образцы которого представлены на страницах:
http://www.ipiran.ru/journal/issues/2013_07_01/authors.asp и
http://www.ipiran.ru/journal/issues/2013_07_01_eng/authors.asp;
- аннотация (не менее 100 слов на каждом из языков). Аннотация — это краткое резюме работы, которое может публиковаться отдельно. Она является основным источником информации в информационных системах и базах данных. Английская аннотация должна быть оригинальной, может не быть дословным переводом русского текста и должна быть написана хорошим английским языком. В аннотации не должно быть ссылок на литературу и, по возможности, формул;
- ключевые слова — желательно из принятых в мировой научно-технической литературе тематических тезаурусов. Предложения не могут быть ключевыми словами;
- источники финансирования работы (ссылки на гранты, проекты, поддерживающие организации и т. п.).

9. Требования к спискам литературы.

Ссылки на литературу в тексте статьи нумеруются (в квадратных скобках) и располагаются в каждом из списков литературы в порядке первых упоминаний. Если источник имеет DOI и/или EDN, то их необходимо указывать.

Списки литературы представляются в двух вариантах:

- (1) **Список литературы к русскоязычной части.** Русские и английские работы — на языке и в алфавите оригинала;
- (2) **References.** Русские работы и работы на других языках — в латинской транслитерации с переводом на английский язык; английские работы и работы на других языках — на языке оригинала.

Необходимо для составления списка “References” пользоваться размещенной на сайте <http://www.translit.net/ru/bgn/> бесплатной программой транслитерации русского текста в латиницу.

Список литературы “References” приводится полностью отдельным блоком, повторяя все позиции из списка литературы к русскоязычной части, независимо от того, имеются или нет в нем иностранные источники. Если в списке литературы к русскоязычной части есть ссылки на иностранные публикации, набранные латиницей, они полностью повторяются в списке “References”.

Ниже приведены примеры ссылок на различные виды публикаций в списке “References”.

Описание статьи из журнала:

Zagurenko, A. G., V. A. Korotovskikh, A. A. Kolesnikov, A. V. Timonov, and D. V. Kardymon. 2008. Tekhniko-ekonomicheskaya optimizatsiya dizayna gidrorazryva plasta [Technical and economic optimization of the design of hydraulic fracturing]. *Neftyanoe hozyaystvo* [Oil Industry] 11:54–57.

Zhang, Z., and D. Zhu. 2008. Experimental research on the localized electrochemical micromachining. *Russ. J. Electrochem.* 44(8):926–930. doi:10.1134/S1023193508080077.

Описание статьи из электронного журнала:

Swaminathan, V., E. Lepkoswka-White, and B. P. Rao. 1999. Browsers or buyers in cyberspace? An investigation of electronic factors influencing electronic exchange. *JCMC* 5(2). Available at: <http://www.ascusc.org/jcmc/vol5/issue2/> (accessed April 28, 2011).

Описание статьи из продолжающегося издания (сборника трудов):

Astakhov, M. V., and T. V. Tagantsev. 2006. Eksperimental'noe issledovanie prochnosti soedineniy “stal’—kompozit” [Experimental study of the strength of joints “steel—composite”]. *Trudy MGTU “Matematicheskoe modelirovanie slozhnykh tekhnicheskikh sistem”* [Bauman MSTU “Mathematical Modeling of Complex Technical Systems” Proceedings]. 593:125–130.

Описание материалов конференций:

Usmanov, T. S., A. A. Gusmanov, I. Z. Mullagalin, R. Ju. Muhametshina, A. N. Chervyakova, and A. V. Sveshnikov. 2007. Osobennosti proektirovaniya razrabotki mestorozhdeniy s primeneniem gidrorazryva plasta [Features of the design of field development with the use of hydraulic fracturing]. *Trudy 6-go Mezhdunarodnogo Simpoziuma "Novye resursoberegayushchie tekhnologii nedropol'zovaniya i povysheniya neftegazootdachi"* [6th Symposium (International) "New Energy Saving Subsoil Technologies and the Increasing of the Oil and Gas Impact" Proceedings]. Moscow. 267–272.

Описание книги (монографии, сборники):

Lindorf, L. S., and L. G. Mamikonians, eds. 1972. *Ekspluatatsiya turbogeneratorov s neposredstvennym okhlazhdeniem* [Operation of turbine generators with direct cooling]. Moscow: Energy Publs. 352 p.

Latyshev, V. N. 2009. *Tribologiya rezaniya. Kn. 1: Friksionnye protsessy pri rezanii metallov* [Tribology of cutting. Vol. 1: Frictional processes in metal cutting]. Ivanovo: Ivanovskii State Univ. 108 p.

Описание переводной книги (в списке литературы к русскоязычной части необходимо указать: / Пер. с англ. — после названия книги, а в конце ссылки указать оригинал книги в круглых скобках):

1. В русскоязычной части:

Тимошенко С. П., Янг Д. Х., Уивер У. Колебания в инженерном деле / Пер. с англ. — М.: Машиностроение, 1985. 472 с. (*Timoshenko S. P., Young D. H., Weaver W. Vibration problems in engineering. — 4th ed. — New York, NY, USA: Wiley, 1974. 521 p.*)

2. В англоязычной части:

Timoshenko, S. P., D. H. Young, and W. Weaver. 1974. *Vibration problems in engineering*. 4th ed. New York: Wiley. 521 p.

Описание неопубликованного документа:

Latypov, A. R., M. M. Khasanov, and V. A. Baikov. 2004 (unpubl.). *Geologiya i dobycha (NGT GiD)* [Geology and production (NGT GiD)]. Certificate on official registration of the computer program No. 2004611198.

Описание интернет-ресурса:

Pravila tsitirovaniya istochnikov [Rules for the citing of sources]. Available at: <http://www.scribd.com/doc/1034528/> (accessed February 7, 2011).

Описание диссертации или автореферата диссертации:

Semenov, V. I. 2003. *Matematicheskoe modelirovaniye plazmy v sisteme kompaktnyy tor* [Mathematical modeling of the plasma in the compact torus]. Moscow. D.Sc. Diss. 272 p.

Kozhunova, O. S. 2009. *Tekhnologiya razrabotki semanticheskogo slovary informatsionnogo monitoringa* [Technology of development of semantic dictionary of information monitoring system]. Moscow: IPI RAN. PhD Thesis. 23 p.

Описание ГОСТа:

GOST 8.586.5-2005. 2007. *Metodika vypolneniya izmereniy. Izmerenie raskhoda i kolichstva zhidkostey i gazov s pomoshch'yu standartnykh suzhayushchikh ustroystv* [Method of measurement. Measurement of flow rate and volume of liquids and gases by means of orifice devices]. Moscow: Standardinform Publs. 10 p.

Описание патента:

Bolshakov, M. V., A. V. Kulakov, A. N. Lavrenov, and M. V. Palkin. 2006. *Sposob orientirovaniya po krenu letatel'nogo apparata s opticheskoy golovkoy samonavedeniya* [The way to orient on the roll of aircraft with optical homing head]. Patent RF No. 2280590.

10. Присланные в редакцию материалы авторам не возвращаются.

11. При отправке файлов по электронной почте просим придерживаться следующих правил:

- указывать в поле subject (тема) название журнала и фамилию автора;
- указывать в тексте письма название статьи, авторов и журнал, в который направляется статья;
- использовать attach (присоединение);
- в состав электронной версии статьи должны входить: файл, содержащий текст статьи, и файл(ы), содержащий(е) иллюстрации.

12. Журнал «Информатика и её применения» является некоммерческим изданием. Плата за публикацию не взимается, гонорар авторам не выплачивается.

Адрес редакции журнала «Информатика и её применения»:

Москва 119333, ул. Вавилова, д. 44, корп. 2, ФИЦ ИУ РАН

Тел.: +7 (499) 135-86-92 Факс: +7 (495) 930-45-05

e-mail: ieep@frccsc.ru (Стригина Светлана Николаевна)

<http://www.ipiran.ru/journal/issues/>

Requirements for manuscripts submitted to Journal “Informatics and Applications”

Journal “Informatics and Applications” (Inform. Appl.) publishes theoretical, review, and discussion articles on the research and development in the field of informatics and its applications.

The journal is published in Russian. By a special decision of the editorial board, some articles can be published in English.

The topics covered include the following areas:

- theoretical fundamentals of informatics;
- mathematical methods for studying complex systems and processes;
- information systems and networks;
- information technologies; and
- architecture and software of computational complexes and networks.

1. The Journal publishes original articles which have not been published before and are not intended for simultaneous publication in other editions. An article submitted to the Journal must not violate the Copyright law. Sending the manuscript to the Editorial Board, the authors retain all rights of the owners of the manuscript and transfer the nonexclusive rights to publish the article in Russian (or the language of the article, if not Russian) and its distribution in Russia and abroad to the Founders and the Editorial Board. Authors should submit a letter to the Editorial Board in the following form:

Agreement on the transfer of rights to publish:

“We, the undersigned authors of the manuscript “. . .”, pass to the Founder and the Editorial Board of the Journal “Informatics and Applications” the nonexclusive right to publish the manuscript of the article in Russian (or in English) in both print and electronic versions of the Journal. We affirm that this publication does not violate the Copyright of other persons or organizations.

Author(s) signature(s): (name(s), address(es), date).

This agreement should be submitted in paper form or in the form of a scanned copy (signed by the authors).

If authors used artificial intelligence (AI)-based tools in preparing their manuscript, they must include this information in the text of the article.

2. A submitted article should be attached with **the data on the author(s)** (see item 8). If there are several authors, the contact person should be indicated who is responsible for correspondence with the Editorial Board and other authors about revisions and final approval of the proofs.
3. The Editorial Board of the Journal examines the article according to the established reviewing procedure. If the authors receive their article for correction after reviewing, it does not mean that the article is approved for publication. The corrected article should be sent to the Editorial Board for the subsequent review and approval.
4. The decision on the article publication or its rejection is communicated to the authors. The Editorial Board may also send the reviews on the submitted articles to the authors. Any discussion upon the rejected articles is not possible.
5. The edited articles will be sent to the authors for proofread. The comments of the authors to the edited text of the article should be sent to the Editorial Board as soon as possible.
6. The manuscript of the article should be presented electronically in the MS WORD (.doc or .docx) or L^AT_EX (.tex) formats, and additionally in the .pdf format. All documents may be sent by e-mail or provided on a CD or diskette. A hard copy submission is not necessary.
7. The recommended typesetting instructions for manuscript.

Pages parameters: format A4, portrait orientation, document margins (cm): left — 2.5, right — 1.5, above — 2.0, below — 2.0, footer 1.3.

Text: font — Times New Roman, font size — 14, paragraph indent — 0.5, line spacing — 1.5, justified alignment.

The recommended manuscript size: not more than 10 pages of the specified format. If the specified size exceeded, the editorial board is entitled to require the author to reduce the manuscript.

Use only standard abbreviations. Avoid abbreviations in the title and abstract. The full term for which an abbreviation stands should precede its first use in the text unless it is a standard unit of measurement.

All pages of the manuscript should be numbered.

The templates for the manuscript typesetting are presented on site:

http://www.ipiran.ru/journal/template_iiep_ssi_2024.zip.

8. The articles should enclose data both in **Russian and English**:

- title;
- author’s name and surname;
- affiliation — organization, its address with ZIP code, city, country, and official e-mail address;
- data on authors according to the format (see site):

http://www.ipiran.ru/journal/issues/2013_07_01/authors.asp and

http://www.ipiran.ru/journal/issues/2013_07_01_eng/authors.asp;

- abstract (not less than 100 words) both in Russian and in English. Abstract is a short summary of the article that can be published separately. The abstract is the main source of information on the article and it could be included in leading information systems and data bases. The abstract in English has to be an original text and should not be an exact translation of the Russian one. Good English is required. In abstracts, avoid references and formulae;
- indexing is performed on the basis of keywords. The use of keywords from the internationally accepted thematic Thesauri is recommended.
Important! Keywords must not be sentences; and
- Acknowledgments.

9. References. Russian references have to be presented both in English translation and Latin transliteration (refer <http://www.translit.net/ru/bgn/>).

Please take into account the following examples of Russian references appearance:

Article in journal:

Zhang, Z., and D. Zhu. 2008. Experimental research on the localized electrochemical micromachining. *Russ. J. Electrochem.* 44(8):926–930. doi:10.1134/S1023193508080077.

Journal article in electronic format:

Swaminathan, V., E. Lepkoswka-White, and B. P. Rao. 1999. Browsers or buyers in cyberspace? An investigation of electronic factors influencing electronic exchange. *JCMC* 5(2). Available at: <http://www.ascusc.org/jcmc/vol5/issue2/> (accessed April 28, 2011).

Article from the continuing publication (collection of works, proceedings):

Astakhov, M. V., and T. V. Tagantsev. 2006. Eksperimental'noe issledovanie prochnosti soedineniy “stal’–kompozit” [Experimental study of the strength of joints “steel–composite”]. *Trudy MGTU “Matematicheskoe modelirovanie slozhnykh tekhnicheskikh sistem”* [Bauman MSTU “Mathematical Modeling of Complex Technical Systems” Proceedings]. 593:125–130.

Conference proceedings:

Usmanov, T. S., A. A. Gusmanov, I. Z. Mullagalin, R. Ju. Muhametshina, A. N. Chervyakova, and A. V. Sveshnikov. 2007. Osobennosti proektirovaniya razrabotki mestorozhdeniy s primeneniem gidrorazryva plasta [Features of the design of field development with the use of hydraulic fracturing]. *Trudy 6-go Mezhdunarodnogo Simpoziuma “Novye resursoberegayushchie tekhnologii nedropol’zovaniya i povysheniya neftegazootdachi”* [6th Symposium (International) “New Energy Saving Subsoil Technologies and the Increasing of the Oil and Gas Impact” Proceedings]. Moscow. 267–272.

Books and other monographs:

Lindorf, L. S., and L. G. Mamikonians, eds. 1972. *Ekspluatatsiya turbogeneratorov s neposredstvennym okhlazhdeniem* [Operation of turbine generators with direct cooling]. Moscow: Energy Publs. 352 p.

Dissertation and Thesis:

Kozhunova, O. S. 2009. Tekhnologiya razrabotki semanticheskogo slovary informatsionnogo monitoringa [Technology of development of semantic dictionary of information monitoring system]. Moscow: IPI RAN. PhD Thesis. 23 p.

State standards and patents:

GOST 8.586.5–2005. 2007. Metodika vypolneniya izmereniy. Izmerenie raskhoda i kolichstva zhidkostey i gazov s pomoshch'yu standartnykh suzhayushchikh ustroystv [Method of measurement. Measurement of flow rate and volume of liquids and gases by means of orifice devices]. M.: Standardinform Publs. 10 p.

Bolshakov, M. V., A. V. Kulakov, A. N. Lavrenov, and M. V. Palkin. 2006. Sposob orientirovaniya po krenu letatel'nogo apparata s opticheskoy golovkoy samonavedeniya [The way to orient on the roll of aircraft with optical homing head]. Patent RF No. 2280590.

References in Latin transcription are presented in the original language.

References in the text are numbered according to the order of their first appearance; the number is placed in square brackets. All items from the reference list should be cited.

10. Manuscripts and additional materials are not returned to Authors by the Editorial Board.

11. Submissions of files by e-mail must include:

- the journal title and author’s name in the “Subject” field;
- the article title, authors’ names, and the journal title, whereto the paper is being submitted, in the text of the email;
- an article and additional materials have to be attached using the “attach” function; and
- an electronic version of the article should contain the file with the text and a separate file with figures.

12. “Informatics and Applications” journal is not a profit publication. There are no charges for the authors as well as there are no royalties.

Editorial Board address:

FRC CSC RAS, 44, block 2, Vavilov Str., Moscow 119333, Russia

Ph.: +7 (499) 135 86 92, Fax: +7 (495) 930 45 05

e-mail: iiep@frccsc.ru (to Svetlana Strigina)

<http://www.ipiran.ru/english/journal.asp>