ISSN 0555-2923

РОССИЙСКАЯ АКАДЕМИЯ НАУК

Проблемы передачи информации

том 59 вып. 2

2023

РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан в январе 1965 г. **ISSN: 0555-2923** **Выходит 4 раза в год**

Том 59, 2023 **Вып. 2**

Москва

СОДЕРЖАНИЕ

CONTENTS

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.291 : 519.725

© 2023 г. **И.Ю. Могильных, Ф.И. Соловьева**

КОНСТРУКЦИИ И ИНВАРИАНТЫ ОПТИМАЛЬНЫХ КОДОВ В МЕТРИКЕ ЛИ[1]

Предложены каскадный и свитчинговый методы построения совершенных и диаметральных совершенных кодов, исправляющих одну ошибку, в метрике Ли. Рассмотрены ранги и ядра диаметральных совершенных кодов, полученных свитчинговой конструкцией.

Ключевые слова: метрика Ли, совершенный код, диаметральный совершенный код, код Васильева, код Моллара, каскадная конструкция.

DOI: 10.31857/S0555292323020018, **EDN:** POEKDW

§ 1. Введение

Исследования совершенных кодов в метрике Ли восходят к работе [1], в которой выдвинута гипотеза о несуществовании совершенных кодов в метрике Ли над алфавитами мощности больше 3, исправляющих более одной ошибки.

Параметры всех совершенных кодов, исправляющих одну ошибку, в метрике Ли, были перечислены в работе [2]. Для каждого набора допустимых параметров кодов показано существование линейного, т.е. образующего подгруппу относительно покоординатного сложения в $\mathbb{Z}_q$, совершенного кода. В работе [3] была предложена серия новых конструкций для нелинейных совершенных и диаметральных совершенных кодов, исправляющих одну ошибку. Некоторые из них являются вариантами известных конструкций совершенных кодов в метрике Хэмминга, таких как конструкция Соловьевой [4] для кодов в метрике Ли. В недавней работе [5] был развит конструктивный аппарат для построения совершенных и диаметральных совершенных кодов в метрике Ли. Многие предложенные в [5] конструкции используют разбиения на оптимальные коды. С помощью построения различных разбиений были получены рекордные оценки числа совершенных и диаметральных совершенных кодов в метрике Ли.

Данная статья является продолжением предыдущих исследований [5–7]. Предложены две конструкции кодов, исправляющих одну ошибку: для совершенных кодов – каскадная, и для диаметральных совершенных кодов – свитчинговая.

Предложенная каскадная конструкция для совершенных кодов в метрике Ли идейно восходит к методу Моллара [8], который впоследствии был обобщен в [9] для совершенных q-ичных кодов в метрике Хэмминга. С помощью подхода работы [9] в [10] было получено рекордное количество троичных совершенных кодов длины 13, а также установлено точное число классов эквивалентности кодов конструкции [9], их оказалось более 93 миллионов. Отметим, что конструкция работ [8, 9] оказалась также продуктивной с точки зрения алгебраических кодов в метрике Хэмминга.

[1] Исследование выполнено за счет гранта Российского научного фонда № 22-21-00135, https://rscf.ru/project/22-21-00135.

В работах [6, 11] было установлено, что используя любой автоморфизм любой регулярной подгруппы общей аффинной группы, этой конструкцией можно построить пропелинейный совершенный код, и изучены ранги таких кодов.

В § 2 приведены определения и свойства рассматриваемых кодов. В п. 2.1 описана группа автоморфизмов метрического пространства Ли, которая по своей структуре близка к таковой для графа Хэмминга для алфавита мощности 3. В частности, из описания вытекает, что такие классические кодовые характеристики, как ранг и мощность ядра, являющиеся инвариантами класса эквивалентности лишь для двоичных и троичных кодов в метрике Хэмминга, являются таковыми и для кодов в метрике Ли для произвольной мощности алфавита.

В § 3 приводится каскадная конструкция для совершенных кодов в декартовом произведении графов. Характер конструкции позволяет применять ее также для бесконечных графов, например, для построения кодов в манхэттенской метрике. В § 4 показано, что вариант данной конструкции для метрики Ли позволяет строить совершенные коды со всеми допустимыми параметрами, ранее перечисленными в [2], а также нелинейные коды. Каскадные методы для построения кодов в метрике Ли уже были известны ранее [3, 12, 13]. Дальнейшим развитием предложенного в статье метода может быть получение аналога этой конструкции для кодов с большим кодовым расстоянием, что для кодов в метрике Хэмминга было ранее получено в [11].

Для диаметральных совершенных кодов с минимальным расстоянием 4 в метрике Ли предложен свитчинговый метод на основе конструкции Васильева [14]. В недавней работе [7] этот подход был обобщен для получения кодов с параметрами двоичных кодов Рида – Маллера с разнообразными свойствами спектра расстояний. В отличие от кодов в метрике Хэмминга, ядра кодов для метрики Ли являются инвариантом. Более того, за счет большого числа различных делителей мощности алфавита в случае, когда код является диаметральным совершенным, для полученного семейства кодов показано большое разнообразие значений мощности ядра.

§ 2. Обозначения, определения и основные свойства

2.1. Коды в графах. Граф называется *r-регулярным*, если все его вершины имеют одну и ту же степень r. Все рассматриваемые в статье графы являются неориентированными, регулярными, не обязательно конечными графами.

Определим *декартово произведение* графов Γ_1 и Γ_2 с множествами вершин $V(\Gamma_1)$ и $V(\Gamma_2)$, соответственно, как граф $\Gamma_1 \times \Gamma_2$ с множеством вершин

$$\{(a, b) : \ a \in V(\Gamma_1),\ b \in V(\Gamma_2)\},$$

пара вершин (a, b) и (a', b') которого смежна тогда и только тогда, когда a смежна с a' в Γ_1 и $b = b'$, или b смежна с b' в Γ_2 и $a = a'$.

Кодом в графе Γ будем называть произвольную совокупность C его вершин. *Минимальным расстоянием* кода C называется

$$d = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y),$$

где $d(x, y)$ – минимальное число ребер во всех путях графа Γ, соединяющих x и y. *Мощностью* кода C называется число вершин в C.

Циклическую группу порядка q по сложению будем обозначать через $\langle \mathbb{Z}_q, + \rangle$, ее элементы являются числами $\{0, \ldots, q-1\}$ относительно операции сложения по модулю q. Для делителя r числа q через $r\mathbb{Z}_q$ будем обозначать подгруппу $\mathbb{Z}_q$, состоящую из чисел, кратных r. Элементами группы $\mathbb{Z}_q^n$ будут слова длины n в алфавите $\{0, \ldots, q-1\}$ относительно покоординатного сложения в $\mathbb{Z}_q$. Нулевой вектор будем обозначать через $\mathbf{0}$, его длина будет вытекать из контекста.

Весом Ли слова $x \in \mathbb{Z}_q^n$ называется

$$w_L(x) = \sum_{i=1}^{n} \min\{|x_i|, |q - x_i|\},$$

а *расстоянием Ли* между словами x и y называется число

$$d_L(x, y) = w_L(x - y).$$

Рассмотрим граф $L(n, q)$, вершинами которого являются слова из $\mathbb{Z}_q^n$, находящиеся на расстоянии Ли 1. Граф $L(n, q)$ есть n-я декартова степень графа $L(1, q)$. В свою очередь, при $q \geqslant 3$ граф $L(1, q)$ представляет собой цикл длины q. Другими словами, $L(n, q)$ – граф Кэли группы $\mathbb{Z}_q^n$ относительно множества образующих $\{\pm e_i : i \in \{1, \ldots, n\}\}$, где слово e_i длины n содержит 1 в i-й позиции и нули в остальных. Граф $L(n, q)$ совпадает с графом Хэмминга $H(n, q)$ для $q = 2, 3$, а граф $L(n, 4)$ изоморфен графу Хэмминга $H(2n, 2)$ под действием отображения Грея. Коды в графе $L(n, q)$ будем называть *кодами в метрике Ли*. Код в метрике Ли длины n над алфавитом $\mathbb{Z}_q$ называется *линейным*, если он образует подгруппу группы $\mathbb{Z}_q^n$. Матрицу H будем называть *проверочной* для линейного кода C, если $C = \{x \in \mathbb{Z}_q^n : Hx^T = \mathbf{0} \bmod q\}$.

Учитывая смежность в графе $L(n, q)$, имеем следующий частный случай теоремы о столбцах.

Утверждение 1. *Пусть $H = [h_1, \ldots, h_n]$ – проверочная матрица линейного кода C в метрике Ли. Верно следующее*:

1. *Минимальное расстояние кода C равно 1 тогда и только тогда, когда один из столбцов H является нулевым.*
2. *В коде C существуют кодовые слова веса Ли 2 тогда и только тогда, когда существуют $i, j \in \{1, \ldots, n\}$, такие что $h_i = h_j$ и $i \neq j$ или $h_i = -h_j$.*
3. *В коде C существуют кодовые слова веса Ли 3 тогда и только тогда, когда существуют $i, j, k \in \{1, \ldots, n\}$, $\alpha, \beta, \gamma \in \{-1, 1\}$, такие что $\alpha h_i + \beta h_j + \gamma h_k = \mathbf{0}$.*

Для подсчета мощности кода, задаваемого некоторыми проверочными соотношениями в арифметике по модулю q, мы используем следующий известный факт.

Утверждение 2. *Если b делится на наибольший общий делитель ℓ чисел a и q, то сравнение $ax = b \bmod q$ имеет ровно ℓ решений.*

Для $x \in \mathbb{Z}_q^n$, перестановки $\pi \in S_n$ и слова y длины n, состоящего из 1 и -1, рассмотрим преобразование (x, y, π), определяемое следующим образом:

$$(x, y, \pi)(z) = x + (y_1 z_{\pi^{-1}(1)}, \ldots, y_n z_{\pi^{-1}(n)})$$

для $z \in \mathbb{Z}_q^n$. Несложно видеть, что всякая такая биекция $\mathbb{Z}_q^n$ на себя является автоморфизмом графа $L(n, q)$, т.е. сохраняет расстояние Ли между словами из $\mathbb{Z}_q^n$.

Покажем, что группа автоморфизмов графа $L(n, q)$ исчерпывается преобразованиями, введенными выше. Отметим, что схема доказательства во многом повторяет доказательство подобного утверждения для группы автоморфизмов графа Хэмминга, поэтому доказательство изложено в несколько сокращенной форме.

Лемма 1. *Пусть $q \geqslant 5$. Всякое слово из $\mathbb{Z}_q^n$ веса Ли больше 1 однозначно определяется множеством своих соседей в $L(n, q)$ веса на единицу меньше.*

Доказательство. Утверждение, очевидно, верно для вершин веса не менее 2, имеющих ровно один ненулевой символ, так как оно верно при $n = 1$ для циклического графа $L(1, q)$.

Всякая вершина веса Ли не меньше 2 в графе $L(n,q)$, имеющая хотя бы два ненулевых символа, имеет хотя бы два соседа на единицу меньшего веса. Покажем, что эти соседи не могут совпадать. Предположим противное: пусть x и y, $w_L(x) = w_L(y) = w \geqslant 2$, имеют хотя бы два общих соседа x' и y', $w_L(x') = w_L(y') = w - 1$.

Удалив совпадающие символы в словах, без ограничения общности рассмотрим случай $n = 2$, слово $x = (x_1, x_2)$ и его соседей $x' = (x_1 + \alpha, x_2)$ и $y' = (x_1, x_2 + \beta)$, где

$$w_L(x_1 + \alpha) - w_L(x_1) = w_L(x_2 + \beta) - w_L(x_2) = -1.$$

В силу покоординатного определения смежности в графе $L(2,q)$ слово y, соседями которого являются x' и y', таково, что $y = (x_1 + \alpha, x_2 + \beta)$. Таким образом, y имеет вес $w_L(x) - 2$, противоречие. ▲

Лемма 2. *Стабилизатор слова* $\mathbf{0}$ *группы автоморфизмов графа* $L(n,q)$, $q \geqslant 5$, *равен*

$$\{(\mathbf{0}, y, \pi) : \ y \in \{\pm 1\}^n, \ \pi \in S_n\}.$$

Доказательство. Рассмотрим действие произвольного автоморфизма f, такого что $f(\mathbf{0}) = \mathbf{0}$ на словах веса Ли 1, т.е. $\{\pm e_i : \ i \in \{1, \ldots, n\}\}$. Предположим, что

$$f(e_i) = \alpha e_j, \quad f(-e_j) = \beta e_k$$

для некоторых $i \in \{1, \ldots, n\}$ и $j \neq k$, $\alpha, \beta \in \{-1, 1\}$. Так как $q \geqslant 5$, то у слов e_i и $-e_i$ имеется один общий сосед в графе $L(n,q)$, а именно вершина $\mathbf{0}$. С другой стороны, αe_j и βe_k имеют двух общих соседей, а именно слова $\mathbf{0}$ и $\alpha e_j + \beta e_k$, противоречие.

Следовательно, автоморфизм f действует на n различных двухэлементных множествах $\{e_i, -e_i\}$, $i = 1, \ldots, n$:

$$f(e_i) = \alpha_i e_k, \quad f(-e_i) = -\alpha_i e_k, \quad \text{где } \alpha_i \in \{1, -1\}.$$

Всякое такое действие можно единственным образом задать с помощью определенного выше автоморфизма $(\mathbf{0}, y, \pi)$ для единственного слова y и единственной перестановки π. Более того, в силу леммы 1, используя индукцию по весу слов, мы видим, что всякий автоморфизм f, оставляющий на месте $\mathbf{0}$, однозначно задается действием f на словах веса Ли 1, откуда вытекает требуемое. ▲

Теорема 1. *Пусть* $q \geqslant 3$, $q \neq 4$. *Группа автоморфизмов графа* $L(n,q)$ *состоит из преобразований*

$$\{(x, y, \pi) : \ x \in \mathbb{Z}_q^n, \ y \in \{\pm 1\}^n, \ \pi \in S_n\}.$$

Доказательство. При $q = 3$ граф $L(n,q)$ совпадает с $H(n,q)$, откуда имеем требуемое в силу описания группы автоморфизмов графа Хэмминга. Пусть $q \geqslant 5$. Так как группа из q^n преобразований

$$\{(x, (1, \ldots, 1), \mathrm{Id}) : \ x \in \mathbb{Z}_q^n\}$$

действует транзитивно на словах из $\mathbb{Z}_q^n$, и учитывая, что по лемме 2 стабилизатор $\mathbf{0}$ группы автоморфизмов графа $L(n,q)$ совпадает с

$$\{(\mathbf{0}, y, \pi) : \ y \in \{\pm 1\}^n, \ \pi \in S_n\},$$

получаем требуемое описание группы автоморфизмов графа $L(n,q)$. ▲

Два кода в графе будем называть *эквивалентными*, если существует автоморфизм графа, переводящий один код в другой.

Для кода $C \subseteq \mathbb{Z}_q^n$ в метрике Ли через $\langle C\rangle$ будем обозначать подгруппу $\mathbb{Z}_q^n$, порожденную элементами C. *Рангом* кода C будем называть величину $\log_q|\langle C\rangle|$. Таким образом, в общем случае ранг кода в метрике Ли является рациональным числом. Отметим, что существуют и другие определения ранга кодов в метрике Ли, например, в [15] ранг кода C определяется как минимальное число образующих группы $\langle C\rangle$. *Ядром* q-ичного кода C длины n в метрике Ли назовем множество слов $x \in \mathbb{Z}_q^n$, таких что $\{x + c : c \in C\} = C$.

Следствие 1. *Если $q \neq 4$, то ранг и мощность ядра кода $C \subseteq \mathbb{Z}_q^n$, содержащего слово* $\mathbf{0}$, *являются инвариантами класса эквивалентности этого кода.*

Доказательство. Хорошо известно, что при $q = 2, 3$ ранг является инвариантом кода в метрике Хэмминга. Так как в этом случае метрики Ли и Хэмминга совпадают, имеем требуемое.

Пусть $q \geqslant 5$. Рассмотрим содержащие $\mathbf{0}$ коды C и

$$\{(x, y, \pi)(c) : c \in C\}, \quad \text{где} \quad x \in \mathbb{Z}_q^n, \quad y \in \{-1, 1\}^n, \quad \pi \in S_n,$$

и покажем, что их ранги равны. Очевидно, перестановка и умножение на -1 в произвольных координатных позициях не поменяют ранг, следовательно, ранг кода $\{(\mathbf{0}, y, \pi)(c) : c \in C\}$ совпадает с рангом кода C. Так как $\{(x, y, \pi)(c) : c \in C\}$ содержит слово $\mathbf{0}$, то $\{(\mathbf{0}, y, \pi)(c) : c \in C\}$ содержит $-x$. Следовательно, подгруппа $\mathbb{Z}_q^n$, порожденная $\{(\mathbf{0}, y, \pi)(c) : c \in C\}$, совпадает с группой, порожденной

$$\{x + (\mathbf{0}, y, \pi)(c) : c \in C\} = \{(x, y, \pi)(c) : c \in C\}.$$

Следовательно, ранги кодов C и $\{(x, y, \pi)(c) : c \in C\}$ равны.

Аналогичные рассуждения имеют место и для ядра кода C. ▲

Замечание 1. Напомним, что для q-ичных кодов, где q – степень простого числа, в метрике Хэмминга ранг кода, определяемый как размерность линейной оболочки, натянутой на кодовые слова, не является инвариантом класса эквивалентности при $q \geqslant 4$. Например, используя посимвольные перестановки, из кода Хэмминга можно получить коды любого ранга, не меньшего его размерности [6].

Также отметим, что определенный выше ранг для метрики Ли не является инвариантом для четверичных кодов. Граф $L(n, 4)$ в этом случае изоморфен графу Хэмминга $H(2n, 2)$ и имеет бóльшую группу автоморфизмов, чем описанная в теореме 1.

2.2. Совершенные и диаметральные совершенные коды. В данной статье рассматриваются лишь совершенные коды и диаметральные совершенные коды с минимальными расстояниями 3 и 4 соответственно.

Код в r-регулярном графе Γ будем называть *совершенным*, если он имеет минимальное расстояние 3 и его мощность достигает границы Хэмминга, т.е.

$$|C| = \frac{|V(\Gamma)|}{r+1},$$

где $r + 1$ – объем шара радиуса 1 в графе Γ. В доказательствах будем использовать следующее эквивалентное определение. Совершенным называется код C с минимальным расстоянием 3, такой что всякая вершина из $\overline{C}$ смежна с вершиной из C. Для графа $L(n, q)$ выражение для мощности совершенного кода принимает следующий вид:

$$|C| = \frac{q^n}{2n+1}.$$

Теорема 2 [2]. *Пусть* $\{p_1, \dots, p_k\}$– *множество простых делителей числа* q. *Линейный* q-*ичный совершенный код длины* n *в метрике Ли существует тогда и только тогда, когда*

$$2n + 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad \textit{для} \quad \alpha_i \geqslant 0, \quad i = 1, \dots, k.$$

Отметим, что из выражения для мощности совершенных кодов следует, что q^n делится на $2n + 1$. Отсюда q с необходимостью делится на любой простой делитель числа $2n + 1$. Таким образом, теорема 2 описывает параметры всех совершенных кодов в метрике Ли (не обязательно линейных). Отметим, что ситуация для кодов в схеме Хэмминга другая, а именно задача существования совершенных кодов в метрике Хэмминга (над алфавитами, мощность которых не является степенью простого числа) является известной открытой проблемой.

Код $C \subseteq \mathbb{Z}_q^n$ в метрике Ли будем называть *диаметральным совершенным* с минимальным расстоянием 4, если его мощность достигает границы Дельсарта для кода и антикода [3], т.е.

$$|C| = \frac{q^n}{4n}.$$

В качестве антикода диаметра 3 выступает объединение двух шаров радиуса 1 с центрами в соседних вершинах, имеющее мощность $4n$. Другими словами, код C – диаметрально совершенный, если для любой пары соседних вершин шары радиуса 1 с центрами в этих вершинах содержат ровно одну вершину из кода C.

Подробное изложение понятия антикода и границы Дельсарта можно найти в работах [16–18]. Известная граница Дельсарта для кодов и антикодов была впервые сформулирована в [16] для кодов в дистанционно-регулярных графах. Помимо дистанционно-регулярных графов, эта граница также имеет место для графов Кэли с произвольным минимальным расстоянием, в частности, для кодов в метрике Ли и перестановочных кодов. Для графов Кэли доказательство этого утверждения можно найти в [18, теорема 13], хотя для кодов в метрике Ли эта граница была известна ранее [3].

§ 3. Каскадная конструкция совершенного кода в декартовом произведении графов

Пусть Γ_1 является регулярным графом валентности r, вершины которого разбиваются на совершенные коды $C_0, \dots, C_r$. Пусть M – некоторый код в графе Γ_2, такой что:

M является кодом с минимальным расстоянием 2; (1)

любая вершина из $\overline{M}$ смежна ровно с $r + 1$ вершинами из M в графе Γ_2. (2)

Для двух кодов C и D в графах Γ_1 и Γ_2 через $C \times D$ будем обозначать код $\{(x, y) : x \in C, y \in D\}$ в графе $\Gamma_1 \times \Gamma_2$.

Теорема 3. *Пусть* $C_0, \dots, C_r$ – *разбиение вершин* r-*регулярного графа* Γ_1 *на совершенные коды,* M – *код в регулярном графе* Γ_2, *удовлетворяющий условиям* (1) *и* (2), $D_0, \dots, D_r$ – *разбиение кода* M *на коды с минимальным расстоянием не менее* 3. *Для всякой перестановки* τ *на элементах* $\{0, \dots, r\}$ *код*

$$\mathcal{C}_\tau = \bigcup_{i \in \{0,\dots,r\}} C_i \times D_{\tau(i)}$$

является совершенным в графе $\Gamma_1 \times \Gamma_2$.

Доказательство. Код $\mathcal{C}_\tau$ имеет минимальное расстояние 3. Действительно, если $i \neq j$, то пара вершин $(u,v) \in C_i \times D_{\tau(i)}$ и $(x,y) \in C_j \times D_{\tau(j)}$ таковы, что u не совпадает с x, и так как $v, y \in D_{\tau(i)} \cup D_{\tau(j)} \subseteq M$, то согласно (1) вершина $v \in M$ не смежна с $y \in M$. Таким образом, (u,v) и (x,y) находятся на расстоянии не менее 3 в графе $\Gamma_1 \times \Gamma_2$. Если вершины (u,v), (x,y) принадлежат $C_i \times D_{\tau(i)}$ для некоторого $i \in \{0,\dots,r\}$, то они находятся на расстоянии не менее 3, поскольку или u и x различны и находятся на расстоянии не меньше 3, так как принадлежат совершенному коду C_i, или v и y различны и находятся на расстоянии не менее 3, так как принадлежат коду $D_{\tau(i)}$ с минимальным расстоянием не менее 3.

Пусть (u,v) – произвольная вершина графа $\Gamma_1 \times \Gamma_2$, не принадлежащая $\mathcal{C}_\tau$. Так как Γ_1 разбивается на совершенные коды, то $u \in C_i$ для некоторого $i \in \{0,\dots,r\}$. Изучим множество соседей вершины (u,v) в графе $\Gamma_1 \times \Gamma_2$ и покажем, что оно всегда содержит кодовое слово кода $\mathcal{C}_\tau$.

Рассмотрим несколько случаев.

1. Пусть $v \in D_{\tau(j)}$, где $j \neq i$. Тогда в силу того, что Γ_1 разбивается на совершенные коды, вершина u смежна с вершиной u' из C_j. В силу определения смежности в графе $\Gamma_1 \times \Gamma_2$ вершина (u,v) смежна с $(u',v) \in C_j \times D_{\tau(j)} \subset \mathcal{C}_\tau$.

2. Пусть $v \in \overline{M}$. Тогда согласно (2) вершина v смежна с $r+1$ вершинами из M в графе Γ_1. Так как код M разбивается на $r+1$ кодов $D_0,\dots D_r$ с минимальным расстоянием 3, то в каждом из этих $r+1$ кодов содержится ровно один сосед вершины v. В частности, в коде $D_{\tau(i)}$ содержится сосед v' вершины v в графе Γ_2. Таким образом, (u,v) смежна с вершиной $(u,v') \in C_i \times D_{\tau(i)} \subset \mathcal{C}_\tau$.

Мы заключаем, что код C_τ является совершенным в графе $\Gamma_1 \times \Gamma_2$. ▲

Отметим, что условие теоремы 3, а именно (1) и (2) сформулированы в локальных терминах, не использующих понятие мощности кода. Таким образом, она имеет место для любых регулярных графов Γ_1 и Γ_2, в том числе с бесконечным числом вершин. В частности, теорема 3 предлагает новый способ к построению совершенных кодов в манхэттенской метрике [3, раздел 5], т.е. для графов, являющихся декартовой степенью бесконечной цепи.

§ 4. Каскадная конструкция совершенного кода в метрике Ли

Рассмотрим частный случай конструкции из предыдущего параграфа для кодов в метрике Ли.

Пусть $\{p_1,\dots,p_k\}$ – множество простых делителей числа q, и пусть

$$2n_1+1 = p_1^{\alpha_1}\dots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0, \quad i=1,\dots,k.$$

Выберем $j \in \{1,\dots,k\}$ и зададим q-ичный линейный код M следующей проверочной матрицей:

$$H_M = \left(\frac{q}{p_j} \dots \frac{q}{p_j} \,\middle|\, \frac{2q}{p_j} \dots \frac{2q}{p_j} \,\middle|\, \dots \,\middle|\, \frac{(p_j-1)q}{2p_j} \dots \frac{(p_j-1)q}{2p_j} \right). \tag{3}$$

В матрице H_M каждый ненулевой элемент $\mathbb{Z}_q$, меньший $q/2$ и кратный $\dfrac{q}{p_j}$, повторяется в точности $2n_1+1$ раз, поэтому код M имеет длину

$$n_2 = \frac{(2n_1+1)(p_j-1)}{2}.$$

Все элементы проверочной матрицы H_M ненулевые, и имеются одинаковые элементы, следовательно, в силу утверждения 1 код $M = \{x : Hx^T = 0\}$ имеет минимальное расстояние 2.

Теорема 4. *Пусть* $\{p_1, \ldots, p_k\}$ – *множество простых делителей числа* q, $q \geqslant 3$, *и пусть*

$$2n_1 + 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0, \quad i = 1, \ldots, k.$$

Пусть $C_0, \ldots, C_{2n_1}$ – *разбиение* $\mathbb{Z}_q^{n_1}$ *на* q*-ичные совершенные коды в метрике Ли,* M – *код длины*

$$n_2 = \frac{(2n_1 + 1)(p_j - 1)}{2}$$

с проверочной матрицей (3) *для некоторого* $j \in \{1, \ldots, k\}$, $D_0, \ldots, D_{2n_1}$ – *разбиение кода* M *на коды с минимальным расстоянием Ли не менее* 3. *Тогда*

$$\mathcal{C}_\tau = \bigcup_{i \in \{0, \ldots, 2n_1\}} C_i \times D_{\tau(i)}$$

является совершенным q*-ичным кодом длины* $\dfrac{(2n_1 + 1)p_j - 1}{2}$ *в метрике Ли.*

Доказательство. Код M имеет минимальное расстояние 2, т.е. выполнено условие (1). В силу структуры проверочной матрицы H_M каждый элемент $\mathbb{Z}_q$, кратный $\dfrac{q}{p_j}$, но меньший $\dfrac{q}{2}$, встречается ровно $2n_1 + 1$ раз как элемент матрицы H_M. Рассмотрим синдром $H_M y^T$ произвольного слова y из $\overline{M}$. В силу выражения (3) для H_M вектор $H_M y^T$ равен $i\dfrac{q}{p_j}$, $1 \leqslant i \leqslant p_j - 1$. Если $i \leqslant \left\lfloor \dfrac{p_j - 1}{2} \right\rfloor$, то в силу (3) найдется в точности $2n_1 + 1$ векторов из стандартного базиса, вычитание которых из y дает слово с нулевым синдромом. Если $i > \left\lfloor \dfrac{p_j - 1}{2} \right\rfloor$, то найдется в точности $2n_1 + 1$ векторов из стандартного базиса, прибавление которых к y дает слово с нулевым синдромом. Другими словами, каждое слово из $\overline{M}$ находится на расстоянии Ли 1 от ровно $2n_1 + 1$ слов из кода M, т.е. выполнено условие (2), и из теоремы 3 получаем требуемое. ▲

Отметим что по теореме 2 существует линейный совершенный q-ичный код длины n_1, такой что $2n_1 + 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где $\{p_1, \ldots, p_k\}$ – множество простых делителей числа q. Следовательно, существует также разбиение $\mathbb{Z}_q^{n_1}$ на совершенные коды, представляющие собой смежные классы по такому коду.

Теперь приведем явную конструкцию разбиения кода M с проверочной матрицей (3) и длиной $n_2 = \dfrac{(2n_1 + 1)(p_j - 1)}{2}$ на коды $D_0, \ldots, D_{2n_1}$ с минимальным расстоянием 3. Для этого разобьем кодовые слова кода M на смежные классы по коду D со следующей проверочной матрицей:

$$H_D = \left(\begin{array}{c|c|c|c|c} \dfrac{q}{p_j} \ldots \dfrac{q}{p_j} & \dfrac{2q}{p_j} \ldots \dfrac{2q}{p_j} & \ldots & \ldots & \dfrac{(p_j - 1)q}{2p_j} \\ \hline A & A & \ldots & \ldots & A \end{array} \right), \tag{4}$$

где A – матрица, состоящая из всех слов из множества $\left(\dfrac{q}{p_1}\mathbb{Z}_q\right)^{\alpha_1} \times \ldots \times \left(\dfrac{q}{p_k}\mathbb{Z}_q\right)^{\alpha_k}$, т.е. первые α_1 символов этих слов являются элементами $\mathbb{Z}_q$, кратными $\dfrac{q}{p_1}$, следующие α_2 символов – это символы $\mathbb{Z}_q$, кратные $\dfrac{q}{p_2}$, и т.д.

Заметим, что в матрице H_D не существует двух столбцов, разность или сумма которых равна $\mathbf{0}$. Более того, в силу того, что элементы первой строки меньше $\dfrac{q}{2}$, умножение на 2 любого столбца не является нулевым столбцом. Следовательно, по утверждению 1 код D, представляющий собой нуль-пространство матрицы H_D, не

содержит слов веса Ли 1 и 2. С другой стороны, несложно видеть, что слова веса 3 при $q \geqslant 3$ в коде с проверочной матрицей H_D существуют, и таким образом, код D имеет минимальное расстояние 3.

Для того чтобы доказать, что линейный код M разбивается на $2n_1 + 1$ смежных классов по линейному подкоду D, покажем, что мощность кода M равна $(2n_1+1)|D|$. Рассмотрим подробнее подматрицу A матрицы H_D, которую без ограничения общности, переставляя столбцы, можно преобразовать к следующему виду:

$$\left(\begin{array}{c|c|c|c|c|c} 0 & \frac{q}{p_1}E_{\alpha_1} & 0 & \dots & 0 & B_{\frac{q}{p_1}} \\ 0 & 0 & \frac{q}{p_2}E_{\alpha_2} & \dots & 0 & B_{\frac{q}{p_2}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & \frac{q}{p_k}E_{\alpha_k} & B_{\frac{q}{p_k}} \end{array}\right),$$

где для каждого $i = 1, \dots, k$ матрица E_{α_i} – единичная размера α_i, а матрица $B_{\frac{q}{p_i}}$, $i = 1, \dots, k$, состоит лишь из элементов $\mathbb{Z}_q$, кратных $\frac{q}{p_i}$. Таким образом, H_D приобретает следующий вид:

$$H_D = \left(\begin{array}{c|c|c|c|c|c} \frac{q}{p_j} & \frac{q}{p_j} \dots \frac{q}{p_j} & \dots & \dots & \frac{q}{p_j} & a_{\frac{q}{p_j}} \\ 0 & \frac{q}{p_1}E_{\alpha_1} & 0 & \dots & 0 & C_{\frac{q}{p_1}} \\ 0 & 0 & \frac{q}{p_2}E_{\alpha_2} & \dots & 0 & C_{\frac{q}{p_2}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & \frac{q}{p_k}E_{\alpha_k} & C_{\frac{q}{p_k}} \end{array}\right), \tag{5}$$

где матрицы $C_{\frac{q}{p_i}}$, $i = 1, \dots, k$, состоят лишь из элементов, кратных $\frac{q}{p_i}$, а элементы строки $a_{\frac{q}{p_j}}$ кратны $\frac{q}{p_j}$.

Для решения системы $H_D x^T = 0$ сравнений по модулю q рассмотрим последние $n_2 - \left(1 + \sum\limits_{i=1,\dots,k} \alpha_i\right)$ переменных слова x^T как свободные, т.е. принимающие произвольные значения из $\mathbb{Z}_q$. Из выражения (5) каждое s-е проверочное уравнение, $2 \leqslant s \leqslant 1 + \sum\limits_{i=1,\dots,k} \alpha_i$, представляет собой

$$\frac{q}{p_\ell} x_s = \sum_{2+\sum\limits_{i=1,\dots,k} \alpha_i \leqslant m \leqslant n_2} a_{\ell m} x_m$$

для некоторого ℓ, где $a_{\ell m}$ делится на $\frac{q}{p_\ell}$. По утверждению 2 это уравнение имеет в точности $\frac{q}{p_\ell}$ решений относительно x_s в $\mathbb{Z}_q$ при фиксированных переменных, входящих в сумму в правой стороне равенства, все из которых являются свободными. Первое проверочное соотношение равносильно

$$\frac{q}{p_j} x_1 = \sum_{\ell=2,\dots,n_2} a_{\ell 1} x_\ell,$$

где $a_{\ell 1}$ делится на $\frac{q}{p_j}$, поэтому, учитывая утверждение 2, имеем $\frac{q}{p_j}$ решений относительно x_1.

Таким образом, в коде D имеется

$$q^{n_2-\left(1+\sum\limits_{i=1,\dots,k}\alpha_i\right)}\left(\prod_{i=1,\dots,k}\left(\frac{q}{p_i}\right)^{\alpha_i}\right)\frac{q}{p_j}=\frac{q^{n_2}}{p_j\prod\limits_{i=1,\dots,k}p_i^{\alpha_i}}=\frac{q^{n_2}}{p_j(2n_1+1)}$$

кодовых слов.

Все элементы проверочной матрицы H_M делятся на $\frac{q}{p_j}$, поэтому по утверждению 2 код M имеет мощность $\frac{q^{n_2}}{p_j}$. Следовательно, код M разбивается в точности на $2n_1+1$ смежных классов по коду D. Таким образом, имеем следующую конструкцию.

Теорема 5. *Пусть* $\{p_1,\dots,p_k\}$ – *множество простых делителей числа* q, $q\geqslant 3$, *пусть*

$$2n_1+1=p_1^{\alpha_1}\dots p_k^{\alpha_k},\quad \alpha_i\geqslant 0,\quad i=1,\dots,k,$$

и пусть τ – *произвольная перестановка на множестве* $\{0,\dots,2n_1\}$. *Кроме того, пусть* $C_0,\dots,C_{2n_1}$ – *разбиение* $\mathbb{Z}_q^{n_1}$ *на совершенные коды в метрике Ли,* $D_0,\dots,D_{2n_1}$ – *разбиение кода* M *с проверочной матрицей* (3) *на смежные классы по коду с проверочной матрицей* (4) *длины* $\frac{(2n_1+1)(p_j-1)}{2}$ *для некоторого* $j\in\{1,\dots,k\}$. *Тогда код*

$$\bigcup_{i\in\{0,\dots,2n_1\}} C_i\times D_{\tau(i)}$$

представляет собой совершенный q*-ичный код в метрике Ли длины* $\frac{(2n_1+1)p_j-1}{2}$.

В работе [2] была приведена алгебраическая характеризация линейных совершенных кодов Ли. В свою очередь, с помощью теоремы 5, в частности, получаются все линейные коды в метрике Ли. В дополнение к алгебраическому описанию совершенных линейных кодов [2] линейные коды получают интерпретацию в терминах проверочных матриц.

Пусть $p_1,\dots,p_k$ – простые делители числа q. В качестве базиса индукции возьмем разбиение на смежные классы по q-ичному линейному совершенному коду C длины $\frac{p_{j_0}-1}{2}$ для произвольного $j_0\in\{1,\dots,k\}$ со следующей проверочной матрицей:

$$\left(\frac{q}{p_{j_0}}\quad\frac{2q}{p_{j_0}}\quad\dots\quad\frac{(p_{j_0}-1)q}{2p_{j_0}}\right),$$

и будем последовательно применять конструкцию теоремы 5 с тождественной перестановкой τ и всевозможными значениями $j\in\{1,\dots,k\}$. При этом будем нумеровать смежные классы $C_0,\dots,C_{2n_1}$ и $D_0,\dots,D_{2n_1}$ следующим образом. Для каждого $i\in\{0,\dots,2n_1\}$ синдромы смежных классов C_i и D_i подберем таким образом:

$$H_D(D_i^T)=\begin{pmatrix}0\\-H_C(C_i^T)\end{pmatrix}. \tag{6}$$

В силу выбранной нумерации смежных классов проверочная матрица получаемого из теоремы 5 кода $\mathcal{C}_\tau$ с тождественной подстановкой τ имеет следующий вид:

$$\left(\begin{array}{c|c}\mathbf{0}&H_D\\H_C&\end{array}\right),$$

где $\mathbf{0}$ – строка из нулей. Действительно, если (x, y) таковы, что $x \in C_i$, $y \in D_i$ для произвольного $i \in \{0, \ldots, 2n_1\}$, то в силу (6) имеем следующее:

$$\left(\begin{array}{c|c} \mathbf{0} & H_D \\ H_C & \end{array}\right)(x_i, y_i)^T = \begin{pmatrix} 0 \\ H_C(C_i^T) \end{pmatrix} + \begin{pmatrix} 0 \\ -H_C(C_i^T) \end{pmatrix} = \mathbf{0}.$$

Варьируя $j_0 \in \{1, \ldots, k\}$, получим линейные коды длины N, где $2N + 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ для произвольных $\alpha_1, \ldots, \alpha_k \geqslant 0$, одновременно не равных нулю.

Замечание 2. С помощью теоремы 5 можно также получать q-ичные коды, отличные от линейных, для любой допустимой длины n (т.е. удовлетворяющей теореме 2), неравной $(p-1)/2$, где p – простой делитель q. Для этого рассмотрим код $C_{\tau'}$, где $\tau' = (i, j)$ в теореме 5. Тогда код $C_{\tau'}$ будет иметь

$$\frac{|C_\tau|(2n_1 - 1)}{2n_1 + 1}$$

общих кодовых слов с линейным кодом C_τ, где τ – тождественная перестановка. Так как две различные подгруппы одного порядка имеют пересечение не больше половины их порядка, заключаем, что код $C_{\tau'}$ – нелинейный.

Отметим также, что спектр получаемых длин совершенных кодов широкий. Несложно убедиться, что с помощью теоремы 5 можно построить совершенные коды простой длины, к примеру, длины 31 над алфавитом мощности 21, используя разбиения на коды длины 10 и 21. Таким образом, имеет место отделимость от других каскадных конструкций совершенных и других кодов в метрике Ли [3, 5, 13], длина которых – всегда составное число.

Интересной задачей для кодов в метрике Ли представляется нахождение существующей формулы [19] для ранга кодов, получаемых аналогом этой конструкции для метрики Хэмминга.

Замечание 3. Отметим, что теорема 4 приведена в более общем виде, чем теорема 5. Для построения различных разбиений $D_0, \ldots, D_{2n_1}$ в конструкции теоремы 4 кода M в метрике Ли можно использовать методы построения, предложенные в работах [10, 20] для аналога этой конструкции в метрике Хэмминга. Большого количества совершенных кодов в теореме 4 можно достичь, варьируя разбиения на совершенные коды $C_0, \ldots, C_{n_1}$ в метрике Ли, полученные ранее в [5].

§ 5. Свитчинговая конструкция диаметральных совершенных кодов на основе конструкции Васильева

Далее обозначим через P четновесовой код той же длины, что и q-ичный диаметральный совершенный код C длины n в метрике Ли. В этом случае $|C| = \dfrac{q^n}{4n}$, поэтому q является четным числом. При четном q несложно видеть, что четновесовой q-ичный подкод P является подгруппой $\mathbb{Z}_q^n$ (т.е. линейным кодом) с минимальным расстоянием Ли, равным 2.

Теорема 6. *Пусть C – q-ичный диаметральный совершенный код длины n с минимальным расстоянием 4 в метрике Ли,*

$$P = \{x : x \in \mathbb{Z}_q^n,\ w_L(x) = 0 \bmod 2\},$$

и пусть $\lambda \colon C \to \{\mathbf{0}, e_1\}$ – произвольная функция. Тогда код

$$C^\lambda = \{(x - y + \lambda(y), x + \lambda(y)) : x \in P,\ y \in C\}$$

является диаметральным совершенным кодом длины $2n$ с минимальным расстоянием 4 в метрике Ли.

Доказательство. Мощность кода C^λ равна

$$|P||C| = \frac{q^n}{2}\frac{q^n}{4n} = \frac{q^{2n}}{8n}$$

и совпадает с мощностью диаметрального q-ичного совершенного кода длины $2n$ в метрике Ли.

Покажем что минимальное расстояние кода C^λ равно 4. Рассмотрим для этого два различных кодовых слова кода C^λ:

$$(x - y + \lambda(y), x + \lambda(y)), \quad (x' - y' + \lambda(y'), x' + \lambda(y')),$$

где x, x' имеют четный вес, $y, y' \in C$, и покажем, что расстояние между ними не меньше 4.

Имеем следующее равенство:

$$d_L\big((x - y + \lambda(y), x + \lambda(y)), (x' - y' + \lambda(y'), x' + \lambda(y'))\big) =$$
$$= w_L\big(x - x' + \lambda(y) - \lambda(y') - (y - y')\big) + w_L\big(x - x' + \lambda(y) - \lambda(y')\big).$$

Рассмотрим два случая.

Случай 1. Пусть $y = y'$. Тогда $x \neq x'$ и

$$w_L\big(x - x' + \lambda(y) - \lambda(y') - (y - y')\big) + w_L\big(x - x' + \lambda(y) - \lambda(y')\big) = 2w_L(x - x').$$

Так как при четном q четновесовой подкод P является подгруппой $\mathbb{Z}_q^n$, то $x - x'$ имеет четный вес, откуда $2w_L(x - x') \geqslant 4$.

Случай 2. Пусть $y \neq y'$. Воспользуемся неравенством треугольника

$$w_L(\widetilde{x} - \widetilde{y}) \geqslant w_L(\widetilde{y}) - w_L(\widetilde{x})$$

для метрики Ли в случае, когда

$$\widetilde{x} = x - x' + \lambda(y) - \lambda(y'), \quad \widetilde{y} = y' - y.$$

Имеем следующие оценки:

$$w_L\big(x - x' + \lambda(y) - \lambda(y') - (y - y')\big) + w_L\big(x - x' + \lambda(y) - \lambda(y')\big) \geqslant$$
$$\geqslant w_L(\widetilde{y}) - w_L(\widetilde{x}) + w_L(\widetilde{x}) = w_L(\widetilde{y}) = w_L(y - y') \geqslant 4,$$

где последнее неравенство вытекает из минимального расстояния кода C. Заключаем, что C^λ является диаметральным совершенным кодом. ▲

Замечание 4. Число различных и неэквивалентных кодов, получаемых приведенной выше конструкцией, велико в силу небольшого объема объединения двух шаров в метрике Ли, а именно $4n$, и сравнительно небольшого порядка группы автоморфизмов графа $L(n, q)$ (теорема 1), которая по структуре ближе к группе автоморфизмов графа Хэмминга над полем из трех элементов. Даже если использовать в качестве кода C фиксированный линейный код, то число попарно неэквивалентных кодов достаточно велико. А именно, имеем следующую нижнюю оценку числа таких кодов:

$$\frac{2^{|C|}}{|\mathrm{Aut}(L(2n, q))|} = \frac{2^{\frac{q^n}{4n}}}{q^{2n}(2n)!\,2^{2n}} \geqslant \frac{2^{\frac{q^n}{4n}}}{q^{2n}n^{2n}2^{4n}} = 2^{\frac{q^n}{4n} - 2n\log_2(4nq)},$$

где $|\mathrm{Aut}(L(n, q))|$ – порядок группы автоморфизмов, описанной в теореме 1. В частности, при $n = 6$, $q = 12$ (конструкция диаметрального совершенного кода с такими

параметрами приведена в примере в конце статьи) получим не менее

$$2^{6\cdot 12^4 - 2n\log_2(4nq)} > 2^{124416-100} = 2^{124316}$$

попарно неэквивалентных кодов Ли длины 12 над алфавитом мощности 12, получаемых указанной выше конструкцией.

В частном случае, когда код C линеен, несложно построить нелинейный код C^λ, содержащий нулевое слово. Действительно, возьмем $\lambda(\mathbf{0}) = \mathbf{0}$ и $y, y' \in C$, такие что

$$\lambda(y) + \lambda(y') - \lambda(y + y') \neq e_1.$$

Рассмотрим следующую линейную комбинацию трех кодовых слов кода C^λ:

$$(-y + \lambda(y), \lambda(y)) + (-y' + \lambda(y'), \lambda(y')) - (-y - y' + \lambda(y + y'), \lambda(y + y')) = (e_1, e_1).$$

Код C^λ не является линейным, так как группа, порожденная кодом, с ним не совпадает в силу того, что содержит слово веса 2.

Более того, в этом случае ранг кода C^λ равен $\log_q |C^\lambda| + \log_q 2$. Действительно, в силу того, что (e_1, e_1) принадлежит группе, порожденной C^λ, а функция λ принимает значения либо $\mathbf{0}$, либо e_1, имеем

$$\begin{aligned}
&|\langle C^\lambda\rangle| = |\langle\{(x - y + \lambda(y), x + \lambda(y)) :\ x \in P,\ y \in C\}\rangle| = \\
&= |\langle\{(x, x) :\ x \in P\} \cup (e_1, e_1) \cup \{(-y, \mathbf{0}) :\ y \in C\}\rangle| = \\
&= |\langle\{(x, x) :\ x \in \mathbb{Z}_q^n\} \cup \{(-y, \mathbf{0}) :\ y \in C\}\rangle| = 2|P||C| = 2|C^\lambda|.
\end{aligned}$$

Таким образом, получаем следующее утверждение.

Следствие 2. *Пусть C – линейный диаметральный совершенный код с минимальным расстоянием 4 в метрике Ли, и пусть функция $\lambda\colon C \to \{\mathbf{0}, e_1\}$ такова, что $\lambda(\mathbf{0}) = \mathbf{0}$. Если для любых различных $y, y' \in C$ справедливо равенство*

$$\lambda(y) + \lambda(y') - \lambda(y + y') = 0,$$

то код C^λ является линейным. В противном случае ранг кода равен

$$\log_q |C^\lambda| + \log_q 2.$$

В отличие от рангов, мощности ядер кодов C^λ в случае линейного кода C обладают бóльшим разнообразием.

Следствие 3. *Пусть D – линейный подкод линейного диаметрального совершенного кода C в метрике Ли с минимальным расстоянием 4, $|D| < \dfrac{|C|}{2}$, и пусть функция $\lambda\colon C \to \{e_1, \mathbf{0}\}$ такова, что $\lambda(y) = \mathbf{0}$ тогда и только тогда, когда $y \in D$. Тогда мощность ядра кода C^λ равна $\dfrac{q^n|D|}{2}$, и код C^λ не является линейным.*

Доказательство. Так как код C^λ представляет собой объединение смежных классов по подгруппе $\{(x, x) :\ x \in P\}$, то его ядро содержит эту подгруппу.

Разобьем код C^λ на два подкода согласно четности веса слова во второй половине координатных позиций:

$$\begin{aligned}
C_0^\lambda &= \{(x - y, x) :\ y \in D,\ x \in P\},\\
C_1^\lambda &= \{(x - y + e_1, x + e_1) :\ y \in C \setminus D,\ x \in P\}.
\end{aligned}$$

В силу того, что D – подгруппа C, код C_1^λ представляет собой объединение смежных классов по подгруппе C_0^λ. Следовательно, ядро кода C^λ содержит хотя бы $|P||D|$ слов, принадлежащих C_0^λ.

С другой стороны, любое слово из C_1^λ не принадлежит ядру. Предположим противное. Пусть слово $(-y' + x' + e_1, x' + e_1)$ принадлежит ядру кода C и подкоду C_1^λ, т.е. $-y' \in C \setminus D$, $x \in P$. Так как четновесовой код P является группой, то

$$\begin{aligned}&(-y' + x' + e_1, x' + e_1) + C_1^\lambda = \\ &= \{(-y - y' + 2e_1 + x', 2e_1 + x') : \ x \in P, \ y' \in C \setminus D\} = \\ &= \{(-y - y' + x'', x'') : \ x'' \in P, \ y' \in C \setminus D\}.\end{aligned}$$

Таким образом, в коде $(-y' + x' + e_1, x' + e_1) + C^\lambda$ имеется $|C \setminus D||P|$ слов, подслова которых, состоящие из правой половины символов, имеют четный вес. С другой стороны, все слова из C^λ, подслова которых, состоящие из правой половины символов, имеют четный вес, образуют подкод C_0^λ. Так как $|C|/2 > |D|$, то

$$|C \setminus D||P| > |D||P| = |C_0^\lambda|,$$

и таким образом, $(-y' + x' + e_1, x' + e_1) + C^\lambda$ не совпадает с кодом C^λ, т.е. слово $(-y' + x' + e_1, x' + e_1)$ не принадлежит ядру кода C^λ. ▲

В силу этого утверждения мы видим, что для любого делителя ℓ числа $|C|$, $\ell < \dfrac{|C|}{2}$, существует нелинейный код C^λ с ядром мощности $\dfrac{\ell q^n}{2}$. Все эти коды попарно неэквивалентны, поскольку имеют различные ядра.

Пример. Рассмотрим код C длины $n = 6$ над алфавитом $q = 12$, задаваемый следующей проверочной матрицей:

$$H = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 2 & 4 & 6 & 8 & 10 \end{pmatrix}.$$

В матрице H отсутствуют одинаковые, противоположные по знаку и нулевые столбцы. Следовательно, минимальное расстояние кода не меньше 3. В силу того, что первая строка состоит из символов 3, а мощность алфавита равна $q = 12$, никакая сумма или разность трех столбцов (не обязательно различных) не равна нулевому слову в $\mathbb{Z}_{12}^2$. Таким образом, в силу утверждения 1 в пространстве решений системы сравнений с матрицей H отсутствуют слова веса Ли 1, 2 и 3. В силу того, что наибольший общий делитель первой строки проверочной матрицы равен 3, а ненулевых элементов второй строки – 2, по утверждению 2 мощность кода равна $3 \cdot 2 \cdot 12^4 = \dfrac{12^6}{4 \cdot 6}$, т.е. совпадает с мощностью диаметрального совершенного кода. Мы заключаем, что C – линейный диаметральный совершенный код с минимальным расстоянием 4.

Мощность кода равна $\dfrac{12^6}{4 \cdot 6} = 2^9 3^5$, и это число имеет $(9 + 1)(5 + 1) = 60$ различных делителей. Таким образом, имеем 58 различных значений порядков подгрупп, меньших половины порядка C. В силу следствия 3 существует не менее 58 кодов C^λ длины 12 с попарно различными мощностями ядер. Все эти коды являются попарно неэквивалентными в силу следствия 1.

СПИСОК ЛИТЕРАТУРЫ

1. *Golomb S.W., Welch L.R.* Perfect Codes in the Lee Metric and the Packing of the Polyominoes // SIAM J. App. Math. 1970. V. 18. № 2. P. 302–317. https://doi.org/10.1137/0118025
2. *AlBdaiwi B., Horak P., Milazzo L.* Enumerating and Decoding Perfect Linear Lee Codes // Des. Codes Cryptogr. 2009. V. 52. № 2. P. 155–162. https://doi.org/10.1007/s10623-009-9273-3

3. *Etzion T.* Product Constructions for Perfect Lee Codes // IEEE Trans. Inform. Theory. 2011. V. 57. № 11. P. 7473–7481. https://doi.org/10.1109/TIT.2011.2161133
4. *Соловьева Ф.И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск: Ин-т матем. СО АН СССР, 1981. С. 65–76.
5. *Соловьева Ф.И.* Разбиения на совершенные коды в метриках Хэмминга и Ли // Пробл. передачи информ. 2022. Т. 58. № 3. С. 58–69. https://www.mathnet.ru/rus/ppi2375
6. *Могильных И.Ю.* О q-ичных пропелинейных совершенных кодах на основе регулярных подгрупп общей аффинной группы // Пробл. передачи информ. 2022. Т. 58. № 1. С. 65–79. https://doi.org/10.31857/S0555292322010041
7. *Могильных И.Ю., Соловьева Ф.И.* О весовом спектре класса кодов с параметрами кодов Рида – Маллера // Пробл. передачи информ. 2022. Т. 58. № 3. С. 33–44. https://www.mathnet.ru/rus/ppi2373
8. *Mollard M.* Une novelle famille de 3-codes parfaits sur GF(q) // Discrete Math. 1984. V. 49. № 2. P. 209–212. https://doi.org/10.1016/0012-365X(84)90121-3
9. *Romanov A.M.* On Non-Full-Rank Perfect Codes over Finite Fields // Des. Codes Cryptogr. 2019. V. 87. № 5. P. 995–1003. https://doi.org/10.1007/s10623-018-0506-1
10. *Shi M., Krotov D.S.* An Enumeration of 1-Perfect Ternary Codes // Discrete Math. 2023. V. 346. № 7. Paper No. 113437 (16 pp.). https://doi.org/10.1016/j.disc.2023.113437
11. *Mogilnykh I.Yu., Solov'eva F.I.* A Concatenation Construction for Propelinear Perfect Codes from Regular Subgroups of GA($r, 2$) // Сиб. электрон. матем. изв. 2019. Т. 16. С. 1689–1702. https://doi.org/10.33048/semi.2019.16.119
12. *Зиновьев В.А., Зиновьев Д.В.* Об обобщенной каскадной конструкции кодов в модульной метрике и метрике Ли // Пробл. передачи информ. 2021. Т. 57. № 1. С. 81–95. https://doi.org/10.31857/S0555292321010046
13. *Bos A.* Codes over Groups with Arbitrary Metrics // T.H.-Report 80-WSK-06, Dept. of Mathematics, Eindhoven Univ. of Technology. Eindhoven, The Netherlands, 1980.
14. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
15. *Byrne E., Weger V.* Bounds in the Lee Metric and Optimal Codes. https://arxiv.org/abs/2112.06635 [cs.IT], 2021.
16. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10 (97 pp.).
17. *Ahlswede R., Aydinian H.K., Khachatrian L.H.* On Perfect Codes and Related Concepts // Des. Codes Cryptogr. 2001. V. 22. № 3. P. 221–237. https://doi.org/10.1023/A:1008394205999
18. *Tamo I., Schwartz M.* Correcting Limited-Magnitude Errors in the Rank-Modulation Scheme // IEEE Trans. Inform. Theory. 2010. V. 56. № 6. P. 2551–2560. https://doi.org/10.1109/TIT.2010.2046241
19. *Mogilnykh I.Yu.* q-ary Propelinear Perfect Codes from the Regular Subgroups of the $GA(r, q)$ and Their Ranks. https://arxiv.org/abs/2112.08659 [math.CO], 2021.
20. *Романов А.М.* О совершенных кодах и кодах Рида – Маллера над конечными полями // Пробл. передачи информ. 2021. Т. 57. № 3. С. 3–16. https://doi.org/10.31857/S0555292321030013

Могильных Иван Юрьевич
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
ivmog@math.nsc.ru
Соловьева Фаина Ивановна
(15.08.1952 – 09.08.2022)

Поступила в редакцию
07.06.2023
После доработки
20.10.2023
Принята к публикации
23.10.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 519.72

© 2023 г. **И.В. Воробьев**

ПОКРЫВАЮЩИЕ КОДЫ ДЛЯ МЕТРИКИ ЛЕВЕНШТЕЙНА ФИКСИРОВАННОЙ ДЛИНЫ[1]

Покрывающим кодом или покрытием называется множество кодовых слов, такое что объединение шаров с центрами в этих кодовых словах покрывает все пространство. Как правило, задача состоит в минимизации мощности покрывающего кода. Для классической метрики Хэмминга размер минимального покрывающего кода фиксированного радиуса R известен с точностью до постоянного множителя. Аналогичный результат был недавно получен для кодов с R вставками и кодов с R удалениями. В данной статье изучаются покрытия пространства для метрики Левенштейна фиксированной длины, т.е. для R вставок и R удалений. Для $R = 1$ и 2 доказываются новые нижние и верхние оценки минимальной мощности покрывающего кода, которые отличаются лишь в константу раз.

Ключевые слова: покрывающие коды, граница сферической упаковки, метрика Левенштейна, вероятностный метод.

DOI: 10.31857/S055529232302002X, **EDN:** PPPXTQ

§ 1. Введение

Покрывающие коды являются важным объектом в теории кодирования и дискретной математике. Они нашли применения в таких областях, как сжатие данных [1], схемная сложность [2], поиск ближайшего соседа [3], в различных задачах на решетках [4] и даже в футбольных тотализаторах [5]. Подробное описание этих приложений и многих других можно найти в книге [1].

Большинство работ о покрывающих кодах посвящено метрике Хэмминга, т.е. заменам. В последнее время резко возрос интерес к биологическим приложениям теории кодирования, в частности к хранению данных с помощью молекул ДНК (см. [6–8]). Известно, что в ДНК-хранилищах наряду с заменами распространены также вставки и удаления, что является мотивацией для изучения кодов, исправляющих такие ошибки.

Основным отличием задачи построения покрывающих кодов для случая вставок и удалений от кодов для замен является отсутствие симметрии. В метрике Хэмминга объем шара радиуса R не зависит от центра. Это же верно и для случая вставок. Однако при появлении удалений это свойство нарушается, и объем шара получается разным для разных центров, что усложняет задачу.

В табл. 1 мы приводим известные результаты о минимальной мощности покрывающего кода для случаев R замен, R удалений и R вставок. Величины $V_H^q(n, R)$

[1] Исследование выполнено за счет гранта Российского научного фонда № 22-41-02028.

Таблица 1

Границы на минимальную мощность покрывающих кодов

Тип покрывающего кода	Нижняя граница	Верхняя граница	Ссылка
Одна замена, q – степень простого числа	$\dfrac{q^n}{(q-1)n+1}$	$\dfrac{q^n(1+o(1))}{(q-1)n+1}$	[9]
R замен	$\dfrac{q^n}{V_H^q(n,R)}$	$\dfrac{cR\log Rq^n(1+o(1))}{V_H^q(n,R)}$	[10]
R удалений	$\dfrac{q^nR!\,(1+o(1))}{n^R(q-1)^R}$	$\dfrac{cR\log Rq^nR!\,(1+o(1))}{n^R(q-1)^R}$	[11]
R вставок	$\dfrac{q^{n+R}}{V_I^q(n,R)}$	$\dfrac{cR\log Rq^{n+R}(1+o(1))}{V_I^q(n,R)}$	[11]

и $V_I^q(n,R)$ обозначают объемы шаров радиуса R для замен и вставок соответственно, т.е.

$$V_H^q(n,R)=\sum_{i=0}^{R}\binom{n}{i}(q-1)^i,$$

$$V_I^q(n,R)=\sum_{i=0}^{R}\binom{n+R}{i}(q-1)^i.$$

Отметим, что для каждого из этих трех случаев верхняя и нижняя границы отличаются в $O(R\log R)$ раз. Зависимость же мощности кода от длины одинакова в верхней и нижней границах. Для случая одной замены и размера алфавита q, равного степени простого числа, верхняя и нижняя границы асимптотически эквивалентны.

В данной статье мы рассматриваем случай, в котором возможны одновременно и вставки, и удаления. Мы концентрируемся на случае, когда количество вставок и удалений одинаково и равно R. Основным результатом статьи является получение нижних и верхних оценок минимального размера покрывающего кода, которые имеют одинаковую (а значит, оптимальную) зависимость от длины кода n для $R=1,2$.

Оставшаяся часть статьи имеет следующую структуру. В § 2 введены основные обозначения и определения, а § 3 посвящен доказательству нижней границы для радиуса 1. Затем в § 4 получена верхняя граница минимального размера покрывающего кода. Случай радиуса $R>1$ рассматривается в § 5. В § 6 даны заключительные замечания.

§ 2. Определения и обозначения

Алфавит $\{0,1,\ldots,q-1\}$ из q символов будем обозначать через Σ_q. Множество последовательностей длины n с символами из алфавита Σ_q обозначим через Σ_q^n. Кодом $\mathcal{C}$ будем называть произвольное подмножество в Σ_q^n. Знак $\triangleq$ будет означать равенство по определению.

Определение 1. *Расстоянием в метрике Левенштейна фиксированной длины* (fixed length Levenstein metric) между двумя последовательностями $\boldsymbol{x}$ и $\boldsymbol{y}$ одинаковой длины назовем минимальное число R, такое что из $\boldsymbol{x}$ можно получить $\boldsymbol{y}$ с помощью R удалений и R вставок. Будем обозначать такое расстояние через $d_{\mathrm{FLL}}(\boldsymbol{x},\boldsymbol{y})$.

Определение 2. *Шаром* $B(\boldsymbol{x},R)$ с центром в $\boldsymbol{x}$ и радиусом R в метрике Левенштейна фиксированной длины будем называть множество всех последовательно-

стей, которые находятся на расстоянии не более R от $\boldsymbol{x}$, т.е.

$$B(\boldsymbol{x}, R) \triangleq \{\boldsymbol{y} \in \Sigma_q^n \mid d_{\mathrm{FLL}}(\boldsymbol{x}, \boldsymbol{y}) \leqslant R\}.$$

В случае $R = 1$ будем обозначать шар через $B(\boldsymbol{x})$.

Определение 3. Будем говорить, что код $\mathcal{C}$ является *покрывающим кодом* (или просто *покрытием*) радиуса R в метрике Левенштейна фиксированной длины, если объединение шаров радиуса R с центрами в кодовых словах покрывает все пространство, т.е. иными словами, если $\bigcup\limits_{\boldsymbol{x} \in \mathcal{C}} B(\boldsymbol{x}, R) = \Sigma_q^n$.

В дальнейшем будем называть такой код покрывающим кодом радиуса R, а слова о метрике Левенштейна фиксированной длины будем опускать. Следующие понятия являются важными характеристиками, влияющими на размер шара.

Определение 4. *Серией* (run) в строке $\boldsymbol{x}$ будем называть максимальный по включению непрерывный подотрезок строки $\boldsymbol{x}$, состоящий из одинаковых символов. Количество серий в строке $\boldsymbol{x}$ будем обозначать через $r(\boldsymbol{x})$. Например, $r(01101) = 4$, $r(000000) = 1$.

Определение 5. *Отрезком чередования* (alternating segment) в строке $\boldsymbol{x}$ называется максимальный по включению непрерывный подотрезок строки $\boldsymbol{x}$, состоящий из двух чередующихся символов алфавита, т.е. на четных позициях стоит один символ, а на нечетных другой. Например, в строке 021211 есть три отрезка чередования: 02, 2121 и 1.

§ 3. Нижняя граница мощности покрытия радиуса 1

Начнем с доказательства простейшей нижней границы мощности покрывающего кода.

Предложение 1. *Мощность покрывающего кода $\mathcal{C}$ радиуса 1 не меньше чем*

$$\frac{q^n(1 + o(1))}{(q-1)n^2}.$$

Доказательство. Если у нас есть слово длины n, то количество удалений не больше n, количество последующих вставок не больше $n(q-1)+1$. Таким образом, количество покрываемых слов, считая исходное, не больше $n^2(q-1)(1+o(1))$. Поэтому необходимо не менее $\dfrac{q^n(1+o(1))}{(q-1)n^2}$ кодовых слов. ▲

Эту границу можно улучшить, воспользовавшись методом сферической упаковки для несимметричных шаров, предложенным в [12, 13].

Лемма 1 [13]. *Для любого слова $\boldsymbol{x}$ определим $S(\boldsymbol{x})$ как множество слов, которые покрываются шаром с центром в $\boldsymbol{x}$. Пусть задана весовая функция $w\colon \Sigma_q^n \to \mathbb{R}$, причем для всех $\boldsymbol{x}$ выполняются неравенства*

$$\sum_{\boldsymbol{y} \in S(\boldsymbol{x})} w(\boldsymbol{y}) \leqslant 1. \tag{1}$$

Тогда размер любого покрытия C удовлетворяет неравенству

$$|C| \geqslant \sum_{\boldsymbol{x} \in \Sigma_q^n} w(x).$$

Докажем следующую оценку.

Теорема 1. *Мощность покрывающего кода $\mathcal{C}$ радиуса 1 не меньше чем*

$$\frac{q^{n+1}(1+o(1))}{(q-1)^2 n^2}.$$

Отметим, что эта оценка асимптотически в $\frac{q}{q-1}$ раз превосходит оценку из предложения 1.

Доказательство. Воспользуемся леммой 1 для доказательства оценки. В качестве множеств $S(\boldsymbol{x})$ возьмем шары $B(\boldsymbol{x})$. Определим весовую функцию

$$w(\boldsymbol{x}) = \frac{1}{\max\limits_{\boldsymbol{y}\in B(\boldsymbol{x})} |B(\boldsymbol{y})|},$$

тогда условие (1) выполняется, так как суммируется $|B(\boldsymbol{x})|$ слагаемых, каждое из которых не больше $|B(\boldsymbol{x})|^{-1}$.

Для объема шара радиуса 1 известна следующая формула [14]:

$$|B(\boldsymbol{x})| = r(\boldsymbol{x})(n(q-1)-1) + 2 - \sum_{i=1}^{a(\boldsymbol{x})} \frac{(s_i-1)(s_i-2)}{2}, \tag{2}$$

где $a(\boldsymbol{x})$ – количество отрезков чередования в $\boldsymbol{x}$, а s_i – длины этих отрезков. Воспользуемся следующей верхней оценкой объема шара:

$$|B(\boldsymbol{x})| \leqslant r(\boldsymbol{x})(q-1) + 1.$$

Несложно видеть, что количество серий при одном удалении и одной вставке может измениться не более чем на 2. Таким образом,

$$w(\boldsymbol{x}) \geqslant \frac{1}{(r(\boldsymbol{x})+2)n(q-1)+1}.$$

Нам осталось оценить снизу сумму весов всех слов. Число слов с k сериями равно

$$q(q-1)^{k-1}\binom{n-1}{k-1},$$

так как есть q способов выбрать первый символ, а потом надо выбрать позиции начал всех серий, кроме первого, а также символы для этих серий. Поэтому из леммы 1 вытекает следующее неравенство:

$$|C| \geqslant \sum_{k=1}^{n} \frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{(k+2)n(q-1)+1}.$$

Нам понадобится следующее утверждение.

Предложение 2. *Число серий в случайной строке из Σ_q^n лежит в интервале*

$$I = \left(\frac{(q-1)n}{q} - \sqrt{n}\ln n, \frac{(q-1)n}{q} + \sqrt{n}\ln n\right)$$

с вероятностью $1 - n^{-\ln n(1+o(1))}$.

Доказательство. Заметим, что число серий случайного слова дается выражением $r(\boldsymbol{x}) = 1 + \xi$, где ξ – биномиальная случайная величина $\mathrm{Bin}\left(n-1, \frac{q-1}{q}\right)$.

Таким образом, вероятность того, что количество серий не попадает в интервал I, можно оценить по неравенству Хёфдинга [15]:

$$\mathbf{P}\left(\left|r(\boldsymbol{x})-\frac{(q-1)n}{q}\right|\geqslant\sqrt{n}\ln n\right)\leqslant 2\exp\left\{\frac{-2n\ln^2 n}{n}(1+o(1))\right\}<$$
$$<n^{-\ln n(1+o(1))}. \quad \blacktriangle$$

Теперь оценим мощность кода C:

$$|C|\geqslant\sum_{k=1}^{n}\frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{(k+2)n(q-1)+1}\geqslant\sum_{k\in I}\frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{(k+2)n(q-1)+1}.$$

Заметим, что при $k\in I$ знаменатель равен $\dfrac{(q-1)^2n^2}{q}(1+o(1))$. Сумма же выражений в числителе по $k\in I$ равна вероятности того, что количество серий в случайной строке принадлежит отрезку I, умноженной на q^n. Воспользовавшись только что доказанным предложением 2, получаем следующее:

$$|C|\geqslant\sum_{k\in I}\frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{(k+2)n(q-1)+1}=\frac{q^n(1-n^{-\ln n(1+o(1))})}{(q-1)^2n^2q^{-1}(1+o(1))}\geqslant$$
$$\geqslant\frac{q^{n+1}}{(q-1)^2n^2}(1+o(1)),$$

что завершает доказательство теоремы. $\blacktriangle$

§ 4. Верхняя оценка минимальной мощности покрытия радиуса 1

В этом параграфе мы докажем верхнюю оценку минимальной мощности покрытия, т.е. докажем существование покрытия определенной мощности.

Нам понадобятся некоторые факты о размерах шаров. В работах [16,17] доказано, что размер случайного шара радиуса 1 и 2 в метрике Левенштейна фиксированной длины достаточно близок к своему математическому ожиданию с вероятностью, стремящейся к 1. Нам нужна чуть более сильная оценка, которая, тем не менее, доказывается похожим образом.

Введем дополнительное определение.

Определение 6. Назовем слово $\boldsymbol{x}\in\Sigma_q^n$ *плохим*, если выполнено хотя бы одно из следующих условий:

1. Число серий не принадлежит интервалу

$$I=\left(\frac{q-1}{q}n-\sqrt{n}\ln n,\frac{q-1}{q}n+\sqrt{n}\ln n\right).$$

2. Максимальный отрезок чередования имеет длину не менее $4\log n$.

Множество плохих слов будем обозначать через $\mathcal{B}$. Все остальные слова назовем *хорошими* и будем обозначать через $\mathcal{G}$.

Лемма 2. *Справедливы следующие утверждения*:

1. *Количество плохих слов не превосходит* $o\left(\dfrac{q^n}{n^2}\right)$;
2. *Количество хороших слов не менее* $q^n(1-o(n^{-2}))$;

3. *Размер шара $B(\boldsymbol{x})$ для $\boldsymbol{x} \in \mathcal{G}$ имеет порядок*

$$|B(\boldsymbol{x})| \sim \frac{n^2(q-1)^2}{q}.$$

Доказательство. Докажем утверждение 1. Как было показано выше в предложении 2, количество серий $r(\boldsymbol{x})$ не принадлежит интервалу $I = \left(\frac{q-1}{q}n - \sqrt{n}\ln n, \frac{q-1}{q}n + \sqrt{n}\ln n\right)$ с вероятностью $\leqslant n^{-\ln n(1+o(1))}$.

Теперь оценим вероятность появления отрезка чередования длины $k = 4\log n$. Вероятность конкретного отрезка чередования в конкретном месте равна q^{-k}. Оценим вероятность существования отрезка чередования длины k как сумму вероятностей по всем позициям и по всем парам символов алфавита:

$$\mathbf{P}(\text{существование отрезка чередования длины } k) \leqslant q^2 q^{-k} n = o(n^{-2}).$$

Утверждение 2 тривиально следует из предыдущего.

Утверждение 3 следует из определения хороших слов и формулы (2) для размера шара. ▲

Теперь докажем случайную верхнюю границу.

Теорема 2. *Существует покрытие $\mathcal{C}$ радиуса 1 и мощности не более*

$$\frac{2q^{n+1}\ln n}{(q-1)^2 n^2}.$$

Доказательство. Опишем покрывающий код $\mathcal{C}$. Все плохие слова сразу добавим в код $\mathcal{C}$. Хорошие слова будем включать в код случайным образом, а именно каждое хорошее слово будем включать в код независимо с вероятностью p. Для каждого хорошего слова $\boldsymbol{x}$ определим вероятность p_0 того, что оно не покрыто. Тогда

$$p_0 \leqslant (1-p)^{|B(\boldsymbol{x})|} = (1-p)^{\frac{n^2(q-1)^2}{q}(1+o(1))}.$$

В конце добавим все непокрытые слова в код.

Математическое ожидание размера кода оценивается следующим образом:

$$\mathbf{E}\,|\mathcal{C}| \leqslant q^n(p + p_0) + o(q^n/n^2).$$

Если взять $p = \dfrac{2q\ln n}{(q-1)^2 n^2}$, то получим

$$p_0 \leqslant e^{-2\ln n(1+o(1))} = n^{-2+o(1)},$$

а математическое ожидание размера кода не превосходит

$$\frac{2q^{n+1}\ln n}{(q-1)^2 n^2}(1 + o(1)).$$

Очевидно, что существует код, размер которого не превосходит математического ожидания. ▲

Отметим, что случайная верхняя граница отличается от доказанной ранее нижней в $O(\ln n)$ раз. Эту границу можно улучшить, строя покрытия из покрытий в пространствах меньшей размерности, а также кодов, покрывающих не все пространство, но его существенную часть. Наше рассуждение во многом повторяет работу [11], где похожая лемма использовалась для построения покрывающих кодов для случая одной вставки. Также аналогичная стратегия использовалась в работе [18].

Лемма 3. *Пусть*

$$S, T \subset \Sigma_q^{n_1}, \quad T = \Sigma_q^{n_1} \setminus \bigcup_{\boldsymbol{x} \in S} B(\boldsymbol{x}).$$

Пусть код C_{n_2} длины n_2 является покрывающим кодом радиуса 1 в метрике Левенштейна фиксированной длины. Тогда код

$$(S \otimes \Sigma_q^{n_2}) \cup (T \otimes C_{n_2})$$

является покрывающим кодом радиуса 1, длины $n_1 + n_2$ и размера $|S|q^{n_2} + |T||C_{n_2}|$, где

$$A \otimes B = \{\boldsymbol{ab} \mid \boldsymbol{a} \in A,\ \boldsymbol{b} \in B\},$$

а $\boldsymbol{ab}$ – конкатенация слов $\boldsymbol{a}$ и $\boldsymbol{b}$.

Доказательство. Рассмотрим произвольное слово длины $n = n_1 + n_2$. Разобьем его на две части $\boldsymbol{xy}$, где длина $\boldsymbol{x}$ равна n_1, а длина $\boldsymbol{y}$ равна n_2. Если $\boldsymbol{x}$ покрывается множеством S, то и все слово покрыто множеством $S \otimes \Sigma_q^{n_2}$. В противном случае $\boldsymbol{x} \in T$. Так как код C_{n_2} покрывает все слова $\boldsymbol{y}$ длины n_2, то в этом случае $\boldsymbol{xy}$ покрывается множеством $T \otimes C_{n_2}$.

Определим функцию $\mu(n, q)$ следующим образом. Пусть $\mu(1, q) = 1$. Для $n > 1$ определим $\mu(n, q)$ как минимальное число, такое что существуют натуральные числа n_1 и n_2, $n = n_1 + n_2$, а также множества $S, T \subset \Sigma_q^{n_1}$, где S покрывает $\Sigma_q^{n_1} \setminus T$, удовлетворяющие неравенству

$$|S| + \frac{\mu(n_2, q)|T|}{n_2^2} \leqslant \frac{\mu(n, q) q^{n_1}}{n^2}. \tag{3}$$

Следующая лемма позволит нам доказать верхнюю границу мощности минимального покрытия с помощью индукции.

Лемма 4. *Справедливы следующие утверждения*:

1. *Для любого $n > 1$ существуют натуральные числа n_1 и n_2, $n = n_1 + n_2$, а также множества $S, T \subset \Sigma_q^{n_1}$, где S покрывает $\Sigma_q^{n_1} \setminus T$, удовлетворяющие неравенству* (3);
2. *Для любого q для верхнего предела $\bar{\mu}(q) \triangleq \limsup\limits_{n \to \infty} \mu(n, q)$ справедливо неравенство $\bar{\mu}(q) \leqslant \mu(q)$, где $\mu(q)$ определяется как минимальное положительное значение*

$$\mu(q) = \frac{c(1-\alpha)^2}{\alpha^2\left((1-\alpha)^2 - e^{-\frac{c(q-1)^2}{q}}\right)} \tag{4}$$

   по всем $c > 0$ и $\alpha \in (0, 1)$;
3. *При $q \to \infty$ выполняется $\mu(q) = O(q^{-1})$. Точнее, подставляя $c = \dfrac{5{,}282}{q}$ и $\alpha = 0{,}851$, получаем $\mu(q) \leqslant \dfrac{9{,}459}{q}(1 + o(1))$.*

Доказательство. Утверждение 1 леммы следует из определения функции $\mu(n, q)$.

Для доказательства утверждения 2 покажем, как можно строить множества S и T. На длине n_1 построим множество $S_0 \subset \mathcal{G} \subset \Sigma_q^{n_1}$ случайным образом, включая в него каждое хорошее слово с вероятностью p. Определим S как объединение множества S_0 с плохими словами $S = S_0 \cup \mathcal{B}$.

Пользуясь леммой 2, оценим математическое ожидание величины

$$W = |S| + \frac{\mu(n_2, q)|T|}{n_2^2},$$

равной выражению в левой части (3), при $n \to \infty$ следующим образом:

$$\mathbf{E}\, W \leqslant o\left(\frac{q^{n_1}}{n_1^2}\right) + q^{n_1}p + \frac{\mu(n_2, q)q^{n_1}(1-p)^{\frac{n_1^2(q-1)^2}{q}(1+o(1))}}{n_2^2}.$$

Пусть $p = \dfrac{c}{n_1^2}$, $n_1 = \alpha n$, $n_2 = (1-\alpha)n$. Формально следовало бы написать $\lfloor \alpha n \rfloor$, но мы будем игнорировать знаки целой части, так как мы все равно делаем оценку с точностью до умножения на $1 + o(1)$. Тогда неравенство можно переписать следующим образом:

$$\mathbf{E}\, W \leqslant \frac{cq^{n_1}}{\alpha^2 n^2}(1 + o(1)) + \frac{q^{n_1}\mu(n_2, q)e^{-\frac{c(q-1)^2}{q}(1+o(1))}}{(1-\alpha)^2 n^2} =$$

$$= \frac{q^{n_1}}{n^2}\left(\frac{c}{\alpha^2} + \frac{\mu(n_2, q)e^{-\frac{c(q-1)^2}{q}}}{(1-\alpha)^2}\right)(1 + o(1)),$$

откуда следует, что выполняется неравенство

$$\mu(n, q) \leqslant \left(\frac{c}{\alpha^2} + \frac{\mu(n_2, q)e^{-\frac{c(q-1)^2}{q}}}{(1-\alpha)^2}\right)(1 + o(1)). \tag{5}$$

Зафиксируем $\alpha \in (0, 1)$ и $c > 0$ и возьмем верхний предел левой и правой части при $n \to \infty$. Получим

$$\bar{\mu}(q) \leqslant \frac{c}{\alpha^2} + \frac{\bar{\mu}(q)e^{-\frac{c(q-1)^2}{q}}}{(1-\alpha)^2}.$$

Пусть c и α выбраны так, что выполняется неравенство

$$\frac{e^{-\frac{c(q-1)^2}{q}}}{(1-\alpha)^2} < 1.$$

Тогда $\bar{\mu}(q) < +\infty$, так как из неравенства (5) следует, что если для некоторого достаточно большого M выполняется $\mu(n_2, q) > M$, то $\mu(n, q) < \mu(n_2, q)$. Элементарные преобразования приводят к формуле (4). Выполнение неравенства $\dfrac{e^{-\frac{c(q-1)^2}{q}}}{(1-\alpha)^2} < 1$ эквивалентно тому условию, что $\mu(q)$ должно быть положительно. Утверждение 2 доказано.

Для доказательства утверждения 3 убедимся, что если положить $c = \dfrac{A}{q}$, то

$$\mu(q) \leqslant \frac{A(1-\alpha)^2}{q\alpha^2((1-\alpha)^2 - e^{-A})}(1 + o(1)),$$

откуда следует $\mu(q) = O(q^{-1})$. Значения параметров A и α найдены с помощью компьютерного перебора. ▲

Для $q = 2$ константа $\mu(2) \approx 18{,}53$ при $c \approx 11{,}42$ и $\alpha \approx 0{,}85$. Для $q = 3$ константа $\mu(3) \approx 6{,}95$ при $c \approx 4{,}28$ и $\alpha \approx 0{,}85$.

Теперь мы готовы к доказательству верхней границы.

Теорема 3. *Существует покрытие $\mathcal{C}$ радиуса 1 мощности*

$$M \leqslant \frac{\mu(n,q)q^n}{n^2}.$$

Доказательство. Будем доказывать теорему по индукции. Для $n = 1$ функция $\mu(1,q) = 1$, и утверждение теоремы очевидно выполнено.

Допустим, что теорема доказана для всех длин не выше $n-1$. Применяя лемму 4, получаем, что существуют множества $S, T \subset \Sigma_q^{n_1}$, где S покрывает $\Sigma_q^{n_1} \setminus T$, удовлетворяющие неравенству (3). Применяя к этим множествам лемму 3, получаем, что существует покрывающий код длины n и мощности $M \leqslant \frac{\mu(n,q)q^n}{n^2}$, что и требовалось. ▲

Сравнивая полученные в нашей статье нижнюю и верхнюю границу, получаем, что при $n \to \infty$ они отличаются в $\frac{\mu(q)(q-1)^2}{q}$ раз. Как следует из последнего утверждения леммы 4, при $q \to \infty$ это отношение стремится к константе, не большей 9,459.

§ 5. Случай радиуса, большего 1

В данном параграфе обсуждается обобщение полученных результатов на случай радиуса $R > 1$.

5.1. Нижняя граница. Снова начнем с наивной нижней границы мощности покрытия.

Предложение 3. *Мощность покрывающего кода $\mathcal{C}$ радиуса R не меньше чем*

$$\frac{q^n(R!)^2(1+o(1))}{(q-1)^R n^{2R}}.$$

Доказательство. Если у нас есть слово длины n, то количество удалений не больше $\binom{n}{R}$, а количество последующих вставок не больше

$$\sum_{i=0}^{R}\binom{n}{i}(q-1)^i = \binom{n}{R}(q-1)^R(1+o(1)).$$

Таким образом, количество покрываемых слов не больше

$$\binom{n}{R}^2(q-1)^R(1+o(1)).$$

Поэтому необходимо не менее чем $\frac{q^n(R!)^2(1+o(1))}{(q-1)^R n^{2R}}$ кодовых слов.

Докажем более сильную оценку.

Теорема 4. *Мощность покрывающего кода $\mathcal{C}$ радиуса R не меньше чем*

$$\frac{q^{n+R}(R!)^2}{(q-1)^{2R}n^{2R}}(1+o(1)).$$

Отметим, что эта оценка асимптотически в $\left(\frac{q}{q-1}\right)^R$ раз превосходит наивную.

Доказательство. Снова воспользуемся леммой 1 для доказательства оценки, только теперь $S(\boldsymbol{x}) = B(\boldsymbol{x}, R)$. Аналогично случаю $R = 1$ определим весовую функцию

$$w(\boldsymbol{x}) = \frac{1}{\max\limits_{\boldsymbol{y}\in B(\boldsymbol{x},R)} |B(\boldsymbol{y}, R)|},$$

что гарантирует выполнение условия (1).

Для объема шара радиуса $R > 1$ точной формулы не известно, но мы можем использовать следующую верхнюю оценку:

$$|B(\boldsymbol{x}, R)| \leqslant \binom{r(\boldsymbol{x}) + R - 1}{R} \sum_{i=0}^{R} \binom{n}{i} (q-1)^i,$$

где первый множитель – это максимальное количество слов, которое может получиться из $\boldsymbol{x}$ после R удалений [19], а второй – количество различных слов, которые могут получиться из одного слова длины $n - R$ с помощью R вставок [20].

Отметим, что количество серий при R удалениях и R вставках может измениться не более чем на $2R$. Таким образом,

$$w(\boldsymbol{x}) \geqslant \frac{1}{\binom{r(\boldsymbol{x}) + 3R - 1}{R} \sum\limits_{i=0}^{R} \binom{n}{i} (q-1)^i}.$$

Вспоминая, что число слов с k сериями равно $q(q-1)^{k-1}\binom{n-1}{k-1}$, из леммы 1 получаем оценку

$$|C| \geqslant \sum_{k=1}^{n} \frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{\binom{k+3R-1}{R} \sum\limits_{i=0}^{R} \binom{n}{i} (q-1)^i} \geqslant \sum_{k\in I} \frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{\binom{k+3R-1}{R} \sum\limits_{i=0}^{R} \binom{n}{i} (q-1)^i}.$$

Заметим, что для $k \in I$

$$\binom{k+3R-1}{R} \sum_{i=0}^{R} \binom{n}{i} (q-1)^i = \frac{n^R (q-1)^R}{R! q^R} \frac{n^R (q-1)^R}{R!} (1 + o(1)). \tag{6}$$

В то же время из предложения 2 следует, что

$$\sum_{k\in I} q(q-1)^{k-1}\binom{n-1}{k-1} = q^n \big(1 - n^{-\ln n(1+o(1))}\big). \tag{7}$$

Используя формулы (6), (7), получаем

$$|C| \geqslant \sum_{k\in I} \frac{q(q-1)^{k-1}\binom{n-1}{k-1}}{\binom{k+3R-1}{R} \sum\limits_{i=0}^{R} \binom{n}{i} (q-1)^i} =$$

$$= \frac{(R!)^2 q^R (1 + o(1))}{n^{2R}(q-1)^{2R}} \sum_{k\in I} q(q-1)^{k-1}\binom{n-1}{k-1} = \frac{q^{n+R}(R!)^2}{(q-1)^{2R} n^{2R}} (1 + o(1)),$$

что завершает доказательство теоремы. ▲

5.2. Верхняя граница. Для доказательства верхней границы мощности минимального покрытия нам необходима нижняя граница мощности шара. В работе [17] была сформулирована следующая гипотеза об объеме шара в метрике Левенштейна фиксированной длины.

Гипотеза 1. *Для размера шара $B(\boldsymbol{x}, R)$ со случайно выбранным согласно равномерному распределению центром выполняется следующее*:

$$\mathbf{E}\,|B(\boldsymbol{x}, R)| = \frac{(q-1)^{2R}}{(R!)^2 q^R} n^{2R} + o(n^{2R}),$$
$$\mathbf{P}\left(\left||B(\boldsymbol{x}, R)| - \frac{(q-1)^{2R}}{(R!)^2 q^R} n^{2R}\right| = o(n^{2R})\right) = 1 - o(1).$$

На текущий момент гипотеза доказана только для $R = 1$, 2 (см. [16, 17]). Но для нашего метода доказательства нам нужно более точное утверждение о концентрации мощностей шаров, а именно следующее.

Гипотеза 2. *Для размера шара $B(\boldsymbol{x}, R)$ со случайно выбранным согласно равномерному распределению центром выполняется следующее*:

$$\mathbf{P}\left(\left||B(\boldsymbol{x}, R)| - \frac{(q-1)^{2R}}{(R!)^2 q^R} n^{2R}\right| > n^{2R-0,5} \ln n\right) = o(n^{-2R}).$$

Для случая $R = 1$ доказательство гипотезы 2 фактически приведено в § 4. Доказательство гипотезы 1 для случая $R = 2$, приведенное в работе [17], работает и для гипотезы 2 с минимальными изменениями. Для $R > 2$ задача доказательства гипотезы 2 остается открытой.

Мы же докажем, что из выполнения гипотезы 2 следует верхняя оценка мощности покрытия.

Теорема 5. *В случае выполнения гипотезы* 2 *существует покрытие $\mathcal{C}$ радиуса R и мощности $M \leqslant \dfrac{\lambda q^n}{n^{2R}}$ для некоторой константы λ.*

Доказательство. Доказательство проведем по индукции по длине кода n. Для любого фиксированного n_0 мы можем добиться выполнения утверждения теоремы выбором достаточно большой константы λ. Допустим, что теорема доказана для всех длин не выше $n-1$, $n > n_0$, и докажем ее для длины n. Нам понадобится следующее утверждение, аналогичное лемме 3.

Лемма 5. *Пусть*

$$S, T \subset \Sigma_q^{n_1}, \quad T = \Sigma_q^{n_1} \setminus \bigcup_{\boldsymbol{x} \in S} B(\boldsymbol{x}, R).$$

Пусть код C_{n_2} длины n_2 является покрывающим кодом радиуса R в метрике Левенштейна фиксированной длины. Тогда код

$$(S \otimes \Sigma_q^{n_2}) \cup (T \otimes C_{n_2})$$

является покрывающим кодом радиуса R, длины $n_1 + n_2$ и размера $|S|q^{n_2} + |T||C_{n_2}|$, где

$$A \otimes B = \{\boldsymbol{ab} \mid \boldsymbol{a} \in A,\ \boldsymbol{b} \in B\},$$

а $\boldsymbol{ab}$ – конкатенация слов $\boldsymbol{a}$ и $\boldsymbol{b}$.

Доказательство леммы полностью аналогично доказательству леммы 3.

Теперь построим множества S и T. Сначала добавим в множество S все слова $\boldsymbol{x}$, для которых выполнено неравенство

$$\left||B(\boldsymbol{x},R)| - \frac{(q-1)^{2R}}{(R!)^2 q^R} n_1^{2R}\right| > n_1^{2R-0,5}\ln n_1.$$

Остальные слова будем включать в множество независимо с вероятностью p.

Оценим математическое ожидание величины $W = |S| + \frac{\lambda|T|}{n_2^{2R}}$. Оценка математического ожидания

$$\mathbf{E}\,|S| < o\left(\frac{q^{n_1}}{n_1^{2R}}\right) + q^{n_1}p$$

следует из гипотезы 2. Для оценки математического ожидания мощности множества T отметим, что для попадания слова $\boldsymbol{x} \notin S$ в это множество все слова из шара $B(\boldsymbol{x},R)$ должны быть не включены в множество S, т.е.

$$\mathbf{E}\,|T| \leqslant q^{n_1}(1-p)^{|B(\boldsymbol{x},R)|} \leqslant q^{n_1}(1-p)^{\frac{(q-1)^{2R}}{(R!)^2 q^R} n_1^{2R}(1+o(1))},$$

где последнее неравенство следует из того, что $\boldsymbol{x}$ не лежит в множестве S, а значит, для него выполнено

$$\left||B(\boldsymbol{x},R)| - \frac{(q-1)^{2R}}{(R!)^2 q^R} n_1^{2R}\right| \leqslant n_1^{2R-0,5}\ln n_1.$$

Итак, математическое ожидание $\mathbf{E}\,W$ оценивается следующим образом:

$$\mathbf{E}\,W \leqslant o\Big(\frac{q^{n_1}}{n_1^{2R}}\Big) + q^{n_1}p + \frac{q^{n_1}\lambda(1-p)^{\frac{(q-1)^{2R}}{(R!)^2 q^R} n_1^{2R}(1+o(1))}}{n_2^{2R}}.$$

Пусть $p = \frac{c}{n_1^{2R}}$, $n_1 = \alpha n$, $n_2 = (1-\alpha)n$. Тогда неравенство можно переписать в виде

$$\mathbf{E}\,W \leqslant \frac{cq^{n_1}}{\alpha^{2R}n^{2R}}(1+o(1)) + \frac{q^{n_1}\lambda e^{-\frac{c(q-1)^{2R}}{(R!)^2 q^R}(1+o(1))}}{(1-\alpha)^{2R}n^{2R}} =$$
$$= \frac{q^{n_1}}{n^{2R}}\left(\frac{c}{\alpha^{2R}} + \frac{\lambda e^{-\frac{c(q-1)^{2R}}{(R!)^2 q^R}}}{(1-\alpha)^{2R}}\right)(1+o(1)).$$

Подберем α, c и λ так, чтобы выполнялось неравенство

$$\frac{c}{\alpha^{2R}} + \frac{\lambda e^{-\frac{c(q-1)^{2R}}{(R!)^2 q^R}}}{(1-\alpha)^{2R}} < \lambda.$$

Тогда при достаточно большом $n > n_0$ будет выполнено

$$\mathbf{E}\,W \leqslant \frac{\lambda q^{n_1}}{n^{2R}}.$$

Возьмем множества S и T, для которых выполнено неравенство $W \leqslant \frac{\lambda q^{n_1}}{n^{2R}}$. Применяя лемму 5 к ним, а также к минимальному покрытию C_{n_2}, верхняя оценка на мощность которого известна из предположения индукции, получаем новое покрытие

радиуса R, мощность которого не превосходит

$$|S|q^{n_2} + |T||C_{n_2}| \leqslant \frac{\lambda q^n}{n^{2R}},$$

что завершает доказательство теоремы. ▲

Таким образом, для $R = 2$ верна верхняя оценка мощности минимального покрытия $\frac{\lambda q^n}{n^{2R}}$, которая отличается от нижней лишь в константу раз.

§ 6. Заключение

В статье доказаны новые нижние и верхние оценки минимальной мощности покрывающего кода для метрики Левенштейна фиксированной длины при $R = 1$ и 2. Как и в случае покрывающих кодов для замен, вставок и удалений, нижние и верхние оценки отличаются лишь в константу раз. Доказательство аналогичных результатов для $R > 2$ сведено к гипотезе 2 о распределении размера шара в метрике Левенштейна фиксированной длины со случайно выбранным центром. Естественным следующим шагом исследования является доказательство гипотезы 2, которая интересна не только своей связью с покрывающими кодами, но и как самостоятельный факт.

СПИСОК ЛИТЕРАТУРЫ

1. *Cohen G., Honkala I., Listyn S., Lobstein A.* Covering Codes. Amsterdam: Elsevier, 1997.
2. *Smolensky R.* On Representations by Low-Degree Polynomials // Proc. 34th Annu. Symp. on Foundations of Computer Science. Palo Alto, CA, USA. Nov. 3–5, 1993. P. 130–138. https://doi.org/10.1109/SFCS.1993.366874
3. *Pagh R.* Locality-sensitive Hashing without False Negatives // Proc. 27th Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'2016). Arlington, VA, USA. Jan. 10–12, 2016. P. 1–9. https://doi.org/10.1137/1.9781611974331.ch1
4. *Micciancio D.* Almost Perfect Lattices, the Covering Radius Problem, and Applications to Ajtai's Connection Factor // SIAM J. Comput. 2004. V. 34. № 1. P. 118–169. https://doi.org/10.1137/S0097539703433511
5. *Hämäläinen H., Honkala I., Litsyn S., Östergård P.* Football Pools—A Game for Mathematicians // Amer. Math. Monthly. 1995. V. 102. № 7. P. 579–588. https://doi.org/10.2307/2974552
6. *Ceze L., Nivala J., Strauss K.* Molecular Digital Data Storage Using DNA // Nat. Rev. Genet. 2019. V. 20. № 8. P. 456–466. https://doi.org/10.1038/s41576-019-0125-3
7. *Bornholt J., Lopez R., Carmean D.M., Ceze L., Seelig G., Strauss K.* A DNA-Based Archival Storage System // Proc. 21st Int. Conf. on Architectural Support for Programming Languages and Operating Systems (ASPLOS'16). Atlanta, GA, USA. Apr. 2–6, 2016. P. 637–649. https://doi.org/10.1145/2872362.2872397
8. *Church G.M., Gao Y., Kosuri S.* Next-Generation Digital Information Storage in DNA // Science. 2012. V. 337. № 6102. P. 1628. https://doi.org/10.1126/science.1226355
9. *Кабатянский Г.А., Панченко В.И.* Упаковки и покрытия хэммингова пространства единичными шарами // Докл. АН СССР. 1988. Т. 303. № 3. С. 550–552. https://www.mathnet.ru/rus/dan7368
10. *Krivelevich M., Sudakov B., Vu V.H.* Covering Codes with Improved Density // IEEE Trans. Inform. Theory. 2003. V. 49. № 7. P. 1812–1815. https://doi.org/10.1109/TIT.2003.813490
11. *Lenz A., Rashtchian C., Siegel P.H., Yaakobi E.* Covering Codes Using Insertions or Deletions // IEEE Trans. Inform. Theory. 2020. V. 67. № 6. P. 3376–3388. https://doi.org/10.1109/TIT.2020.2985691
12. *Fazeli A., Vardy A., Yaakobi E.* Generalized Sphere Packing Bound // IEEE Trans. Inform. Theory. 2015. V. 61. № 5. P. 2313–2334. https://doi.org/10.1109/TIT.2015.2413418

13. *Applegate D., Rains E.M., Sloane N.J.A.* On Asymmetric Coverings and Covering Numbers // J. Combin. Des. 2003. V. 11. № 3. P. 218–228. https://doi.org/10.1002/jcd.10022
14. *Sala F., Dolecek L.* Counting Sequences Obtained from the Synchronization Channel // Proc. 2013 IEEE Int. Symp. on Information Theory (ISIT'2013). Istanbul, Turkey. July 7–12, 2013. P. 2925–2929. https://doi.org/10.1109/ISIT.2013.6620761
15. *Hoeffding W.* Probability Inequalities for Sums of Bounded Random Variables // J. Amer. Statist. Assoc. 1963. V. 58. № 301. P. 13–30. https://doi.org/10.2307/2282952. Reprinted in: The Collected Works of Wassily Hoeffding. New York: Springer, 1994. P. 409–426.
16. *Wang G., Wang Q.* On the Size Distribution of Levenshtein Balls with Radius One, arXiv: 2204.02201 [cs.IT], 2022.
17. *He L., Ye M.* The Size of Levenshtein Ball with Radius 2: Expectation and Concentration Bound // Proc. 2023 IEEE Int. Symp. on Information Theory (ISIT'2023). Taipei, Taiwan. June 25–30, 2023. P. 850–855. https://doi.org/10.1109/ISIT54713.2023.10206888
18. *Cooper J.N., Ellis R.B., Kahng A.B.* Asymmetric Binary Covering Codes // J. Combin. Theory Ser. A. 2002. V. 100. № 2. P. 232–249. https://doi.org/10.1006/jcta.2002.3290
19. *Левенштейн В.И.* Двоичные коды с исправлением выпадений, вставок и замещений символов // Докл. АН СССР. 1965. Т. 163. № 4. С. 845–848. https://www.mathnet.ru/rus/dan31411
20. *Levenshtein V.I.* Efficient Reconstruction of Sequences from Their Subsequences or Supersequences // J. Combin. Theory Ser. A. 2001. V. 93. № 2. P. 310–332. https://doi.org/10.1006/jcta.2000.3081

Воробьев Илья Викторович
Технический университет Мюнхена, Германия
vorobyev.i.v@yandex.ru

Поступила в редакцию
14.10.2023
После доработки
28.11.2023
Принята к публикации
28.11.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 519.216.3

© 2023 г. **Н.Г. Докучаев**

ПОЧТИ ИДЕАЛЬНЫЕ ПРЕДИКТОРЫ И КАУЗАЛЬНЫЕ ФИЛЬТРЫ ДЛЯ ДИСКРЕТНЫХ СИГНАЛОВ

Представлены линейные предикторы и каузальные фильтры для дискретных сигналов, имеющих различные виды дегенерации спектра. Эти предикторы и фильтры основаны на аппроксимации идеальных некаузальных передаточных функций каузальными передаточными функциями, представленными многочленами от Z-преобразования дискретной функции Хевисайда.

Ключевые слова: дискретные временные сигналы, прогнозирование, предикторы, фильтры, каузальные передаточные функции, каузальная аппроксимация, высокочастотные сигналы, низкочастотные сигналы.

DOI: 10.31857/S0555292323020031, **EDN:** PPTSEI

§ 1. Введение

Известно, что определенная дегенерация спектра может обеспечить возможности для прогнозирования и интерполяции сигналов (см., например, [1–9]). В данной статье рассматриваются дискретные сигналы в детерминированной среде, где наблюдается только одна траектория сигнала, а не набор выборок траекторий, которые позволили бы применить статистические методы. Метод, который мы используем, основан на частотном анализе. Известно, что эти сигналы, в принципе, могут быть предсказаны, т.е. позволяют однозначные экстраполяции из их прошлых наблюдений, если у них есть разрыв спектра, т.е. их Z-преобразование обращается в ноль на некотором сегменте единичной окружности $\mathbb{T} = \{z \in \mathbb{C} : \ |z| = 1\}$ (см., например, [10]). Этот разрыв может быть произвольно малым и может быть даже сведен к одной точке при определенных условиях на дегенерацию спектра в окрестности этой точки. Соответственно, идеальный фильтр низких или высоких частот преобразует непредсказуемый сигнал в предсказуемый. Вот почему эти идеальные фильтры не могут быть каузальными.

Для дискретных временных сигналов в [10,11] были получены некоторые предикторы, основанные на иррациональных каузальных передаточных функциях. Соответствующие передаточные функции были представлены через экспоненты рациональных функций или степенных функций. В [12] также были построены некоторые фильтры нижних частот на основе аналогичного принципа.

В данной статье рассматриваются задачи предсказания и фильтрации для дискретных временных сигналов; предлагаются новые предикторы и каузальные фильтры, приближающие идеальные фильтры. Каузальные передаточные функции для этих предикторов и фильтров представлены в виде многочленов Z-преобразования дискретной функции Хевисайда, т.е. многочленов $(1 - z^{-1})^{-1}$. Для предикторов соответствующие передаточные функции аппроксимируют функцию $e^{i\omega T}$ на $\mathbb{T}$, где $\omega \in (-\pi, \pi]$ представляет частоту, а целое число $T > 0$ – предвыбранный гори-

зонт предсказания. Для фильтров соответствующие передаточные функции аппроксимируют вещественную ступенчатую функцию, представляющую след на $\mathbb{T}$ для Z-преобразования идеального фильтра. Аппроксимация возможна для сигналов с некоторым произвольно малым промежутком спектра; полученный сигнал может иметь более широкий предвыбранный промежуток спектра. Этот метод аппроксимации основан на подходе, разработанном в [13, 14] для предсказания непрерывных временных сигналов.

Результаты применимы как для высокочастотных сигналов, так и для сигналов, для которых спектр отсутствует на любом заданном сегменте $\mathbb{T}$, например, для низкочастотных сигналов. Более того, в статье показывается, что некоторые сигналы с недегенеративным спектром также могут быть предсказаны на половине временной оси при выполнении некоторых условий на некоторые специальные частотные характеристики, определяемые значениями сигнала только на этой половине временной оси.

Эти новые предикторы и фильтры позволяют явное представление во временной и частотной областях; кроме того, они не зависят от спектральных характеристик входных сигналов с заданной степенью спектральной дегенерации. Предлагается некоторый вычислительный подход на основе модельной подгонки.

Статья организована следующим образом. В § 2 формулируются определения. В § 3 формулируются основные теоремы о предсказуемости и предикторах (теоремы 1 и 2). В § 4 обсуждается представление передаточных функций во временной области. В § 5 обсуждаются некоторые проблемы реализации. В § 6 предлагается метод вычисления приближенных функций для экспонент $e^{i\omega}$. В § 7 предлагается расширение результатов на низкочастотные и другие сигналы. В § 8 содержатся доказательства.

§ 2. Постановка задачи

Некоторые обозначения. Через $\mathbb{Z}$ обозначаем множество всех целых чисел.

Через ℓ_r обозначаем множество всех функций (сигналов) $x\colon \mathbb{Z} \to \mathbb{C}$, для которых

$$|x|_{\ell_r} := \left(\sum_{t=-\infty}^{\infty} |x(t)|^r \right)^{1/r} < +\infty$$

для $r \in [1, \infty)$.

Для $x \in \ell_1$ или $x \in \ell_2$ мы обозначаем через $X = \mathcal{Z}x$ соответствующее Z-преобразование

$$X(z) = \sum_{t=-\infty}^{\infty} x(t) z^{-t}, \quad z \in \mathbb{T}.$$

Обратное Z-преобразование $\mathcal{Z}^{-1}X$ определяется как

$$x(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} X\left(e^{i\omega}\right) e^{i\omega t} d\omega, \quad t = 0, \pm 1, \pm 2, \ldots$$

Если $x \in \ell_2$, то $X|_{\mathbb{T}}$ определено как элемент пространства $L_2(\mathbb{T}; \mathbb{C})$.

Через Ind обозначаем индикаторную функцию.

Некоторые определения. Пусть $E = \mathbb{R}$ или $E = \mathbb{C}$.

Пусть $\mathcal{X} \subset \ell_\infty$ – некоторое множество дискретных сигналов, принимающих значения в E.

Пусть $\mathcal{P}(\mathcal{X})$ – множество всех непрерывных отображений $p\colon \mathcal{X} \to \ell_\infty$, таких что для любых $x_1, x_2 \in \mathcal{X}$ и $\bar{t} \in \mathbb{Z}$ выполняется

$$p(x_1(\cdot))(t) = p(x_2(\cdot))(t)$$

для всех $t \leqslant \bar{t}$, если $x_1(t) = x_2(t)$ для всех $t \leqslant \bar{t}$. Другими словами, это множество "каузальных" отображений; мы будем искать предикторы и фильтры в этом классе.

Рассмотрим сначала проблему прогнозирования. Пусть задано целое число $T \geqslant 1$. Цель состоит в оценке значений $x(t+T)$ в текущие моменты времени t с использованием исторических значений наблюдаемого процесса $x(s)|_{s\leqslant t}$. Поэтому T является горизонтом прогнозирования в этом контексте.

Определение 1. Пусть $\mathcal{X} \subset \ell_\infty$ и $\tau \in \{-1, 0, +\infty\}$.

(i) Будем говорить, что класс $\mathcal{X}$ является предсказуемым с горизонтом прогнозирования T до времени τ, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}(\mathcal{X})$ такая, что

$$\sup_{\substack{t\in\mathbb{Z}\\ t\leqslant\tau-T}} |x(t+T) - \widetilde{y}_d(t)| \to 0 \quad \text{при} \quad d \to +\infty \quad \forall x \in \mathcal{X},$$

где

$$\widetilde{y}_d(\cdot) = \widetilde{p}_d(x(\cdot)).$$

(ii) Мы говорим, что класс $\mathcal{X}$ равномерно предсказуем с горизонтом прогнозирования T до времени τ, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}$, такая что

$$\sup_{\substack{t\in\mathbb{Z}\\ t\leqslant\tau-T}} |x(t+T) - \widetilde{y}_d(t)| \to 0 \quad \text{при} \quad d \to +\infty \quad \text{равномерно по} \quad x \in \mathcal{X},$$

где $\widetilde{y}_d$ определена, как в пункте (i).

Функции $\widetilde{y}_d(t)$ в определении выше могут рассматриваться как приблизительные предсказания процесса $x(t+T)$.

Теперь рассмотрим задачу фильтрации.

Пусть задано некоторое $\Omega \in (0, \pi)$. Пусть функция $\Phi_\Omega\colon \mathbb{T} \to \mathbb{R}$ определена так, что

$$\Phi_\Omega(e^{i\omega}) = \mathrm{Ind}_{|\omega|\geqslant\Omega}\,.$$

Рассмотрим идеальный высокочастотный фильтр, для которого след от его передаточной функции на $\mathbb{T}$ равен $\Phi_\Omega(e^{i\omega})$, $\omega \in (-\pi, \pi]$, т.е. полосой подавления фильтра является $(-\Omega, \Omega)$. Цель – найти такие каузальные передаточные функции, которые аппроксимируют некаузальную передаточную функцию высокочастотного фильтра $\Phi_\Omega(e^{i\omega})$ произвольно близко.

Определение 2. Пусть $\mathcal{X} \subset \ell_\infty$.

(i) Будем говорить, что класс $\mathcal{X} \subset \ell_2$ допускает каузальную высокочастотную фильтрацию с полосой подавления $(-\Omega, \Omega)$, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}(\bar{\mathcal{X}})$, такая что

$$\sup_{t\in\mathbb{Z}} |\widetilde{x}(t) - \widetilde{y}_d(t)| \to 0 \quad \text{при} \quad d \to +\infty \quad \forall x \in \mathcal{X},$$

где

$$\widetilde{x} = \mathcal{Z}^{-1}(\Phi_\Omega X), \quad \widetilde{y}_d = \widetilde{p}_d(x(\cdot)).$$

(ii) Будем говорить, что класс $\mathcal{X}$ допускает равномерную каузальную высокочастотную фильтрацию с полосой подавления $(-\Omega, \Omega)$, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}$, такая что

$$\sup_{t\in\mathbb{Z}} |\widetilde{x}(t) - \widetilde{y}_d(t)| \to 0 \quad \text{равномерно по} \quad x \in \mathcal{X},$$

где $\widetilde{x}$ и $\widetilde{y}_d$ определены, как в пункте (i).

В последнем определении операторы p_d представляют собой близкие к идеальным каузальные фильтры, которые обеспечивают для класса $\mathcal{X}$ произвольно близкую аппроксимацию некаузального идеального фильтра высоких частот, определенного его передаточной функцией Φ_Ω.

§ 3. Основной результат

Для $d = 0, 1, 2, \ldots$ пусть Ψ_d^E – множество всех функций $\psi\colon \mathbb{C} \setminus \{1\} \to \mathbb{C}$, представленных в виде

$$\psi(z) = \sum_{k=0}^{d} \frac{a_k}{(1 - z^{-1})^k}, \tag{1}$$

где $a_k \in E$ могут быть любыми. Положим

$$\Psi^E := \bigcup_d \Psi_d^E.$$

Лемма 1. *Для $\bar{\Omega} \in (0, \pi)$ пусть функция $\zeta\colon [-\pi, \pi] \to \mathbb{C}$ определена либо как $\zeta(\omega) = e^{i\omega T}$, либо как $\zeta(\omega) = \mathrm{Ind}_{|\omega|\geqslant\bar{\Omega}}$. Тогда для любого $\varepsilon > 0$ существует целое число $d = d(\varepsilon, T) > 0$ и функции $\psi_d \in \Psi_d^{\mathbb{R}}$, такие что*

$$\sup_{\substack{\omega\in[-\pi,\pi]\\ |\omega|\geqslant\bar{\Omega}}} |\zeta(\omega) - \psi_d(e^{i\omega})| \leqslant \varepsilon. \tag{2}$$

Для $\bar{\Omega} \in (0, \pi)$ определим $\mathcal{X}(\bar{\Omega})$ как множество всех сигналов $x\colon \mathbb{Z} \to E$, таких что $x(\cdot) \in \ell_2$ и $X(e^{i\omega}) = 0$ для $\omega \in (-\bar{\Omega}, \bar{\Omega})$ и $X = \mathcal{Z}x$.

Кроме того, для $\tau = -1, 0$ определим $\mathcal{X}(\tau, \bar{\Omega})$ как множество всех действительных сигналов $x\colon \mathbb{Z} \to \mathbb{R}$, таких что $x(\cdot) \in \ell_2$ и выполняется следующее:

- Если $\tau = 0$, то

$$2\sum_{t=-\infty}^{-1} \cos(\omega t)x(t) + x(0) = 0 \quad \text{для} \quad \omega \in (-\bar{\Omega}, \bar{\Omega}). \tag{3}$$

- Если $\tau = -1$, то

$$\sum_{t=-\infty}^{-1} \sin(\omega t)x(t) = 0 \quad \text{для} \quad \omega \in (-\bar{\Omega}, \bar{\Omega}). \tag{4}$$

Описанную выше особенность процессов из $\mathcal{X}(\tau, \bar{\Omega})$ мы назовем левосторонней вырожденностью спектра.

Далее, определим $\mathcal{X}(\infty, \bar{\Omega})$ как $\mathcal{X}(\bar{\Omega})$.

Теорема 1. *Пусть заданы $\Omega \in (0, \pi)$ и $\tau \in \{-1, 0, +\infty\}$. Для $x \in \mathcal{X}(\tau, \Omega)$, рассмотренного в определении* 1(i), *а также для*

$$x \in \mathcal{X}(\tau, \Omega) \cap \{x \in \ell_2 : |x|_{\ell_2} \leqslant 1\},$$

рассмотренного в определении 1(ii), *предсказуемость до времени* τ *и равномерная предсказуемость до времени* τ *могут быть обеспечены последовательностью предикторов*

$$p_d\colon \mathcal{X}(\Omega) \to \ell_2, \quad d = 1, 2, \dots,$$

определенных своими передаточными функциями $\psi_d(z)$, *выбранными, как в лемме* 1, *с* $\zeta(\omega) = e^{i\omega T}$. *Более точно, для любого* $\bar{\varepsilon} > 0$ *и* $\widehat{y}_d(t) = p_d(x(\cdot))(t)$ *оценка*

$$\sup_{\substack{t\in\mathbb{Z}\\ t\leqslant\tau-T}} |x(t+T) - \widehat{y}_d(t)| \leqslant \varepsilon$$

выполняется, если d *и* ψ_d *таковы, что* (2) *справедливо с* $\zeta(\omega) = e^{i\omega T}$ *для достаточно маленького* ε.

Теорема 2. *Для* $\Omega \in (0, \pi)$ *и любого* $\Omega_0 \in (0, \Omega)$, *для* $x \in \mathcal{X}(\Omega_0)$ *каузальная фильтрация, рассмотренная в определении* 2(i), *а также равномерная каузальная фильтрация для*

$$x \in \mathcal{X}(\Omega_0) \cap \{x \in \ell_2 : \, |x|_{\ell_2} \leqslant 1\},$$

рассмотренная в определении 2(ii), *могут быть обеспечены последовательностью каузальных фильтров*

$$p_d\colon \mathcal{X}(\Omega) \to \ell_2, \quad d = 1, 2, \dots,$$

определенных своими передаточными функциями $\psi_d(z)$, *выбранными как в лемме* 1, *с* $\zeta(\omega) = \operatorname{Ind}|\omega| \geqslant \Omega$. *Более точно, для любого* $\bar{\varepsilon} > 0$ *и* $\widehat{y}_d(t) = p_d(x(\cdot))(t)$ *и любого* $\widetilde{x} = \mathcal{Z}^{-1}(\Phi_\Omega X)$ *оценка*

$$\sup_{t\in\mathbb{Z}} |\widetilde{x}(t) - \widehat{y}_d(t)| \leqslant \varepsilon$$

выполнена, если d *и* ψ_d *выбраны таким образом, что* (2) *выполняется с* $\zeta(\omega) = \operatorname{Ind}_{|\omega|\geqslant\Omega}$ *при достаточно малых* ε.

Согласно этой теореме процесс с произвольно малым спектральным зазором $(-\Omega_0, \Omega_0)$ может быть преобразован с использованием каузальных операций в процесс с большим спектральным зазором до $(-\Omega, \Omega)$.

Можно отметить, что:

- Передаточные функции $\psi_d(z)$ являются аналитическими в области $\mathbb{C} \setminus \{1\}$. Если мы применим их следы $\psi_d(e^{i\omega})\big|_{\omega\in(-\pi,\pi]}$ на $\mathbb{T}$ для расчета выходных процессов для входов $x \in \mathcal{X}(\Omega)$, то мы получим те же выходы, что и для функций $\psi_d(e^{i\omega}) \operatorname{Ind}_{\omega\in(-\pi,\pi],\, |\omega|\geqslant\Omega}$.
- Для вещественных входных процессов x выходы этих предикторов и фильтров являются вещественными.
- $p_d(\cdot)$ зависит от T и Ω через коэффициенты a_k в условиях теоремы 1, а $p_d(\cdot)$ зависит от Ω и Ω_0 через коэффициенты a_k в условиях теоремы 2.

§ 4. Представление операторов $p_d(\cdot)$ во временной области

Предположим, что $\bar{\Omega} = \Omega$ или $\bar{\Omega} = \Omega_0$.

Рассмотрим операторы h_k, определенные на $\mathcal{X}(\bar{\Omega})$ через их передаточные функции

$$H_k(z) = (1 - z^{-1})^{-k}, \quad k = 0, 1, 2, \dots$$

Другими словами, если $y = h_k(x)$ для $x \in \mathcal{X}(\bar{\Omega})$, то

$$Y(z) = (1 - z^{-1})^{-k} X(z)$$

для $Y = \mathcal{Z}y$ и $X = \mathcal{Z}x$. Очевидно, что

$$H_{k+1}(z) = H_1(z)H_k(z), \quad h_{k+1}(x(\cdot)) = h_1(h_k(x(\cdot))), \quad k = 0, 1, 2, 3, \ldots$$

Следовательно, $h_k(x(\cdot)) \in \mathcal{X}(\bar{\Omega})$ для всех $k = 0, 1, 2, \ldots$, $x \in \mathcal{X}(\bar{\Omega})$. Значит, Z-преобразования процессов $h_k(x(\cdot))$ обращаются в нуль на множестве

$$\{e^{i\omega},\ \omega \in [-\pi, \pi],\ |\omega| < \bar{\Omega}\},$$

и операторы $h_k \colon \mathcal{X}(\bar{\Omega}) \to \ell_2$ непрерывны при условии, что $\mathcal{X}(\bar{\Omega})$ является подпространством ℓ_2, снабженным ℓ_2-нормой.

Пусть $\boldsymbol{h}_1 \in \ell_\infty$ определен таким образом, что $\boldsymbol{h}_1(t) = 0$ для $t < 0$ и $\boldsymbol{h}_1(t) = 1$ для $t \geqslant 0$, т.е. $\boldsymbol{h}_1 = \mathcal{Z}^{-1}H_1(z)$.

Пусть

$$I_{\bar{\Omega}} := [-\pi, -\bar{\Omega}] \cup [\bar{\Omega}, \pi]$$

и $x \in \mathcal{X}(\bar{\Omega})$. Докажем, что во временной области оператор $h_1(x(\cdot))$ может быть представлен через свертку с ядром $\boldsymbol{h}_1$, т.е. если $x \in \mathcal{X}(\bar{\Omega})$, то

$$h_1(x(\cdot))(t) = \sum_{s=-\infty}^{t} x(s).$$

Пусть

$$\boldsymbol{h}_{1,m}(t) = \boldsymbol{h}_1(t) \operatorname{Ind}_{\{t<m-1\}}.$$

Ясно, что $\boldsymbol{h}_{1,m} \in \ell_2$. Положим

$$H_{1,m}(z) := \mathcal{Z}\boldsymbol{h}_{1,m} = \frac{1 - z^{-m}}{1 - z^{-1}}, \quad R_m(z) := \mathcal{Z}(\boldsymbol{h}_1 - \boldsymbol{h}_{1,m}) = \frac{z^{-m}}{1 - z^{-1}}.$$

Очевидно, что

$$(1 - e^{-i\cdot})^{-1} e^{it\cdot} X(e^{i\cdot}) \in L_2(I_{\bar{\Omega}}, \mathbb{C})$$

для любого t. Следовательно,

$$\int_{-\pi}^{\pi} R_m(e^{i\omega}) e^{i\omega t} X(e^{i\omega})\, d\omega = \int_{I_{\bar{\Omega}}} \frac{e^{-im\omega}}{1 - e^{-i\omega}} e^{i\omega t} X(e^{i\omega})\, d\omega \to 0 \quad \text{при} \quad m \to +\infty$$

для каждого $t \in \mathbb{Z}$. Отсюда следует, что если $x \in \mathcal{X}(\bar{\Omega})$, то

$$h_1(x(\cdot))(t) = \sum_{s=-\infty}^{t} x(s) = \lim_{m\to+\infty} \mathcal{Z}^{-1}(R_m + \mathcal{Z}\boldsymbol{h}_{1,m})(t) = \lim_{m\to+\infty} \sum_{s=-m}^{t} x(s),$$

и ряд сходится для каждого $t \in \mathbb{Z}$.

Это означает, что

$$h_k(x(\cdot))(t) = \sum_{s=-\infty}^{t} (h_{k-1}(x(\cdot))(s), \quad k = 1, 2, 3, \ldots$$

Следовательно, операторы p_d в теоремах 1, 2 можно представить в виде

$$p_d(x(\cdot))(t) = \sum_{k=0}^{d} a_k h_k(x(\cdot))(t),$$

где

$$h_k(x(\cdot))(t) = \sum_{s_{k-1}=-\infty}^{t} \sum_{s_{k-2}=-\infty}^{s_{k-1}} \dots \sum_{s_1=-\infty}^{s_2} \sum_{s=-\infty}^{s_1} x(s). \tag{5}$$

Все ряды здесь сходятся, как описано выше для h_1.

Отметим, что если $x \in \mathcal{X}(\bar{\Omega}) \cap \ell_1$, то ряд $\sum\limits_{s=-\infty}^{t} x(s)$ сходится абсолютно; однако для общего типа $x \in \mathcal{X}(\bar{\Omega})$ нет гарантии, что $x \in \ell_1$ или $h_k(x(\cdot)) \in \ell_1$.

§ 5. О вычислительных применениях теорем 1 и 2

Прямое применение предикторов, введенных в теоремах 1 и 2, требует вычисления сумм для полубесконечных рядов, что на практике невыполнимо. Однако эти теоремы могут привести к методам прогнозирования, обходящим этот расчет. Обсудим эти возможности.

Пусть $t_1 \in \mathbb{R}$ задано таким образом, что $t_1 < \tau$, где τ в условиях теоремы 1 описывается соответственным образом, и $\tau = +\infty$ в условиях теоремы 2. Пусть $x_k := h_k(x)$ для $x \in \mathcal{X}(\Omega_0)$, $k = 1, 2, \dots$, и пусть

$$\eta_k := x_k(t_1 - 1).$$

Лемма 2. *В обозначениях теорем* 1, 2 *для любого* t, *такого что* $t_1 \leqslant t < \tau + 1$, *имеем, что* $\widehat{y}_d = p_d(x(\cdot))$ *может быть представлено как*

$$\widehat{y}_d(t) = a_0 x(t) + \sum_{k=1}^{d} a_k \left(\sum_{l=1}^{k} c_l(t)\eta_l + f_k(t) \right). \tag{6}$$

Здесь $a_k \in \mathbb{R}$ *являются коэффициентами для функций*

$$\psi_d(z) = \sum_{k=1}^{d} a_k (1 - z^{-1})^{-k}$$

из теорем 1, 2,

$$f_k(t) = \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \dots \sum_{s=t_1}^{\tau_k} x_0(s)$$

и

$$c_1(t) = \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \dots \sum_{\tau_k=t_1}^{\tau_{k-1}} (\tau_k - t_1 + 1),$$

$$c_2(t) = \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \dots \sum_{\tau_{k-1}=t_1}^{\tau_{k-2}} (\tau_{k-1} - t_1 + 1),$$

$$c_l(t) = \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \dots \sum_{\tau_{l-1}=t_1}^{\tau_{k-l}} (\tau_{l-1} - t_1 + 1), \quad l = 1, 2, \dots, k-2,$$

$$c_{k-1}(t) = \sum_{\tau_1=t_1}^{t} (\tau_1 - t_1 + 1), \qquad c_k(t) = t - t_1 + 1.$$

Эта лемма показывает, что вычисление $\widehat{y}_d(t) = p_d(x(\cdot))(t)$ становится простым для $t > t_1$, если мы знаем все η_k, $k = 1, \ldots, d$, и наблюдаем $x(s)|_{s=t_1,\ldots,t}$.

Обсудим некоторые способы оценки η_k без вычисления бесконечных сумм. Во-первых, заметим, что (6) влечет за собой полезное свойство, которое приведено ниже.

Следствие 1. *Для любого $\varepsilon > 0$ существует целое число $d = d(\varepsilon) > 0$ и $a_0, a_1, \ldots, a_d \in \mathbb{R}$, такие что для любого $t_1 \in \mathbb{Z}$ существуют $\bar{\eta}_1, \bar{\eta}_1, \ldots, \bar{\eta}_d \in \mathbb{R}$, такие что*

$$|\widetilde{x}(t) - y_d(t)| \leqslant \varepsilon \quad \textit{для всех } t \geqslant t_1,$$

где

$$y_d(t) = y_d(t, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d) := a_0 x(t) + \sum_{k=1}^{d} a_k \left(\sum_{l=1}^{k} c_l(t) \bar{\eta}_l + f_k(t) \right). \tag{7}$$

В этом следствии $d = d(\varepsilon)$ и $a_k \in \mathbb{R}$ определяются, как в теоремах 1, 2.

Случай задачи прогнозирования: условия теоремы 1. Рассмотрим использование формул (6) и (7) для вычисления η_k в условиях теоремы 1.

Предположим, что $\theta > t_1$ и $\theta < \tau + 1$. Пусть цель состоит в прогнозировании значения $\widetilde{x}(t) = x(t + T)$, используя наблюдения за период времени $t \leqslant \theta$, в условиях теоремы 1. Если $\theta > t_1 + T$, то согласно следствию 1 есть возможность построить предсказатели, подгоняя параметры $\eta_0, \ldots, \eta_d$ с использованием наблюдений из прошлого, доступных для $t = t_1, \ldots, \theta - T$: можно сопоставить значения $y_d(t, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d)$ с наблюдениями из прошлого $x(t+T)$. Далее предполагаем, что $\theta > t_1 + T$.

Пусть d достаточно велико, чтобы $x(t + T)$ можно было приблизить значениями $\widehat{y}_d(t)$, как описано в теореме 1, т.е.

$$\sup_{t \in \mathbb{Z}} |x(t + T) - \widehat{y}_d(t)| \leqslant \varepsilon$$

для некоторого достаточно малого $\varepsilon > 0$ и некоторого выбора a_k.

Как приближение истинных $\eta_1, \ldots, \eta_d$ можно принять множество $\bar{\eta}_1, \ldots, \bar{\eta}_d$, такое что

$$|x(t + T) - y_d(t, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d)| \leqslant \varepsilon, \quad t = t_1, \ldots, \theta - T. \tag{8}$$

(Напомним, что в момент времени θ значения $x(t+T)$ и $y_d(t, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d)$ наблюдаемы для $t = t_1, \ldots, \theta - T$.) Если (8) выполнено, мы можем заключить, что величина $y_d(t, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d)$ дает приемлемое предсказание для $x(t+T)$ для этих t. Ясно, что теорема 1 подразумевает, что множество $\bar{\eta}_1, \ldots, \bar{\eta}_d$, обеспечивающее (8), существует, так как это неравенство выполняется при $\bar{\eta}_k = \eta_k$.

Соответствующее значение $y_d(\theta, x(t), \bar{\eta}_1, \ldots, \bar{\eta}_d)$ дало бы оценку для $\widehat{y}_d(\theta)$ и, соответственно, для $x(\theta + T)$.

Далее, поиск множества $\bar{\eta}_1, \ldots, \bar{\eta}_d$, обеспечивающего (8), может быть сложным. Вместо этого можно рассмотреть подгонку предсказаний и наблюдений в конечном числе точек $t = t_1, \ldots, T - \theta$.

Пусть дано целое число $\bar{d} \geqslant d$ и выбрано множество $\{t_m\}_{m=1}^{\bar{d}} \subset \mathbb{Z}$, такое что

$$t_1 < t_2 < t_3 < \ldots < t_{\bar{d}-1} < t_{\bar{d}} \leqslant \theta - T.$$

Мы предлагаем использовать наблюдения $x(t)$ в моменты времени $t = t_m$. Рассмотрим систему уравнений

$$a_0 x(t_m) + \sum_{k=1}^{d} a_k \left(\sum_{l=1}^{k} c_l(t_m)\bar{\eta}_l + f_k(t_m) \right) = \zeta_m, \quad m = 1, \ldots, \bar{d}. \tag{9}$$

Рассмотрим сначала случай, когда $\bar{d} = d$. В этом случае мы можем выбрать $\zeta_m = x(t_m+T)$; эти значения наблюдаются напрямую, без вычисления полубесконечных рядов, требующихся для $\widehat{y}_d(t_m)$. Соответствующий выбор $\bar{\eta}_k$ обеспечивает нулевую ошибку предсказания для $x(t_m + T)$, $m = 1, \ldots, \bar{d}$.

Включение в рассмотрение большего числа наблюдений, т.е. выбор более крупного $\bar{d} > d$ и более крупного множества $\{t_1, \ldots, \theta - T\}$, улучшает оценку η_k. Если мы рассмотрим случай $\bar{d} > d$, то в общем случае не удастся добиться того, чтобы

$$y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d) = x(t_m + T) \quad \text{для всех } m,$$

так как нельзя гарантировать, что система (9) разрешима для $\zeta_m \equiv x(t_m+T)$: система будет переопределенной. Тем не менее оценка, представленная в (8), по-прежнему может быть получена для любого произвольно большого $\bar{d}$, так как выполнено (8). Решение можно найти, используя методы подгонки линейных моделей.

В настоящий момент неясна сходимость оценок, полученных из этих процедур, поскольку выбор меньшего ε приводит к большему d. Анализ этих методов оставляем для дальнейших исследований.

Случай проблемы каузальной фильтрации в рамках теоремы 2. В условиях теоремы 2 прошлые значения истинного неизвестного процесса $\widetilde{x}(t)$ не наблюдаются, и следовательно, не могут быть использованы для подгонки значений $\eta_1, \ldots, \eta_d$. Однако мы можем использовать то, что значения $\eta_1, \ldots, \eta_k$ в (6), (7) по-прежнему такие же, как в условиях теоремы 2, где $\widetilde{x}(t) = x(t + T)$. Поскольку прошлые значения $x(s)|_{s=t_1,\ldots,t}$ наблюдаемы, мы можем использовать процедуру подгонки, основанную на теореме 1, для оценки $\eta_1, \ldots, \eta_d$ с использованием (6), (7) с коэффициентами a_k, определенными для аппроксимации $\zeta(\omega) = e^{i\omega T}$, и с наблюдениями $x(t_m)$, $t_m \leqslant t$, как описано выше. После этого мы можем оценить $\widetilde{x}(t)$ с помощью уравнения (6) снова с новыми коэффициентами a_k, определенными для аппроксимации $\zeta(\omega) = \operatorname{Ind} |\omega| \leqslant \Omega$.

§ 6. Возможный выбор ψ_d для предикторов в условиях теоремы 1

Коэффициенты a_k для функций ψ_n могут быть найдены с использованием численных методов из классического анализа, таких как процедура Грама – Шмидта. В случае теоремы 1 для предикторов нахождение этих коэффициентов может быть упрощено, особенно для $T = 1$.

Продемонстрируем это.

Предположим, что $T = 1$. Для вещественного $\nu > 0$ определим на $\mathbb{C} \setminus 1$ функцию

$$\widetilde{\psi}(\nu, z) := z \left(1 - \exp \frac{\nu}{1 - z} \right).$$

Эта функция является модификацией передаточной функции, введенной в [10] для предсказания сигналов с одноточечным спектральным вырождением.

Очевидно,

$$\operatorname{Re} \frac{\nu}{1 - e^{i\omega}} = \nu \frac{1 - \cos(\omega)}{|1 - e^{i\omega}|^2} \to 0 \quad \text{при} \quad \nu \to -\infty$$

равномерно на множестве $\{e^{i\omega},\ \omega \in (-\pi,\pi],\ |\omega| \geqslant \Omega\}$. Следовательно,

$$\psi(\nu, z) \to z \quad \text{при} \quad \nu \to -\infty$$

равномерно на множестве $\{e^{i\omega},\ \omega \in (-\pi,\pi],\ |\omega| \geqslant \Omega\}$.

Далее, для $\varepsilon > 0$ выберем $\nu < 0$ таким образом, чтобы

$$|\psi(\nu, e^{i\omega}) - e^{i\omega}| \leqslant \frac{\varepsilon}{2}, \quad \omega \in (-\pi,\pi], \quad |\omega| \geqslant \Omega.$$

Функция $\widetilde{\psi}(\nu,\cdot)$ является аналитической на $\mathbb{C} \setminus 1$ и ограничена на множестве $\mathbb{C} \setminus \{z \in \mathbb{C} :\ |1-z| > \delta\}$ для любого $\delta > 0$. Очевидно, что

$$\widetilde{\psi}(\nu, z) := z\left(1 - \left(1 + \frac{\nu}{1-z} + \frac{1}{2}\left[\frac{\nu}{1-z}\right]^2 + \frac{1}{3!}\left[\frac{\nu}{1-z}\right]^3 + \ldots + \frac{1}{d!}\left[\frac{\nu}{1-z}\right]^d + \ldots\right)\right),$$

где

$$\widetilde{\psi}_d(\nu, z) := -\frac{\nu z}{1-z} - \frac{z}{2}\left[\frac{\nu}{1-z}\right]^2 - \frac{z}{3!}\left[\frac{-\nu}{1-z}\right]^3 - \ldots - \frac{z}{d!}\left[\frac{-\nu}{1-z}\right]^d,$$

и где сходимость равномерна на множестве $\{e^{i\omega},\ \omega \in (-\pi,\pi],\ |\omega| \geqslant \Omega\}$.

Можно заметить, что функции $\psi_d(\nu, z)$ принадлежат множеству Ψ_d, так как

$$\frac{z}{1-z} = \frac{1}{1-z^{-1}}, \quad \frac{1}{1-z} = 1 - \frac{1}{1-z^{-1}}, \quad z \in \mathbb{C}, \quad z \neq 1.$$

Например,

$$\frac{z}{2}\left[\frac{\nu}{1-z}\right]^2 = \frac{\nu^2}{2(1-z^{-1})}\left(1 - \frac{1}{1-z^{-1}}\right).$$

Ясно, что можно выбрать d так, чтобы

$$|\psi(\nu, e^{i\omega}) - \psi_d(\nu, e^{i\omega})| \leqslant \frac{\varepsilon}{2}, \quad \omega \in (-\pi,\pi], \quad |\omega| \geqslant \Omega.$$

Для этого d и ν имеем

$$|\psi_d(\nu, e^{i\omega}) - e^{i\omega}| \leqslant \frac{\varepsilon}{2}, \quad \omega \in (-\pi,\pi], \quad |\omega| \geqslant \Omega.$$

Коэффициенты a_k могут быть вычислены из представления ψ_d в виде элемента Ψ_d.

Для случая $T > 1$ можно использовать функции $\psi_d(\nu, z)^T$.

§ 7. Сигналы низкой частоты и другие сигналы

Покажем, что результаты, полученные выше для сигналов высокой частоты, могут быть применены к сигналам более общего типа, описываемым следующим образом.

Пусть заданы $\Omega \in (0,\pi)$, $\Omega_0 \in (0,\Omega)$ и $\theta \in (-\pi,\pi)$, и пусть $\mathcal{Y}(\Omega,\theta)$ – множество всех сигналов $x \in \ell_2$, таких что $X(e^{i(\omega-\theta)}) = 0$ для $|\omega| < \Omega$, $\omega \in [-\pi,\pi]$, где $X = \mathcal{Z}x$.

Например, $\mathcal{Y}(\Omega, 0) = \mathcal{X}(\Omega)$; это множество включает высокочастотные сигналы, такие что $X(e^{i\omega}) = 0$, если $|\omega| < \Omega$. Соответственно, множество $\mathcal{Y}(\Omega,\pi)$ включает низкочастотные сигналы (сигналы с ограниченной полосой частот), такие что $X(e^{i\omega}) = 0$, если $\omega \in (-\pi, -\pi+\Omega) \cup (\pi-\Omega, \pi]$.

Для того чтобы предсказать сигнал $\widehat{x} \in \mathcal{Y}(\Omega, \theta)$, его можно преобразовать в сигнал $x \in \mathcal{X}(\Omega) = \mathcal{Y}(\Omega, 0)$, например, как $x(t) = e^{-i\theta t}\widehat{x}(t)$. Затем можно использовать для x предикторы, введенные в теореме 1. Предсказание $\widehat{y}(t)$ для $\widehat{x}(t)$ можно получить как

$$\widehat{y}(t) = e^{i\theta t}y(t),$$

где $y(t)$ – соответствующее предсказание для $x(t)$.

Аналогичным образом можно построить каузальный фильтр, который для $x \in \mathcal{Y}(\Omega_0, \theta)$ производит приближение $\widehat{x} \in \mathcal{Y}(\Omega, \theta)$, такое что $\widehat{x} = \mathcal{Z}^{-1}\Phi_{\Omega,\theta}X$, где $X = \mathcal{Z}x$ и где $\Phi_{\Omega,\theta}$ задано как Z-преобразование идеального фильтра, такого что

$$\Phi_{\Omega,\theta}(e^{i(\omega-\theta)}) = \mathrm{Ind}_{|\omega|>\Omega,\, \omega\in[-\pi,\pi]}\,.$$

Опять же, его можно преобразовать в сигнал $x \in \mathcal{X}(\Omega_0) = \mathcal{Y}(\Omega_0, 0)$ как $x(t) = e^{-i\theta t}\widehat{x}(t)$. Затем можно использовать для x каузальный фильтр, введенный в теореме 2. Полученный фильтрованный сигнал $\widehat{y}(t)$ для $\widehat{x}(t)$ можно получить как

$$\widehat{y}(t) = e^{i\theta t}y(t),$$

где $y(t)$ является соответствующим фильтрованным сигналом для $x(t)$.

В качестве альтернативы мы можем напрямую построить предикторы и фильтры для сигналов из $\mathcal{Y}(\Omega, \theta)$, аналогично тем, которые были представлены в теоремах 1 и 2, с передаточными функциями

$$\sum_{k=0}^{d} \frac{a_k}{(1 - e^{i\theta}/z)^k},$$

приближающих $e^{i\omega T}$ и $\mathrm{Ind}_{|\omega|>\Omega}$ на $\mathbb{T}$.

В случае, когда $x \in \bigcup\limits_{\theta} \mathcal{Y}(\Omega, \theta)$, а θ неизвестен, можно использовать подход из § 5, чтобы оценить θ из прошлых наблюдений в качестве нового неизвестного параметра.

§ 8. Доказательства

Доказательство леммы 1. Для множества $I \subset [-\pi, 0) \cup (0, \pi]$ пусть $\Gamma^E(I)$ (или $\Gamma^E_d(I)$) означает множество функций $\gamma\colon I \to \mathbb{C}$, заданных как $\gamma(\omega) = \psi(e^{i\omega})$ для некоторой функции ψ из Ψ^E (или из Ψ^E_d, соответственно).

Положим

$$I_{\bar{\Omega}} := [-\pi, -\bar{\Omega}] \cup [\bar{\Omega}, \pi].$$

Ясно, что

$$\frac{1}{1 - z^{-1}} = 1 - \frac{1}{1 - z}$$

для всех $z \in \mathbb{C}$, $z \neq 1$. Следовательно,

$$\overline{\left(\frac{1}{1 - 1/e^{i\omega}}\right)} = \frac{1}{1 - e^{i\omega}} = 1 - \frac{1}{1 - 1/e^{i\omega}}, \quad \omega \in \mathbb{R}, \quad \omega \neq 0.$$

Отсюда следует, что если $\psi(z) \in \Psi^E$, то $\psi(z^{-1}) \in \Psi^E$ для $E = \mathbb{R}$ и $E = \mathbb{C}$. Это означает, что $\overline{\gamma(\omega)} \in \Gamma^E(I_{\bar{\Omega}})$, если $\gamma(\omega) \in \Gamma^E(I_{\bar{\Omega}})$.

Поскольку функция

$$\gamma_1(\omega) = \operatorname{Re} \frac{1}{1 - e^{-i\omega}}$$

строго монотонна на интервалах $(-\infty, 0)$ и $(0, \infty)$ и имеет разные знаки на этих двух интервалах, мы имеем, что $\gamma_1(\alpha) \neq \gamma_1(\beta)$ для всех $\alpha, \beta \in I_{\bar{\Omega}}$, $\alpha \neq \beta$. Отсюда следует, что множество функций $\Gamma^{\mathbb{C}}(I_\Omega)$ разделяет точки на компактном множестве $I_{\bar{\Omega}}$.

Из теоремы Стоуна – Вейерштрасса для комплекснозначных непрерывных функций на компактных множествах действительных чисел следует, что множество $\Gamma(I_{\bar{\Omega}})$ полно в пространстве $C(I_{\bar{\Omega}}; \mathbb{C})$ непрерывных комплекснозначных функций, заданных на I_Ω с супремум-нормой (см., например, [15, теорема 10, с. 238]). Отсюда следует, что для любого $\varepsilon > 0$ существуют $d > 0$ и $\widehat{\gamma}_d \in \Gamma_d^{\mathbb{C}}(I_{\bar{\Omega}})$, представленная как

$$\widehat{\gamma}_d(\omega) = \sum_{k=0}^{d} \frac{A_k}{\left(1 - e^{-i\omega}\right)^k},$$

определенная для $\omega \in \mathbb{R} \setminus 0$, где $A_k \in \mathbb{C}$, так что

$$\left(\int\limits_{I_\Omega} |\zeta(\omega) - \widehat{\gamma}_d(\omega)|^2 \, d\omega \right)^{1/2} \leqslant \varepsilon.$$

Для $\zeta(\omega) = e^{i\omega T}$ это следует непосредственно из теоремы 10 в [15, с. 238], упомянутой выше. Для $\zeta(\omega) = \operatorname{Ind}_{|\omega| \geqslant \bar{\Omega}}$ это следует из того факта, что множество $C(I_\Omega; \mathbb{C})$ всюду плотно в $L_2(I_{\bar{\Omega}}; \mathbb{C})$, а сходимость в $C(I_{\bar{\Omega}}; \mathbb{C})$ влечет за собой сходимость в $L_2(I_{\bar{\Omega}}; \mathbb{C})$.

Покажем, что для $\gamma_d \in \Gamma_d^{\mathbb{R}}(I_\Omega)$ выполняется та же оценка, где

$$\gamma_d(\omega) = \sum_{k=0}^{d} \frac{a_k}{\left(1 - e^{-i\omega}\right)^k},$$

а $a_k = \operatorname{Re} A_k$.

Предположим, что $\operatorname{Im} A_k \neq 0$ для некоторого k. Ясно, что действительная и мнимая части функции

$$\frac{i \operatorname{Im} A_k}{\left(1 - e^{-i\omega}\right)^k}$$

являются четной и нечетной функциями соответственно. С другой стороны, функции $\operatorname{Re} e^{i\omega T} = \cos(\omega T)$ и $\operatorname{Im} e^{i\omega T} = \sin(\omega T)$ являются, соответственно, нечетной и четной на $\mathbb{R}$. Следовательно, замена A_k на $a_k = \operatorname{Re} A_k$ не может испортить оценку. Таким образом, передаточная функция

$$\psi_d(e^{i\omega}) = \gamma_d(\omega) = \sum_{k=0}^{d} \frac{a_k}{\left(1 - e^{-i\omega}\right)^k}$$

удовлетворяет требуемой оценке. ▲

Доказательство теорем 1, 2. Рассмотрим сначала случай, когда $x \in \mathcal{X}(\infty, \Omega) = \mathcal{X}(\Omega)$.

Продолжим доказательство одновременно для теоремы 1 (с $\tau = +\infty$) и теоремы 2. Для доказательства теоремы 1 далее предполагаем, что $\bar{\Omega} = \Omega$ и функция $\zeta\colon I_\Omega \to \mathbb{C}$ определена как $\zeta(\omega) = e^{i\omega T}$. Для доказательства теоремы 2 далее предполагаем, что $\bar{\Omega} = \Omega_0$ и $\zeta(\omega) = \operatorname{Ind}_{|\omega| \geqslant \Omega}$.

Предположим, что оценка (2) выполняется для выбранных d, γ_d, ψ_d. Тогда

$$\widetilde{x}(t) - \widehat{y}_d(t) = \int\limits_{-\pi}^{\pi} e^{i\omega t}(\zeta(\omega) - \psi_d(e^{i\omega}))X(e^{i\omega})\,d\omega,$$

где $\widetilde{x}(t) = x(t+T)$ в постановке теоремы 1, а $\widetilde{x}(t)$ является идеальным отфильтрованным процессом в постановке теоремы 2. Очевидно, что

$$|\widetilde{x}(t) - \widehat{y}_d(t)| \leqslant \left(\int\limits_{-\pi}^{\pi} |\zeta(\omega) - \psi_d(e^{i\omega})|\,d\omega\right)^{1/2} \leqslant$$

$$\leqslant \left(\int\limits_{I_\Omega} |\zeta(\omega) - \psi_d(e^{i\omega})|^2\,d\omega\right)^{1/2} \left(\int\limits_{-\pi}^{\pi} |X(e^{i\omega})|^2\,d\omega\right)^{1/2} \leqslant \varepsilon.$$

Имеем

$$\left(\int\limits_{-\pi}^{\pi} |X(e^{i\omega})|^2\,d\omega\right)^{1/2} = \|x\|_{\ell_2}.$$

Следовательно, $|\widetilde{x}(t) - \widehat{y}_d(t)| \leqslant \varepsilon\|x\|_{\ell_2}$. Это дает доказательство теоремы 1 для случая $\tau = +\infty$ и теоремы 2.

Докажем теперь теорему 1 для случая $\tau = 0$. Пусть $x \in \mathcal{X}(0,\Omega)$. Определим четную функцию $\widetilde{x}\colon \mathbb{Z} \to \mathbb{R}$ так, что $\widetilde{x}(t) = x(t)$ для $t \leqslant 0$ и $\widetilde{x}(t) = x(-t)$ для $t > 0$. Положим $\widetilde{X} = \mathcal{Z}\widetilde{x}$. Можно показать, что

$$\operatorname{Re}\widetilde{X}(e^{i\omega}) = 2\sum_{t=-\infty}^{-1} \cos(\omega t)x(t) + x(0)$$

и

$$\operatorname{Im}\widetilde{X}(e^{i\omega}) = 0$$

для $\omega \in (-\pi, \pi]$. Это означает, что $\widetilde{x} \in \mathcal{X}(\Omega)$. Кроме того, поскольку предикторы p_d являются каузальными операторами, следовательно, получаем

$$p_d(\widetilde{x}(\cdot))(t) = p_d(x(\cdot))(t) \quad \text{для всех } t \leqslant 0.$$

Тогда доказательство для $\tau = 0$ следует из доказательства для случая $\tau = +\infty$.

Случай $\tau = -1$ можно рассмотреть аналогично. Для $x \in \mathcal{X}(-1,\Omega)$ определим нечетную функцию $\widetilde{x}\colon \mathbb{Z} \to \mathbb{R}$ так, что $\widetilde{x}(t) = x(t)$ для $t \leqslant -1$, $\widetilde{x}(0) = 0$ и $\widetilde{x}(t) = -x(-t)$ для $t > 0$. Положим $\widetilde{X} = \mathcal{Z}\widetilde{x}$. Можно показать, что

$$\operatorname{Re}\widetilde{X}(e^{i\omega}) = 0$$

и

$$\operatorname{Im}\widetilde{X}(e^{i\omega}) = 2\sum_{t=-\infty}^{-1} \sin(\omega t)\widetilde{x}(t)$$

для $\omega \in (-\pi, \pi]$. Отсюда следует, что $\widetilde{x} \in \mathcal{X}(\Omega)$. Опять же, поскольку предикторы p_d являются каузальными, получаем

$$p_d(\widetilde{x}(\cdot))(t) = p_d(x(\cdot))(t) \quad \text{для всех } t \leqslant -1.$$

Таким образом, доказательство для $\tau = -1$ следует из доказательства для случая $\tau = +\infty$, что завершает доказательство теоремы 1. ▲

Доказательство леммы 2. Имеем

$$x_k(t) = \eta_k + \sum_{s=t_1}^{t} x_{k-1}(s) = \sum_{l=1}^{k} c_l(t)\eta_l + f_k(t).$$

Далее, для любого $t \geqslant t_1$ имеем

$$y_d(t) = a_0 x(t) + \sum_{k=1}^{d} a_k x_k(t),$$

т.е.

$$y_d(t) = a_0 x(t) + \sum_{k=1}^{d} a_k \left(\eta_k + \sum_{s=t_1}^{t} x_{k-1}(s) \right). \tag{10}$$

Здесь мы предполагаем, что $x_0 := x$.

Кроме того, имеем

$$\sum_{\tau=t_1}^{t} x_1(\tau) = \sum_{\tau=t_1}^{t} \left(\eta_1 + \sum_{s=t_1}^{\tau} x_0(s) \right) = \eta_1(t - t_1 + 1) + \sum_{\tau=t_1}^{t} \sum_{s=t_1}^{\tau} x_0(s)$$

и

$$\sum_{\tau_1=t_1}^{t} x_2(\tau_1) = \sum_{\tau_1=t_1}^{t} \left(\eta_2 + \sum_{s=t_1}^{\tau_1} x_1(s) \right) = \eta_2(t - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \sum_{s=t_1}^{\tau_1} x_1(s) =$$
$$= \eta_2(t - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \left[\eta_1(\tau_1 - t_1 + 1) + \sum_{\tau_2=t_1}^{\tau_1} \sum_{s=t_1}^{\tau_2} x_0(s) \right] =$$
$$= \eta_2(t - t_1 + 1) + \eta_1 \sum_{\tau_1=t_1}^{t} (\tau_1 - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \sum_{s=t_1}^{\tau_2} x_0(s).$$

Аналогично

$$\sum_{\tau_1=t_1}^{t} x_3(\tau_1) = \sum_{\tau_1=t_1}^{t} \left(\eta_3 + \sum_{s=t_1}^{\tau_1} x_2(s) \right) = \eta_3(t - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \sum_{s=t_1}^{\tau_1} x_2(s) =$$
$$= \eta_3(t - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \left[\eta_2(\tau_1 - t_1 + 1) + \sum_{\tau_2=t_1}^{\tau_1} \sum_{s=t_1}^{\tau_2} x_1(s) \right] =$$
$$= \eta_3(t - t_1 + 1) + \eta_2 \sum_{\tau_1=t_1}^{t} (\tau_1 - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \sum_{\tau_3=t_1}^{\tau_2} x_1(\tau_3) =$$
$$= \eta_3(t - t_1 + 1) + \eta_2 \sum_{\tau_1=t_1}^{t} (\tau_1 - t_1 + 1) + \sum_{\tau_1=t_1}^{t} \sum_{\tau_2=t_1}^{\tau_1} \sum_{\tau_3=t_1}^{\tau_2} \left[\eta_1 + \sum_{s=t_1}^{\tau_3} x_0(s) \right] =$$
$$= \eta_3(t - t_1 + 1) + \eta_2 \sum_{\tau_1=t_1}^{t} (\tau_1 - t_1 + 1) +$$

$$+\sum_{\tau_1=t_1}^{t}\sum_{\tau_2=t_1}^{\tau_1}\Big[\eta_1(\tau_2-t_1+1)+\sum_{s=t_1}^{\tau_2}\sum_{s=t_1}^{\tau_3}x_0(s)\Big]=$$

$$=\eta_3(t-t_1+1)+\eta_2\sum_{\tau_1=t_1}^{t}(\tau_1-t_1+1)+\sum_{\tau_1=t_1}^{t}\sum_{\tau_2=t_1}^{\tau_1}\eta_1(\tau_2-t_1+1)+$$

$$+\sum_{\tau_1=t_1}^{t}\sum_{\tau_2=t_1}^{\tau_1}\sum_{s=t_1}^{\tau_2}\sum_{s=t_1}^{\tau_3}x_0(s)$$

Аналогично получаем, что для $k>2$ выполнено

$$\sum_{s=t_1}^{t}x_k(s)=\eta_k(t-t_1+1)+\eta_{k-1}\sum_{\tau_1=t_1}^{t}(\tau_1-t_1+1)+\ldots+$$

$$+\eta_1\sum_{\tau_1=t_1}^{t}\sum_{\tau_2=t_1}^{\tau_1}\ldots\sum_{\tau_k=t_1}^{\tau_{k-1}}(\tau_k-t_1+1)+\sum_{\tau_1=t_1}^{t}\sum_{\tau_2=t_1}^{\tau_1}\ldots\sum_{s=t_1}^{\tau_k}x_0(s).$$

Следовательно,

$$x_k(t)=\eta_k+\sum_{s=t_1}^{t}x_{k-1}(s)=\sum_{l=1}^{k}c_l(t)\eta_l+f_k(t).$$

Вместе с (10) это доказывает (7) и завершает доказательство леммы. ▲

§ 9. Заключительные замечания

(i) Предложенный в данной статье подход позволяет дальнейшие модификации. В частности, другие некаузальные дискретные передаточные функции могут быть аппроксимированы каузальными передаточными функциями из Ψ^E. Фактически, любая передаточная функция $H(z)$ может быть аппроксимирована таким образом, если

$$\int_{-\pi}^{\pi}|H(e^{i\omega})|^2\,d\omega<+\infty.$$

(ii) Можно показать, что в соответствии с [15, теорема 10, с. 238] аппроксимация

$$\zeta(\omega)=\mathrm{Ind}_{|\omega|\geqslant\bar{\Omega}}$$

в лемме 1 может быть достигнута на множестве действительных функций, представленных в виде

$$\gamma_d(\omega)=\psi_d(e^{i\omega})=\sum_{k=0}^{d}b_k\left|\frac{1}{1-e^{i\omega}}\right|^{2k}=\sum_{k=0}^{d}b_k\left(\frac{1}{1-e^{-i\omega}}\right)^k\left(1-\frac{1}{1-e^{i\omega}}\right)^k$$

с $b_k\in\mathbb{R}$. Это может помочь упростить вычисления, так как это множество меньше, чем Ψ^R. Если b_k найдены, то мы можем получить коэффициенты a_k, необходимые для подгонки η_k через (6), (7).

(iii) Предикторы, введенные в [10,11], не позволяют применять описанную в § 5 процедуру подгонки, поскольку ядра соответствующих каузальных сверток сильно зависят от времени.

(iv) В данной статье мы рассматриваем L_2-аппроксимацию некаузальных передаточных функций; это позволяет аппроксимировать не непрерывные на $\mathbb{T}$ передаточные функции, используемые для задачи фильтрации. Кроме того, это позволяет использовать процедуру Грама – Шмидта для построения функций ψ_d. В непрерывном случае [14], где требовалась равномерная аппроксимация на бесконечных интервалах, это было невозможно.

(v) В общем случае можно ожидать, что аппроксимирующие функции $\psi_d(e^{i\omega})$ принимают большие значения внутри интервала $(-\bar{\Omega}, \bar{\Omega})$ для больших d в терминах леммы 1. Однако некоторую устойчивость предсказания и фильтрации с учетом зашумления можно установить аналогично [10]. Мы оставляем это для будущих исследований.

(vi) Процессы из $\mathcal{X}(\tau, \Omega)$ не обязательно имеют спектральное вырождение для $\tau = -1, 0$ и $\Omega \in (0, \pi)$; их Z-преобразования могут быть отделены от нуля на $\mathbb{T}$. Однако теорема 1 показывает, что эти процессы предсказуемы на левой половине временной оси вследствие левосторонней вырожденности спектра, определенной в (3), (4).

СПИСОК ЛИТЕРАТУРЫ

1. *Butzer P.L., Stens R.L.* Linear Prediction by Samples from the Past // Advanced Topics in Shannon Sampling and Interpolation Theory. New York: Springer, 1993. P. 157–183. https://doi.org/10.1007/978-1-4613-9757-1_5
2. *Higgins J.R.* Sampling Theory in Fourier and Signal Analysis: Foundations. Oxford: Clarendon; New York: Oxford Univ. Press, 1996.
3. *Li Z., Han J., Song Y.* On the Forecasting of High-Frequency Financial Time Series Based on ARIMA Model Improved by Deep Learning // J. Forecast. 2020. V. 39. № 7. P. 1081–1097. https://doi.org/10.1002/for.2677
4. *Luo S., Tian C.* Financial High-Frequency Time Series Forecasting Based on Sub-step Grid Search Long Short-Term Memory Network // IEEE Access. 2020. V. 8. P. 203183–203189. https://doi.org/10.1109/ACCESS.2020.3037102
5. *Knab J.J.* Interpolation of Band-Limited Functions Using the Approximate Prolate Series // IEEE Trans. Inform. Theory. 1979. V. 25. № 6. P. 717–720. https://doi.org/10.1109/TIT.1979.1056115
6. *Lyman R.J., Edmonson W.W., McCullough S., Rao M.* The Predictability of Continuous-Time, Bandlimited Processes // IEEE Trans. Signal Process. 2000. V. 48. № 2. P. 311–316. https://doi.org/10.1109/78.823959
7. *Lyman R.J., Edmonson W.W.* Linear Prediction of Bandlimited Processes with Flat Spectral Densities // IEEE Trans. Signal Process. 2001. V. 49. № 7. P. 1564–1569. https://doi.org/10.1109/78.928709
8. *Papoulis A.* A Note on the Predictability of Band-limited Processes // Proc. IEEE. 1985. V. 73. № 8. P. 1332–1333. https://doi.org/10.1109/PROC.1985.13284
9. *Vaidyanathan P.P.* On Predicting a Band-limited Signal Based on Past Sample Values // Proc. IEEE. 1987. V. 75. № 8. P. 1125–1127. https://doi.org/10.1109/PROC.1987.13856
10. *Dokuchaev N.* Predictors for Discrete Time Processes with Energy Decay on Higher Frequencies // IEEE Trans. Signal Process. 2012. V. 60. № 11. P. 6027–6030. https://doi.org/10.1109/TSP.2012.2212436
11. *Dokuchaev N.* On Predictors for Band-limited and High-Frequency Time Series // Signal Process. 2012. V. 92. № 10. P. 2571–2575. https://doi.org/10.1016/j.sigpro.2012.04.006
12. *Dokuchaev N.* Near-ideal Causal Smoothing Filters for the Real Sequences // Signal Process. 2016. V. 118. № 1. P. 285–293. https://doi.org/10.1016/j.sigpro.2015.07.002
13. *Dokuchaev N.* Limited Memory Predictors Based on Polynomial Approximation of Periodic Exponentials // J. Forecast. 2022. V. 41. № 5. P. 1037–1045. https://doi.org/10.1002/for.2843

14. *Докучаев Н.Г.* Предикторы для высокочастотных сигналов на основе аппроксимации периодических экспонент рациональными многочленами // Пробл. передачи информ. 2022. Т. 58. № 4. С. 84–94. https://doi.org/10.31857/S0555292322040076

15. *Stone M.H.* The Generalized Weierstrass Approximation Theorem // Math. Mag. 1948. V. 21. № 4. P. 167–184; № 5. P. 237–254 (continued). https://doi.org/10.2307/3029750; https://doi.org/10.2307/3029337

Докучаев Николай Геннадьевич
Институт ZJU-UIUC (Чжэцзянский университет – Иллинойский университет в Урбане-Шампейне), Чжэцзянский университет, Хайнин, провинция Чжэцзян, Китай
Dokuchaev@intl.zju.edu.cn

Поступила в редакцию
25.02.2023
После доработки
15.03.2023
Принята к публикации
15.03.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 517.938 : 519.722

© 2023 г. **Г.Д. Дворкин**

ГЕОМЕТРИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ЭНТРОПИИ СОФИЧЕСКИХ СИСТЕМ[1]

Рассматривается геометрический подход к понятию метрической энтропии. Обоснована возможность такого подхода для класса борелевских вероятностных инвариантных эргодических мер на софических системах, что является первым результатом такой общности для немарковских систем.

Ключевые слова: метрическая энтропия, локальная скорость деформации границ, символическая система, синхронизованная система, софическая система, инвариантная эргодическая мера, производное пространство, марковская граница.

DOI: 10.31857/S0555292323020043, **EDN:** PPWQAP

Памяти Бориса Марковича Гуревича

§ 1. Введение

Данная статья является продолжением работ автора [1, 2], посвященных геометрическому подходу к определению энтропии Колмогорова – Синая. Такой подход был впервые предложен в физической литературе [3], после чего был строго формализован и обоснован для класса марковских систем Б.М. Гуревичем в [4]. Дальнейшее развитие идей работы [4] Гуревичем и С.А. Комечем в [5, 6] позволило распространить геометрическую интерпретацию энтропии на широкий класс синхронизованных систем, но с наложением дополнительного ограничения – условия Комеча (более подробно история вопроса описана в [1]). В работе [1] достигнуты новые продвижения в двух смыслах:

1) Для синхронизованных систем ослаблено дополнительное ограничение (движение вглубь – усиление результатов для уже рассмотренных систем);

2) Впервые получены результаты для несинхронизованных систем – сдвигов Дика (движение вширь – рассмотрение новых классов систем).

Работа [2] полностью посвящена второму подходу, и в ней получен достаточно общий результат. Исследования же в первом направлении ограничиваются одним параграфом в [1]. Полученная в этом параграфе теорема ослабляет условие Комеча и позволяет рассмотреть некоторые случаи, в которых это условие не выполняется, но при этом все описанные примеры использования данной теоремы либо тривиальны, либо искусственны (хотя и интересны). Кроме того, после ослабления дополнительное ограничение становится в некотором смысле неявным (см. далее), и его проверка представляет отдельную проблему. Таким образом, результаты в описываемом направлении выглядят незавершенными, и возникает естественная задача

[1] Работа выполнена при финансовой поддержке гранта Фонда развития теоретической физики и математики “БАЗИС”.

нахождения значимых примеров, в которых возможна явная проверка ослабленного условия. Решению этой задачи, а также развитию первого направления в целом и посвящена данная статья.

Очевидной программой-максимум первого направления является полное избавление от дополнительного условия и получение результата для любой борелевской вероятностной инвариантной эргодической меры, т.е. в общности, изначально предложенной в [4], но после [4] ни одного результата в указанной общности получено не было. В этой статье такой результат получен для софических систем, а именно показано, что результаты [1] позволяют полностью избавится от условия Комеча в софическом случае. Более того, для синхронизованных систем получено новое достаточное условие, являющееся более общим, чем условие Комеча, и явно проверяемым.

§ 2. Определения и обозначения

В этом параграфе вводятся только базовые определения и обозначения. Понятия, относящиеся к теории производных пространств Томсена (являющейся основным инструментом доказательства), будут введены отдельно.

Пусть A – конечное множество, и пусть $A^{\mathbb{Z}}$ – пространство бесконечных двусторонних последовательностей символов из A.

Множество A будем называть алфавитом, любую конечную последовательность символов (букв) из A – (конечным) словом этого алфавита. Количество букв в слове w называют его длиной и обозначают $|w|$. Слово нулевой длины называют пустым.

Элементы $A^{\mathbb{Z}}$ будем называть бесконечными словами, при этом в данной терминологии бесконечные слова словами не являются.

Определение 1. Назовем *полным сдвигом* пару $(A^{\mathbb{Z}}, T)$, где A – конечное множество, а T – сдвиг на шаг вправо в пространстве последовательностей $A^{\mathbb{Z}}$.

Для $x \in A^{\mathbb{Z}}$ и целых a и b, таких что $a \leqslant b$, обозначим слово $(x(a), x(a+1), \ldots, x(b))$ через $x_{[a;b]}$. Если слово w равно $x_{[a;b]}$ для некоторых a и b, то будем говорить, что w является *подсловом* бесконечного слова x (аналогично определяется подслово конечного слова). Вместо $x_{[a;a]}$ будем писать $x_{[a]}$.

Введем метрику d на $A^{\mathbb{Z}}$: примем $d(x,x) = 0$, а для несовпадающих точек x и y положим $d(x,y) = (1/2)^m$, где $m = m(x,y)$ – целое неотрицательное число, равное нулю, если $x_{[0]} \neq y_{[0]}$, и удовлетворяющее условиям

$$x_{[-(m-1);m-1]} = y_{[-(m-1);m-1]}, \quad x_{[-m;m]} \neq y_{[-m;m]}$$

в противном случае. Эта метрика порождает топологию Θ, которая далее считается фиксированной.

Определение 2. Будем называть *символической системой* пару (X, T), где X – замкнутое T-инвариантное подмножество $A^{\mathbb{Z}}$ с топологией, индуцированной топологией Θ, а также первый элемент этой пары, считая сдвиг и топологию заданными по умолчанию.

Пусть далее в этом параграфе X – символическая система.

Множество всех подслов всех $x \in X$ называется *языком* символической системы X и обозначается $W(X)$, кроме того, обозначим через $W_n(X)$ множество всех слов из языка длины n. Слова алфавита системы, которые не входят в $W(X)$, будем называть *запрещенными*.

Префикс слова – любое его подслово, начинающееся с начала этого слова. *Суффикс* слова – любое его подслово, заканчивающееся в конце этого слова. Через a^ℓ обозначим конкатенацию ℓ букв или слов a (a^0 считаем пустым словом).

Определение 3. Множество

$$\{w\}_c^X := \{x \in X : \ x_{[c;c+|w|-1]} = w\}$$

называется *цилиндром* в X с *основанием* $w \in W(X)$. Всюду далее

$$\{w\}_c := \{w\}_c^X, \quad \{x_{[a;b]}\} := \{x_{[a;b]}\}_a.$$

Рассмотрим T-инвариантную борелевскую вероятностную меру μ на X. Под мерой $\mu(w)$ слова $w \in W(X)$ понимаем меру цилиндра $\{w\}_0$ (из T-инвариантности меры очевидно, что $\mu(\{w\}_a) = \mu(\{w\}_0)$ для любого целого a).

Введем следующие обозначения:

$k(\varepsilon) := \min\{\ell \in \mathbb{Z} : \ (1/2)^{(\ell+1)} \leqslant \varepsilon\}$ (часто будем писать просто k);

$O_\varepsilon^X(x)$ – открытая ε-окрестность точки x в пространстве X;

$O_\varepsilon^X(C)$ – открытая ε-окрестность множества C в пространстве X.

В случаях, когда рассматриваемое пространство фиксировано, верхний индекс будем опускать.

Определение 4. *Метрическая энтропия* (энтропия Колмогорова – Синая) символической динамической системы (X, T) с инвариантной мерой μ может быть определена как средняя условная энтропия настоящего при условии прошлого (общее определение для произвольной динамической системы см. в [7, 8]):

$$h_\mu(X, T) = \lim_{n\to\infty} H_\mu(x_0 \mid x_{-1}, x_{-2}, \ldots, x_{-n}).$$

Определение 5. Для $x \in X$ определим *локальную скорость деформации границ* (ЛСДГ):

$$P_{X,T,\mu}(x) := \lim_{\varepsilon\to 0} \frac{1}{n(\varepsilon)} \log\left(\frac{\mu\left(O_\varepsilon\left(T^{n(\varepsilon)}\left(O_\varepsilon(x)\right)\right)\right)}{\mu\left(O_\varepsilon(x)\right)}\right),$$

где $n(\varepsilon)$ – положительная целочисленная функция со свойствами

$$n(\varepsilon) \to \infty \quad \text{и} \quad n(\varepsilon) = o(|\log(\varepsilon)|) = o(k(\varepsilon)) \quad \text{при } \varepsilon \to 0$$

(часто будем писать просто n). Такие функции n будем называть *медленными*. Допредельное выражение будем обозначать через $P^\varepsilon_{X,T,\mu}(x)$ и называть *ε-ЛСДГ*.

Далее нам понадобятся понятия марковской, софической (софика) и синхронизованной системы.

Определение 6. Символическая система $X \subseteq A^{\mathbb{Z}}$ называется *марковской* (subshift of finite type), если существует конечное множество слов $Z \subset W(A^{\mathbb{Z}})$, такое что $x \in A^{\mathbb{Z}}$ принадлежит X тогда и только тогда, когда ни один элемент из Z не является подсловом x.

Определение 7. Множество

$$P_w = \{v \in W(X) : \ wv \in W(X)\}$$

будем называть *продолжением* слова $w \in W(X)$, а также для каждого $v \in W(X)$, такого что $vw \in W(X)$, введем *v-продолжение* слова w как $P_w(v) = P_{vw}$. Множество

$$\{P_w : \ w \in W(X)\}$$

назовем *множеством продолжений* слов языка $W(X)$.

Определение 8. Символическая система X называется *софической*, если множество продолжений слов ее языка конечно.

Замечание 1. Несложно понять (см. [9]), что система X софична тогда и только тогда, когда для каждого $w \in W(X)$ образ $P_w(v)$ (как функции v) конечен.

Определение 9. Система X *транзитивна*, если в ней есть точка со всюду плотной орбитой.

Замечание 2. Для символической системы X транзитивность эквивалентна тому, что для любой упорядоченной пары слов $u, v \in W(X)$ существует $w \in W(X)$, такое что $uwv \in W(X)$.

Определение 10. Будем называть слово $w \in W(X)$ *волшебным*, или *синхронизующим*, если для любых $u, v \in W(X)$, таких что $uw, wv \in W(X)$, выполнено $uwv \in W(X)$.

Определение 11. Символическая система X *синхронизована*, если она транзитивна и в ее языке есть волшебное слово.

Укажем соотношение между классами марковских, софических и синхронизованных систем.

Замечание 3. Любая марковская система софична. Любая софическая система имеет волшебное слово, в частности, любая транзитивная софическая система синхронизована (см. [10]). Далее софиком будем называть только транзитивный софик.

§ 3. Мотивационная часть и предварительные результаты

Пусть $M(X)$ – некоторый подкласс класса борелевских вероятностных инвариантных эргодических мер на символической динамической системе (X, T) (весь этот класс будем обозначать $M_0(X)$). Во всех случаях, когда из контекста будет ясно, что такое X, будем писать просто M и M_0.

Связь между энтропией и ЛСДГ в разных системах может быть различной и формально выражаться одним из следующих утверждений:

Точечная гипотеза (ТГ). $P_{X,T,\mu}(x) = h(\mu, X, T)$ *для всех* $\mu \in M(X)$, *любой медленной функции* $n(\varepsilon)$, *любого* $x \in X$.

Обобщенная точечная гипотеза (ОТГ). $P_{X,T,\mu}(x) = h(\mu, X, T)$ *для всех* $\mu \in M(X)$, *любой медленной функции* $n(\varepsilon)$, μ*-почти любого* $x \in X$.

Основная гипотеза (ОГ). $P_{X,T,\mu}(x) = h(\mu, X, T)$ *для всех* $\mu \in M(X)$ *и любой медленной функции* $n(\varepsilon)$, *где выражение в левой части понимается как предел в* $L_1(X, \mu)$.

Замечание 4. Далее, если один из перечисленных видов сходимости имеет место для конкретной меры, то будим говорить, что соответствующая гипотеза верна для этой меры и отвечающей ей измеримой системы.

ТГ очевидным образом влечет ОТГ и ОГ, при этом ОТГ и ОГ друг из друга, вообще говоря, не вытекают и не влекут ТГ.

Точечная и обобщенная точечная гипотезы верны для многих важных систем (ТГ, например, выполняется для автоморфизмов тора с мерой Лебега, а утверждения, близкие к ОТГ, верны для существенно более общих диффеоморфизмов Аносова с мерой Синая – Рюэлля – Боуэна, подробнее см. [6]), но, как показано в [1], эти гипотезы неверны даже для класса бернуллиевских мер на полном сдвиге (контрпримером может служить любая несимметричная бернуллиевская мера при достаточно медленном росте функции $n(\varepsilon)$).

Основная гипотеза, в отличие от двух других, подтверждается для многих символических систем. Базовый результат в этом направлении получен в [5].

Определение 12. Будем говорить, что мера $\mu \in M_0(X)$ на синхронизованной системе X удовлетворяет *условию Комеча*, если существует волшебное слово w, такое что $\mu(w) > 0$.

Основная теорема (ОТ). *Пусть символическая динамическая система (X,T) синхронизована, и пусть борелевская T-инвариантная эргодическая вероятностная мера μ на X удовлетворяет условию Комеча, тогда для (X,μ,T) верна основная гипотеза.*

В [1] условие Комеча ослаблено и получено более сильное утверждение.

Обобщенная основная теорема (ООТ). *Пусть символическая динамическая система (X,T) и борелевская T-инвариантная эргодическая вероятностная мера μ на X удовлетворяют следующему условию: в X имеется синхронизованный подсдвиг L (T-инвариантное замкнутое подмножество) полной меры, обладающий хотя бы одним волшебным словом положительной меры. Тогда для (X,μ,T) верна основная гипотеза.*

Отступление (теорема наследования). Свойство, позволяющее перейти от ОТ к ООТ, можно сформулировать в общем виде, в котором оно верно для произвольной символической системы. Оказывается, что равенство энтропии и ЛСДГ наследуется большей системой от меньшей.

Теорема 1. *Пусть (X,T,μ_X) и (Y,T,μ_Y) – измеримые символические системы над алфавитом A, причем $X\subseteq Y$ и мера $\mu_Y\in M_0$ индуцирована мерой $\mu_X\in M_0$, т.е. $\mu_Y(B)=\mu_X(B\cap X)$ для любого борелевского $B\in 2^Y$. Тогда, если в системе (X,T,μ_X) ЛСДГ и энтропия равны (в смысле ОГ), то они равны и в (Y,T,μ_Y).*

Доказательство. Рассмотрим также систему $(A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}})$, где $\mu_{A^{\mathbb{Z}}}$ – индуцированная μ_X мера:

$$\mu_{A^{\mathbb{Z}}}(B)=\mu_X(B\cap X)$$

для любого борелевского $B\subseteq A^{\mathbb{Z}}$. Очевидно, все три рассматриваемые системы метрически изоморфны (изоморфизм – тождественное отображение), а значит, их метрические энтропии равны:

$$h(\mu_{A^{\mathbb{Z}}},A^{\mathbb{Z}},T)=h(\mu_Y,Y,T)=h(\mu_X,X,T):=h.$$

Понятно, что для любого $\varepsilon>0$ ε-ЛСДГ в каждой точке не убывает при индуцировании меры на большее множество (см. доказательство теоремы 1 в [1]), т.е. для любого $x\in X$

$$P^{\varepsilon}_{X,T,\mu_X}(x)\leqslant P^{\varepsilon}_{Y,T,\mu_Y}(x)\leqslant P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}(x).$$

Кроме того, $P^{\varepsilon}_{X,T,\mu_X}$ сходится в среднем к h по условию теоремы, а $P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}$ сходится в среднем к h по ОТ (любая мера из M_0 на полном сдвиге удовлетворяет ОТ). С учетом этого такая же сходимость для $P^{\varepsilon}_{Y,T,\mu_Y}$ непосредственно следует из теоремы о пределе промежуточной функции. Более подробно, зафиксируем $\delta>0$ и найдем такое $\varepsilon_0>0$, что для любого положительного $\varepsilon\leqslant\varepsilon_0$ выполнено

$$\|P^{\varepsilon}_{X,T,\mu_X}-h\|_{L_1}<\delta/2\quad\text{и}\quad\|P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}-h\|_{L_1}<\delta/2.$$

Для каждого такого ε рассмотрим два измеримых множества

$$E^{\varepsilon}_{-}=\{x\in X:\ P^{\varepsilon}_{Y,T,\mu_Y}(x)\leqslant h\}\quad\text{и}\quad E^{\varepsilon}_{+}=\{x\in X:\ P^{\varepsilon}_{Y,T,\mu_Y}(x)>h\}.$$

Очевидно, что

$$Y=E^{\varepsilon}_{-}\sqcup E^{\varepsilon}_{+}\sqcup Y\setminus X,$$

причем $\mu_Y(Y \setminus X) = 0$, тогда

$$\|P^{\varepsilon}_{Y,T,\mu_Y} - h\|_{L_1} = \int\limits_{E^{\varepsilon}_{+}} |P^{\varepsilon}_{Y,T,\mu_Y}(x) - h| + \int\limits_{E^{\varepsilon}_{-}} |P^{\varepsilon}_{Y,T,\mu_Y}(x) - h| =$$

$$= \int\limits_{E^{\varepsilon}_{+}} (P^{\varepsilon}_{Y,T,\mu_Y}(x) - h) + \int\limits_{E^{\varepsilon}_{-}} (h - P^{\varepsilon}_{Y,T,\mu_Y}(x)) \leqslant \int\limits_{E^{\varepsilon}_{+}} (P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}(x) - h) +$$

$$+ \int\limits_{E^{\varepsilon}_{-}} (h - P^{\varepsilon}_{X,T,\mu_X}(x)) = \int\limits_{E^{\varepsilon}_{+}} |P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}(x) - h| + \int\limits_{E^{\varepsilon}_{-}} |h - P^{\varepsilon}_{X,T,\mu_X}(x)| \leqslant$$

$$\leqslant \int\limits_{A^{\mathbb{Z}}} |P^{\varepsilon}_{A^{\mathbb{Z}},T,\mu_{A^{\mathbb{Z}}}}(x) - h| + \int\limits_{X} |h - P^{\varepsilon}_{X,T,\mu_X}(x)| < \delta.$$

Таким образом, для любого положительного $\varepsilon \leqslant \varepsilon_0$ выполнено

$$\|P^{\varepsilon}_{Y,T,\mu_Y} - h\|_{L_1} < \delta,$$

т.е. $P^{\varepsilon}_{Y,T,\mu_Y}$ сходится в среднем к h, что и требовалось. ▲

Возникает естественный вопрос: возможно ли полностью избавиться от условия Комеча и получить результат для любой меры из M_0:

a) для всего класса синхронизованных систем?

b) сузив рассмотрение на некоторый подкласс, если ответ на a) отрицателен или неясен?

В этом параграфе будет показано, что синхронизованность в общем случае не несет никакой информации об энтропии и ЛСДГ, что исключает получение ответа на вопрос a) на основании собственных свойств класса синхронизованных систем, делает саму постановку первого вопроса бесперспективной и показывает логичность перехода к вопросу b). Вопрос b) будет рассмотрен в § 4.

Сначала введем необходимые определения.

Определение 13. Пусть X – синхронизованная система. Множество

$$dX = \{x \in X : \text{любое подслово } x \text{ не волшебное}\}$$

будем называть *производным пространством* X, а множество $S(X) = X \setminus dX$ – *синхронизующей частью* X.

Несложно понять, что dX – символическая система, а $S(X)$ – T-инвариантное (но не обязательно замкнутое) множество.

Определение 14. Меру μ на синхронизованной системе X будем называть *синхронизованной*, если $\mu(S(X)) = 1$.

Определение 15. Синхронизованную систему X будем называть *синхронизованной первообразной* символической системы Y, если $Y = dX$.

Теорема 2. *Любая транзитивная несинхронизованная система имеет синхронизованную первообразную.*

Доказательство. Пусть $Y \subset A^{\mathbb{Z}}$ – транзитивная несинхронизованная система, т.е. язык $W(Y)$ не содержит волшебных слов. Введем "разделитель" – новый символ $\{|\}$, не принадлежащий A, и определим систему X ее языком $W(X)$. Язык $W(X)$ над алфавитом $A \cup \{|\}$ построим следующим образом: $w \in W(X)$ тогда и только тогда, когда оно пусто или имеет вид

$$|^{k_0} w_1 |^{k_1} w_2 |^{k_2} w_3 |^{k_3} \ldots . w_n |^{k_n},$$

где

$$n, k_1, \ldots, k_{n-1} \in \mathbb{N}, \quad k_0, k_n \in \mathbb{N} \cup \{0\}, \quad w_1, w_2, \ldots, w_n \in W(Y).$$

Таким образом, $W(X)$ состоит из всех слов $W(Y)$ и любых их конечных последовательностей, разделенных одним или несколькими разделителями. Нетрудно понять, что $W(X)$ действительно язык, так как он продолжаем и факторизуем (см. [11, предложение 1.3.4]). Система X транзитивна, так как любые два слова из $W(X)$ можно написать через разделитель ($u, v \in W(x)$, тогда $u\,|\,v \in W(X)$), и транзитивность следует из замечания 1. Более того, система X синхронизована, так как разделитель является волшебным словом по построению (а значит, и любые слова, его содержащие).

С другой стороны, любые слова, не содержащие разделитель, неволшебные. Действительно, пусть $w \in W(X)$ и w не содержит символа $|$, тогда по построению $w \in W(Y)$, но Y по условию не содержит волшебных слов, а значит, w неволшебно в Y, т.е. для некоторых $u, v \in W(Y)$, таких что $uw, wv \in W(Y)$, слово $uvw \notin W(Y)$. При этом uvw, очевидно, не содержит разделителей, а значит, не является и словом языка $W(X)$. С учетом того, что $W(Y) \subseteq W(X)$, получаем, что $uw, wv \in W(X)$, но $uvw \notin W(X)$, т.е. w неволшебно в X. Таким образом, волшебные слова в X – это в точности те, что содержат разделитель. Отсюда непосредственно следует $dX = Y$, т.е. X – искомая синхронизованная первообразная Y. ▲

Теорема 3. *Для любой измеримой транзитивной символической системы существует измеримая синхронизованная система с той же энтропией и ЛСДГ.*

Доказательство. Если система синхронизована, то искомой является она сама. Если же она не синхронизована, то искомой является ее синхронизованная первообразная с перенесенной на нее мерой исходной системы. Действительно, пусть (Y, T, μ_Y) – исходная система, (X, T) – ее синхронизованная первообразная. Определим меру на X следующим образом:

$$\mu_X(A) = \mu_Y(A \cap Y)$$

для любого борелевского множества A. Очевидно, что (Y, T, μ_Y) и (X, T, μ_X) метрически изоморфны, а значит,

$$h(\mu_Y, Y, T) = h(\mu_X, X, T).$$

Рассмотрим теперь ε-ЛСДГ этих систем и покажем их равенство для фиксированного ε и $x \in Y$. Так как

$$\mu_X\big(O_\varepsilon^X(x)\big) = \mu_Y\big(O_\varepsilon^X(x) \cap Y\big) = \mu_Y\big(O_\varepsilon^Y(x)\big),$$

то достаточно показать, что

$$O_1 := O_\varepsilon^X\big(T^{n(\varepsilon)}\big(O_\varepsilon^X(x)\big)\big) \cap Y$$

и

$$O_2 := O_\varepsilon^Y\big(T^{n(\varepsilon)}\big(O_\varepsilon^Y(x)\big)\big)$$

совпадают. Включение $O_2 \subseteq O_1$ очевидно. Пусть $y \in O_1$, тогда существует $z \in \in O_\varepsilon^X(x)$, такое что

$$(T^{n(\varepsilon)}(z))_{[-k;k]} = y_{[-k;k]},$$

т.е.

$$z_{[-k-n;k-n]} = y_{[-k;k]}. \tag{1}$$

Кроме того,

$$z_{[-k;k]} = x_{[-k;k]}. \tag{2}$$

Так как $x, y \in Y$, то из (1), (2) получаем

$$z_{[-k;k]}, z_{[-k-n;k-n]} \in W(Y),$$

т.е. эти слова не содержат разделителей, но тогда и $z_{[-k-n;k]} \in W(X)$ их не содержит, т.е. $z_{[-k-n;k]} \in W(Y)$, а значит, существует $w \in Y$, такое что

$$z_{[-k-n;k]} = w_{[-k-n;k]}. \tag{3}$$

Из (1)–(3) получаем $w \in O_\varepsilon^Y(x)$ и

$$(T^{n(\varepsilon)}(w))_{[-k;k]} = y_{[-k;k]},$$

что и означает $y \in O_2$. Таким образом, $O_1 \subseteq O_2$, т.е. $O_1 = O_2$, что влечет равенство числителей выражений под логарифмом ε-ЛСДГ, и по отмеченному выше – самих ε-ЛСДГ. Итак,

$$P^\varepsilon_{X,T,\mu_X}(x) = P^\varepsilon_{Y,T,\mu_Y}(x)$$

для любого $x \in Y$, а значит, для μ_X-почти любого $x \in X$, т.е.

$$P^\varepsilon_{X,T,\mu_X} = P^\varepsilon_{Y,T,\mu_Y}$$

в $L_1(X, \mu_x)$, а значит, ЛСДГ, как пределы в среднем этих функций, совпадают (в том числе существуют и не существуют одновременно). Таким образом, у систем X и Y совпадают энтропии и ЛСДГ. ▲

Теорема 2 означает, что если не налагать на измеримые синхронизованные системы никаких дополнительных ограничений, то некоторые такие системы (синхронизованные первообразные транзитивных несинхронизованных систем) окажутся синхронизованными лишь формально, и с точки зрения интересующих нас величин будут полностью эквивалентны своим несинхронизованным производным, причем производные могут быть любыми несинхронизованными транзитивными системами. Таким образом, для получения какого-либо результата, основанного на синхронизованности системы, нужно исключить из рассмотрения, как минимум, синхронизованные первообразные транзитивных несинхронизованных систем.

§ 4. Теория производных пространств Томсена и геометрическая интерпретация энтропии софических систем

Несмотря на то что рассуждения предыдущего параграфа показывают невозможность использования свойства синхронизованности без наложения дополнительных условий на меру в общем случае, эти рассуждения не исключают возможности применения данного свойства без дополнительных ограничений на меру в некотором подклассе (не содержащем “плохих” систем, описанных выше). В этом параграфе будет предложен подход, который позволяет обойти условие Комеча и дает полное решение вопроса, как минимум, для софических систем.

Сначала изложим идею подхода неформально. Пусть имеется измеримая синхронизованная система. Если в ней есть волшебное слово положительной меры, то применяем ОТ, и задача решена. Если же все волшебные слова имеют нулевую меру, то логично избавиться от всех элементов системы, содержащих волшебные слова, т.е. от синхронизующей части, и рассмотреть получившуюся после этого систему

(производное пространство) полной меры. Если она удовлетворяет условию Комеча, то применима ООТ и задача решена, если же нет, то избавиться от волшебных слов новой системы и снова перейти к производному пространству и продолжать так далее, пока не получим систему, в которой имеется хотя бы одно волшебное слово положительной меры.

При реализации данного алгоритма могут возникнуть следующие очевидные проблемы:

1) Система, получившаяся на очередном шаге, не имеет волшебных слов;
2) На каждом шаге система имеет волшебные слова, но не удовлетворяет условию Комеча, т.е. процесс никогда не завершится.

В реальности ситуация оказывается еще более сложной, так как на некотором шаге мы можем получить не транзитивную систему, которая даже при наличии волшебных слов не будет синхронизованной. Тем не менее К. Томсену в [9] (при изучении вопросов, не связанных с геометрической интерпретацией энтропии) удалось построить теорию, реализующую приведенную выше идею.

Суть метода Томсена состоит в следующем: оказывается, что все вышеописанные проблемы реализации алгоритма могут быть сформулированы в терминах сосредоточения меры на некоторых "плохих" частях системы. В частности, проблемы 1) и 2) вызваны тем, что мера сосредоточена на пересечении производных пространств всех уровней (производные пространства высших уровней определяются рекурсивным применением определения 13 с некоторой предварительной регуляризацией в нетранзитивном случае, см. ниже), которое далее обозначено через $d^\infty X$ (в первом случае это пересечение совпадает со всеми производными пространствами достаточно высокого уровня, во втором – является собственным подмножеством любого из них). Обозначенная в предыдущем абзаце проблема нетранзитивности стандартно решается выделением транзитивных компонент ($\overline{X_c}$), причем по построению эти компоненты автоматически оказываются синхронизованными системами. Предварительно на каждом шаге производится регуляризация – удаление из рассмотрения "плохой" (апериодической) части системы, которая не может быть отнесена ни к одной компоненте, после чего рассматриваемая система оказывается (с некоторыми нюансами) дизъюнктным объединением синхронизующих частей компонент $\overline{X_c}$ (на самом деле некоторых подмножеств $\widetilde{X}_c$ синхронизующих частей) и производного пространства следующего уровня.

Таким образом, следуя алгоритму, мы фактически разбиваем исследуемую синхронизованную систему на (возможно, пустой) неанализируемый центр $d^\infty X$ и не более чем счетное количество слоев, каждый из которых, в свою очередь, разбивается на не более чем счетное число инвариантных компонент $\widetilde{X}_c$ и "плохую" апериодическую часть (см. разложение (7)). Ключевым оказывается тот факт, что все вышеописанные "плохие" (не поддающиеся анализу) части оказываются подмножествами некоторого подсдвига $d_M X$, который имеет удобное для наших целей комбинаторное описание и вырождается в софическом случае, что позволяет получить достаточно сильные результаты без исследования этих частей.

Теперь перейдем к формальному изложению. Начнем с основных определений. Пусть X – произвольная символическая система. Пусть $\mathrm{Per}(X)$ – множество ее периодических точек, а $R(X)$ – замыкание этого множества. Через $\mathrm{Rec}(X)$ обозначим множество бирекуррентных точек в X, т.е. множество таких $x \in X$, что для любого натурального n множество

$$\{i : x_{[i;i+2n]} = x_{[-n;n]}\}$$

не ограничено ни сверху, ни снизу. Понятно, что множества $R(X)$ и $\mathrm{Rec}(X)$ являются T-инвариантными, более того, $R(X)$ – подсдвиг. По теореме Пуанкаре о возвращении $\mu(\mathrm{Rec}(X)) = 1$ для любой инвариантной меры.

Введем понятия марковской границы и производного пространства.

Определение 16. Введем множество

$$W_\infty(X) = \{w \in W(X) : \text{ образ функции } P_w(\cdot) \text{ бесконечен}\}.$$

Это множество является языком (см. [9]), а значит, определяет некоторый подсдвиг $d_M X \subseteq X$, который назовем *марковской границей* X.

Замечание 5. Из замечания 2 понятно, что марковская граница пуста тогда и только тогда, когда X – софик. Кроме того, в [9] показано, что $d_M X \neq X$ тогда и только тогда, когда X синхронизована.

Определение 17. Множество

$$dX = \{x \in R(X) : x \text{ не содержит волшебных слов } R(X) \text{ в качестве подслов}\}$$

будем называть *производным пространством* X.

Замечание 6. Для синхронизованных систем X известно (см. [12]), что $R(X) = X$, а значит, определение 15 обобщает определение 12 на произвольные символические системы.

Несложно видеть, что dX – подсдвиг, а значит, для него тоже определено производное пространство, которое логично назвать вторым производным пространством X.

Определение 18. Для любого $k \in \mathbb{N}$ индуктивно определим

$$d^0 X = X, \quad d^k X = d(d^{k-1} X),$$

а также положим

$$d^\infty X = \bigcap_{k=0}^{\infty} d^k X.$$

Число k будем называть *уровнем* производного пространства $d^k X$, а величину

$$\mathrm{dp}(X) = \sup\{k : d^k X \neq \varnothing\}$$

– *глубиной* системы X.

Наша цель – получить разложение X на не более чем счетное число компонент, одна из которых – марковская граница, а остальные имеют подходящую для наших целей структуру. Из определения производных пространств понятно, что выполнено равенство

$$X = \bigsqcup_{k=0}^{\infty} (d^k X \setminus d^{k+1} X) \sqcup d^\infty X. \tag{4}$$

В [9] показано, что

$$d^\infty X \subseteq d_M X, \tag{5}$$

а "апериодические" части производных пространств $d^k X \setminus R(d^k X)$ лежат в марковской границе mod 0, т.е.

$$\mu\big(d^k X \setminus R(d^k X) \setminus d_M X\big) = 0 \tag{6}$$

для любой T-инвариантной меры μ. Теперь для фиксированного целого неотрицательного k рассмотрим

$$S_k(X) := R(d^k X) \setminus d^{k+1} X.$$

Из определения видно, что $S_k(X)$ содержится в замыкании своих периодических точек и что любая точка $S_k(X)$ содержит некоторое волшебное слово $R(d^kX)$ как подслово. Эти свойства позволяют покрыть $S_k(X)$ счетным множеством синхронизованных систем.

Определим отношение $\sim$ на множестве V_k волшебных слов $R(d^kX)$ следующим образом: $u \sim v$ тогда и только тогда, когда найдутся такие $x, y \in W(R(d^kX))$, что $uxv, vyu \in W(R(d^kX))$. Из плотности множества периодических точек в $R(X)$ следует, что отношение $\sim$ рефлексивно, симметричность очевидна, а транзитивность обеспечивается волшебностью рассматриваемых слов. Таким образом, $\sim$ является отношением эквивалентности. Положим $C_k = V_k/\sim$. Для каждого класса эквивалентности $c \in C_k$ определим

$$X_c = \Big\{x \in R(d^kX) : \sup_{i\in\mathbb{Z}} \inf(j - i > 0 : \ x_{[i;j]} \in c) < \infty\Big\},$$

т.е. X_c – это множество элементов $R(d^kX)$, содержащих волшебные слова из класса c с ограниченными промежутками между ними. Множества X_c – инвариантные подмножества S_k, но не обязательно замкнутые. Легко видеть, что каждая периодическая точка $y \in S_k(X)$ лежит в некотором X_c, а значит, объединение всех X_c плотно в $S_k(X)$.

Рассмотрим замыкание $\overline{X_c}$ – это символическая система, которая транзитивна (любое слово его языка является подсловом некоторого элемента из X_c и поэтому является частью некоторого волшебного слова из класса c, а эти волшебные слова отвечают критерию транзитивности из замечания 1 по построению отношения $\sim$), а слова из c являются ее волшебными словами. Таким образом, $\overline{X_c}$ – синхронизованная система. Более того, из плотности объединения X_c следует, что

$$\bigcup_{c\in C_k} \overline{X_c} \supseteq S_k(X).$$

При этом ни X_c, ни $\overline{X_c}$ не подходят для разбиения $S_k(X)$. Множества X_c совокупно плотны в $S_k(X)$, но их объединение может быть "мало" с точки зрения меры, а $\overline{X_c}$ образуют покрытие $S_k(X)$ синхронизованными системами, но не обязательно лежат в $S_k(X)$ и могут пересекаться; более того, с точки зрения основного вопроса этой статьи для меры $\mu \in M_0(X)$, сосредоточенной на $\overline{X_c}$, не гарантируется выполнение условия Комеча в $\overline{X_c}$. Поэтому введем более подходящие T-инвариантные множества $\widetilde{X}_c$.

Пусть C_v – множество точек в X, содержащих слово $v \in W(X)$. Положим

$$\widetilde{X}_c = \bigcup_{v\in c} \mathrm{Rec}(\overline{X_c} \cap C_v)$$

(напомним, что c обозначает класс эквивалентности волшебных слов). Легко видеть, что различные $\widetilde{X}_c$ не пересекаются (иначе получаем эквивалентность элементов из различных классов C_k), а также что $\widetilde{X}_c \subseteq S_k(X)$ для любого $c \in C_k$. Более того, в [9] показано, что $\widetilde{X}_c$ покрывают все рекуррентные точки $S_k(X)$, а значит, по теореме Пуанкаре о возвращении и все $S_k(X)$, кроме некоторого множества M_k, такого что $\mu(M_k) = 0$ для любой T-инвариантной меры μ. Таким образом, множества

$$\{\widetilde{X}_c,\ c \in C_k\}$$

образуют mod 0 разбиение $S_k(X)$. Отсюда с учетом (4)–(6), обозначив множества из равенства (6) через I_k, а $M_k \setminus d_M X$ – через N_k, получаем, что

$$[b]X = \bigsqcup_{k=0}^{\infty} (d^k X \setminus d^{k+1} X) \sqcup d^\infty X =$$
$$= \bigsqcup_{k=0}^{\infty} \Big(\big(d^k X \setminus R(d^k X)\big) \sqcup \big(R(d^k X) \setminus d^{k+1} X\big) \Big) \sqcup d^\infty X =$$
$$= d_M X \bigsqcup_{k=0}^{\infty} \left(\bigsqcup_{c \in C_k} (\widetilde{X}_c \setminus d_M X) \sqcup N_k \sqcup I_k \right) = d_M X \sqcup \bigsqcup_{c \in C} (\widetilde{X}_c \setminus d_M X) \sqcup N, \qquad (7)$$

где

$$C = \bigsqcup_{k=0}^{\mathrm{dp}(X)} C_k,$$

а множество

$$N = \bigsqcup_{k=0}^{\infty} (N_k \sqcup I_k)$$

имеет меру ноль для любой T-инвариантной меры.

Разложение (7) дает возможность сформулировать достаточное условие выполнения ОГ в терминах марковской границы.

Теорема 4. *Пусть X – синхронизованная система, и пусть $\mu \in M_0(X)$ сосредоточена вне марковской границы X (т.е. $\mu(d_M X) = 0$), тогда в (X, T, μ) имеет место сходимость в среднем ε-ЛСДГ к энтропии.*

Доказательство. Из разложения (7) и эргодичности ясно, что мера ровно одного множества из $\widetilde{X}_c$ и $d_M X$ равна 1, а мера остальных 0. По условию мера марковской границы нулевая, а значит, существует $c \in C$, такое что $\mu(\widetilde{X}_c) = 1$. Из определения $\widetilde{X}_c$ получаем, что это множество лежит в

$$A_c := \bigcup_{v \in c} C_v = \bigcup_{v \in c} \bigcup_{i \in \mathbb{Z}} \{v\}_i,$$

значит, $\mu(A_c) = 1$. Если мера всех цилиндров $\{v\}_i$ равна нулю, то $\mu(A_c) = 0$ – противоречие, т.е. существуют $i \in \mathbb{Z}$ и $v \in c$, такие что $\mu(\{v\}_i) > 0$, т.е. $\mu(v) > 0$. Таким образом, μ отвечает условию Комеча на $\overline{X_c}$, и применяя ООТ, мы получаем желаемое. ▲

Замечание 7. Теорема 3 тривиально верна и для несинхронизованных систем (вся система является своей марковской границей, и множество рассматриваемых мер пусто).

Замечание 8. Так как для волшебных слов w системы X образ функции $P_w(\cdot)$ одноточечен, любое такое слово лежит вне языка марковской границы, а значит, условие Комеча (в смысле ОТ) влечет неполномерность марковской границы и по эргодичности ее нулевую меру. Таким образом, теорема 3 влечет ОТ и, как показывают нижеследующее следствие и финальная ремарка, сильнее ОТ. С другой стороны, теорема 3 слабее ООТ, следствием которой является (так как ООТ дает нетривиальные результаты и для несинхронизованных систем, см. [1]), но в отличие от ООТ теорема 3 задает условия выполнения ОГ явно.

Следствие (геометрическая интерпретация энтропии софических систем). *Пусть X – софическая система и $\mu \in M_0(X)$, тогда в (X, T, μ) справедлива ОГ без каких-либо дополнительных условий.*

Доказательство. По замечанию 3 марковская граница X пуста (кроме того, глубина X и мощность множества C конечны, см. [12]), а значит, условия теоремы 3 выполнены автоматически. ▲

Финальная ремарка (нетривиальность главного результата). У читателя может возникнуть подозрение, что главный заявленный результат данной статьи тривиален в том смысле, что в софическом случае любая мера из M_0 автоматически отвечает условию Комеча на всей системе. Именно так происходит в более узком марковском случае (см. [4]). Тем не менее с помощью теории Томсена легко показать, что в случае немарковских софиков дело обстоит иначе. Действительно, для того чтобы мера из класса M_0 не отвечала условию Комеча на синхронизованной системе X, очевидно, достаточно (и необходимо), чтобы эта мера была сосредоточена на dX. С другой стороны, в [12] показано, что (транзитивный) софик имеет нулевую глубину тогда и только тогда, когда он является марковской системой, т.е. у любого немарковского софика X производное пространство dX непусто, и любая мера, сосредоточенная на нем, не будет удовлетворять условию Комеча. Существование такой меры гарантируется теоремой Крылова – Боголюбова. В качестве конкретных примеров можно взять построенные Томсеном софические системы любой конечной глубины [12, замечание 6.12].

Таким образом, главный результат данной статьи нетривиален.

Автор благодарен своему научному руководителю Б.М. Гуревичу за постановку задачи геометрической интерпретации энтропии и дальнейшее содействие в научном поиске. К сожалению, за несколько месяцев до публикации Бориса Марковича не стало, поэтому статья посвящается его памяти.

Также автор благодарит С.А. Комеча за плодотворное обсуждение вопроса и полезные комментарии, М. Гайсинского за ценные советы на финальном этапе подготовки статьи и фонд “Базис” за поддержку данной работы.

Отдельно хотелось бы поблагодарить Ефима Наумовича Малкина за многолетнюю поддержку интереса автора к научной деятельности, которая сыграла важную роль в появлении этой и двух предыдущих публикаций.

СПИСОК ЛИТЕРАТУРЫ

1. *Дворкин Г.Д.* Геометрическая интерпретация энтропии: новые результаты // Пробл. передачи информ. 2021. Т. 57. № 3. С. 90–101. https://doi.org/10.31857/S0555292321030062
2. *Дворкин Г.Д.* Геометрическая интерпретация энтропии для систем Дика // Пробл. передачи информ. 2022. Т. 58. № 2. С. 41–47. https://www.mathnet.ru/ppi2367
3. *Заславский Г.М.* Стохастичность динамических систем. М.: Наука, 1984.
4. *Gurevich B.M.* Geometric Interpretation of Entropy for Random Processes // Sinai's Moscow Seminar on Dynamical Systems. Providence, RI: Amer. Math. Soc., 1996. P. 81–87.
5. *Комеч С.А.* Скорость искажения границы в синхронизованных системах: геометрический смысл энтропии // Пробл. передачи информ. 2012. Т. 48. № 1. С. 15–25. http://mi.mathnet.ru/ppi2065
6. *Гуревич Б.М., Комеч С.А.* Скорость деформации границ в системах Аносова и близких к ним // Тр. МИАН. 2017. Т. 297. С. 211–223. https://doi.org/10.1134/S037196851702011X
7. *Синай Я.Г.* О понятии энтропии динамической системы // ДАН СССР. 1959. Т. 124. С. 768–771.
8. *Корнфельд И.П., Синай Я.Г., Фомин С.В.* Эргодическая теория. М.: Наука, 1980.

9. *Thomsen K.* On the Ergodic Theory of Synchronized Systems // Ergodic Theory Dynam. Systems. 2006. V. 26. № 4. P. 1235–1256. https://doi.org/10.1017/S0143385706000290
10. *Fiebig D., Fiebig U.-R.* Covers for Coded Systems // Symbolic Dynamics and Its Applications (New Haven, CT, 1991). Contemp. Math. V. 135. Providence, RI: Amer. Math. Soc., 1992. P. 139–180.
11. *Lind D., Marcus B.* An Introduction to Symbolic Dynamics and Coding. Cambridge: Cambridge Univ. Press, 1995.
12. *Thomsen K.* On the Structure of a Sofic Shift Space // Trans. Amer. Math. Soc. 2004. V. 356. № 9. P. 3557–3619. https://doi.org/10.1090/S0002-9947-04-03437-3

Дворкин Григорий Дмитриевич
Московский государственный университет
им. М.В. Ломоносова, механико-математический факультет,
кафедра математической статистики и случайных процессов
grisha230531415@gmail.com

Поступила в редакцию
10.04.2023
После доработки
18.07.2023
Принята к публикации
24.07.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 519.218.5

© 2023 г. **Е.А. Жижина, С.А. Пирогов**

ИНВАРИАНТНЫЕ МЕРЫ ДЛЯ ПРОЦЕССОВ КОНТАКТОВ С ИНТЕНСИВНОСТЯМИ РОЖДЕНИЯ И ГИБЕЛИ, ЗАВИСЯЩИМИ ОТ СОСТОЯНИЯ

Рассматриваются процессы контактов на локально компактных сепарабельных метрических пространствах с неоднородными по пространству интенсивностями рождения и гибели. Формулируются условия на интенсивности, обеспечивающие существование инвариантных мер этих процессов. Одним из условий является так называемое условие критического режима. Для доказательства существования инвариантных мер использован подход, предложенный в предыдущей работе авторов. Подробно рассматривается маркированная модель контактов с компактным пространством марок (квазивидов), в которой интенсивности как рождения, так и гибели зависят от марок.

Ключевые слова: маркированная модель контактов в непрерывном пространстве, процесс рождения и гибели в непрерывной среде, критический режим, корреляционные функции.

DOI: 10.31857/S0555292323020055, **EDN:** PQGTBP

Посвящается Вадиму Александровичу Малышеву, выдающемуся математику, ясно видевшему математику в биологии

§ 1. Введение

Процессы контактов широко используются для описания эволюции и предсказания асимптотического поведения в различных моделях популяционной динамики. Учитывая применение процессов контактов при моделировании распространения эпидемических заболеваний или роста популяций, одной из основных задач при рассмотрении этих процессов является вопрос о существовании стационарного режима и доказательство существования инвариантных мер. Процессы контактов на решетке были введены в пионерских работах [1, 2]; см. также монографию [3]. Хотя в большинстве работ процессы контактов рассматривались на решетке, в последние годы все больший интерес вызывает изучение процессов контактов, протекающих в непрерывных пространствах (см., например, [4–6]). Этот класс процессов является частным случаем процессов рождения и гибели с непрерывным временем. Одной из основных особенностей процесса контактов является кластеризация системы, когда частицы группируются в облака высокой плотности, которые расположены на больших расстояниях друг от друга. Следует отметить, что возникновение предельного инвариантного состояния обычно рассматривается в так называемом критическом режиме, т.е. при определенном балансе между рождением и гибелью. Как было показано в [4], для процессов контактов в $\mathbb{R}^d$, $d \geqslant 3$, существует континуум инвариантных мер в критическом режиме с постоянными интенсивностями гибели. Явление кластеризации становится более заметным в случае малых размерностей.

В [5] было доказано, что для процессов контактов в $\mathbb{R}^d$, $d = 1, 2$, инвариантные меры существуют только в том случае, если ядро рассеяния (интенсивность рождения) имеет тяжелый хвост на бесконечности. В случае легких хвостов парная корреляционная функция неограниченно возрастает при $t \to \infty$, и следовательно, инвариантные меры не существуют. Таким образом, оказывается, что тяжелые хвосты ядер рассеивания, в отличие от легких, делают критический режим более устойчивым.

В [7] доказано существование инвариантных мер в маркированной модели контактов в $\mathbb{R}^d$, $d \geqslant 3$, с компактным пространством марок при постоянных интенсивностях гибели. Аналогичная модель с иммиграцией изучена в [8]. Такие модели используются, в частности, для описания эволюции в квазивидовых популяциях с мутациями (см. [9]).

В настоящей статье рассматривается класс процессов контактов на локально компактных сепарабельных метрических пространствах в критическом режиме с интенсивностями рождения и гибели, зависящими от состояния. Эта статья является обобщением нашей предыдущей работы [10], в которой были сформулированы условия, обеспечивающие существование инвариантных мер для процессов контактов на общих пространствах с однородной интенсивностью гибели. При этом инвариантные меры описываются простыми рекуррентными соотношениями между их корреляционными функциями и образуют новый класс точечных случайных полей. В этой статье мы формулируем условия, включая условие критического режима, гарантирующие существование инвариантных мер для общих процессов контактов с неоднородными интенсивностями рождения и гибели, которые зависят от состояния, и доказываем существование семейства инвариантных мер.

Наш подход основан на анализе бесконечной системы иерархических уравнений для корреляционных функций; см. например, [4, 10]. В § 2 представлена модель и сформулированы предположения на нее, в том числе условие критического режима. В § 3 формулируется основной результат. В § 4 содержится доказательство основной теоремы. В § 5 мы применяем общие результаты из §§ 2, 3 к анализу многокомпонентных моделей контактов в непрерывной среде с компактным пространством марок и интенсивностями рождения и гибели, зависящими от состояния.

§ 2. Модель

В этом параграфе мы сформулируем предположения о модели, которые обеспечивают существование инвариантных мер для процессов контактов в общих пространствах.

Пусть $\mathfrak{X}$ – локально компактное сепарабельное метрическое пространство, $\mathcal{B}(\mathfrak{X})$ – его борелевская σ-алгебра, а через m обозначим локально конечную меру Бореля на $\mathcal{B}(\mathfrak{X})$, т.е. m конечна на компактных множествах. Обозначим через $\mathcal{M}(\mathfrak{X})$ пространство локально конечных мер Бореля на $\mathcal{B}\mathfrak{X})$, а через $\mathcal{B}_{\mathrm{b}}(\mathfrak{X})$ – систему всех компактных множеств из $\mathcal{B}(\mathfrak{X})$.

Конфигурация $\gamma \in \Gamma(\mathfrak{X})$ на $\mathfrak{X}$ – это конечное или счетное локально конечное неупорядоченное множество точек в $\mathfrak{X}$, причем некоторые из точек могут быть кратными, т.е. допускаются повторения. Если мера $m \in \mathcal{M}(\mathfrak{X})$ является атомарной, то $\Gamma(\mathfrak{X})$ содержит конфигурации с кратными точками. Так будет на графах, где мера m является считающей. В качестве фазового пространства Γ непрерывной модели контактов в том случае, когда мера m неатомарна (см., например, [4–6]), можно взять множество локально конечных конфигураций в $\mathfrak{X}$ с различными элементами:

$$\Gamma_c = \Gamma_c(\mathfrak{X}) := \big\{\gamma \subset \mathfrak{X} \;\big|\; |\gamma \cap \Lambda| < \infty \text{ для всех } \Lambda \in \mathcal{B}_{\mathrm{b}}(\mathfrak{X})\big\}, \tag{1}$$

где через $|\cdot|$ обозначается число элементов множества.

Каждой конфигурации $\gamma \in \Gamma$ можно сопоставить целочисленную меру

$$\sum_{x\in\gamma} \delta_x \in \mathcal{M}(\mathfrak{X}),$$

где δ_x – мера Дирака с единичной массой, а сумма берется с учетом кратности элементов в конфигурации γ. Для любого множества $\Lambda \in \mathcal{B}_{\mathrm{b}}(\mathfrak{X})$ обозначим через $|\gamma \cap \Lambda|$ значение $\gamma(\Lambda)$ меры γ на Λ.

Модель контактов представляет собой марковский процесс с непрерывным временем на $\Gamma(\mathfrak{X})$, который является частным случаем общего процесса рождения и гибели. В данной статье рассматривается процесс с неоднородными интенсивностями рождения и гибели. Модель задается эвристическим генератором, определенным на соответствующем классе функций $F\colon \Gamma \to \mathbb{R}$ следующим образом:

$$(LF)(\gamma) = \sum_{x\in\gamma} V(x)\,(F(\gamma \setminus x) - F(\gamma)) +$$

$$+ \int_{\mathfrak{X}} \sum_{x\in\gamma} a(y,x)(F(\gamma \cup y) - F(\gamma))\, m(dy). \tag{2}$$

Обозначения $\gamma\setminus x$ и $\gamma\cup x$ в (2) означают удаление и добавление одной частицы в точке $x \in \mathfrak{X}$. Аналогично, $x \in \gamma$ означает любую частицу из конфигурации γ. Первый член в (2) соответствует гибели частицы в точке x: каждый элемент $x \in \gamma$ конфигурации $\gamma \in \Gamma$ может погибнуть с интенсивностью $V(x)$. Второй член (2) описывает рождение новой частицы в окрестности dy точки y с плотностью интенсивности рождения

$$A(y,\gamma) := \sum_{x\in\gamma} a(y,x).$$

Фактически мы даже не знаем, кто является родителем, поскольку рождение новой частицы в точке y имеет суммарную интенсивность $\sum\limits_{x\in\gamma} a(y,x)$. Функция $a(x,y)$ называется ядром рассеивания.

Одна из целей этой статьи – сформулировать условия на интенсивности в (2), гарантирующие существование инвариантных мер соответствующих процессов контактов. Решающим условием существования стационарного режима в процессе контактов, как и в других процессах рождения и гибели, является так называемое условие критического режима. Это условие описывает "стохастическое равновесие между рождением и гибелью".

В случае $V(x) \equiv 1$, т.е. когда интенсивность гибели постоянна, условие критического режима имеет вид

$$\int_{\mathfrak{X}} a(x,y)\Psi(y)\, m(dy) = \Psi(x) \quad \text{для всех } x \in \mathfrak{X}, \tag{3}$$

где $\Psi(x)$ – строго положительная ограниченная измеримая функция. Модели с условием критического режима в виде (3) изучались и ранее – см., например, [4, 10]. В [4] рассматривалась контактная модель в непрерывной среде с

$$\mathfrak{X} = \mathbb{R}^d, \quad a(x,y) = \alpha(x-y), \quad V(x) \equiv 1,$$

и для этой модели $\Psi(x) \equiv 1$. Более общий случай, когда $\mathfrak{X} = \mathbb{R}^d \times S$ для компактного метрического пространства S (пространства видов), был изучен в [10]. В этом случае условие (3) выполняется для функции $\Psi(x) = q(s)$, зависящей только от марки $s \in S$. Аналогичная маркированная непрерывная модель контактов с непостоянной функцией $V(s)$, $s \in S$, будет рассмотрена далее в § 5.

В случае, когда $V(x)\colon \mathfrak{X} \to \mathbb{R}_+$ – положительная ограниченная функция, условие *критического режима* становится следующим: существует строго положительно ограниченная измеримая функция $\Psi(x)$, $\Psi(x) \geqslant p_0 > 0$, такая что

$$\int_{\mathfrak{X}} a(x,y)\Psi(y)\, m(dy) = V(x)\Psi(x) \quad \text{для всех } x \in \mathfrak{X}. \tag{4}$$

Это условие представляет собой уравнение баланса. Оно означает, что если частицы изначально распределены с плотностью $\Psi(x)$, то эта плотность сохраняется в динамике, т.е. $\Psi(x)$ – плотность стационарного распределения частиц. Обсудим новый вид (4) условия критического режима. В предположении, что условие критического режима (4) выполняется для исходного генератора (2) (т.е. для $a(x,y)$ и $m(dy)$), можно определить новую меру $\bar{\mathfrak{m}}$ и новую интенсивность рождения $b(x,y)$

$$\bar{\mathfrak{m}}(dy) = \Psi(y)\, m(dy), \quad b(x,y) = \frac{a(x,y)}{\Psi(x)}, \tag{5}$$

так что условие (4) примет вид

$$\int_{\mathfrak{X}} b(x,y)\, \bar{\mathfrak{m}}(dy) = V(x) \quad \text{для всех } x \in \mathfrak{X}. \tag{6}$$

Тогда генератор (2) принимает вид

$$(LF)(\gamma) = \sum_{x\in\gamma} V(x)\,(F(\gamma \setminus x) - F(\gamma)) + \\ + \int_{\mathfrak{X}} \sum_{x\in\gamma} b(y,x)(F(\gamma \cup y) - F(\gamma))\, \bar{\mathfrak{m}}(dy). \tag{7}$$

Следует отметить, что из формул (5) вытекает, что вторые слагаемые в правых частях уравнений (2) и (7) одинаковы.

В этой статье мы всегда будем предполагать, что условие критического режима (4) выполнено. Поэтому в дальнейшем мы будем рассматривать генератор L, заданный формулой (7), где b и V удовлетворяют условию (6).

Теперь мы готовы сформулировать условия на интенсивности рождения и гибели генератора (7). Будем предполагать, что интенсивности рождения $b(y,x)$ и гибели $V(x)$ процесса контактов удовлетворяют следующим условиям:

1. Условие *измеримости*: $b\colon \mathfrak{X}\times\mathfrak{X} \to [0,\infty)$ – неотрицательная ограниченная измеримая функция, а $V\colon \mathfrak{X} \to (0,\infty)$ – строго положительная ограниченная измеримая функция

$$0 < V_{\min} = \inf_{\mathfrak{X}} V(x) \leqslant V(x) \leqslant \sup_{\mathfrak{X}} V(x) = V_{\max} < \infty; \tag{8}$$

2. Условие *регулярности*: существует константа $C > 0$, такая что

$$\sup_{x\in\mathfrak{X}} \int_{\mathfrak{X}} b(y,x)\, \bar{\mathfrak{m}}(dy) < C; \tag{9}$$

3. Условие *критического режима*:

$$\int_{\mathfrak{X}} b(x,y)\, \bar{\mathfrak{m}}(dy) = V(x) \quad \text{для всех } x \in \mathfrak{X}; \tag{10}$$

4. Условие *транзиентности*. Рассмотрим скачкообразный марковский процесс с непрерывным временем, который задается генератором

$$\mathcal{L}f(x) = \int\limits_{\mathfrak{X}} b(x,y)(f(y)-f(x))\,\bar{\mathfrak{m}}(dy). \tag{11}$$

Будем предполагать, что для двух независимых экземпляров $X(t)$ и $Y(t)$ этого процесса, стартующих с $X(0)=x$ и $Y(0)=y$, выполнено следующее условие:

$$\sup_{x,y} \int\limits_0^\infty \mathbf{E}_{x,y}\, b(X(t),Y(t))\,dt < H \tag{12}$$

для некоторой константы $H>0$. Более того, будем предполагать, что интеграл в (12) сходится равномерно по x и y.

Непрерывный по времени скачкообразный марковский процесс с генератором (11) можно описать следующим образом: $V(x)$ – интенсивность скачка в состоянии x, а переходное распределение скачков задается следующим образом:

$$\frac{b(x,y)\,\bar{\mathfrak{m}}(dy)}{V(x)} = \frac{a(x,y)\Psi(y)\,m(dy)}{\Psi(x)V(x)}. \tag{13}$$

Отметим, что формула (13) описывает распределение предков в модели контактов с генератором (2) (или (7)).

Предложение 1. *Неравенство* (12) *вместе с равномерной сходимостью интеграла следует из оценки*

$$\int\limits_0^\infty \sup_{x,y} \mathbf{E}_x\, b(X(t),y)\,dt < H. \tag{14}$$

Доказательство. Обозначим через $p(x,dy,t)$ переходную функцию скачкообразного марковского процесса с генератором (11) в момент времени t. Тогда

$$\sup_{x,y} \int\limits_0^\infty \mathbf{E}_{x,y}\, b(X(t),Y(t))\,dt = \sup_{x,y} \int\limits_0^\infty \int\limits_{\mathfrak{X}} \int\limits_{\mathfrak{X}} b(x',y')\,p(x,dx',t)\,p(y,dy',t)\,dt \leqslant$$

$$\leqslant \sup_y \int\limits_0^\infty \int\limits_{\mathfrak{X}} \left(\sup_x \int\limits_{\mathfrak{X}} b(x',y')\,p(x,dx',t) \right) p(y,dy',t)\,dt =$$

$$= \sup_y \int\limits_0^\infty \int\limits_{\mathfrak{X}} \Big(\sup_x \mathbf{E}_x\, b(X(t),y') \Big)\, p(y,dy',t)\,dt \leqslant$$

$$\leqslant \int\limits_0^\infty \sup_y \int\limits_{\mathfrak{X}} \Big(\sup_{y'} \sup_x \mathbf{E}_x\, b(X(t),y') \Big)\, p(y,dy',t)\,dt = \int\limits_0^\infty \sup_{x,y'} \mathbf{E}_x\, b(X(t),y')\,dt.$$

Таким образом, из условия (14) следует равномерная сходимость в (12). ▲

§ 3. Эволюция корреляционных функций. Основные результаты

Обозначим через $\mathcal{M}_{\mathrm{fm}}(\Gamma)$ множество всех вероятностных мер μ, имеющих конечные локальные моменты всех порядков, т.е.

$$\int_{\Gamma} |\gamma \cap \Lambda|^n \, \mu(d\gamma) < \infty$$

для всех $\Lambda \in \mathcal{B}_b(\mathfrak{X})$ и $n \in N$.

Вместе с конфигурационным пространством Γ определим пространство Γ_0 конечных конфигураций, и пусть

$$\Gamma_{0,\Lambda}^{(n)} = \{\eta \subset \Lambda : \, |\eta| = n\}$$

– множество n-точечных конфигураций в множестве $\Lambda \in \mathcal{B}_b(\mathfrak{X})$. Если мера $\mu \in \in \mathcal{M}_{\mathrm{fm}}(\Gamma)$ локально абсолютно непрерывна относительно меры Лебега – Пуассона

$$\lambda_{z,\bar{\mathfrak{m}}} = \sum_{n=0}^{\infty} \frac{z^n}{n!} \bar{\mathfrak{m}}^{\otimes n},$$

т.е.

$$\lambda_{z,\bar{\mathfrak{m}}}\big(\Gamma_{0,\Lambda}^{(n)}\big) = \frac{z^n (\bar{\mathfrak{m}}(\Lambda))^n}{n!}, \quad n = 0, 1, \ldots,$$

где

$$\bar{\mathfrak{m}}(\Lambda) = \int_{\Lambda} \bar{\mathfrak{m}}(dx),$$

то имеется соответствующая система корреляционных функций, т.е. плотностей корреляционной меры относительно меры Лебега – Пуассона. Эта терминология возникла в статистической механике (см., например, [11, гл. 4]). Обозначим через $\mathcal{M}_{\mathrm{corr}}(\Gamma)$ подкласс класса $\mathcal{M}_{\mathrm{fm}}(\Gamma)$, состоящий из вероятностных мер на Γ, для которых существуют корреляционные функции.

Уравнение эволюции для системы n-точечных корреляционных функций, соответствующих модели контактов в $\mathfrak{X}$, имеет следующий рекуррентный вид (см., например, [4, 10]):

$$\frac{\partial k_t^{(n)}}{\partial t} = \widehat{L}_n^* k_t^{(n)} + f_t^{(n)}, \quad n \geqslant 1, \qquad k_t^{(0)} \equiv 1, \tag{15}$$

где

$$\widehat{L}_n^* k_t^{(n)}(x_1, \ldots, x_n) = -\left(\sum_{i=1}^{n} V(x_i)\right) k_t^{(n)}(x_1, \ldots, x_n) +$$

$$+ \sum_{i=1}^{n} \int_{\mathfrak{X}} b(x_i, y) k_t^{(n)}(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n) \, \bar{\mathfrak{m}}(dy). \tag{16}$$

Здесь $f_t^{(n)}$ – функции на $\mathfrak{X}^n$, заданные при $n \geqslant 2$ равенствами

$$f_t^{(n)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} k_t^{(n-1)}(x_1, \ldots, \check{x}_i, \ldots, x_n) \sum_{j \neq i} b(x_i, x_j), \tag{17}$$

а $f_t^{(1)} \equiv 0$. Обозначение $\check{x}_i$ означает, что эта координата исключается.

Пусть $\mathbb{X}_n = \mathbb{B}(\mathfrak{X}^n)$ – банахово пространство всех измеримых вещественнозначных ограниченных функций на $\mathfrak{X}^n$ с sup-нормой. Рассмотрим оператор $\widehat{L}_n^*$ как оператор на банаховом пространстве $\mathbb{X}_n$ для произвольного $n \geqslant 1$. Тогда он является ограниченным линейным оператором в $\mathbb{X}_n$, и из рассуждений, основанных на формуле Дюамеля, следует, что

$$k_t^{(n)} = e^{t\widehat{L}_n^*} k_0^{(n)} + \int_0^t e^{(t-s)\widehat{L}_n^*} f_s^{(n)}\, ds, \tag{18}$$

где $f_s^{(n)}$ выражается через $k_s^{(n-1)}$ по формуле (17). Таким образом, решение задачи Коши (15) в $\mathbb{X}_n$ с произвольными начальными данными $k_0^{(n)} \in \mathbb{X}_n$ существует и единственно при условии, что $f_t^{(n)}$ рекуррентно строится через решение той же задачи Коши (15) для $n-1$.

Целью данной статьи является доказательство существования семейства инвариантных мер для процесса контактов в критическом режиме, порождаемых операторами вида (7). Эти меры описываются в терминах соответствующих корреляционных функций $\{k^{(n)}\}_{n\geqslant 0}$, которые являются решениями следующей системы:

$$\widehat{L}_n^* k^{(n)} + f^{(n)} = 0, \quad n \geqslant 1, \qquad k^{(0)} \equiv 1, \tag{19}$$

где $\widehat{L}_n^*$ и $f^{(n)}$ определены в (16) и (17). В дальнейшем будем говорить, что функция $k\colon \Gamma_0 \to \mathbb{R}$ решает систему (19) в банаховых пространствах $(\mathbb{X}_n)_{n\geqslant 1}$, если соответствующие $k^{(n)} \in \mathbb{X}_n$, $n \geqslant 1$, образуют решение системы (19).

Основным результатом статьи является следующая

Теорема 1. *Предположим, что интенсивности рождения $b(y,x)$ и гибели $V(x)$ процесса контактов удовлетворяют условиям измеримости, регулярности* (9), *критического режима* (10) *и транзиентности* (12). *Тогда справедливы следующие утверждения.*

(i) *Для любой положительной константы $\varrho > 0$ существует вероятностная мера $\mu^\varrho \in \mathcal{M}_{\mathrm{corr}}(\Gamma)$ на Γ, такая что ее корреляционная функция $k_\varrho\colon \Gamma_0 \to \mathbb{R}_+$ дает решение системы* (19) *в банаховых пространствах $(\mathbb{X}_n)_{n\geqslant 1}$, а соответствующая система $\{k_\varrho^{(n)}\}_{n\geqslant 1}$ удовлетворяет условию $k_\varrho^{(1)} \equiv \varrho$. Более того, для всех $(x_1,\dots,x_n) \in \mathfrak{X}^n$ справедливы следующие оценки*:

$$k_\varrho^{(n)}(x_1,\dots,x_n) \leqslant DH^n (n!)^2, \quad \textit{где} \quad D = \sum_{n=1}^{\infty} \frac{(\varrho/H)^n}{(n!)^2}, \tag{20}$$

где H – та же константа, что и в (12).

(ii) *Пусть $\{k_{\varrho,t}^{(n)}\}_{n\geqslant 1}$ – решение задачи Коши* (15) *с начальными условиями*

$$k_0 = \{k_0^{(n)}\},$$

соответствующими пуассоновской мере π_ϱ с интенсивностью ϱ:

$$k_0^{(0)} = 1, \quad k_0^{(n)}(x_1,\dots,x_n) = \varrho^n, \quad n \geqslant 1. \tag{21}$$

Тогда

$$\big\|k_{\varrho,t}^{(n)} - k_\varrho^{(n)}\big\|_{\mathbb{X}_n} \to 0, \quad t \to \infty, \quad \forall n \geqslant 1. \tag{22}$$

Основная стратегия доказательства следует той же схеме, что и в работе [10]. Однако в настоящей статье нам потребуется адаптировать некоторые шаги предыдущего доказательства для процессов контактов с неоднородными интенсивностями.

§ 4. Доказательство теоремы 1

Для первой корреляционной функции $k^{(1)}$ из (16) и (19) получаем следующее уравнение:

$$-V(x)k^{(1)}(x) + \int\limits_{\mathfrak{X}} b(x,y)k^{(1)}(y)\,\bar{\mathfrak{m}}(dy) = 0, \tag{23}$$

которое можно записать с использованием условия критического режима (10) как

$$\int\limits_{\mathfrak{X}} b(x,y)\big(k^{(1)}(y) - k^{(1)}(x)\big)\,\bar{\mathfrak{m}}(dy) = 0. \tag{24}$$

Очевидно, что функция $k^{(1)}(x) \equiv \varrho$ является элементом пространства $\mathbb{X}_1$ и что она дает решение задачи (24) (а также (23)). Заметим, что ϱ можно интерпретировать как пространственную плотность частиц.

В доказательстве первого утверждения теоремы 1 применим индукцию по $n \in \mathbb{N}$. Если для любого $n > 1$ удастся решить уравнение (19) и выразить $k^{(n)}$ через $f^{(n)}$, то, зная, как $f^{(n)}$ выражается через $k^{(n-1)}$ (см. (17)), мы рекуррентным образом получим решение $\{k^{(n)}\}_{n\geqslant 1}$ полной системы (19).

Лемма 1. *Оператор $e^{t\widehat{L}_n^*}$, где $\widehat{L}_n^*$ определено в* (16), *является положительным, т.е. отображает неотрицательные функции в неотрицательные.*

Доказательство. Оператор

$$A^i k^{(n)}(x_1,\dots,x_n) := \int\limits_{\mathfrak{X}} b(x_i,y)k^{(n)}(x_1,\dots,x_{i-1},y,x_{i+1},\dots,x_n)\,\bar{\mathfrak{m}}(dy)$$

положителен и ограничен на $\mathbb{X}_n$ для любого $1 \leqslant i \leqslant n$. Положим

$$\mathcal{L}^i k^{(n)}(x_1,\dots,x_n) = \int\limits_{\mathfrak{X}} b(x_i,y)k^{(n)}(x_1,\dots,x_{i-1},y,x_{i+1},\dots,x_n)\,\bar{\mathfrak{m}}(dy) -$$
$$- V(x_i)k^{(n)}(x_1,\dots,x_n). \tag{25}$$

Применяя формулу Троттера для суммы $A + B$ двух ограниченных операторов

$$e^{t(A+B)} = \lim_{n\to\infty}\Big(e^{\frac{tA}{n}}e^{\frac{tB}{n}}\Big)^n,$$

заключаем, что

$$e^{t\mathcal{L}^i}f = \lim_{n\to\infty}\Big(e^{t\frac{A^i}{n}}e^{-t\frac{V}{n}}\Big)^n f \geqslant e^{-tV_{\max}}e^{tA^i}f \geqslant 0 \tag{26}$$

для любой неотрицательной функции f. Здесь V – оператор умножения на положительную ограниченную функцию V, а константа $V_{\max}$ определена в (8).

Из представления (16) получаем

$$e^{t\widehat{L}_n^*} = \bigotimes_{i=1}^{n} e^{t\mathcal{L}^i}.$$

Отсюда с учетом того, что

$$\bigotimes_{i=1}^{n} e^{-tV_{\max}} e^{tA^i}$$

является положительным оператором, получаем требуемое утверждение. ▲

Пусть $k^{(1)}$ – произвольная положительная константа. Далее мы построим решение системы (19), удовлетворяющее оценке (20). Как следует из (17), функция $f^{(n)}$ является суммой функций вида

$$f_{i,j}(x_1,\dots,x_n) = k^{(n-1)}(x_1,\dots,\check{x}_i,\dots,x_n)b(x_i,x_j), \quad i \neq j. \tag{27}$$

Предположим по индукции, что

$$k^{(n-1)}(x_1,\dots,x_{n-1}) \leqslant K_{n-1} \quad \text{для всех } (x_1,\dots,x_{n-1}) \in \mathfrak{X}^{n-1}, \quad n \geqslant 2,$$

где $K_n = DC^n(n!)^2$, а D и C – некоторые константы. Тогда

$$f_{i,j}(x_1,\dots,x_n) \leqslant K_{n-1}b(x_i,x_j), \quad (x_1,\dots,x_n) \in \mathfrak{X}^n. \tag{28}$$

Используя положительность оператора $e^{t\widehat{L}_n^*}$ и неравенство (28), получаем

$$\bigl(e^{t\widehat{L}_n^*} f_{i,j}\bigr)(x_1,\dots,x_n) \leqslant K_{n-1}\bigl(e^{t\widehat{L}_n^*} b(\cdot_i,\cdot_j)\bigr)(x_1,\dots,x_n). \tag{29}$$

С учетом условия критического режима (10) заключаем, что

$$e^{t\mathcal{L}^i}\mathbb{1} = \mathbb{1}, \quad \forall i = 1,\dots,n,$$

где $\mathcal{L}$ дается формулой (25), а $\mathbb{1}(x) \equiv 1$. Таким образом,

$$\bigl(e^{t\widehat{L}_n^*} b(\cdot_i,\cdot_j)\bigr)(x_1,\dots,x_n) = \bigl(e^{t(\mathcal{L}^i+\mathcal{L}^j)} b(\cdot_i,\cdot_j)\bigr)(x_1,\dots,x_n). \tag{30}$$

Отметим, что последняя функция зависит только от переменных x_i и x_j.

Заметим, что функция $e^{t\widehat{L}_n^*} f_{i,j}$ интегрируема относительно t на $\mathbb{R}_+$. Действительно, из соотношений (27), (29), условия (12) и тождества

$$e^{t\widehat{L}_n^*} b(x,y) = \mathbf{E}_{x,y}\, b(X(t),Y(t)) \tag{31}$$

следует, что

$$v_{i,j}^{(n)} = \int_0^\infty e^{t\widehat{L}_n^*} f_{i,j}\, dt \leqslant K_{n-1}H, \tag{32}$$

где H – та же константа, что и в (12).

Начиная с этого момента доказательство основного результата полностью повторяет рассуждения из доказательства теоремы 3.1 работы [10]. Однако для удобства читателя мы изложим здесь все последующие шаги. Обозначим

$$v^{(n)} = \sum_{i\neq j} v_{i,j}^{(n)} = \int_0^\infty e^{t\widehat{L}_n^*} f^{(n)}\, dt, \quad f^{(n)} = \sum_{i\neq j} f_{i,j}, \tag{33}$$

где $f_{i,j}$ заданы равенством (27). Теперь докажем, что функция $v^{(n)}$ является решением системы (19) в $\mathbb{X}_n$. Из (32) и процедуры индукции легко видеть, что $v^{(n)} \in \mathbb{X}_n$.

Поскольку $e^{t\widehat{L}_n^*}$ – сильно непрерывная полугруппа, имеем

$$e^{t\widehat{L}_n^*}f^{(n)} - f^{(n)} = \widehat{L}_n^* \int\limits_0^t e^{s\widehat{L}_n^*}f^{(n)}\,ds. \tag{34}$$

Перепишем (34) в виде

$$e^{t\widehat{L}_n^*}f^{(n)} = f^{(n)} + \widehat{L}_n^* \int\limits_0^t e^{s\widehat{L}_n^*}f^{(n)}\,ds. \tag{35}$$

Теперь, используя условие (12), неравенство (28), лемму 1 и тот факт, что $\widehat{L}_n^*$ – ограниченный оператор, заключаем, что правая часть выражения (35) имеет равномерный по $x_1, \ldots, x_n$ предел при $t \to \infty$, и следовательно, левая часть (35), т.е. $e^{t\widehat{L}_n^*}f^{(n)}$, также сходится в $\mathbb{X}_n$. Более того, предел является неотрицательной функцией в $\mathbb{X}_n$. Однако если эта функция где-то строго положительна, то получим противоречие с условием (12), так как в этом случае интеграл по t будет неограниченным. Таким образом, получаем, что в $\mathbb{X}_n$ имеет место следующий предел:

$$e^{t\widehat{L}_n^*}f^{(n)} \to 0, \quad t \to \infty. \tag{36}$$

Переход к пределу в (34) при $t \to \infty$ вместе с (36) показывает, что функцию $v^{(n)}$, определенную в (33), можно взять в качестве решения $k^{(n)}$ системы (19) в $\mathbb{X}_n$.

Поскольку функция $f^{(n)}$ является суммой функций $f_{i,j}$, $i \neq j$, то из (32) следует, что $v^{(n)}$ ограничена величиной $n^2K_{n-1}H$. Таким образом, получаем рекуррентное неравенство

$$K_n \leqslant n^2K_{n-1}H, \tag{37}$$

и отсюда по индукции получаем, что

$$K_n \leqslant H^n(n!)^2k^{(1)}. \tag{38}$$

Таким образом, для этого решения $k^{(n)} = v^{(n)}$ справедлива оценка

$$v^{(n)}(x_1, \ldots, x_n) \leqslant H^n(n!)^2k^{(1)}. \tag{39}$$

Разумеется, любое семейство функций вида

$$k^{(1)} \equiv \varrho, \qquad k^{(n)} = \int\limits_0^\infty e^{t\widehat{L}_n^*}f^{(n)}\,dt + A_n, \quad n \geqslant 2,$$

с произвольной константой A_n также является решением системы (19). Здесь $f^{(n)}$ задается, как и выше, равенством (27). Полагая $A_n = \varrho^n$, получаем, что

$$k_\varrho^{(1)} \equiv \varrho, \qquad k_\varrho^{(n)} = \int\limits_0^\infty e^{t\widehat{L}_n^*}f^{(n)}\,dt + \varrho^n, \quad n \geqslant 2, \tag{40}$$

является искомым решением стационарной задачи (19) в банаховых пространствах $(\mathbb{X}_n)_{n\geqslant 1}$. Чтобы подчеркнуть зависимость функции $f^{(n)}$ от ϱ, будем для $f^{(n)}$ использовать обозначение $f_\varrho^{(n)}$. Для решений $\{k_\varrho^{(n)}\}_{n\geqslant 1}$ из (40) вместо (37) имеем рекур-

рентное соотношение

$$K_n \leqslant n^2 K_{n-1} H + \varrho^n. \tag{41}$$

Полагая

$$L_n = \frac{K_n}{H^n (n!)^2},$$

из (41) получаем

$$L_n \leqslant L_{n-1} + \frac{\varrho^n}{H^n (n!)^2} \leqslant D \quad \forall n = 1, 2, \dots, \qquad L_0 = 0.$$

Отсюда

$$K_n \leqslant D H^n (n!)^2, \quad \text{где} \quad D = \sum_{n=1}^{\infty} \frac{(\varrho/H)^n}{(n!)^2}. \tag{42}$$

Чтобы убедиться в том, что построенная система $\{k_\varrho^{(n)}\}_{n \geqslant 1}$ является системой корреляционных функций, т.е. соответствует вероятностной мере μ^ϱ на конфигурационном пространстве Γ, далее мы докажем, что $\{k_\varrho^{(n)}\}_{n \geqslant 1}$ можно построить как предел при $t \to \infty$ системы корреляционных функций $\{k_t^{(n)}\}_{n \geqslant 1}$, связанных с решением задачи Коши (15) с начальными условиями (21).

Напомним, что для решения задачи Коши (15) имеется представление (18). С другой стороны, выше мы доказали существование решения $\{k_\varrho^{(n)}\}_{n \geqslant 1}$ стационарной задачи

$$\widehat{L}_n^* k_\varrho^{(n)} = -f_\varrho^{(n)}, \tag{43}$$

где

$$f_\varrho^{(n)}(x_1, \dots, x_n) = \sum_{i,j:\, i \neq j} k_\varrho^{(n-1)}(x_1, \dots, \check{x}_i, \dots, x_n) b(x_i, x_j).$$

Это решение задается формулой (40), и из (43) вытекает следующее соотношение:

$$\big(e^{t\widehat{L}_n^*} - 1\big) k_\varrho^{(n)} = -\int_0^t \frac{d}{ds} e^{(t-s)\widehat{L}_n^*} k_\varrho^{(n)}\, ds = -\int_0^t e^{(t-s)\widehat{L}_n^*} f_\varrho^{(n)}\, ds. \tag{44}$$

Поэтому из (18) и (44) получаем

$$k_t^{(n)} - k_\varrho^{(n)} = e^{t\widehat{L}_n^*}\big(k_0^{(n)} - k_\varrho^{(n)}\big) + \int_0^t e^{(t-s)\widehat{L}_n^*}\big(f_s^{(n)} - f_\varrho^{(n)}\big)\, ds. \tag{45}$$

Докажем теперь, что оба члена в правой части (45) при $t \to \infty$ сходятся к 0 в норме пространства $\mathbb{X}_n$.

Из (40) получаем

$$e^{t\widehat{L}_n^*}\big(k_0^{(n)} - k_\varrho^{(n)}\big) = -e^{t\widehat{L}_n^*} v^{(n)}, \tag{46}$$

где согласно (33) имеем

$$v^{(n)} = \int\limits_0^\infty e^{s\widehat{L}_n^*} f_\varrho^{(n)}\, ds.$$

Следовательно, первый член в правой части (45) можно преобразовать с помощью (46) и (33) следующим образом:

$$e^{t\widehat{L}_n^*} v^{(n)} = \int\limits_0^\infty e^{(t+s)\widehat{L}_n^*} f_\varrho^{(n)}\, ds = \int\limits_t^\infty e^{r\widehat{L}_n^*} f_\varrho^{(n)}\, dr.$$

В силу структуры (27) функции $f_\varrho^{(n)}$ и равномерной сходимости интеграла в (12) заключаем, что

$$\left\| e^{t\widehat{L}_n^*} v^{(n)} \right\|_{\mathbb{X}_n} \to 0, \quad t \to \infty. \tag{47}$$

Второй член в правой части (45) также стремится к 0, что можно доказать тем же способом, что и в предыдущих наших работах (см., например, [7]).

Таким образом, мы доказали (22), что завершает доказательство второй части теоремы 1.

Теперь вернемся к первой части теоремы 1. Заключительный шаг доказательства состоит в том, чтобы показать, что система корреляционных функций $\left\{k_\varrho^{(n)}\right\}_{n\geqslant 1}$ соответствует некоторой вероятностной мере μ^ϱ на конфигурационном пространстве Γ. Для этого выше мы построили $k_\varrho^{(n)}$ как предел при $t \to \infty$ решения $k_t^{(n)}$ задачи Коши (15) с начальными условиями (21):

$$k_\varrho^{(n)} = \lim_{t\to\infty} k_t^{(n)}. \tag{48}$$

Далее можно показать, что решение $k_t^{(n)}$ задачи Коши удовлетворяет условию положительности по Ленарду и условию роста момента (см. [12,13]). Подробное доказательство этого факта можно найти в [5]. Наконец, из этих условий следует, что для любого $\varrho > 0$ существует единственная вероятностная мера $\mu^\varrho \in \mathcal{M}_{\mathrm{corr}}(\Gamma)$, корреляционные функции которой имеют вид $\left\{k_\varrho^{(n)}\right\}_{n\geqslant 1}$. Это завершает доказательство теоремы 1.

§ 5. Маркированная непрерывная модель контактов в критическом режиме

В этом параграфе рассматривается модель контактов в непрерывном пространстве, в которой каждый элемент конфигурации характеризуется как своим расположением в пространстве, так и своей маркой. Аналогичная модель с постоянной интенсивностью гибели $V(x) \equiv 1$ изучалась в [7,8], причем в первой работе рассматривался критический режим, а во второй – субкритический.

Конфигурация $\gamma \in \Gamma(\mathfrak{X})$ – это конечное или локально конечное счетное неупорядоченное множество точек в $\mathfrak{X}$, где $\mathfrak{X} = \mathbb{R}^d \times S$, а S – компактное метрическое пространство (пространство марок). Мера m берется в виде

$$m = l \otimes \nu,$$

где $l(dy) = dy$ – мера Лебега на $\mathbb{R}^d$, а $\nu(ds)$ – конечная мера Бореля на S. Для точек $x \in \mathfrak{X}$ будем использовать обозначение

$$x = (\xi, s), \quad \xi \in \mathbb{R}^d, \quad s \in S.$$

Рассмотрим интенсивность рождения $a(x, x')$ следующего вида:

$$a(x, x') = \alpha(\xi - \xi')Q(s, s'),$$

где $\alpha(\cdot) \geqslant 0$ – ограниченная измеримая функция, удовлетворяющая условию нормировки

$$\int\limits_{\mathbb{R}^d} \alpha(u)\, du = 1, \tag{49}$$

а $Q\colon S \times S \to \mathbb{R}_+$ – непрерывная (и поэтому ограниченная) строго положительная функция. Для интенсивности гибели полагаем, что $V(\xi, s) = v(s)$, т.е. $V(x)$ зависит только от марки, и $v\colon S \to \mathbb{R}_+$ также является непрерывной строго положительной функцией. Поэтому из теоремы Крейна – Рутмана следует, что существуют положительное число $r > 0$ и строго положительная непрерывная функция $q(s)$ на S, такие что

$$\int\limits_S \frac{Q(s, s')}{v(s)} q(s')\, \nu(ds') = rq(s) \tag{50}$$

при $0 < q_{\min} \leqslant q(s) \leqslant q_{\max} < \infty$. Если предположить, что $\Psi(x)$ зависит только от $s \in S$, то условие критического режима (4) эквивалентно утверждению о том, что компактный положительный оператор $\widetilde{Q}$ с ядром $\dfrac{Q(s, s')}{v(s)}$ имеет максимальное положительное собственное значение $r = 1$, т.е. равенство (50) выполняется при $r = 1$:

$$\int\limits_S \frac{Q(s, s')}{v(s)} q(s')\, \nu(ds') = q(s), \tag{51}$$

и $\Psi(x) = q(s)$.

Теорема 2. *Пусть $d \geqslant 3$, и пусть интенсивности рождения имеют вид*

$$a(x, x') = \alpha(\xi - \xi')Q(s, s'), \quad \xi \in \mathbb{R}^d, \quad s \in S,$$

где $\alpha(\cdot) \geqslant 0$ – ограниченная измеримая функция, удовлетворяющая условию (49), *а $Q\colon S \times S \to \mathbb{R}_+$ – непрерывная строго положительная функция. Предположим, что $V(\xi, s) = v(s)$, где $v\colon S \to \mathbb{R}_+$ – непрерывная строго положительная функция*:

$$0 < V_{\min} \leqslant v(s) \leqslant V_{\max} < \infty.$$

Пусть выполнено условие критического режима (51) *при* $\int\limits_S q(s)\, \nu(ds) = 1$, *и $\Psi(x) = q(s)$. Тогда выполнены все условия теоремы* 1, *и следовательно, для любого $\varrho > 0$ существует инвариантная мера μ^ϱ, корреляционные функции которой (относительно меры Лебега – Пуассона с интенсивностью $m(dy)$) удовлетворяют следующим оценкам*:

$$k_\varrho^{(n)}(x_1, \ldots, x_n) \leqslant DH^n (n!)^2 \prod_{i=1}^n q(s_i) \quad \text{для всех } (x_1, \ldots, x_n) \in \mathfrak{X}^n, \tag{52}$$

где D определено в (20), *а H – та же константа, что и в* (12).

Более того, корреляционные функции $k_\varrho^{(n)}$, $n = 1, 2, \ldots$, *инвариантной меры* μ^ϱ *для любого* $\varrho > 0$ *можно построить как предел корреляционных функций задачи Коши с соответствующими начальными условиями. Действительно, для любых* $n = 1, 2, \ldots$ *решение* $k^{(n)}(t)$ *задачи Коши* (15) *с начальными условиями*

$$k_0^{(0)} = 1, \quad k_0^{(n)}(x_1, \ldots, x_n) = \varrho^n \prod_{i=1}^n q(s_i)$$

сходится к решению системы (19) *стационарных* (*не зависящих от времени*) *уравнений при* $t \to \infty$:

$$\left\| k^{(n)}(t) - k_\varrho^{(n)} \right\|_{\mathbb{X}_n} \to 0, \quad t \to \infty. \tag{53}$$

Доказательство. Для доказательства рассмотрим новую меру

$$\bar{\mathfrak{m}}(dy) = \Psi(y)\, m(dy)$$

и новую интенсивность рождения

$$b(x, y) = \frac{a(x, y)}{\Psi(x)},$$

задаваемые формулами (5) с $\Psi(\xi, s) = q(s)$, и теперь требуется проверить, что выполнены все условия теоремы 1 для b и $\bar{\mathfrak{m}}(dy)$.

Условия измеримости и регулярности справедливы в силу ограниченности функции Ψ. Далее, если у нас будет хорошая оценка сверху на $\mathbf{E}_x\, b(X(t), y)$, то из (14) будет вытекать условие транзиентности (12). Следующая лемма гарантирует равномерную сходимость интеграла в (14) при $d \geqslant 3$.

Лемма 2. *Для всех* $t > 0$ *имеет место следующая равномерная верхняя оценка*:

$$\mathbf{E}_x\, b(X(t), y) \leqslant \min\Big\{ \|b\|_\infty, \frac{C}{t^{d/2}} \Big\}, \tag{54}$$

где C *– некоторая положительная константа.*

Доказательство. Рассмотрим скачкообразный марковский процесс на $\mathfrak{X}$ с генератором

$$\mathcal{L}f(x) = \int_{\mathfrak{X}} b(x, y)(f(y) - f(x))\, \bar{\mathfrak{m}}(dy),$$

где $b(x, y)$ и $\bar{\mathfrak{m}}(dy)$ определены в (5). Генератор L можно переписать в виде

$$\mathcal{L}f(x) = V(x) \int_{\mathfrak{X}} \frac{b(x, y)}{V(x)} (f(y) - f(x))\, \bar{\mathfrak{m}}(dy). \tag{55}$$

Используя условие критического режима (51) для $\Psi(\xi, s) = q(s)$, получаем

$$\int_{\mathfrak{X}} \frac{b(x, y)}{V(x)}\, \bar{\mathfrak{m}}(dy) = \int_{\mathbb{R}^d} \int_S \frac{\alpha(\xi - \xi') Q(s, s') q(s')}{v(s) q(s)}\, d\xi'\, \nu(ds') = 1.$$

Следовательно, скачкообразный марковский процесс $X(t)$ с генератором (55) можно описать следующим образом: начиная с состояния $X(0) = (\xi, s)$ процесс делает скач-

ки с интенсивностью $v(s)$, а распределение нового положения $X(t)$ имеет плотность

$$\frac{\alpha(\xi-\xi')Q(s,s')q(s')}{v(s)q(s)}$$

относительно меры $l\otimes\nu$. Таким образом, координаты ξ' и s' условно независимы при начальном условии $X(0)=(\xi,s)$, и можно записать $X(t)=(\xi(t),s(t))$.

Обозначим

$$\Theta(s,s')=\frac{Q(s,s')q(s')}{v(s)q(s)}.$$

Тогда из условия критического режима (51) получаем

$$\int\limits_S \Theta(s,s')\,\nu(ds')=1. \tag{56}$$

Вторая компонента $s(t)$ процесса $X(t)$ является скачкообразным марковским процессом в S с непрерывным временем и с генератором

$$\mathcal{L}_S\varphi(s)=v(s)\int\limits_S \Theta(s,s')(\varphi(s')-\varphi(s))\,\nu(ds'). \tag{57}$$

Первая компонента $\xi(t)$ из $X(t)$ не является марковским процессом с непрерывным временем (когда $v(s)\not\equiv 1$). Рассмотрим последовательность $\xi(0),\xi(1),\dots$, где $\xi(n)\in\mathbb{R}^d$ – первая координата $X(t)$ после n-го скачка. Тогда $\xi(n)$ представляет собой случайное блуждание в $\mathbb{R}^d$, т.е. сумму независимых одинаково распределенных случайных величин с общим распределением скачков, равным $\alpha(u)$. Однако случайные интервалы времени между скачками не являются независимыми одинаково распределенными случайными величинами.

Применяя представление (5) для $b(X(t),y)$ и выбирая $x=(\xi_0,s_0)$, $y=(\xi_1,s_1)$, имеем

$$\mathbf{E}_x\, b(X(t),y)=\mathbf{E}_{(\xi_0,s_0)}\,\frac{\alpha(\xi(t)-\xi_1)Q(s(t),s_1)}{q(s(t))}\leqslant \varkappa\,\mathbf{E}_{\xi_0}\,\alpha(\xi(t)-\xi_1), \tag{58}$$

где

$$\varkappa=\frac{\max Q(s,s')}{q_{\min}}.$$

Используя для распределения процесса $\xi(t)$ разложение на сингулярную и регулярную части, получаем

$$\mathbf{E}_{\xi_0}\,\alpha(\xi(t)-\xi_1)=e^{-v(s_0)t}\alpha(\xi_0-\xi_1)+\int\limits_{\mathbb{R}^d} P(t,\xi,\xi_0)\alpha(\xi-\xi_1)\,d\xi, \tag{59}$$

где $P(t,\xi,\xi_0)$ – регулярная часть распределения процесса $\xi(t)$:

$$P(t,\xi,\xi_0)=\sum_{n=1}^{\infty}\alpha^{*n}(\xi-\xi_0)p_n(t). \tag{60}$$

Здесь α^{*n} – n-кратная свертка функции α, а

$$p_n(t)=\Pr(n_X(t)=n)$$

– вероятность того, что процесс $X(t)$ имеет n скачков до момента времени t. Следует отметить, что

$$\Pr(n_X(t)=n)=\Pr(n_s(t)=n),$$

где $n_s(t)$ – число скачков процесса $s(t)$ на интервале времени $[0,t]$. В дальнейшем (см. (64)) будем обозначать через $P_{v(\cdot)}$ меру на пространстве целочисленных траекторий, соответствующих процессу $n_s(t)$.

Оценим α^{*n} и $p_n(t)$ по отдельности.

Лемма 3. *Предположим, что*

$$\alpha(\xi)\geqslant 0,\quad \alpha(\xi)\in L^1(\mathbb{R}^d)\cap L^\infty(\mathbb{R}^d)\quad u\quad \int \alpha(\xi)\,d\xi=1.$$

Тогда справедлива следующая оценка сверху:

$$\alpha^{*n}(\xi)\leqslant \frac{K}{n^{d/2}}. \tag{61}$$

Доказательство. Рассматривая $\alpha(\cdot)$ как распределение случайной величины, получаем, что соответствующая характеристическая функция $\varphi(k)$ обладает следующими свойствами:

$$\varphi\in L^2(\mathbb{R}^d)\cap C_0(\mathbb{R}^d),\qquad \varphi(0)=1,\qquad |\varphi(k)|<1,\quad k\neq 0,$$

где $C_0(\mathbb{R}^d)$ – пространство непрерывных функций, обращающихся в нуль на бесконечности: $|\varphi(k)|\to 0$ при $|k|\to\infty$. Из утверждения [14, лемма 1.5] следует, что существуют $\delta>0$ и $\gamma>0$, такие что

$$|\varphi(k)|\leqslant e^{-\gamma k^2}\quad \text{для всех } |k|\leqslant\delta. \tag{62}$$

Более того, из свойств функции φ вытекает, что

$$|\varphi(k)|\leqslant C,\quad \text{где}\quad 0<C<1,\quad \text{для всех } |k|>\delta. \tag{63}$$

Так как $\varphi^n(k)$ является характеристической функцией $\alpha^{*n}(\xi)$, то применяя обратное преобразование Фурье вместе с (62) и (63), получаем следующую равномерную верхнюю оценку:

$$\alpha^{*n}(\xi)=\frac{1}{(2\pi)^d}\int\limits_{\mathbb{R}^d} e^{-iku}\varphi^n(k)\,dk\leqslant\frac{1}{(2\pi)^d}\left(\int\limits_{|k|\leqslant\delta}|\varphi(k)|^n\,dk+\int\limits_{|k|>\delta}|\varphi(k)|^n\,dk\right)\leqslant$$

$$\leqslant\frac{1}{(2\pi)^d}\int\limits_{\mathbb{R}^d}e^{-\gamma k^2 n}\,dk+\frac{1}{(2\pi)^d}C^{n-2}\int\limits_{\mathbb{R}^d}|\varphi(k)|^2\,dk\leqslant\frac{\widehat{C}}{n^{d/2}}+\frac{C^{n-2}}{(2\pi)^d}\,\|\varphi\|^2_{L^2}\leqslant\frac{K}{n^{d/2}}.$$

Здесь $\widehat{C}$ и K – некоторые константы, а $0<C<1$ – та же константа, что и в (63). Таким образом, оценка (61) доказана. ▲

Обозначим через $F_{\alpha_j}(t)$, $j=1,2$, функции распределения случайных величин, имеющих экспоненциальное распределение с параметрами $\alpha_1>0$ и $\alpha_2>0$ соответственно, т.е.

$$F_{\alpha_j}(t)=1-e^{-\alpha_j t},\quad t\geqslant 0.$$

Если $\alpha_2>\alpha_1$, то

$$F_{\alpha_2}(t)>F_{\alpha_1}(t),\quad \forall t>0.$$

Будем обозначать через

$$P_{v(s(\tau))}(n(t) \leqslant k) = P_{v(\cdot)}(n(t) \leqslant k)$$

пуассоновский процесс с интенсивностью $v(s(\tau))$, зависящей от скачкообразного марковского процесса $s(\tau)$ с генератором (57). Очевидно, что

$$\Pr(n_X(t) \leqslant k) = P_{v(\cdot)}(n(t) \leqslant k). \tag{64}$$

Предложение 2. *Пусть* $0 < \lambda_0 \leqslant v(s) \leqslant \lambda_1 < \infty$, *тогда*

$$P_{v(\cdot)}(n(t) \leqslant k) \leqslant P_{\lambda_0}(n(t) \leqslant k), \quad \forall k \in \mathbb{N}. \tag{65}$$

Доказательство. Неравенство (65) равносильно следующему:

$$P_{v(\cdot)}(n(t) \geqslant k) \geqslant P_{\lambda_0}(n(t) \geqslant k), \quad \forall k \in \mathbb{N}. \tag{66}$$

Из условия предложения следует, что $F_{v(\cdot)}(t) \geqslant F_{\lambda_0}(t)$, $\forall t \geqslant 0$. Напомним, что свертка функций распределения определяется следующим образом:

$$(F_1 * F_2)(t) = \int\limits_{-\infty}^{+\infty} F_1(t-x)\, F_2(dx).$$

Тогда, используя тот факт, что $F_1 * F_2 = F_2 * F_1$, получаем, что для любых s_i, s_j

$$(F_{v(s_i)} * F_{v(s_j)})(t) \geqslant (F_{\lambda_0} * F_{v(s_j)})(t) = (F_{v(s_j)} * F_{\lambda_0})(t) \geqslant (F_{\lambda_0} * F_{\lambda_0})(t).$$

С учетом (56) для любых $v_1 = v(s_1)$ и $s_1 = s(0)$ получаем следующее неравенство:

$$\begin{aligned} &P_{v(\cdot)}(n(t) \geqslant k) = \\ &= \int\limits_{S^{k-1}} \Theta(s_1, s_2) \ldots \Theta(s_{k-1}, s_k)(F_{v_1} * F_{v_2} * \ldots * F_{v_k})(t)\, \nu(ds_2) \ldots \nu(ds_k) \geqslant \\ &\geqslant F^{*k}_{\lambda_0}(t) = P_{\lambda_0}(n(t) \geqslant k), \end{aligned}$$

где $v_j = v(s_j) \geqslant \lambda_0$ $\forall j = 1, \ldots, k$. Здесь мы использовали тот факт, что для заданных состояний $s_1, \ldots, s_k$ процесса $s(t)$ интервалы $t_1, \ldots, t_k$ времени ожидания соответствующего перехода условно независимы и имеют экспоненциальные распределения с параметрами $v(s_1), \ldots, v(s_k)$ соответственно.

Таким образом, неравенства (66) и (65) доказаны. ▲

Теперь воспользуемся неравенствами (61) и (65) для получения верхней оценки для регулярной части $P(t)\xi, \xi_0)$ распределения $\xi(t)$.

Лемма 4. *Для* $P(t, \xi, \xi_0)$ *при всех* $t > 0$ *справедлива следующая оценка*:

$$P(t, \xi, \xi_0) \leqslant \min\left\{M, \frac{\widetilde{K}}{t^{d/2}}\right\}. \tag{67}$$

Доказательство. Чтобы вывести верхнюю оценку на $P(t, \xi, \xi_0)$, разобьем сумму в (60) на две части:

$$\sum_{n=1}^{\infty} \alpha^{*n}(\xi) p_n(t) = \sum_{n=1}^{[\frac{1}{2}\lambda_0 t]} \alpha^{*n}(\xi) p_n(t) + \sum_{n=[\frac{1}{2}\lambda_0 t]+1}^{\infty} \alpha^{*n}(\xi) p_n(t), \tag{68}$$

где $\lambda_0 > 0$ – то же, что и в предложении 2, и оценим каждую из сумм в правой части (68) по отдельности. Из ограниченности функции $\alpha(\cdot)$ и условия нормировки (49) следует, что

$$M = \sup_{\substack{k\in\mathbb{N}\\ \xi\in\mathbb{R}^d}} \alpha^{*k}(\xi) = \|\alpha\|_\infty \tag{69}$$

и

$$\sup_\xi \alpha^{*(n+k)}(\xi) \leqslant \sup_\xi \alpha^{*n}(\xi), \quad \forall k = 1, 2, \dots \tag{70}$$

Применяя (65) и формулу Стирлинга, для первой суммы в (68) получаем

$$\sum_{n=1}^{[\frac{1}{2}\lambda_0 t]} \alpha^{*n}(\xi) p_n(t) \leqslant M \sum_{n=1}^{[\frac{1}{2}\lambda_0 t]} p_n(t) \leqslant M \Pr\Big(n_X(t) \leqslant \Big[\frac{1}{2}\lambda_0 t\Big]\Big) \leqslant$$

$$\leqslant M P_{\lambda_0}\Big(n(t) \leqslant \Big[\frac{1}{2}\lambda_0 t\Big]\Big) = M \sum_{n=0}^{[\frac{1}{2}\lambda_0 t]} \frac{(\lambda_0 t)^n}{n!} e^{-\lambda_0 t} \leqslant \big(\widetilde{M} t + M\big) e^{-B\lambda_0 t} \tag{71}$$

для положительного

$$B = \frac{1 - \ln 2}{2}$$

и

$$\widetilde{M} = \frac{1}{2} M \lambda_0.$$

Для оценки второй суммы в (68) применим (61) и (70), а также неравенство

$$\sum_{n=[\frac{1}{2}\lambda_0 t]+1}^{\infty} p_n(t) < 1.$$

Тогда

$$\sum_{n=[\frac{1}{2}\lambda_0 t]+1}^{\infty} \alpha^{*n}(\xi) p_n(t) \leqslant \sup_{n>[\frac{1}{2}\lambda_0 t]} \sup_\xi \alpha^{*n}(\xi) \leqslant \frac{K}{\Big(1 + \Big[\dfrac{\lambda_0 t}{2}\Big]\Big)^{d/2}}. \tag{72}$$

Наконец, из (71) и (72) получаем утверждение (67) леммы 4. ▲

Объединяя (58), (59) и (67), получаем неравенство (54). Итак, лемма 2, а вместе с ней и теорема 2, полностью доказаны. ▲

§ 6. Дополнение

В нашу модель контактов помимо рождения и гибели можно включить скачки. Аналогичная модель в $\mathbb{R}^d$ рассматривалась ранее в [5]. А именно, рассмотрим следующий эвристический генератор $L + L_J$, где L задается формулой (2), а

$$L_J F(\gamma) = \int_{\mathfrak{X}} \sum_{x\in\gamma} J(y, x)\big(F((\gamma \setminus x) \cup y) - F(\gamma)\big)\, m(dy). \tag{73}$$

Предположим, что общая интенсивность скачков $\int J(y,x)\,m(dy)$ равномерно ограничена по x:

$$\sup_x \int_{\mathfrak{X}} J(y,x)\,m(dy) < C. \tag{74}$$

Тогда модифицированное условие критического режима принимает вид

$$\int_{\mathfrak{X}} (a(x,y)+J(x,y))\Psi(y)\,m(dy) = \left(V(x)+\int_{\mathfrak{X}} J(y,x)\,m(dy)\right)\Psi(x). \tag{75}$$

Это снова означает, что если первоначальная плотность частиц равна $\Psi(x)$, то эта плотность сохраняется.

Выберем $b(x,y)$ и $\bar{\mathfrak{m}}(dy)$ таким же образом, как определялось в (5). Тогда генератор $\mathcal{L}_J$ скачкообразного процесса имеет вид

$$\mathcal{L}_J f(x) = \int_{\mathfrak{X}} \left(b(x,y)+\frac{J(x,y)}{\Psi(x)}\right)(f(y)-f(x))\,\bar{\mathfrak{m}}(dy), \tag{76}$$

а условие транзиентности (12) теперь можно записать следующим образом:

$$\sup_{x,y} \int_0^\infty \mathbf{E}_{x,y}\, b\big(\widetilde{X}(t),\widetilde{Y}(t)\big)\,dt < H, \tag{77}$$

где $\widetilde{X}(t)$ и $\widetilde{Y}(t)$ – два независимых экземпляра марковского процесса с генератором $\mathcal{L}_J$, заданным формулой (76).

СПИСОК ЛИТЕРАТУРЫ

1. *Harris T.E.* Contact Interactions on a Lattice // Ann. Probab. 1974. V. 2. № 6. P. 969–988. https://doi.org/10.1214/aop/1176996493
2. *Holley R., Liggett T.M.* The Survival of Contact Processes // Ann. Probab. 1978. V. 6. № 2. P. 198–206. https://doi.org/10.1214/aop/1176995567
3. *Liggett T.M.* Interacting Particle Systems. New York: Springer-Verlag, 1985.
4. *Kondratiev Yu., Kutoviy O., Pirogov S.* Correlation Functions and Invariant Measures in Continuous Contact Model // Infin. Dimens. Anal. Quantum Probab. Relat. Top. 2008. V. 11. № 2. P. 231–258. https://doi.org/10.1142/S0219025708003038
5. *Kondratiev Yu.G., Kutoviy O.V., Pirogov S.A., Zhizhina E.* Invariant Measures for Spatial Contact Model in Small Dimensions // Markov Process. Related Fields. 2021. V. 27. № 3. P. 413–438. https://math-mprf.org/journal/articles/id1616
6. *Kondratiev Yu., Skorokhod A.* On Contact Processes in Continuum // Infin. Dimens. Anal. Quantum Probab. Relat. Top. 2006. V. 9. № 2. P. 187–198. https://doi.org/10.1142/S0219025706002305
7. *Kondratiev Yu., Pirogov S., Zhizhina E.* A Quasispecies Continuous Contact Model in a Critical Regime // J. Stat. Phys. 2016. V. 163. № 2. P. 357–373. https://doi.org/10.1007/s10955-016-1480-5
8. *Pirogov S., Zhizhina E.*, A Quasispecies Continuous Contact Model in a Subcritical Regime // Moscow Math. J. 2019. V. 19. № 1. P. 121–132. https://doi.org/10.17323/1609-4514-2019-19-1-121-132
9. *Nowak M.* What Is a Quasispecies? // Trends Ecol. Evol. 1992. V. 7. № 4. P. 118–121. https://doi.org/10.1016/0169-5347(92)90145-2

10. *Pirogov S., Zhizhina E.* Contact Processes on General Spaces. Models on Graphs and on Manifolds // Electron. J. Probab. 2022. V. 27. Article no. 41 (14 pp.). doi.org/10.1214/22-EJP765
11. *Ruelle D.* Statistical Mechanics: Rigorous Results. New York: Benjamin, 1969.
12. *Lenard A.* Correlation Functions and the Uniqueness of the State in Classical Statistical Mechanics // Commun. Math. Phys. 1973. V. 30. № 1. P. 35–44. https://doi.org/10.1007/BF01646686
13. *Lenard A.* States of Classical Statistical Mechanical Systems of Infinitely Many Particles. II. Characterization of Correlation Measures // Arch. Rational Mech. Anal. 1975. V. 59. № 3. P. 241–256. https://doi.org/10.1007/BF00251602
14. *Petrov V.V.* Limit Theorems of Probability Theory: Sequences of Independent Random Variables. Oxford: Clarendon; New York: Oxford Univ. Press, 1995.

Жижина Елена Анатольевна
Пирогов Сергей Анатольевич
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
ejj@iitp.ru
s.a.pirogov@bk.ru

Поступила в редакцию
26.06.2023
После доработки
26.06.2023
Принята к публикации
20.10.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 519.173 : 004.722

© 2023 г. **В. Гао, Х.М. Башконуш, К. Каттани**

ЭФФЕКТИВНОСТЬ ПЕРЕДАЧИ ДАННЫХ ПРИ АТАКАХ С ТОЧКИ ЗРЕНИЯ ВАРИАНТА ИЗОЛИРОВАННОЙ ЖЕСТКОСТИ[1]

Модель сетевого графа является удобным инструментом для анализа сетей передачи информации, где возможность передачи в условиях атаки на объект можно описывать с помощью дробных критических графов, а уязвимость сети можно измерять с помощью варианта параметра изолированной жесткости. Рассматривается как устойчивость сети, так и реализуемость передачи данных при повреждении узлов, и определяется граница на вариант изолированной жесткости для дробных (a, b, n)-критических графов, где параметр n означает количество поврежденных узлов в определенный момент времени. С помощью контрпримера доказывается точность полученной границы на вариант изолированной жесткости. Основной теоретический вывод позволяет находить оптимальное соотношение между производительностью и стоимостью при проектировании топологии сети.

Ключевые слова: теория информации, сеть, граф, вариант изолированной жесткости, дробный (a, b, n)-критический граф.

DOI: 10.31857/S0555292323020067, **EDN:** PQHKAT

§ 1. Введение

В прошлом веке теория информации Шеннона заложила основы передачи информации по сетям и гарантировала реализуемость такой передачи. В настоящее время обработка информации в сети претерпела принципиальные изменения. Объем передаваемых данных резко возрос, и это приводит к тому, что при передаче информации необходимо учитывать ограниченность пропускной способности канала, ограниченный объем памяти в узлах, задержку в канале при стыковке фрагментов информации, сетевые атаки и другие факторы. В рамках модели сетевого графа вершины соответствуют узлам, ребра – каналам между узлами, а реализуемость передачи данных по сети может быть охарактеризована наличием дробного потока (дробный коэффициент работает как суррогатная модель) в соответствующем графе. В этой постановке из-за ограниченной пропускной способности канала большие данные разбиваются на несколько небольших фрагментов, передаются по различным каналам, и наконец, собираются воедино в конечной вершине (теоретический анализ см. в [1, 2]).

Однако реальная ситуация не так проста, как представляется. В случае кибератаки некоторые узлы и каналы повреждаются таким образом, что эффективная передача данных в исходной сети оказывается нарушенной. Кроме того, может понадобиться временно скорректировать первоначально запланированный маршрут передачи данных, т.е. определить, можно ли осуществить передачу данных в не подвергшемся атаке подграфе. С теоретической точки зрения дробный критический

[1] Работа выполнена при частичной финансовой поддержке Национального научного фонда Китая (номер гранта 12161094).

граф определяет, существует ли дробный фактор в подграфе, оставшемся после удаления фиксированного числа вершин из исходного графа, и позволяет эффективно измерять возможность передачи данных в условиях кибератаки (см. [3, 4]).

С топологической точки зрения чем плотнее структура сети, тем она устойчивее. Напротив, разреженная сеть в результате атаки повреждается сильнее и оказывается более неустойчивой. Однако стоимость построения высокоплотной сети очень велика. В общем случае инженерам необходимо находить баланс между производительностью и стоимостью сети, а также снижать эксплуатационные расходы при условии выполнения поставленных требований. В связи с этим возникают следующие вопросы:

1) Как измерять топологию сети?
2) Как оценивать передачу данных в сети, подвергающейся атаке?
3) Как находить упомянутый оптимальный баланс?

Как уже говорилось выше, различные варианты дробных критических графов применяются для характеризации передачи данных в подвергающейся атакам сети, а значит, для решения второй из поставленных выше задач. Что касается первой задачи, то для нее вводится несколько параметров графов для измерения топологии сетей, моделируемых графами, таких как связующее число [5], жесткость [6] и ее вариант [7], изолированная жесткость [8] и ее вариант [9], и т.д. К нашему удовольствию, исследования последних двух десятилетий показали, что существует тесная взаимосвязь между этими параметрами графа и существованием дробных факторов, в том числе дробных критических графов, при различных обстоятельствах.

В последние годы многочисленные теоретические достижения в области условий на параметры дробных факторов заложили солидный фундамент в области передачи данных по сетям. В частности, достижения в области границ на параметры для дробных критических графов в основном были связаны с передачей данных в условиях сетевых атак. В работе [10] была получена точная граница на вариант изолированной жесткости для графа с дробным k-фактором. В [11] исследованы нечеткие дробные коэффициенты в нечетких графах, соответствующих сетям с неопределенной информацией. В [12] получена точная граница на изолированную жесткость, при которой граф является дробным (k, n)-критическим. В [13] исследовано условие объединения окрестностей для дробных (a, b, k)-критических покрытых графов. В [14] дробные (a, b, k)-критические покрытые графы рассматривались с точки зрения минимальной степени и окрестностей независимых множеств. Совсем недавно в работе [15] была установлена точная граница на изолированную жесткость, при которой граф является дробным (a, b, n)-критическим, а именно: граф G является дробным (a, b, n)-критическим, если

$$\delta(G) \geqslant a + n$$

и

$$I(G) > a - 1 + \frac{n+1}{n_{a,b}},$$

где $n_{a,b}$ – наибольшее целое число, удовлетворяющее условию

$$b \geqslant (n_{a,b} - 1)a.$$

Несмотря на то, что уже получены обширные результаты об условиях существования дробных факторов через параметры графа, вопрос о точных границах на параметры графа в большинстве случаев остается открытым. Следует отметить, что нахождение точной границы на вариант изолированной жесткости, при которой существуют дробные факторы в конкретных постановках, является ключом к ответу на поставленный выше третий вопрос. Чем больше вариант изолированной

жесткости, тем больше плотность сети, тем устойчивее она к атакам и тем выше ее безопасность. Однако чем больше вариант изолированной жесткости, тем дороже построение соответствующей сети. Точная граница на вариант изолированной жесткости для дробных критических графов при определенных ограничениях позволяет инженерам находить оптимальный баланс между производительностью и стоимостью. С одной стороны, сеть, удовлетворяющая этой точной границе, обладает определенной степенью устойчивости и гарантирует передачу данных с определенной пропускной способностью при определенном уровне атак на узлы; с другой стороны, поскольку для варианта изолированной жесткости сети берется только нижняя граница, стоимость ее построения будет не слишком высока. Таким образом, это является стимулом для вывода точной границы на вариант изолированной жесткости для дробных критических графов в конкретных постановках.

Основным результатом данной статьи является определение точной границы на вариант изолированной жесткости для дробных (a, b, n)-критических графов. Дальнейшая часть статьи построена следующим образом. Вначале в § 2 приводятся обозначения и терминология, а также необходимые леммы. Затем в § 3 дается основная теорема и ее подробное доказательство. В заключительном § 4 обсуждаются некоторые перспективные направления для дальнейшей работы.

§ 2. Предварительные сведения

На протяжении всей статьи сети моделируются простыми конечными графами (т.е. ребра не имеют весов и направлений, петли отсутствуют, нет кратных ребер, число вершин конечно). Граф G состоит из множества вершин $V(G)$ и множества ребер $E(G)$, через $d_G(v)$ и $N_G(v)$ (или просто через $d(v)$ и $N(v)$) обозначаются, соответственно, степень и окрестность вершины v в G, и

$$\delta(G) = \min\{d_G(v) : v \in V(G)\}.$$

Пусть $G[S]$ – подграф графа G, индуцированный множеством $S \subseteq V(G)$. Обозначим через $i(G)$ число изолированных вершин в G. Оператор $\vee$ в записи $G_1 \vee G_2$ означает вставку ребер во всех парах (v_1, v_2), таких что $v_1 \in V(G_1)$ и $v_2 \in V(G_2)$. Используемые нами, но не определяемые здесь обозначения и термины можно найти в стандартном учебнике по теории графов [16].

Пусть a, b, k – натуральные числа, такие что $1 \leqslant a \leqslant b$, и пусть $h\colon E(G) \to [0, 1]$ – индикаторная функция, заданная на множестве ребер. *Дробным* $[a, b]$*-фактором* называется остовный подграф, состоящий из множества ребер

$$E_h = \{e \in E(G) \mid h(e) > 0\},$$

такой что

$$a \leqslant d_G^h(v) = \sum_{v' \in N(v)} h(vv') \leqslant b \tag{1}$$

для любой $v \in V(G)$. Граф G допускает дробный $[a, b]$-фактор, если существует индикаторная функция h, удовлетворяющая условию (1). Для числа $n \in \mathbb{N}$ граф G называется *дробным* (a, b, n)*-критическим графом*, если при удалении любых n вершин из G остающийся подграф по-прежнему является дробным $[a, b]$-фактором. В частности, если $a = b = k$, то понятия дробного $[a, b]$-фактора и дробного (a, b, n)-критического графа вырождаются до дробного k-фактора и дробного (k, n)-критического графа соответственно. В модели сетевых графов дробный (a, b, n)-критический граф означает, что соответствующая сеть позволяет передавать данные (в заданном интервале пропускной способности) синхронно по различным каналам, когда n ее узлов повреждены при атаке.

Одним из важных параметров графа является *вариант изолированной жесткости*, введенный в [9], который формально определяется как

$$I'(G) = \min\left\{ \frac{|S|}{i(G-S)-1} \;\Big|\; S \subset V(G),\ i(G-S) \geqslant 2 \right\},$$

если G не является полным графом, и $I'(G) = +\infty$, если граф G полный, так как в последнем случае подмножества вершин S, удовлетворяющего указанному условию, не существует. Следует отметить, что $I'(G)$ – единственный возможный вариант понятия изолированной жесткости. Представим себе, что имеется еще один вариант изолированной жесткости, выражаемый как наименьшее отношение $|S|$ к $i(G-S)-t$ для целого $t \geqslant 2$. В этом случае, чтобы знаменатель не оказался равен нулю, нужно ограничивать множество S условием $i(G-S) \geqslant t+1$, но такое подмножество вершин S не имеет никакого практического смысла (заметим, что наше условие $i(G-S) \geqslant 2$ означает, что S является разрезом в смысле изолированных вершин).

Для доказательства нашей основной теоремы в следующем параграфе нам потребуется необходимое и достаточное условие существования дробного (a,b,n)-критического графа.

Лемма 1 [17]. *Пусть a, b, n – положительные целые числа, такие что $a \leqslant b$. Тогда граф G является дробным (a,b,n)-критическим графом, если и только если условие*

$$b|S| - a|T| + \sum_{x \in T} d_{G-S}(x) \geqslant bn$$

выполнено для любого $S \subseteq V(G)$, такого что $|S| \geqslant n$, где

$$T = \{x \in V(G) - S \mid d_{G-S}(x) \leqslant a\}$$

(или, что равносильно, $T = \{x \in (G) - S \mid d_{G-S}(x) \leqslant a-1\}$).

При доказательстве основной теоремы в следующем параграфе для удобства рассуждений мы будем в основном использовать следующий равносильный вариант.

Лемма 2 [17]. *Пусть a, b, n – положительные целые числа, такие что $a \leqslant b$. Тогда граф G является дробным (a,b,n)-критическим графом, если и только если условие*

$$b|S| - a|T| + \sum_{x \in T} d_{G-S}(x) \geqslant bn$$

выполнено для любых непересекающихся подмножеств $S, T \subseteq V(G)$, таких что $|S| \geqslant n$.

§ 3. Основной результата и доказательство

Наш основной результат, представляющий точную границу на вариант изолированной жесткости, при которой граф является дробным (a,b,n)-критическим графом, состоит в следующем.

Теорема 1. *Пусть G – граф, и пусть a, b, n – натуральные числа, такие что*

$$2 \leqslant a \leqslant b \quad \text{и} \quad (n_{a,b}-1)a \leqslant b \leqslant n_{a,b}a - 1,$$

где $n_{a,b} \geqslant 2$ – целое число. Если

$$\delta(G) \geqslant a + n$$

и

$$I'(G) > a - 1 + \frac{a+n}{n_{a,b} - 1},$$

то G является дробным (a, b, n)-критическим графом.

Очевидно, что условие $\delta(G) \geqslant a+n$ является точным для дробных (a, b, n)-критических графов. Чтобы установить точность условия на $I'(G)$ в теореме 1, рассмотрим

$$G = K_{n+1} \vee (n_{a,b}K_a),$$

где a, b, n – натуральные числа, такие что $b \geqslant a \geqslant 2$, а $n_{a,b} \geqslant 2$ – целое число, определенное в теореме 1. Используя определение варианта изолированной жесткости, получаем

$$I'(G) = \frac{(n+1) + n_{a,b}(a-1)}{n_{a,b} - 1} = a - 1 + \frac{a+n}{n_{a,b} - 1}.$$

Полагая $S = V(K_{n+1})$ и $T = V(n_{a,b}K_a)$, получаем

$$b|S| - a|T| + \sum_{x \in T} d_{G-S}(x) = b(n+1) - n_{a,b}a = bn + b - n_{a,b}a < bn,$$

откуда следует, что G не является дробным (a, b, n)-критическим графом в силу леммы 2.

Полагая $a = b = k$ в теореме 1, получаем $n_{a,b} = 2$, и таким образом, для дробных (k, n)-критических графов имеем следующее.

Следствие. *Пусть G – граф, $k \geqslant 2$ и $n \geqslant 1$ – целые числа. Если*

$$\delta(G) \geqslant k + n$$

и

$$I'(G) > 2k + n - 1,$$

то G является дробным (k, n)-критическим графом.

Полагая в этом следствии $n = 0$, немедленно получаем основной результат работы [10], что показывает, что утверждение теоремы 1 улучшает все известные до сих пор условия на вариант изолированной жесткости для дробных факторов.

Далее излагается подробное доказательство.

3.1. Доказательство теоремы 1. Для полного графа утверждение теоремы 1 следует из условия на минимальную степень $\delta(G) \geqslant a+n$. Поэтому в дальнейшем будем рассматривать только неполные графы. Предположим, что граф G удовлетворяет условиям теоремы 1, но не является дробным (a, b, n)-критическим графом. В обозначениях леммы 2 существуют непересекающиеся подмножества S и T множества вершин $V(G)$, такие что $|S| \geqslant n$ и

$$b|S| - a|T| + \sum_{x \in T} d_{G-S}(x) = b|S| + \sum_{x \in T} (d_{G-S}(x) - a) \leqslant bn - 1. \tag{2}$$

Выберем S и T такими, чтобы мощность $|T|$ была минимальной. При таком выборе $T \neq \varnothing$ и $d_{G-S}(x) \leqslant a - 1$ для любого $x \in T$. Более того, поскольку $\delta(G) \geqslant a + n$, можно утверждать следующее.

Наблюдение 1. $|S| \geqslant n + 1$.

Все компоненты в $G[T]$ (обозначим через $\mathcal{C}$ множество всех этих компонент) можно разделить на четыре класса (обозначим их $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ и $\mathcal{C}_4$):

- Класс 1 ($\mathcal{C}_1$): $C \in \mathcal{C}$, такие что $C \cong K_a$;
- Класс 2 ($\mathcal{C}_2$): $C \in \mathcal{C}$, такие что $C \cong K_1$;
- Класс 3 ($\mathcal{C}_3$): $C \in \mathcal{C} - \mathcal{C}_1$, такие что $d_{G-S}(v) = a-1$ для любой $v \in V(C)$;
- Класс 4 ($\mathcal{C}_4$): $C \in \mathcal{C} - \{\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3\}$.

Положим $\ell_1 = |\mathcal{C}_1|$, $\ell_2 = |\mathcal{C}_2|$, и пусть S' — множество вершин, содержащее ровно $a-1$ вершин из каждой компоненты класса $\mathcal{C}_1$.

Если $|\mathcal{C}_3| + |\mathcal{C}_4| = 0$, то в силу неравенства (2) и наблюдения 1 получаем

$$n+1 \leqslant |S| \leqslant \frac{a(\ell_1+\ell_2)-1}{b} + n,$$

т.е. $b \leqslant a(\ell_1+\ell_2)-1$, откуда следует, что $\ell_1+\ell_2 \geqslant 2$ и

$$\ell_1+\ell_2 \geqslant \frac{b+1}{a} \geqslant \frac{(n_{a,b}-1)a+1}{a}.$$

Так как $\ell_1+\ell_2$ – целое число, отсюда следует, что $\ell_1+\ell_2 \geqslant n_{a,b}$. Пользуясь определением варианта изолированной жесткости, убеждаемся, что

$$i(G - S \cup S') = \ell_1+\ell_2 \geqslant 2$$

и

$$I'(G) \leqslant \frac{|S \cup S'|}{i(G-S-S')-1} \leqslant \frac{\left\lfloor \frac{a(\ell_1+\ell_2)-1}{b} + n + \ell_1(a-1) \right\rfloor}{\ell_1+\ell_2-1} \leqslant$$
$$\leqslant \frac{\left\lfloor \left(a-1+\frac{a}{b}\right)(\ell_1+\ell_2-1) + a - 1 + \frac{a-1}{b} + n \right\rfloor}{\ell_1+\ell_2-1} =$$
$$= a-1+\frac{a-1+n+\left\lfloor \frac{a(\ell_1+\ell_2)-1}{b} \right\rfloor}{\ell_1+\ell_2-1}.$$

Положим $a(\ell_1+\ell_2)-1 = n_1 b + \varepsilon_1$, где $n_1 \in \mathbb{N} \cup \{0\}$ и $\varepsilon_1 \in \{0,1,\ldots,b-1\}$. Тогда в силу того, что

$$a-1+n+\frac{a-\varepsilon_1-1}{b} > 0,$$

получаем

$$\max\left\{\frac{a-1+n+\left\lfloor \frac{a(\ell_1+\ell_2)-1}{b} \right\rfloor}{\ell_1+\ell_2-1}\right\} = \max\left\{\frac{a-1+n+\frac{a(\ell_1+\ell_2)-1}{b} - \frac{\varepsilon_1}{b}}{\ell_1+\ell_2-1}\right\} =$$
$$= \frac{a}{b} + \max\left\{\frac{a-1+n+\frac{a-\varepsilon_1-1}{b}}{\ell_1+\ell_2-1}\right\} = \frac{a}{b} + \frac{a-1+n+\frac{a-\varepsilon_1-1}{b}}{n_{a,b}-1},$$

что показывает, что величина

$$a-1+\frac{a-1+n+\left\lfloor \frac{a(\ell_1+\ell_2)-1}{b} \right\rfloor}{\ell_1+\ell_2-1}$$

принимает свое наибольшее значение, когда сумма $\ell_1 + \ell_2$ достигает своей нижней границы $n_{a,b}$. Следовательно,

$$I'(G) \leqslant a - 1 + \frac{a - 1 + n + \left\lfloor \frac{an_{a,b} - 1}{b} \right\rfloor}{n_{a,b} - 1} \leqslant a - 1 + \frac{a - 1 + n + \left\lfloor \frac{an_{a,b} - 1}{(n_{a,b} - 1)a} \right\rfloor}{n_{a,b} - 1} =$$
$$= a - 1 + \frac{a + n}{n_{a,b} - 1},$$

что противоречит условию

$$I'(G) > a - 1 + \frac{a + n}{n_{a,b} - 1}.$$

Следовательно, $|\mathcal{C}_3| + |\mathcal{C}_4| > 0$.

По определению класса $\mathcal{C}_4$ каждая компонента в $\mathcal{C}_4$ имеет вершину степени не выше $a - 2$ в $G - S$. Таки образом, если $\mathcal{C}_4 \neq \varnothing$, то $a \geqslant 3$, и его максимальное независимое множество I_4 можно выбрать с помощью следующей процедуры. Выберем вершину $v \in V(\mathcal{C}_4)$ с минимальной степенью в $G - S$ (степень вычисляется в исходном подграфе $G - S$ в каждом раунде процедуры выбора). Удалим ее замкнутую окрестность в $G - S$ (т.е. $N_{G-S}(v) \cup \{v\}$) и продолжим выбор следующей вершины в $V(\mathcal{C}_4)$ с помощью этого же принципа, пока не получим $V(\mathcal{C}_4) = \varnothing$. В итоге выбранная последовательность вершин и даст нам множество I_4.

Следующее наблюдение следует из того, что $\delta(G) \geqslant a + n$ и при этом в $\mathcal{C}_4$ есть по крайней мере одна вершина степени не выше $a - 2$ в $G - S$.

Наблюдение 2. Если $\mathcal{C}_4 \neq \varnothing$, то $|S| \geqslant n + 2$.

Положим $\Omega = V(G) - S - T$, выберем I_3 как максимальное независимое множество в $\mathcal{C}_3$, и пусть $\Theta = S \cup S' \cup N_{G-S}(I_3) \cup N_{G-S}(I_4)$. В общей ситуации следует рассмотреть два возможных случая.

Случай 1: $\boldsymbol{\ell_1 + \ell_2 \geqslant 1}$. Убедимся, что множества $\mathcal{C}_3$ и $\mathcal{C}_4$ не могут существовать поодиночке. Для этого докажем следующие два утверждения.

Утверждение 1. *Если $\ell_1 + \ell_2 \geqslant 1$, то $\mathcal{C}_4 \neq \varnothing$.*

Доказательство. Предположим, что $\mathcal{C}_4 = \varnothing$. Тогда $\mathcal{C}_3 \neq \varnothing$, так как $|\mathcal{C}_3| + |\mathcal{C}_4| > 0$.

Заметим, что I_3 можно разделить на следующие два подмножества I_{31} и I_{32}:

- $v \in I_{31}$, если существует $v' \in I_3 \setminus \{v\}$, такая что $N_{G-S}(v) \cap N_{G-S}(v') \neq \varnothing$;
- $v \in I_{32}$, если $N_{G-S}(v) \cap N_{G-S}(I_3 \setminus \{v\}) = \varnothing$.

Тогда получаем

$$b|S| \leqslant |V(\mathcal{C}_3)| + a\ell_1 + a\ell_2 + bn - 1 \leqslant$$
$$\leqslant \left(a - \frac{1}{2}\right)|I_{31}| + (a - 1)|I_{32}| + a(\ell_1 + \ell_2) + bn - 1$$

и

$$|S| \leqslant \left(\frac{a}{b} - \frac{1}{2b}\right)|I_{31}| + \frac{a - 1}{b}|I_{32}| - \frac{1}{b} + \frac{a(\ell_1 + \ell_2)}{b} + n < \frac{a(\ell_1 + \ell_2 + |I_3|)}{b} + n.$$

Используя наблюдение 1, получаем

$$\ell_1 + \ell_2 + |I_3| > \frac{b}{a},$$

и тем самым, $\ell_1 + \ell_2 + |I_3| \geqslant n_{a,b}$. Кроме того,

$$|S \cup S' \cup N_{G-S}(I_3)| \leqslant \Big(\frac{a}{b} - \frac{1}{2b}\Big)|I_{31}| + \frac{a-1}{b}|I_{32}| - \frac{1}{b} + \frac{a(\ell_1+\ell_2)}{b} + n +$$
$$+ \ell_1(a-1) + \Big(a - 1 - \frac{1}{2}\Big)|I_{31}| + (a-1)|I_{32}| = \Big(a - 1 + \frac{a}{b} - \frac{b+1}{2b}\Big)|I_{31}| +$$
$$+ \Big(a - 1 + \frac{a}{b} - \frac{1}{b}\Big)|I_{32}| + \frac{a}{b}\ell_2 + \Big(a - 1 + \frac{a}{b}\Big)\ell_1 + n - \frac{1}{b} \leqslant$$
$$\leqslant \Big(a - 1 + \frac{a}{b}\Big)(\ell_1 + \ell_2) + \Big(a - 1 + \frac{a}{b} - \frac{1}{b}\Big)|I_3| + n - \frac{1}{b} \leqslant$$
$$\leqslant \Big(a - 1 + \frac{a}{b}\Big)(|I_3| + \ell_1 + \ell_2) + n - \frac{2}{b},$$

и таким образом,

$$I'(G) \leqslant \frac{|S \cup S' \cup N_{G-S}(I_3)|}{i(G - S \cup S' \cup N_{G-S}(I_3)) - 1} \leqslant$$
$$\leqslant \frac{\Big\lfloor \Big(a - 1 + \frac{a}{b}\Big)(|I_3| + \ell_1 + \ell_2 - 1) + a - 1 + \frac{a-2}{b} + n \Big\rfloor}{|I_3| + \ell_1 + \ell_2 - 1} =$$
$$= a - 1 + \frac{\Big\lfloor \frac{a(|I_3| + \ell_1 + \ell_2) - 2}{b} \Big\rfloor + a - 1 + n}{|I_3| + \ell_1 + \ell_2 - 1}.$$

Пусть $a(|I_3| + \ell_1 + \ell_2) - 2 = n_2 b + \varepsilon_2$, где $n_2 \in \mathbb{N} \cup \{0\}$ и $\varepsilon_2 \in \{0, 1, \ldots, b-1\}$. Тогда получаем

$$\max\left\{ \frac{\Big\lfloor \frac{a(|I_3| + \ell_1 + \ell_2) - 2}{b} \Big\rfloor + a - 1 + n}{|I_3| + \ell_1 + \ell_2 - 1} \right\} =$$
$$= \max\left\{ \frac{\frac{a(|I_3| + \ell_1 + \ell_2) - 2 - \varepsilon_2}{b} + a - 1 + n}{|I_3| + \ell_1 + \ell_2 - 1} \right\} =$$
$$= \frac{a}{b} + \max\left\{ \frac{a - 1 + n + \frac{a - 2 - \varepsilon_2}{b}}{|I_3| + \ell_1 + \ell_2 - 1} \right\}.$$

Так как $a - 1 + n + \frac{a-2-\varepsilon_2}{b} > 0$, то величина

$$\frac{\Big\lfloor \frac{a(|I_3| + \ell_1 + \ell_2) - 2}{b} \Big\rfloor + a - 1 + n}{|I_3| + \ell_1 + \ell_2 - 1}$$

принимает свое максимальное значение, когда сумма $|I_3| + \ell_1 + \ell_2$ достигает своей нижней границы $n_{a,b}$. Следовательно,

$$I'(G) \leqslant a - 1 + \frac{\Big\lfloor \frac{a n_{a,b} - 2}{b} \Big\rfloor + a - 1 + n}{n_{a,b} - 1} \leqslant a - 1 + \frac{\Big\lfloor \frac{a n_{a,b} - 2}{(n_{a,b} - 1)a} \Big\rfloor + a - 1 + n}{n_{a,b} - 1} =$$
$$= a - 1 + \frac{n + a}{n_{a,b} - 1},$$

что противоречит предположению о величине $I'(G)$. ▲

Утверждение 2. *Если* $\ell_1 + \ell_2 \geqslant 1$, *то* $\mathcal{C}_3 \neq \varnothing$.

Доказательство. Если $\mathcal{C}_3 = \varnothing$, то $\mathcal{C}_4 \neq \varnothing$, так как $|\mathcal{C}_3| + |\mathcal{C}_4| > 0$, и следовательно, $a \geqslant 3$.

Пусть $I_4 = \{v_1, v_2, \ldots, v_{|I_4|}\}$, где $d_{G-S}(v_1) \leqslant a-2$ и

$$d_{G-S}(v_1) \leqslant d_{G-S}(v_2) \leqslant \ldots \leqslant d_{G-S}(v_{|I_4|}).$$

Тогда имеем $|T| = |V(\mathcal{C}_4)| + a\ell_1 + \ell_2$,

$$b|S| \leqslant a|T| - d_{G-S}(T) + bn - 1 \leqslant$$
$$\leqslant a\ell_1 + a\ell_2 + \sum_{i=1}^{|I_4|}(d_{G-S}(v_i)+1)(a - d_{G-S}(v_i)) + bn - 1$$

и

$$|S| \leqslant \frac{a(\ell_1+\ell_2)}{b} + \frac{\sum\limits_{i=1}^{|I_4|}(d_{G-S}(v_i)+1)(a-d_{G-S}(v_i))}{b} + n - \frac{1}{b}.$$

Получаем, что $i(G-\Theta) \geqslant 2$, где $\Theta = S \cup S' \cup N_{G-S}(I_4)$, и

$$|\Theta| \leqslant |S| + |S'| + |N_{G-S}(I_4)| \leqslant \frac{a(\ell_1+\ell_2)}{b} +$$
$$+ \frac{\sum\limits_{i=1}^{|I_4|}(d_{G-S}(v_i)+1)(a-d_{G-S}(v_i))}{b} + n - \frac{1}{b} + \ell_1(a-1) + \sum_{i=1}^{|I_4|} d_{G-S}(v_i) =$$
$$= \frac{a\ell_2}{b} + \ell_1\Big(a-1+\frac{a}{b}\Big) + \sum_{i=1}^{|I_4|}\Big(-\frac{d^2_{G-S}(v_i)}{b} + \frac{a+b-1}{b}d_{G-S}(v_i) + \frac{a}{b}\Big) + n - \frac{1}{b} \leqslant$$
$$\leqslant \frac{a\ell_2}{b} + \ell_1\Big(a-1+\frac{a}{b}\Big) + \Big(-\frac{(a-2)^2}{b} + \frac{a+b-1}{b}(a-2) + \frac{a}{b}\Big) +$$
$$+ (|I_4|-1)\Big(-\frac{(a-1)^2}{b} + \frac{a+b-1}{b}(a-1) + \frac{a}{b}\Big) + n - \frac{1}{b} =$$
$$= \frac{a\ell_2}{b} + \ell_1\Big(a-1+\frac{a}{b}\Big) + \Big(a-1+\frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-3}{b}.$$

Чтобы найти экстремум величины $I'(G)$, будем максимизировать $|\Theta|$ при фиксированном значении $|I_4|$, тогда только одна вершина из I_4 имеет степень $a-2$ в $G-S$, а все остальные имеют степень $a-1$ в $G-S$. Чтобы оценить сумму $\ell_1 + \ell_2 + |I_4|$, заново оценим $|S|$ сверху как

$$|S| \leqslant \frac{a(\ell_1+\ell_2)}{b} + \frac{(|I_4|-1)(a-1+1)(a-(a-1)) + (a-2+1)(a-(a-2))}{b} +$$
$$+ n - \frac{1}{b} = \frac{a(\ell_1+\ell_2+|I_4|)+a-3}{b} + n.$$

С учетом наблюдения 2 имеем

$$2 + n \leqslant |S| \leqslant \frac{a(\ell_1+\ell_2+|I_4|)+a-3}{b} + n,$$

откуда

$$\ell_1+\ell_2+|I_4|\geqslant\frac{2b-a+3}{a}\geqslant\frac{2(n_{a,b}-1)a-a+3}{a}=2n_{a,b}-3+\frac{3}{a},$$

т.е. $\ell_1+\ell_2+|I_4|\geqslant 2n_{a,b}-2$.

Используя определение варианта изолированной жесткости, получаем

$$\begin{aligned}
&I'(G)\leqslant\frac{|\Theta|}{i(G-\Theta)-1}\leqslant\\
&\leqslant\frac{\left\lfloor\frac{a\ell_2}{b}+\ell_1\left(a-1+\frac{a}{b}\right)+\left(a-1+\frac{a}{b}\right)|I_4|+n-1+\frac{a-3}{b}\right\rfloor}{|I_4|+\ell_1+\ell_2-1}\leqslant\\
&\leqslant\frac{\left\lfloor\left(a-1+\frac{a}{b}\right)(\ell_1+\ell_2+|I_4|-1)+\left(a-1+\frac{a}{b}\right)+n-1+\frac{a-3}{b}\right\rfloor}{|I_4|+\ell_1+\ell_2-1}=\\
&=a-1+\frac{a+n-2+\left\lfloor\frac{a(\ell_1+\ell_2+|I_4|)+a-3}{b}\right\rfloor}{|I_4|+\ell_1+\ell_2-1}.
\end{aligned}$$

Пусть $a(|I_4|+\ell_1+\ell_2)+a-3=n_3b+\varepsilon_3$, где $n_3\in\mathbb{N}\cup\{0\}$ и $\varepsilon_3\in\{0,1,\ldots,b-1\}$. Тогда получаем

$$\begin{aligned}
&\max\left\{\frac{a+n-2+\left\lfloor\frac{a(\ell_1+\ell_2+|I_4|)+a-3}{b}\right\rfloor}{|I_4|+\ell_1+\ell_2-1}\right\}=\\
&=\max\left\{\frac{a+n-2+\frac{a(\ell_1+\ell_2+|I_4|)+a-3-\varepsilon_3}{b}}{|I_4|+\ell_1+\ell_2-1}\right\}=\\
&=\frac{a}{b}+\max\left\{\frac{a+n-2+\frac{2a-3-\varepsilon_3}{b}}{|I_4|+\ell_1+\ell_2-1}\right\}.
\end{aligned}$$

Следовательно, величина

$$\frac{a+n-2+\left\lfloor\frac{a(\ell_1+\ell_2+|I_4|)+a-3}{b}\right\rfloor}{|I_4|+\ell_1+\ell_2-1}$$

принимает свое максимальное значение, когда сумма $|I_4|+\ell_1+\ell_2$ достигает своей нижней границы $2n_{a,b}-2$, так как

$$a+n-2+\frac{2a-3-\varepsilon_3}{b}>0.$$

Получаем

$$\begin{aligned}
&I'(G)\leqslant a-1+\frac{a+n-2+\left\lfloor\frac{a(2n_{a,b}-2)+a-3}{b}\right\rfloor}{2n_{a,b}-2-1}\leqslant\\
&\leqslant a-1+\frac{a+n-2+\left\lfloor\frac{a(2n_{a,b}-2)+a-3}{(n_{a,b}-1)a}\right\rfloor}{2n_{a,b}-3}=a-1+\frac{a+n}{2n_{a,b}-3},
\end{aligned}$$

что противоречит условиям

$$I'(G) > a - 1 + \frac{n+a}{n_{a,b} - 1}$$

и $n_{a,b} \geqslant 2$. ▲

Итак, в силу утверждений 1, 2 имеем $\mathcal{C}_3 \neq \varnothing$, $\mathcal{C}_4 \neq \varnothing$ и $a \geqslant 3$.
Пусть $I_4 = \{v_1, v_2, \ldots, v_{|I_4|}\}$, как в доказательстве утверждения 2. Тогда имеем

$$|T| = |V(\mathcal{C}_3)| + |V(\mathcal{C}_4)| + \ell_2 + a\ell_1,$$
$$b|S| \leqslant a|T| - d_{G-S}(T) + bn - 1 \leqslant a(\ell_1 + \ell_2) + \Big(a - \frac{1}{2}\Big)|I_{31}| + (a-1)|I_{32}| +$$
$$+ \sum_{i=1}^{|I_4|}(d_{G-S}(v_i) + 1)(a - d_{G-S}(v_i)) + bn - 1$$

и

$$|S| \leqslant \frac{1}{b}\Bigg(a(\ell_1 + \ell_2) + \Big(a - \frac{1}{2}\Big)|I_{31}| + (a-1)|I_{32}| +$$
$$+ \sum_{i=1}^{|I_4|}(d_{G-S}(v_i) + 1)(a - d_{G-S}(v_i)) + bn - 1\Bigg) = \frac{a}{b}(\ell_1 + \ell_2) + \Big(\frac{a}{b} - \frac{1}{2b}\Big)|I_{31}| +$$
$$+ \frac{a-1}{b}|I_{32}| + \frac{\sum\limits_{i=1}^{|I_4|}(d_{G-S}(v_i) + 1)(a - d_{G-S}(v_i))}{b} + n - \frac{1}{b}.$$

Получаем $i(G - \Theta) \geqslant 3$, где

$$\Theta = S \cup S' \cup N_{G-S}(I_3) \cup N_{G-S}(I_4).$$

В соответствии с вычислениями, проведенными в доказательствах утверждений 1, 2, имеем

$$|\Theta| \leqslant \frac{a}{b}(\ell_1 + \ell_2) + \Big(\frac{a}{b} - \frac{1}{2b}\Big)|I_{31}| + \frac{a-1}{b}|I_{32}| +$$
$$+ \frac{\sum\limits_{i=1}^{|I_4|}(d_{G-S}(v_i) + 1)(a - d_{G-S}(v_i))}{b} + n - \frac{1}{b} + \ell_1(a-1) + \Big(a - \frac{1}{2} - 1\Big)|I_{31}| +$$
$$+ (a-1)|I_{32}| + \sum_{i=1}^{|I_4|} d_{G-S}(v_i) \leqslant \frac{a}{b}\ell_1 + \ell_2\Big(a - 1 + \frac{a}{b}\Big) + \Big(a - 1 + \frac{a}{b} - \frac{1}{b}\Big)|I_3| +$$
$$+ \Big(a - 1 + \frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-3}{b} \leqslant (\ell_1 + \ell_2)\Big(a - 1 + \frac{a}{b}\Big) + \Big(a - 1 + \frac{a}{b}\Big)|I_3| +$$
$$+ \Big(a - 1 + \frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-4}{b}.$$

При максимизации $|\Theta|$ только одна вершина из I_4 имеет степень $a-2$ в $G - S$, а остальные имеют степень $a-1$ в $G - S$. Чтобы оценить сумму $\ell_1 + \ell_2 + |I_3| + |I_4|$,

заново оценим $|S|$ сверху как

$$|S| \leqslant \frac{a(\ell_1+\ell_2)}{b} + \Big(\frac{a}{b} - \frac{1}{2b}\Big)|I_3| + \\ + \frac{(|I_4|-1)(a-1+1)(a-(a-1)) + (a-2+1)(a-(a-2))}{b} + n - \frac{1}{b} < \\ < \frac{a(\ell_1+\ell_2+|I_3|+|I_4|)+a-3}{b} + n.$$

Согласно наблюдению 2 получаем

$$2+n \leqslant |S| < \frac{a(\ell_1+\ell_2+|I_3|+|I_4|)+a-3}{b} + n,$$

откуда

$$\ell_1+\ell_2+|I_3|+|I_4| > \frac{2b-a+3}{a} \geqslant \frac{2(n_{a,b}-1)a-a+3}{a} = 2n_{a,b}-3+\frac{3}{a},$$

т.е.

$$\ell_1+\ell_2+|I_3|+|I_4| \geqslant 2n_{a,b}-2.$$

Используя определение величины $I'(G)$, получаем

$$I'(G) \leqslant \frac{|\Theta|}{i(G-\Theta)-1} \leqslant \\ \leqslant \frac{\Big\lfloor \Big(a-1+\frac{a}{b}\Big)(\ell_1+\ell_2+|I_3|+|I_4|-1) + \Big(a-1+\frac{a}{b}\Big) + n - 1 + \frac{a-4}{b} \Big\rfloor}{|I_3|+|I_4|+\ell_1+\ell_2-1} = \\ = a-1+\frac{a+n-2+\Big\lfloor \frac{a(|I_3|+|I_4|+\ell_1+\ell_2)+a-4}{b} \Big\rfloor}{|I_3|+|I_4|+\ell_1+\ell_2-1}.$$

Пусть $a(|I_3|+|I_4|+\ell_1+\ell_2)+a-4 = n_4 b + \varepsilon_4$, где $n_4 \in \mathbb{N}\cup\{0\}$ и $\varepsilon_4 \in \{0,1,\ldots,b-1\}$. Тогда

$$\max\left\{ \frac{a+n-2+\Big\lfloor \frac{a(|I_3|+|I_4|+\ell_1+\ell_2)+a-4}{b} \Big\rfloor}{|I_3|+|I_4|+\ell_1+\ell_2-1} \right\} = \\ = \max\left\{ \frac{a+n-2+\frac{a(|I_3|+|I_4|+\ell_1+\ell_2)+a-4-\varepsilon_4}{b}}{|I_3|+|I_4|+\ell_1+\ell_2-1} \right\} = \\ = \frac{a}{b} + \max\left\{ \frac{a+n-2+\frac{2a-4-\varepsilon_4}{b}}{|I_3|+|I_4|+\ell_1+\ell_2-1} \right\}.$$

Так как

$$a+n-2+\frac{2a-4-\varepsilon_4}{b} > 0,$$

то величина

$$\frac{a+n-2+\frac{2a-4-\varepsilon_4}{b}}{|I_3|+|I_4|+\ell_1+\ell_2-1}$$

принимает свое максимальное значение, когда сумма $|I_3| + |I_4| + \ell_1 + \ell_2$ достигает нижней границы $2n_{a,b} - 2$. Получаем

$$I'(G) \leqslant a - 1 + \frac{a + n - 2 + \left\lfloor \frac{a(2n_{a,b} - 2) + a - 4}{b} \right\rfloor}{2n_{a,b} - 2 - 1} \leqslant$$

$$\leqslant a - 1 + \frac{a + n - 2 + \left\lfloor \frac{a(2n_{a,b} - 2) + a - 4}{(n_{a,b} - 1)a} \right\rfloor}{2n_{a,b} - 3} \leqslant a - 1 + \frac{a + n}{2n_{a,b} - 3},$$

что противоречит условиям

$$I'(G) > a - 1 + \frac{n + a}{n_{a,b} - 1}$$

и $n_{a,b} \geqslant 2$.

Случай 2: $\boldsymbol{\ell_1 + \ell_2 = 0}$. Аналогично случаю 1 утверждения 3 и 4 покажут, что множества $\mathcal{C}_3$ и $\mathcal{C}_4$ не могут существовать поодиночке.

Утверждение 3. *Если $\ell_1 + \ell_2 = 0$, то $\mathcal{C}_4 \neq \varnothing$.*

Доказательство. Если $\mathcal{C}_4 = \varnothing$, то $\mathcal{C}_3 \neq \varnothing$, $|T| = |V(\mathcal{C}_3)|$ и

$$b|S| \leqslant a|T| - d_{G-S}(T) + bn - 1 = |T| + bn - 1.$$

Если $|I_3| = 1$, то $|T| \leqslant a - 1$, и в силу наблюдения 1 имеем

$$n + 1 \leqslant |S| \leqslant \frac{|T| + bn - 1}{b} \leqslant n + \frac{a - 2}{b},$$

противоречие. Следовательно, $|I_3| \geqslant 2$.

В таком случае $i(G - \Theta) \geqslant |I_3| \geqslant 2$, где $\Theta = S \cup N_G(I_3)$, и следуя рассуждениям в доказательстве утверждения 1, получаем

$$|S| \leqslant \Big(\frac{a}{b} - \frac{1}{2b}\Big)|I_{31}| + \frac{a-1}{b}|I_{32}| - \frac{1}{b} + n < \frac{a|I_3|}{b} + n,$$
$$|\Theta| \leqslant \Big(a - 1 + \frac{a-1}{b}\Big)|I_3| + n - \frac{1}{b} \leqslant \Big(a - 1 + \frac{a}{b}\Big)|I_3| + n - \frac{3}{b}.$$

В силу наблюдения 1 получаем, что $|I_3| > \dfrac{b}{a}$, т.е. $|I_3| \geqslant n_{a,b}$.

Следовательно,

$$I'(G) \leqslant \frac{|\Theta|}{i(G - \Theta) - 1} \leqslant \frac{\left\lfloor \Big(a - 1 + \frac{a}{b}\Big)|I_3| + n - \frac{3}{b} \right\rfloor}{|I_3| - 1} =$$
$$= a - 1 + \frac{n + a - 1 + \left\lfloor \frac{a|I_3| - 3}{b} \right\rfloor}{|I_3| - 1}.$$

Пусть $a|I_3| - 3 = n_5 b + \varepsilon_5$, где $n_5 \in \mathbb{N} \cup \{0\}$ и $\varepsilon_5 \in \{0, 1, \ldots, b-1\}$. Тогда получаем

$$\max\left\{ \frac{\left\lfloor \frac{a|I_3| - 3}{b} \right\rfloor + n + a - 1}{|I_3| - 1} \right\} = \max\left\{ \frac{\frac{a|I_3| - 3 - \varepsilon_5}{b} + n + a - 1}{|I_3| - 1} \right\} =$$
$$= \frac{a}{b} + \max\left\{ \frac{n + a - 1 + \frac{a - 3 - \varepsilon_5}{b}}{|I_3| - 1} \right\}.$$

Так как

$$n + a - 1 + \frac{a - 3 - \varepsilon_5}{b} > 0,$$

то величина

$$\frac{n + a - 1 + \left\lfloor \frac{a|I_3| - 3}{b} \right\rfloor}{|I_3| - 1}$$

принимает максимальное значение, когда $|I_3|$ достигает своей нижней границы $n_{a,b}$. Получаем

$$I'(G) \leqslant a - 1 + \frac{\left\lfloor \frac{an_{a,b} - 3}{b} \right\rfloor + n + a - 1}{n_{a,b} - 1} \leqslant$$
$$\leqslant a - 1 + \frac{\left\lfloor \frac{an_{a,b} - 3}{(n_{a,b} - 1)a} \right\rfloor + n + a - 1}{n_{a,b} - 1} \leqslant a - 1 + \frac{n + a}{n_{a,b} - 1},$$

что противоречит условию на вариант изолированной жесткости. ▲

Утверждение 4. *Если* $\ell_1 + \ell_2 = 0$, *то* $\mathcal{C}_3 \neq \varnothing$.

Доказательство. Если $\mathcal{C}_3 = \varnothing$, то $\mathcal{C}_4 \neq \varnothing$ и $a \geqslant 3$.
Если $|I_4| = 1$, положим

$$d_{\min} = \min\{d_{G-S}(v) \mid v \in \mathcal{C}_4\},$$

и пусть $z \in V(\mathcal{C}_4)$ такова, что $d_{G-S}(z) = d_{\min}$, здесь $d_{\min} \in \{1, \ldots, a-2\}$. Тогда получаем

$$b|S| \leqslant a|T| - d_{G-S}(T) + bn - 1 \leqslant |T|(a - d_{\min}) + bn - 1,$$
$$|S| \leqslant \frac{|T|(a - d_{\min}) + bn - 1}{b} \leqslant \frac{(a-1)(a - d_{\min}) - 1}{b} + n$$

и

$$a + n \leqslant \delta(G) \leqslant d_{\min} + |S| \leqslant d_{\min} + \frac{(a-1)(a - d_{\min}) - 1}{b} + n =$$
$$= \frac{a^2}{b} - \frac{a}{b} + \frac{(b - a + 1)d_{\min}}{b} - \frac{1}{b} + n \leqslant \frac{a^2}{b} - \frac{a}{b} + \frac{(b - a + 1)(a-2)}{b} - \frac{1}{b} + n =$$
$$= a - 2 + n + \frac{2a - 3}{b},$$

противоречие.

Следовательно, $|I_4| \geqslant 2$. Пусть $v_1, v_2, \ldots, v_{|I_4|}$ – вершины из I_4, определяемые как в доказательстве утверждения 2, т.е. $d_{G-S}(v_1) \leqslant a - 2$ и

$$d_{G-S}(v_1) \leqslant d_{G-S}(v_2) \leqslant \ldots \leqslant d_{G-S}(v_{|I_4|}).$$

Имеем $|T| = |V(\mathcal{C}_4)|$,

$$b|S| \leqslant a|T| - d_{G-S}(T) + bn - 1 \leqslant \sum_{i=1}^{|I_4|} (d_{G-S}(v_i) + 1)(a - d_{G-S}(v_i)) + bn - 1$$

и

$$|S| \leqslant \frac{\sum\limits_{i=1}^{|I_4|}(d_{G-S}(v_i)+1)(a-d_{G-S}(v_i))}{b} + n - \frac{1}{b}.$$

Значит, $i(G-\Theta) \geqslant |I_4| \geqslant 2$, где $\Theta = S \cup N_{G-S}(I_4)$, и в силу рассуждений в доказательстве утверждения 2 получаем

$$|\Theta| \leqslant |S| + |N_{G-S}(I_4)| \leqslant \Big(a - 1 + \frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-3}{b}.$$

При максимизации $|\Theta|$ только одна вершина из I_4 имеет степень $a-2$ в $G-S$, а остальные имеют степень $a-1$ в $G-S$. Чтобы оценить $|I_4|$, перепишем оценку сверху для $|S|$ в виде

$$|S| \leqslant \frac{(|I_4|-1)(a-1+1)(a-(a-1)) + (a-2+1)(a-(a-2))}{b} + n - \frac{1}{b} \leqslant$$
$$\leqslant \frac{a|I_4| + a - 3}{b} + n.$$

С учетом наблюдения 2 получаем

$$2 + n \leqslant |S| \leqslant \frac{a|I_4| + a - 3}{b} + n,$$

откуда

$$|I_4| \geqslant \frac{2b - a + 3}{a} \geqslant \frac{2(n_{a,b}-1)a - a + 3}{a} = 2n_{a,b} - 3 + \frac{3}{a},$$

т.е. $|I_4| \geqslant 2n_{a,b} - 2$.

Действуя тем же способом, что и выше, получаем

$$I'(G) \leqslant \frac{|\Theta|}{i(G-\Theta)-1} \leqslant \frac{\Big\lfloor \Big(a-1+\frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-3}{b} \Big\rfloor}{|I_4|-1} =$$
$$= a - 1 + \frac{n + a - 2 + \Big\lfloor \frac{a|I_4| + a - 3}{b} \Big\rfloor}{|I_4|-1}.$$

Пусть $a|I_4| + a - 3 = n_6 b + \varepsilon_6$, где $n_6 \in \mathbb{N} \cup \{0\}$ и $\varepsilon_6 \in \{0, 1, \ldots, b-1\}$. Тогда

$$\max\left\{\frac{n + a - 2 + \Big\lfloor \frac{a|I_4| + a - 3}{b} \Big\rfloor}{|I_4|-1}\right\} = \max\left\{\frac{n + a - 2 + \frac{a|I_4| + a - 3 - \varepsilon_6}{b}}{|I_4|-1}\right\} =$$
$$= \frac{a}{b} + \max\left\{\frac{n + a - 2 + \frac{2a - 3 - \varepsilon_6}{b}}{|I_4|-1}\right\}.$$

Так как

$$n + a - 2 + \frac{2a - 3 - \varepsilon_6}{b} > 0,$$

то величина

$$\frac{n + a - 2 + \Big\lfloor \frac{a|I_4| + a - 3}{b} \Big\rfloor}{|I_4|-1}$$

принимает свое максимальное значение, когда $|I_4|$ достигает своей нижней границы $2n_{a,b}-2$. Получаем

$$I'(G) \leqslant a-1+\frac{n+a-2+\left\lfloor\frac{a(2n_{a,b}-2)+a-3}{b}\right\rfloor}{2n_{a,b}-2-1} \leqslant$$

$$\leqslant a-1+\frac{n+a-2+\left\lfloor\frac{a(2n_{a,b}-2)+a-3}{(n_{a,b}-1)a}\right\rfloor}{2n_{a,b}-3} = a-1+\frac{n+a}{2n_{a,b}-3},$$

что противоречит условиям

$$I'(G) > a-1+\frac{n+a}{n_{a,b}-1}$$

и $n_{a,b} \geqslant 2$. ▲

Итак, в силу утверждений 3, 4 имеем

$$\mathcal{C}_3 \neq \varnothing, \quad \mathcal{C}_4 \neq \varnothing, \quad a \geqslant 3, \quad i(G-\Theta) \geqslant 2,$$

где

$$\Theta = S \cup N_{G-S}(I_3) \cup N_{G-S}(I_4),$$

и

$$\begin{aligned}|\Theta| &\leqslant |S| + |N_{G-S}(I_3)| + |N_{G-S}(I_4)| \\ &\leqslant \Big(a-1+\frac{a-1}{b}\Big)|I_3| + \Big(a-1+\frac{a}{b}\Big)|I_4| + n - 1 + \frac{a-3}{b} \\ &\leqslant \Big(a-1+\frac{a}{b}\Big)(|I_3|+|I_4|) + n - 1 + \frac{a-4}{b}.\end{aligned}$$

Рассуждениями, аналогичными случаю 1, убеждаемся, что

$$|I_3| + |I_4| \geqslant 2n_{a,b} - 2,$$

используя наблюдение 2 и заново оценивая $|S|$ сверху.

Таким образом,

$$I'(G) \leqslant \frac{|\Theta|}{i(G-\Theta)-1} \leqslant \frac{\left\lfloor\Big(a-1+\frac{a}{b}\Big)(|I_3|+|I_4|) + n - 1 + \frac{a-4}{b}\right\rfloor}{|I_3|+|I_4|-1} =$$

$$= a-1+\frac{n+a-2+\left\lfloor\frac{a(|I_3|+|I_4|)+a-4}{b}\right\rfloor}{|I_3|+|I_4|-1}.$$

Пусть $a(|I_3|+|I_4|)+a-4 = n_7 b + \varepsilon_7$, где $n_7 \in \mathbb{N}\cup\{0\}$ и $\varepsilon_7 \in \{0,1,\ldots,b-1\}$. Тогда

$$\max\left\{\frac{n+a-2+\left\lfloor\frac{a(|I_3|+|I_4|)+a-4}{b}\right\rfloor}{|I_3|+|I_4|-1}\right\} =$$

$$= \max\left\{\frac{n+a-2+\frac{a(|I_3|+|I_4|)+a-4-\varepsilon_7}{b}}{|I_3|+|I_4|-1}\right\} =$$

$$= \frac{a}{b} + \max\left\{\frac{n+a-2+\frac{2a-4-\varepsilon_7}{b}}{|I_3|+|I_4|-1}\right\}.$$

Так как

$$n + a - 2 + \frac{2a - 4 - \varepsilon_7}{b} > 0,$$

то величина

$$\frac{n + a - 2 + \left\lfloor \frac{a(|I_3| + |I_4|) + a - 4}{b} \right\rfloor}{|I_3| + |I_4| - 1}$$

принимает максимальное значение, когда $|I_3| + |I_4|$ достигает своей нижней границы $2n_{a,b} - 2$. Следовательно,

$$I'(G) \leqslant a - 1 + \frac{n + a - 2 + \left\lfloor \frac{a(2n_{a,b} - 2) + a - 4}{b} \right\rfloor}{2n_{a,b} - 2 - 1} \leqslant$$

$$\leqslant a - 1 + \frac{n + a - 2 + \left\lfloor \frac{a(2n_{a,b} - 2) + a - 4}{(n_{a,b} - 1)a} \right\rfloor}{2n_{a,b} - 3} \leqslant a - 1 + \frac{n + a}{2n_{a,b} - 3},$$

что противоречит условиям

$$I'(G) > a - 1 + \frac{n + a}{n_{a,b} - 1}$$

и $n_{a,b} \geqslant 2$.

Итак, на этом доказательство теоремы 1 завершается.

§ 4. Заключение и направления дальнейшей работы

В статье рассмотрена возможность передачи данных в подвергающейся атакам сети с точки зрения модели дробных критических графов, которая связана с вариантом изолированной жесткости, измеряющим уязвимость сетей. Получена точная граница на вариант изолированной жесткости для дробного (a, b, n)-критического графа, обеспечивающая оптимальный баланс между производительностью сети и ее стоимостью и являющаяся теоретической основой для проектирования топологии сети. Кроме того, полученный вывод позволяет анализировать возможность передачи данных при повреждении узлов в сети в результате атаки.

Тем не менее, данная статья содержит только теоретический анализ и не моделирует реальные сети, которые хотелось бы изучить в будущем. Ниже перечислены наиболее интересные на наш взгляд темы, требующие дальнейшего изучения.

- Дробный фактор моделирует только синхронную передачу данных. Однако в реальных сетях при передаче данных часто возникают задержки. То, как можно охарактеризовать задержку в модели сетевых графов, еще подлежит тщательному изучению.
- Каждый узел в сети имеет свой собственный статус и отдельную функцию, поэтому для описания объема памяти всех узлов не может использоваться единый интервал $[a, b]$. Таким образом, в будущих исследованиях следует заменить дробный $[a, b]$-фактор на дробный (g, f)-фактор. Соответственно, возможность передачи данных должна исследоваться в более широких контекстах.
- В работе [11] введен нечеткий дробный коэффициент в нечетких графах, который позволяет работать с сетями, содержащими неопределенную информацию. Однако в этой работе не было четко сформулировано, как количественно оценивать неопределенность (т.е. как строить функцию принадлежности в сетях передачи данных). Создается впечатление, что существует большой разрыв между

теоретическим анализом и реальными приложениями. Необходимо ввести разумные правила для количественной оценки параметров неопределенности каналов и узлов, таких как коэффициент использования, пропускная способность восходящего и нисходящего каналов, время задержки, качество входа в канал и т.д.

- В теореме 1 для заключения требуются условия как на $\delta(G)$, так и на $I'(G)$, причем $a+n$ является минимальной нижней границей на $\delta(G)$. Если повышать нижнюю границу на $\delta(G)$, то можно ли при этом уменьшить нижнюю границу на $I'(G)$? Если ответ на этот вопрос положительный, то мы получим множество оптимальных решений для $\delta(G)$ и $I'(G)$, что является аналогом фронта Парето в задачах многоцелевой оптимизации (МО). Однако в этих обстоятельствах решение проектировщика сети может стать фатальным, и необходимо находить точку равновесия между $\delta(G)$ и $I'(G)$, аналогичную точке загиба в МО.

Авторы заявляют об отсутствии конфликта интересов при публикации данной статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Zhou S., Liu H., Xu Y.* A Note on Fractional ID-$[a,b]$-Factor-Critical Covered Graphs // Discrete Appl. Math. 2022. V. 319. P. 511–516. https://doi.org/10.1016/j.dam.2021.03.004
2. *Zhou S., Wu J., Bian Q.* On Path-Factor Critical Deleted (or Covered) Graphs // Aequationes Math. 2022. V. 96. № 4. P. 795–802. https://doi.org/10.1007/s00010-021-00852-4
3. *Zhou S., Wu J., Liu H.* Independence Number and Connectivity for Fractional (a,b,k)-Critical Covered Graphs // RAIRO Oper. Res. 2022. V. 56. № 4. P. 2535–2542. https://doi.org/10.1051/ro/2022119
4. *Gao W., Wang W.* New Isolated Toughness Condition for Fractional (g,f,n)-Critical Graphs // Colloq. Math. 2017. V. 147. P. 55–66. https://doi.org/10.4064/cm6713-8-2016
5. *Woodall D.* The Binding Number of a Graph and Its Anderson Number // J. Combin. Theory Ser. B. 1973. V. 15. № 3. P. 225–255. https://doi.org/10.1016/0095-8956(73)90038-5
6. *Chvátal V.* Tough Graphs and Hamiltonian Circuits // Discrete Math. 1973. V. 5. № 3. P. 215–228. https://doi.org/10.1016/0012-365X(73)90138-6
7. *Enomoto H.* Toughness and the Existence of k-Factors. III // Discrete Math. 1998. V. 189. № 1–3. P. 277–282. https://doi.org/10.1016/S0012-365X(98)00059-4
8. *Yang J., Ma Y., Liu G.* Fractional (g,f)-Factors of Graphs // Appl. Math. J. Chinese Univ. Ser. A (Chinese) 2001. V. 16. № 4. P. 385–390.
9. *Ma Y., Liu G.* Isolated Toughness and the Existence of Fractional Factors // Acta Math. Appl. Sin. (Chinese). 2003. V. 26. № 1. P. 133–140.
10. *He Z., Liang L., Gao W.* Isolated Toughness Variant and Fractional k-Factor // RAIRO Oper. Res. 2022. V. 56. № 5. P. 3675–3688. https://doi.org/10.1051/ro/2022177
11. *Gao W., Wang W., Zheng L.* Fuzzy Fractional Factors in Fuzzy Graphs // Int. J. Intell. Syst. 2022. V. 37. № 11. P. 9886–9903. https://doi.org/10.1002/int.23019
12. *Gao W., Wang W., Chen Y.* Tight Isolated Toughness Bound for Fractional (k,n)-Critical Graphs // Discrete Appl. Math. 2022. V. 322. P. 194–202. https://doi.org/10.1016/j.dam.2022.08.028
13. *Zhou S.* A Neighborhood Union Condition for Fractional (a,b,k)-Critical Covered Graphs // Discrete Appl. Math. 2022. V. 323. P. 343–348. https://doi.org/10.1016/j.dam.2021.05.022
14. *Zhang W., Wang S.* Discussion on Fractional (a,b,k)-Critical Covered Graphs // Acta Math. Appl. Sin. Engl. Ser. 2022. V. 38. № 2. P. 304–311. https://doi.org/10.1007/s10255-022-1076-6
15. *Gao W., Wang W., Chen Y.* Isolated Toughness and Fractional (a,b,n)-Critical Graphs // Connect. Sci. 2023. V. 35. № 1. Article 2181482 (15 pp.). https://doi.org/10.1080/09540091.2023.2181482

16. *Bondy J.A., Mutry U.S.R.* Graph Theory. Berlin: Springer, 2008.
17. *Liu S.* On Toughness and Fractional (g, f, n)-Critical Graphs // Inform. Process Lett. 2010. V. 110. № 10. P. 378–382. https://doi.org/10.1016/j.ipl.2010.03.005

Гао Вэй✉ (Gao Wei)
Школа информатики и технологии,
Юньнаньский нормальный университет, Куньмин, Китай
✉gaowei@ynnu.edu.cn
Башконуш Хаджи Мехмет (Başkonuş, Hacı Mehmet)
Факультет математического и естественнонаучного образования, Университет Харрана, Шанлыурфа, Турция
hmbaskonus@gmail.com
Каттани Карло (Cattani, Carlo)
Инженерная школа, Университет Тусции, Витербо, Италия
cattani@unitus.it

Поступила в редакцию
16.01.2023
После доработки
16.07.2023
Принята к публикации
02.08.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.391 : 519.719.2

© 2023 г. **А.А. Илларионов**

СУЩЕСТВОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, УДОВЛЕТВОРЯЮЩИХ РЕКУРРЕНТНЫМ СООТНОШЕНИЯМ БИЛИНЕЙНОГО ТИПА

Рассматриваются последовательности $\{A_n\}_{n=-\infty}^{+\infty}$ элементов произвольного поля $\mathbb{F}$, удовлетворяющие разложениям вида

$$A_{m+n}A_{m-n} = a_1(m)b_1(n) + a_2(m)b_2(n),$$
$$A_{m+n+1}A_{m-n} = \widetilde{a}_1(m)\widetilde{b}_1(n) + \widetilde{a}_2(m)\widetilde{b}_2(n),$$

где $a_1, a_2, b_1, b_2 \colon \mathbb{Z} \to \mathbb{F}$. Доказываются результаты о существовании и единственности таких последовательностей. Полученные результаты используются для построения аналогов криптографических алгоритмов Диффи – Хеллмана и Эль-Гамаля. Задача дискретного логарифмирования ставится в группе $(S, +)$, где множество S состоит из четверок $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$, $n \in \mathbb{Z}$, а $S(n) + S(m) = S(n + m)$.

Ключевые слова: нелинейные рекуррентные последовательности, последовательности Сомоса, криптография с открытым ключом.

DOI: 10.31857/S0555292323020079, **EDN:** PQMLTO

§ 1. Введение

Пусть $\mathbb{F}$ – некоторое поле. Рассмотрим последовательность $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$, удовлетворяющую условиям: существуют целые неотрицательные N_0, N_1 и последовательности

$$a_i, b_i, \widetilde{a}_j, \widetilde{b}_j \colon \mathbb{Z} \to \mathbb{F}, \quad i = 1, \ldots, N_0, \quad j = 1, \ldots, N_1,$$

такие что для всех $n, m \in \mathbb{Z}$ выполнены разложения

$$A_{n+m}A_{n-m} = \sum_{i=1}^{N_0} a_i(n)b_i(m), \tag{1}$$

$$A_{n+m+1}A_{n-m} = \sum_{j=1}^{N_1} \widetilde{a}_i(n)\widetilde{b}_i(m). \tag{2}$$

Эта конструкция была предложена В.А. Быковским [1] при $\mathbb{F} = \mathbb{C}$. В этом случае она тесно связана (см. [2]) с решениями функционального уравнения

$$f(x + y)f(x - y) = \sum_{j=1}^{N} \varphi_j(x)\psi_j(y),$$

возникающего в теории эллиптических функций и полилинейных функционально-дифференциальных уравнений.

Последовательности вида (1), (2) также связаны с последовательностями Сомоса (см. [2]), которые обладают рядом замечательных свойств и изучались многими авторами (см. работы [3–13] и библиографию в них).

В [2] описаны все последовательности A комплексных чисел, удовлетворяющие разложениям (1), (2) при $N_0 + N_1 \leqslant 4$.

Большинство асимметричных криптосистем (кроме RSA), используемых на практике, основаны на трудности решения задачи дискретного логарифмирования (ЗДЛ) в некоторой конечной группе, в качестве которой, как правило, выбирается $\mathbb{Z}_p^*$ (группа приведенных вычетов по простому модулю p) либо группа точек на эллиптической кривой над полем $\mathbb{Z}_p$. Существуют субэкспоненциальные алгоритмы решения ЗДЛ в группе $\mathbb{Z}_p^*$. П. Шор (см. [14]) указал на возможность эффективного решения ЗДЛ в группе $\mathbb{Z}_p^*$ с помощью квантового компьютера. Для ЗДЛ в группе точек эллиптической кривой субэкспоненциальные алгоритмы не известны (за исключением некоторых "плохих" кривых). Если таковые будут найдены, то немедленно возникнет вопрос о поиске новых конечных групп, которые могут быть использованы в криптографии, и в которых ЗДЛ является вычислительно сложной.

В [15] было замечено, что последовательности, удовлетворяющие разложению (1), могут быть использованы для построения криптосистем с открытым ключом. Однако [15] не содержит результатов о существовании таких последовательностей в произвольном поле. Этот пробел частично восполняется в настоящей статье. Кроме того, согласно следствию 2 (см. ниже) не имеет смысла рассматривать последовательности, удовлетворяющие только соотношению (1) (по крайней мере в случае $N_0 = 2$).

В § 3 мы получаем результаты о существовании последовательностей A произвольного поля $\mathbb{F}$, удовлетворяющих разложениям (1), (2) при $N_0, N_1 \leqslant 2$, и в § 4 используем эти факты для построения асимметричных шифров (аналогов алгоритмов Диффи – Хеллмана и Эль-Гамаля). Задача дискретного логарифмирования ставится в группе $(S, +)$, где множество S состоит из четверок $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$, $n \in \mathbb{Z}$, а $S(n) + S(m) = S(n+m)$.

Ниже всюду считаем, что $\mathbb{F}$ – поле с операциями сложения $+$ и умножения $\cdot$. Нейтральные элементы по сложению и умножению обозначаем через 0 и 1. Если $a, b \in \mathbb{F}$, то (как обычно) $a/b = ab^{-1}$, где b^{-1} – обратный (по умножению) к b элемент.

§ 2. Некоторые свойства

Пусть $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$. Будем писать $R_j(A) = N_j$, $j = 0, 1$, если N_0, N_1 – наименьшие неотрицательные целые, для которых существуют последовательности $a_i, b_i, \widetilde{a}_j, \widetilde{b}_j \colon \mathbb{Z} \to \mathbb{F}$, $i = 1, \ldots, N_0$, $j = 1, \ldots, N_1$, удовлетворяющие разложениям (1), (2) для всех $n, m \in \mathbb{Z}$.

Используя определение, нетрудно проверить следующие свойства.

1. Пусть $B_n = A_{n_0+n}$ (или $B_n = A_{n_0-n}$). Тогда $R_j(A) \leqslant 2$, $j = 0, 1$, если и только если $R_j(B) \leqslant 2$, $j = 0, 1$.
2. Если $a, b, c \in \mathbb{F} \setminus \{0\}$ и $B_n = A_n a^{n^2} b^n c$, то $R_j(B) = R_j(A)$, $j = 0, 1$.

Для любой последовательности $A \subset \mathbb{F}$ и целых n_j, m_j определим

$$D_A \begin{pmatrix} m_0 & \ldots & m_k \\ n_0 & \ldots & n_k \end{pmatrix} = \det \begin{pmatrix} A_{m_0+n_0} A_{m_0-n_0} & \ldots & A_{m_0+n_k} A_{m_0-n_k} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_{m_k+n_0} A_{m_k-n_0} & \ldots & A_{m_k+n_k} A_{m_k-n_k} \end{pmatrix},$$

$$\widetilde{D}_A \begin{pmatrix} m_0 & \ldots & m_k \\ n_0 & \ldots & n_k \end{pmatrix} = \det \begin{pmatrix} A_{m_0+n_0+1} A_{m_0-n_0} & \ldots & A_{m_0+n_k+1} A_{m_0-n_k} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_{m_k+n_0+1} A_{m_k-n_0} & \ldots & A_{m_k+n_k+1} A_{m_k-n_k} \end{pmatrix}.$$

Лемма 1. *Пусть* $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ *и* $k \in \mathbb{Z}_+ = \mathbb{Z} \cap [0, +\infty)$.

1. *Неравенство* $R_0(A) \leqslant k$ *эквивалентно тому, что*

$$D_A \begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$

2. *Неравенство* $R_1(A) \leqslant k$ *эквивалентно тому, что*

$$\widetilde{D}_A \begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$

Лемма 2. *Пусть* $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ *и* $R_0(A) \leqslant 2$, *причем* $A_0 = 0$, $A_1A_2A_3 \neq 0$. *Тогда последовательность* A *однозначно определяется своими членами с номерами* ± 1 *и* $2, 3, 4$. *Кроме того, если* $A_{-1} = 0$, *то* $A_n = 0$ *при всех* $n \notin \{1, 2, 3, 4\}$.

Эти леммы доказаны в [2, леммы 5.1, 6.1] при $\mathbb{F} = \mathbb{C}$. Однако приведенные там доказательства остаются верными и в случае произвольного поля. Поэтому мы их опускаем.

§ 3. Существование последовательностей с $R_j(A) \leqslant 2$

Пусть $\alpha_0, \alpha_1 \dots, \alpha_5 \in \mathbb{F}$ и $n_0 \in \mathbb{Z}$. В этом параграфе мы рассматриваем следующий вопрос: при каких условиях на α_j существует единственная последовательность $A\colon \mathbb{Z} \to \mathbb{F}$, удовлетворяющая начальным условиям

$$A_{n_0+j} = \alpha_j, \quad j = 0, 1, \dots, 5,$$

для которой $R_i(A) \leqslant 2$, $i = 0, 1$. Согласно свойству 1 из § 2 выбор n_0 не важен. Кроме того, мы ограничимся случаем, когда среди начальных данных $\alpha_0, \dots, \alpha_5$ есть не более одного нуля.

3.1. Случай, когда среди начальных данных есть ровно один нуль. Основной результат этого пункта заключается в следующем.

Теорема 1. *Пусть* $\alpha, \beta, \gamma \in \mathbb{F}$, *причем* $\alpha\beta \neq 0$. *Существует единственная последовательность* $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$, *такая что*

$$A_{-1} = -\alpha, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma, \tag{3}$$
$$R_0(A) \leqslant 2, \quad R_1(A) \leqslant 2. \tag{4}$$

Более того, для всех $n, k \in \mathbb{Z}$

$$A_{-n} = -\alpha^n A_n, \tag{5}$$
$$A_{n+k}A_{n-k} = \alpha^{k-1}(A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2), \tag{6}$$
$$A_{n+k+1}A_{n-k} = \alpha^{k-1}(A_k A_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}). \tag{7}$$

Единственность вытекает из леммы 2. Перейдем к доказательству существования. Если A удовлетворяет (3), (4), то согласно лемме 1

$$D_A \begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ -\alpha\beta & 0 & 1 \\ A_{-2} & -\alpha & 0 \end{vmatrix} =$$
$$= \alpha A_{n+2}A_{n-2} + A_{-2}A_{n+1}A_{n-1} + \beta\alpha^2 A_n^2 = 0.$$

Исходя из (5), положим $A_{-2} = -\alpha^2$. Следовательно, наша последовательность должна удовлетворять соотношению (уравнение Сомос-4)

$$A_{n+2}A_{n-2} = \alpha A_{n+1}A_{n-1} - \alpha\beta A_n^2. \tag{8}$$

Так как последовательность A содержит нулевые члены, то ее нельзя однозначно восстановить, используя только уравнение (8). Прежде всего, нам нужна дополнительная информация о расположении нулевых членов.

Лемма 3. *Пусть последовательность* $A = \{A_n\}_{n=-1}^{+\infty} \subset \mathbb{F}$ *удовлетворяет начальным условиям* (3) *и уравнению* (8) *для всех* $n \in \mathbb{N}$, *таких что* $A_{n-2} \neq 0$. *Тогда*
a) *если* $n_1, n_2 \in \mathbb{N}$, *причем* $A_{n_1} = A_{n_2} = 0$, *то* $|n_1 - n_2| \geqslant 4$;
b) *уравнение* (8) *выполняется для всех* $n \in \mathbb{N}$.

Доказательство. 1. Докажем, что последовательность A не имеет двух соседних членов, равных нулю. Предположим противное. Пусть m – наименьший номер, такой что $A_m = A_{m+1} = 0$. Тогда $m \geqslant 4$ и $A_{m-1} \neq 0$.

Докажем, что $A_{m-3} \neq 0$. Если $A_{m-4} = 0$, то это следует из выбора m. Если $A_{m-4} \neq 0$, то уравнение (8) выполнено при $n = m - 2$, т.е.

$$0 = \alpha A_{m-1}A_{m-3} - \alpha\beta A_{m-2}^2.$$

Поэтому

$$A_{m-3} = 0 \implies A_{m-2} = 0.$$

Значит, $A_{m-3} \neq 0$ согласно выбору номера m.

Так как $A_{m-3} \neq 0$, то уравнение (8) выполнено при $n = m - 1$. Но тогда $0 = -\alpha\beta A_{m-1}^2$, т.е. $A_{m-1} = 0$. Пришли к противоречию.

2. Предположим, что утверждение a) неверно. Тогда найдется номер m, такой что

$$A_m = 0, \quad A_{m+1}A_{m+2}A_{m+3} = 0.$$

Пусть m – наименьший номер, удовлетворяющий этим свойствам. Тогда

$$m \geqslant 4, \quad A_{m-3}A_{m-2}A_{m-1} \neq 0.$$

Кроме того, $A_{m+1} \neq 0$ согласно доказанному выше. Так как $A_{m-1}A_{m-2} \neq 0$, то (8) верно при $n = m + 1$ и $n = m$, т.е.

$$A_{m+3}A_{m-1} = -\alpha\beta A_{m+1}^2 \neq 0 \implies A_{m+3} \neq 0,$$
$$A_{m+2}A_{m-2} = \alpha A_{m+1}A_{m-1} \neq 0 \implies A_{m+2} \neq 0.$$

Пришли к противоречию. Значит, свойство a) выполняется.

3. Предположим, что утверждение b) неверно. Тогда найдется номер m, такой что

$$A_{m-2} = 0, \quad \underbrace{A_{m+2}A_{m-2}}_{0} \neq \alpha A_{m+1}A_{m-1} - \alpha\beta A_m^2.$$

Пусть m – наименьший номер, удовлетворяющий этим условиям. Тогда $m \geqslant 6$ и уравнение (8) выполнено для всех $1 \leqslant n < m$. Выбирая в нем $n = m - 4, m - 3$, $m - 2, m - 1$, получаем четыре равенства

$$\beta A_{m-4}^2 = A_{m-3}A_{m-5}, \quad A_{m-1}A_{m-5} = -\alpha\beta A_{m-3}^2,$$
$$\alpha A_{m-1}A_{m-3} = A_m A_{m-4}, \quad A_{m+1}A_{m-3} = -\alpha\beta A_{m-1}^2.$$

Следовательно (перемножаем равенства, причем третье из них берем два раза),

$$\beta A_{m-4}^2 A_{m-1} A_{m-5} (\alpha A_{m-1} A_{m-3})^2 A_{m+1} A_{m-3} =$$
$$= A_{m-3} A_{m-5} (-\alpha\beta A_{m-3}^2)(A_m A_{m-4})^2 (-\alpha\beta A_{m-1}^2).$$

Так как $A_{m-5}A_{m-4}A_{m-3}A_{m-1}A_mA_{m+1} \neq 0$ согласно утверждению а), то отсюда следует, что

$$\alpha A_{m+1} A_{m-1} = \alpha\beta A_m^2.$$

Так как $A_{m-2} = 0$, то уравнение (8) выполняется и при $n = m$. ▲

Построим теперь последовательность A. Элементы с номерами от -1 до 4 определим с помощью (3). Элементы с номерами $n \geqslant 5$ вычислим по формулам

$$A_{n+2} = \alpha \frac{A_{n+1}A_{n-1} - \beta A_n^2}{A_{n-2}} \quad \text{при } n \geqslant 3, \quad A_{n-2} \neq 0, \tag{9}$$

$$A_{n+2} = -\alpha\gamma \frac{A_n A_{n-1}}{A_{n-3}} \quad \text{при } n \geqslant 3, \quad A_{n-2} = 0. \tag{10}$$

Если $A_{n-2} = A_{n-3} = 0$, то полагаем $A_{n+2} = 0$. Однако нетрудно заметить, что полученная последовательность удовлетворяет условиям леммы 3. Поэтому случай $A_{n-2} = A_{n-3} = 0$ невозможен. Отметим, что формула (10) получена из равенства

$$\widetilde{D}_A \begin{pmatrix} n-1 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = 0.$$

Элементы $A_{-2}, A_{-3}, \ldots$ определим по формуле

$$A_{-n} = -\alpha^n A_n \quad \text{при } n \geqslant 2. \tag{11}$$

Осталось проверить, что построенная последовательность A удовлетворяет уравнениям (6), (7) (неравенства (4) вытекают из (6), (7) по определению величин $R_j(A)$).

Лемма 4. *Пусть последовательность $A \subset \mathbb{F}$ определяется соотношениями* (3), (9)–(11). *Тогда уравнения* (6), (7) *выполнены при $k = 2$. Кроме того,*

$$\forall n \in \mathbb{Z} \qquad \beta(\alpha A_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2}) = (\alpha + \gamma) A_{n-1} A_n A_{n+1}. \tag{12}$$

Доказательство. 1. Докажем, что (6) выполнено при $k = 2$, т.е. справедливо равенство (8). Из (9) и леммы 3 следует выполнение (8) при $n \geqslant 1$. Используя этот факт, условия (3) и (11), нетрудно проверить, что (8) имеет место и для $n \leqslant 0$.

2. Докажем, что (7) выполнено при $k = 2$, т.е.

$$A_{n+3}A_{n-2} = \alpha\beta A_{n+2}A_{n-1} - \alpha\gamma A_{n+1}A_n. \tag{13}$$

2.1. Используя метод математической индукции, докажем (13) при $n \geqslant -3$.

База индукции вытекает из (3) и (11).

Шаг индукции от $n-1$ к n. Если $A_{n-1} = 0$, то (13) вытекает из (10), в котором n заменяем на $n+1$. Пусть $A_{n-1} \neq 0$. Тогда (13) равносильно соотношению

$$A_{n+3}A_{n-1}A_{n-2} = \alpha\beta A_{n+2}A_{n-1}^2 - \alpha\gamma A_{n+1}A_nA_{n-1}.$$

Согласно (8) левая часть этого соотношения равна

$$\alpha A_{n+2}A_nA_{n-2} - \alpha\beta A_{n+1}^2 A_{n-2}.$$

Значит, (13) эквивалентно равенству

$$A_{n+2}(A_nA_{n-2} - \beta A_{n-1}^2) = A_{n+1}(\beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n).$$

Так как

$$\beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n = \alpha^{-1}A_{n+2}A_{n-3}$$

(по предположению индукции), то это равенство равносильно тому, что

$$A_{n+2}(A_{n+1}A_{n-3} - \alpha A_nA_{n-2} + \alpha\beta A_{n-2}^2) = 0.$$

Последнее соотношение выполнено в силу (8).

2.2. Выполнение (13) при $n < -3$ легко проверяется с помощью начальных условий (3), свойства (11) и утверждения из п. 2.1.

3. Осталось проверить свойство (12). Дважды применяя (8), получаем, что

$$A_{n+3}A_{n-2}A_{n-1} = (A_{n+3}A_{n-1})A_{n-2} = \alpha(A_{n+2}A_nA_{n-2} - \beta A_{n+1}^2A_{n-2}) =$$
$$= \alpha\big((\alpha A_{n+1}A_{n-1} - \alpha\beta A_n^2)A_n - \beta A_{n+1}^2A_{n-2}\big).$$

С другой стороны, в силу (13)

$$A_{n+3}A_{n-2}A_{n-1} = (\alpha\beta A_{n+2}A_{n-1} - \alpha\gamma A_{n+1}A_n)A_{n-1}.$$

Следовательно,

$$(\alpha A_{n+1}A_{n-1} - \alpha\beta A_n^2)A_n - \beta A_{n+1}^2A_{n-2} = \beta A_{n+2}A_{n-1}^2 - \gamma A_{n+1}A_nA_{n-1}.$$

Нетрудно заметить, что это равенство равносильно (12). ▲

Замечание 1. Если последовательность A не имеет нулевых членов, то можно ввести новую последовательность $\tau_n = (A_{n-1}A_{n+1})/A_n^2$. В этих терминах (12) принимает вид

$$\beta(\alpha + \tau_n^2\tau_{n+1} + \tau_n^2\tau_{n-1}) = (\alpha + \gamma)\tau_n.$$

Это соотношение хорошо известно в теории последовательностей Сомос-4 (см., например, работу [16] и библиографию в ней).

Доказательство теоремы 1. Единственность искомой последовательности следует из леммы 2. Пусть A – последовательность из леммы 4. Осталось доказать, что она удовлетворяет условиям (6), (7). Действительно, неравенства (4) являются следствиями (по определению) из (6), (7), а условие (5) – из (11). Согласно (5) уравнения (6), (7) достаточно проверить только при $k \geqslant 0$. Для этого используем индукцию по k.

База индукции. Согласно начальным условиям (3) и свойству (5) соотношения (6), (7) выполнены при $k = 0, 1$. Из леммы 4 вытекает, что они также верны при $k = 2$.

Шаг индукции от k к $k + 1$.

1. Докажем, что выполнено равенство (6), в котором k заменяем на $k + 1$, т.е.

$$A_{n+k+1}A_{n-k-1} = \alpha^k(A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2). \tag{14}$$

1.1. Пусть $A_{n+k}A_{n-k} \neq 0$. Тогда (14) равносильно соотношению

$$A_{n+k+1}A_{n-k-1}A_{n+k}A_{n-k} = \alpha^k(A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2)A_{n+k}A_{n-k}. \tag{15}$$

Согласно предположению индукции (7) левая часть этого соотношения равна

$$A_{n+k+1}A_{n-k-1}A_{n+k}A_{n-k} = (A_{n+k+1}A_{n-k})(A_{n+k}A_{n-k-1}) =$$
$$= \alpha^{2k-2}(A_kA_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_nA_{n+1}) \times$$
$$\times (A_kA_{k+1}A_{n+1}A_{n-2} - A_{k+2}A_{k-1}A_{n-1}A_n),$$

а в силу (6) правая часть равна

$$\alpha^{2k-1}(A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2)(A_k^2A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2).$$

Поэтому (15) можно переписать в следующем эквивалентном виде (раскрываем скобки в левой и правой части):

$$A_k^2A_{k+1}^2A_{n-2}A_{n-1}A_{n+1}A_{n+2} - A_{k-1}A_kA_{k+1}A_{k+2}A_nA_{n-1}^2A_{n+2} -$$
$$- A_{k-1}A_kA_{k+1}A_{k+2}A_{n-2}A_nA_{n+1}^2 + A_{k-1}^2A_{k+2}^2A_{n-1}A_n^2A_{n+1} =$$
$$= \alpha(A_k^2A_{k+1}^2A_{n+1}^2A_{n-1}^2 - A_{k-1}A_{k+1}^3A_{n-1}A_n^2A_{n+1} - A_k^3A_{k+2}A_{n-1}A_n^2A_{n+1} +$$
$$+ A_{k-1}A_kA_{k+1}A_{k+2}A_n^4).$$

Согласно (8) разность первых слагаемых в левой и правой части равна

$$A_k^2A_{k+1}^2A_{n-1}A_{n+1}(A_{n+2}A_{n-2} - \alpha A_{n+1}A_{n-1}) = -\alpha\beta A_k^2A_{k+1}^2A_{n-1}A_n^2A_{n+1},$$

поэтому требуемое равенство равносильно тому, что

$$A_{n-1}A_n^2A_{n+1}(-\alpha\beta A_k^2A_{k+1}^2 + A_{k-1}^2A_{k+2}^2 + \alpha A_{k-1}A_{k+1}^3 + \alpha A_k^3A_{k+2}) =$$
$$= A_{k-1}A_kA_{k+1}A_{k+2}A_n(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2 + \alpha A_n^3).$$

Учитывая, что согласно (8)

$$-\alpha\beta A_k^2A_{k+1}^2 + \alpha A_{k-1}A_{k+1}^3 = A_{k+1}^2(\alpha A_{k-1}A_{k+1} - \alpha\beta A_k^2) = A_{k+1}^2A_{k+2}A_{k-2},$$

перепишем последнее соотношение в эквивалентном виде:

$$A_{n-1}A_n^2A_{n+1}A_{k+2}(A_{k+1}^2A_{k-2} + A_{k-1}^2A_{k+2}^2 + \alpha A_k^3A_{k+2}) =$$
$$= A_{k-1}A_kA_{k+1}A_{k+2}A_n(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2 + \alpha A_n^3).$$

Оно выполняется в силу (12). Случай $A_{n+k}A_{n-k} \neq 0$ полностью рассмотрен.

1.2. Пусть $A_{n+k-1}A_{n-k+1} \neq 0$. Умножая (14) на $A_{n+k-1}A_{n-k+1}$ и учитывая, что по предположению индукции

$$A_{n+k-1}A_{n-k+1} = A_{n+(k-1)}A_{n-(k-1)} = \alpha^{k-2}(A_{k-1}^2A_{n+1}A_{n-1} - A_kA_{k-2}A_n^2),$$
$$A_{n+k+1}A_{n-k+1} = A_{(n+1)+k}A_{(n+1)-k} = \alpha^{k-1}(A_k^2A_{n+2}A_n - A_{k+1}A_{k-1}A_{n+1}^2),$$
$$A_{n+k-1}A_{n-k-1} = A_{(n-1)+k}A_{(n-1)-k} = \alpha^{k-1}(A_k^2A_nA_{n-2} - A_{k+1}A_{k-1}A_{n-1}^2),$$

приходим к выводу, что (14) эквивалентно равенству

$$(A_k^2A_{n+2}A_n - A_{k+1}A_{k-1}A_{n+1}^2)(A_k^2A_nA_{n-2} - A_{k+1}A_{k-1}A_{n-1}^2) =$$
$$= (A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2)(A_{k-1}^2A_{n+1}A_{n-1} - A_kA_{k-2}A_n^2).$$

Последнее после раскрытия скобок и сокращения одинаковых слагаемых принимает вид

$$A_k^4A_{n+2}A_{n-2}A_n^2 - A_{k-1}A_k^2A_{k+1}A_n(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2) =$$
$$= -A_{n-1}A_n^2A_{n+1}A_k(A_{k-2}A_{k+1}^2 + A_{k-1}^2A_{k+2}) + A_{k-2}A_k^2A_{k+2}A_n^4.$$

Подставляя в это равенство соотношения (применили (8))

$$A_k^4 A_{n+2} A_{n-2} A_n^2 = \alpha A_k^4 A_{n-1} A_n^2 A_{n+1} - \alpha\beta A_k^4 A_n^4,$$
$$A_{k-2} A_k^2 A_{k+2} A_n^4 = \alpha A_{k-1} A_k^2 A_{k+1} A_n^4 - \alpha\beta A_k^4 A_n^4,$$

перепишем его в виде

$$\alpha A_k^4 A_{n-1} A_n^2 A_{n+1} - A_{k-1} A_k^2 A_{k+1} A_n (A_{n-1}^2 A_{n+2} + A_{n-2} A_{n+1}^2) =$$
$$= -A_{n-1} A_n^2 A_{n+1} A_k (A_{k-2} A_{k+1}^2 + A_{k-1}^2 A_{k+2}) + \alpha A_{k-1} A_k^2 A_{k+1} A_n^4,$$

или

$$A_{n-1} A_n^2 A_{n+1} A_k (\alpha A_k^3 + A_{k-2} A_{k+1}^2 + A_{k-1}^2 A_{k+2}) =$$
$$= A_{k-1} A_k^2 A_{k+1} A_n (A_{n-1}^2 A_{n+2} + A_{n-2} A_{n+1}^2 + \alpha A_n^3).$$

Это равенство выполнено в силу (12).

1.3. Осталось рассмотреть случай, когда

$$A_{n+k} A_{n-k} = A_{n+k-1} A_{n-k+1} = 0.$$

Так как последовательность A не может иметь двух соседних нулевых членов, то в этом случае $A_{n+k} A_{n-k+1} \neq 0$ или $A_{n+k-1} A_{n-k} \neq 0$. Эти два случая рассматриваются так же, как и предыдущие. В первом случае равенство (14) нужно домножить на $A_{n+k} A_{n-k+1}$, а во втором – на $A_{n+k-1} A_{n-k}$. После этого остается применить предположение индукции, элементарные преобразования и формулу (12).

2. Докажем выполнение формулы (7), в которой k заменяем на $k+1$, т.е.

$$A_{n+k+2} A_{n-k-1} = \alpha^k (A_{k+1} A_{k+2} A_{n+2} A_{n-1} - A_{k+3} A_k A_n A_{n+1}). \tag{16}$$

2.1. Пусть $A_{n+k+1} A_{n-k} \neq 0$. Умножая (16) на $A_{n+k+1} A_{n-k}$ и учитывая, что по предположению индукции и формуле (14)

$$A_{n+k+1} A_{n-k} = \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}),$$
$$A_{n+k+2} A_{n-k} = A_{(n+1)+(k+1)} A_{(n+1)-(k+1)} = \alpha^k (A_{k+1}^2 A_{n+2} A_n - A_{k+2} A_k A_{n+1}^2),$$
$$A_{n+k+1} A_{n-k-1} = A_{n+(k+1)} A_{n-(k+1)} = \alpha^k (A_{k+1}^2 A_{n+1} A_{n-1} - A_{k+2} A_k A_n^2),$$

приходим к выводу, что (16) эквивалентно равенству

$$\alpha (A_{k+1}^2 A_{n+2} A_n - A_{k+2} A_k A_{n+1}^2)(A_{k+1}^2 A_{n+1} A_{n-1} - A_{k+2} A_k A_n^2) =$$
$$= (A_{k+1} A_{k+2} A_{n+2} A_{n-1} - A_{k+3} A_k A_n A_{n+1}) \times$$
$$\times (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}).$$

Последнее после раскрытия скобок и элементарных преобразований принимает вид

$$A_{k+1} A_{n-1} A_n A_{n+1} A_{n+2} (\alpha A_{k+1}^3 + A_{k-1} A_{k+2}^2 + A_k^2 A_{k+3}) + \alpha A_k^2 A_{k+2}^2 A_n^2 A_{n+1}^2 =$$
$$= A_k A_{k+1}^2 A_{k+2} (\alpha A_n^3 A_{n+2} + \alpha A_{n-1} A_{n+1}^3 + A_{n-1}^2 A_{n+2}^2) +$$
$$+ A_{k-1} A_k A_{k+2} A_{k+3} A_n^2 A_{n+1}^2. \tag{17}$$

Разность последних слагаемых в правой и левой части этого равенства равна

$$A_k A_{k+2} A_n^2 A_{n+1}^2 (A_{k+3} A_{k-1} - \alpha A_k A_{k+2}) = -\alpha\beta A_k A_{k+1}^2 A_{k+2} A_n^2 A_{n+1}^2.$$

Поэтому (17) равносильно соотношению

$$A_{k+1}A_{n-1}A_nA_{n+1}A_{n+2}(\alpha A_{k+1}^3 + A_{k-1}A_{k+2}^2 + A_k^2A_{k+3}) =$$
$$= A_kA_{k+1}^2A_{k+2}(\alpha A_n^3A_{n+2} + \alpha A_{n-1}A_{n+1}^3 + A_{n-1}^2A_{n+2}^2 - \alpha\beta A_n^2A_{n+1}^2).$$

Последнее выполнено в силу (12) и равенства

$$\alpha A_n^3A_{n+2} - \alpha\beta A_n^2A_{n+1}^2 = A_n^2(\alpha A_nA_{n+2} - \alpha\beta A_{n+1}^2) = A_n^2A_{n+3}A_{n-1}.$$

2.2. Пусть $A_{n+k+1}A_{n-k} = 0$. Поскольку последовательность A не имеет двух соседних членов, равных нулю, хотя бы одно из произведений $A_{n+k}A_{n-k}$, $A_{n+k}A_{n-k+1}$ или $A_{n+k+1}A_{n-k+1}$ отлично от нуля. Эти случаи рассматриваются аналогично исследованным выше. ▲

Замечание 2. Если A – последовательность из теоремы 1, то $R_0(A) = R_1(A) = 2$. Действительно, из начальных условий вытекает, что

$$D_A\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} = \begin{vmatrix}0 & 1\\ -\alpha & 0\end{vmatrix} = \alpha \neq 0, \quad \widetilde{D}_A\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} = \begin{vmatrix}0 & 1\\ -\alpha & 0\end{vmatrix} = \alpha \neq 0.$$

Отсюда по лемме 1 следует, что $R_j(A) \geqslant 2$, $j = 0, 1$. Значит, $R_0(A) = R_1(A) = 2$.

Следствие 1. *Пусть* $\alpha_{-1}, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}\setminus\{0\}$, $\alpha_4 \in \mathbb{F}$. *Тогда существует единственная последовательность* $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$, *такая что*

$$A_j = \alpha_j, \ \ j = \pm1, 2, 3, 4, \quad A_0 = 0; \qquad R_j(A) \leqslant 2, \ \ j = 0, 1.$$

Более того, для всех $n \in \mathbb{Z}$ *справедливы равенства*

$$A_{-n} = -\bigl(-\alpha_{-1}\alpha_1^{-1}\bigr)^n A_n,$$
$$-\frac{\alpha_{-1}\alpha_2^2}{\alpha_1^3}A_n^3 + A_{n-1}^2A_{n+2} + A_{n+1}^2A_{n-2} = \left(-\frac{\alpha_{-1}\alpha_2^4}{\alpha_1^4\alpha_3} + \frac{\alpha_4\alpha_1}{\alpha_2\alpha_3}\right)A_{n-1}A_nA_{n+1}.$$

Доказательство. Сделаем замену $B_n = A_n\alpha_1^{-1}(\alpha_1/\alpha_2)^{n-1}$. Как отмечалось в § 2, $R_j(B) = R_j(A) \leqslant 2$. Кроме того,

$$B_{-1} = \frac{\alpha_{-1}\alpha_2^2}{\alpha_1^3}, \quad B_0 = 0, \quad B_1 = B_2 = 1, \quad B_3 = \frac{\alpha_1\alpha_3}{\alpha_2^2}, \quad B_4 = \frac{\alpha_4\alpha_1^2}{\alpha_2^3}.$$

Согласно теореме 1 такая последовательность B существует и единственна, причем $B_n = -(-B_{-1})^nB_n$ и выполняется равенство (12), в котором $\alpha = -B_{-1}$, $\beta = B_3$, $\gamma = B_4$ и A_n заменено на B_n. Отсюда вытекают оставшиеся утверждения леммы. ▲

Следствие 2. *Пусть последовательность* $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ *такая, что* $R_0(A) \leqslant 2$ *и* $A_0 = 0$, $A_{-1}A_1A_2A_3 \neq 0$. *Тогда* $R_1(A) \leqslant 2$.

Доказательство. Согласно следствию 1 существует последовательность B, такая что $R_j(B) \leqslant 2$, $j = 0, 1$, и $B_i = A_i$, $-1 \leqslant i \leqslant 4$. Используя лемму 2, получаем, что $A = B$. ▲

Через $|F|$ обозначаем мощность множества F.

Лемма 5. *Пусть в дополнение к условиям следствия* 1 *поле* $\mathbb{F}$ *конечно. Тогда последовательность* A *имеет период* ω, *причем* $\omega \leqslant |\mathbb{F}|^4$ *и* ω *делится на порядок элемента* $\alpha = -\alpha_{-1}\alpha_1^{-1}$.

Доказательство. Используя замену из доказательства следствия 1, нетрудно заметить, что последовательность A удовлетворяет уравнениям вида (8), (12). Из

них вытекает, что существуют функции $f_+, f_-\colon \mathbb{F}^4 \to \mathbb{F}$, такие что

$$A_n = f_+(A_{n-1}, A_{n-2}, A_{n-3}, A_{n-4}), \quad A_n = f_-(A_{n+1}, A_{n+2}, A_{n+3}, A_{n+4}).$$

Так как множество $\mathbb{F}$ конечно, то отсюда следует, что последовательность A имеет период $\omega \leqslant |\mathbb{F}|^4$. Используя этот факт и формулу $A_{-n} = -\alpha^n A_n$, где $\alpha = -\alpha_{-1}\alpha_1^{-1}$, получаем, что

$$A_{-n-\omega} = -\alpha^{n+\omega} A_{n+\omega} = -\alpha^{n+\omega} A_n = \alpha^\omega A_{-n} = \alpha^\omega A_{-n-\omega} \quad \Longrightarrow \quad \alpha^\omega = 1. \quad \blacktriangle$$

Рассмотрим теперь другие варианты, когда среди начальных данных есть ровно один нуль. В силу следствия 1 и свойства 1 из § 2 достаточно рассмотреть только два варианта:

$$A_0 = 0, \quad A_j = \alpha_j,\ j = 1, \ldots, 5, \tag{18}$$

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \quad A_0 = 0, \quad A_j = \alpha_j,\ j = 1, 2, 3. \tag{19}$$

Следствие 3. *Пусть* $\alpha_j \in \mathbb{F}\setminus\{0\}$, $j = 1, \ldots, 5$. *Последовательность* $A\colon \mathbb{Z} \to \mathbb{F}$, *удовлетворяющая* (4), (18), *существует тогда и только тогда, когда* $\alpha_4\alpha_2^3 \neq \alpha_1\alpha_3^3$. *Если такая последовательность существует, то она единственна.*

Доказательство. Если искомая последовательность существует, то

$$D_A \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} \alpha_5\alpha_1 & \alpha_4\alpha_2 & \alpha_3^2 \\ 0 & \alpha_3\alpha_1 & \alpha_2^2 \\ \alpha_3 A_{-1} & 0 & \alpha_1^2 \end{vmatrix} = \alpha_5\alpha_3\alpha_1^4 + \alpha_3 A_{-1}\Delta = 0.$$

где $\Delta = \alpha_4\alpha_2^3 - \alpha_1\alpha_3^3$. Очевидно, что $\Delta \neq 0$. Тогда получаем, что $A_{-1} = \alpha_{-1}$, где $\alpha_{-1} = -\alpha_1^2\alpha_5\alpha_1^2\Delta^{-1}$. Согласно следствию 1 существует единственная последовательность $\widetilde{A}$, такая что

$$R_i(\widetilde{A}) \leqslant 2,\ i = 1, 2, \quad \widetilde{A}_j = \alpha_j,\ j = \pm 1, 2, 3, 4, \quad \widetilde{A}_0 = 0.$$

Нетрудно проверить, что $\widetilde{A}_5 = \alpha_5$. Значит, $\widetilde{A} = A$ – искомая последовательность. $\blacktriangle$

Следствие 4. *Пусть* $\alpha_j \in \mathbb{F} \setminus \{0\}$, $j = \pm 1, \pm 2, \pm 3$. *Если* $\alpha_{-2}\alpha_1 \neq \alpha_2\alpha_{-1}^2$, *то не существует последовательности* $A\colon \mathbb{Z} \to \mathbb{F}$, *удовлетворяющей* (4), (19). *Если* $\alpha_{-2}\alpha_1 = \alpha_2\alpha_{-1}^2$, *то для любого* $\alpha_4 \in \mathbb{F}$ *существует единственная последовательность* $A\colon \mathbb{Z} \to \mathbb{F}$, *удовлетворяющая* (4), (19) *и дополнительному условию* $A_4 = \alpha_4$.

Доказательство. Так как

$$D_A \begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} 0 & \alpha_3\alpha_1 & \alpha_2^2 \\ \alpha_3\alpha_{-1} & 0 & \alpha_1^2 \\ \alpha_2\alpha_{-2} & \alpha_1\alpha_{-1} & 0 \end{vmatrix} = \alpha_1\alpha_2\alpha_3(\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2) = 0,$$

то условие $\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2 = 0$ необходимо для существования искомой последовательности.

Возьмем любой $\alpha_4 \in \mathbb{F}$. Согласно следствию 1 существует единственная последовательность $\widetilde{A}$, такая что

$$R_i(\widetilde{A}) \leqslant 2,\ i = 1, 2; \quad \widetilde{A}_j = \alpha_j,\ j = \pm 1, 2, 3, 4, \quad \widetilde{A}_0 = 0.$$

Если дополнительно $\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2 = 0$, то нетрудно проверить, что $\widetilde{A}_{-2} = \alpha_{-2}$. Значит, $\widetilde{A} = A$ – искомая последовательность. $\blacktriangle$

3.2. Случай, когда среди начальных данных нет нулей. Пусть $a, b, T \in \mathbb{F}$, $ab \neq 0$. Определим расширение $\mathbb{F}(\sqrt{a})$ поля $\mathbb{F}$ следующим образом: если $\sqrt{a} \in \mathbb{F}$ (т.е. уравнение $x^2 = a$ разрешимо в $\mathbb{F}$), то полагаем $\mathbb{F}(\sqrt{a}) = \mathbb{F}$, в противном случае

$$\mathbb{F}(\sqrt{a}) = \{x + y\sqrt{a} : \ x, y \in \mathbb{F}\}$$

с операциями сложения и умножения, определяемыми естественным образом. Другими словами, $\mathbb{F}(\sqrt{a})$ состоит из пар $(x, y) \in \mathbb{F}^2$ и

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + ay_1y_2, x_1y_2 + x_2y_1),$$
$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Нулем является $(0, 0)$, а единицей – $(1, 0)$. Отображение $x \in \mathbb{F} \to (x, 0) \in \mathbb{F}(\sqrt{a})$ задает вложение $\mathbb{F} \subset \mathbb{F}(\sqrt{a})$.

В силу следствия 1 существует единственная последовательность $W \colon \mathbb{Z} \to \mathbb{F}(\sqrt{a})$, такая что

$$W_{-1} = -1, \ \ W_0 = 0, \ \ W_1 = 1, \ \ W_2 = -\sqrt{a}, \ \ W_3 = -b, \ \ W_4 = \sqrt{a}(a^2 + Tb), \tag{20}$$
$$W_{-n} = -W_n, \quad R_i(W) \leqslant 2, \ \ i = 0, 1. \tag{21}$$

Используя эти соотношения и равенства

$$D_W \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = 0, \quad \widetilde{D}_W \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = 0,$$

нетрудно проверить, что для всех $n, k \in \mathbb{Z}$

$$W_{n+k}W_{n-k} = W_k^2W_{n+1}W_{n-1} - W_{k+1}W_{k-1}W_n^2, \tag{22}$$
$$-\sqrt{a}W_{n+k+1}W_{n-k} = W_kW_{k+1}W_{n+2}W_{n-1} - W_{k+2}W_{k-1}W_{n+1}W_n. \tag{23}$$

Замечание 3. В случае $\mathbb{F} = \mathbb{C}$ последовательность W изучена в [17]. При $\mathbb{F} = \mathbb{Q}$ ее называют эллиптической (делимостной) последовательностью.

Лемма 6. *Для любого $n \in \mathbb{Z}$ верно, что $W_{2n+1} \in \mathbb{F}$, $\sqrt{a}W_{2n} \in \mathbb{F}$.*

Доказательство. Выбирая в (22), (23) $k = n - 1$, имеем

$$W_{2n-1} = W_{n-1}^3W_{n+1} - W_n^3W_{n-2}, \quad -\sqrt{a}W_{2n} = W_{n-1}^2W_nW_{n+2} - W_{n-2}W_nW_{n+1}^2.$$

Используя эти соотношения и начальные условия (20), нетрудно проверить требуемое утверждение, используя индукцию по $n = 1, 2, \ldots$ ▲

Лемма 7. *Пусть последовательность $A \colon \mathbb{Z} \to \mathbb{F}$ не содержит нулевых членов и удовлетворяет для любых $n \in \mathbb{Z}$ соотношению*

$$A_{n+2}A_{n-2} = aA_{n+1}A_{n-1} + bA_n^2. \tag{24}$$

Пусть последовательность $W \colon \mathbb{Z} \to \mathbb{F}(\sqrt{a})$ удовлетворяет условиям (20), (21), *где*

$$T = \frac{A_1^2A_{-2} + A_{-1}^2A_2 + aA_0^3}{A_{-1}A_0A_1}.$$

Тогда для всех $k, n \in \mathbb{Z}$

$$A_{n+k}A_{n-k} = W_k^2A_{n+1}A_{n-1} - W_{k-1}W_{k+1}A_n^2, \tag{25}$$
$$A_{n+k+1}A_{n-k} = -\frac{W_{k+1}W_k}{\sqrt{a}}A_{n+2}A_{n-1} + \frac{W_{k+2}W_{k-1}}{\sqrt{a}}A_{n+1}A_n. \tag{26}$$

Доказательство. Так как $k \not\equiv k+1 \pmod 2$ и $k+2 \not\equiv k-1 \pmod 2$, то в силу леммы 6

$$\frac{W_{k+1}W_k}{\sqrt{a}} \in \mathbb{F}, \quad \frac{W_{k+2}W_{k-1}}{\sqrt{a}} \in \mathbb{F}.$$

Соотношение (22) при $k = 2$ принимает вид

$$W_{n+2}W_{n-2} = aW_{n+1}W_{n-1} + bW_n^2. \tag{27}$$

1. Положим $f_n = A_{n-1}A_{n+1}A_n^{-2}$. Тогда согласно (24)

$$f_{n-1}f_n^2 f_{n+1} = af_n + b.$$

Отсюда вытекает, что величина $f_n(f_{n-1} + f_{n+1}) + a/f_n$ не зависит от n. Доказательство этого факта, приведенное в [16, лемма 2.1], остается в силе в случае произвольного поля. Поэтому мы его повторять не будем. Возвращаясь к последовательности A, получаем, что элемент

$$\frac{A_{n+1}^2A_{n-2} + A_{n-1}^2A_{n+2} + aA_n^3}{A_{n-1}A_nA_{n+1}}$$

не зависит от n. Следовательно, для всех $n \in \mathbb{Z}$

$$A_{n+1}^2A_{n-2} + A_{n-1}^2A_{n+2} + aA_n^3 = TA_{n-1}A_nA_{n+1}. \tag{28}$$

Из следствия 1 и начальных условий (20) вытекает, что последовательность W удовлетворяет аналогичному уравнению

$$W_{n+1}^2W_{n-2} + W_{n-1}^2W_{n+2} + aW_n^3 = TW_{n-1}W_nW_{n+1}. \tag{29}$$

2. Докажем соотношения (25). В силу свойства (21) их достаточно проверить при $k \geqslant 0$. Для этого используем индукцию по $k = 0, 1, \ldots$

База индукции. Согласно (20) соотношения (25) выполняются при $k = 0, 1, 2$.

Шаг индукции от k к $k+1$ ($k \geqslant 2$). Нужно доказать, что

$$A_{n+k+1}A_{n-k-1} = W_{k+1}^2A_{n+1}A_{n-1} - W_kW_{k+2}A_n^2. \tag{30}$$

Умножим (30) на $A_{n+k-1}A_{n-k+1}$ и учтем, что по предположению индукции

$$\begin{aligned}
A_{n+k-1}A_{n-k+1} &= A_{n+(k-1)}A_{n-(k-1)} = W_{k-1}^2A_{n+1}A_{n-1} - W_{k-2}W_kA_n^2,\\
A_{n+k-1}A_{n-k-1} &= A_{(n-1)+k}A_{(n-1)-k} = W_k^2A_nA_{n-2} - W_{k-1}W_{k+1}A_{n-1}^2,\\
A_{n+k+1}A_{n-k+1} &= A_{(n+1)+k}A_{(n+1)-k} = W_k^2A_nA_{n+2} - W_{k-1}W_{k+1}A_{n+1}^2.
\end{aligned}$$

В итоге приходим к эквивалентному равенству

$$\begin{aligned}
&(W_k^2A_nA_{n-2} - W_{k-1}W_{k+1}A_{n-1}^2)(W_k^2A_nA_{n+2} - W_{k-1}W_{k+1}A_{n+1}^2) =\\
&= (W_{k+1}^2A_{n+1}A_{n-1} - W_kW_{k+2}A_n^2)(W_{k-1}^2A_{n+1}A_{n-1} - W_{k-2}W_kA_n^2).
\end{aligned}$$

Раскрывая скобки и сокращая одинаковые слагаемые, получаем

$$\begin{aligned}
&W_k^4A_{n-2}A_n^2A_{n+2} + A_{n-1}A_n^2A_{n+1}W_k(W_{k+1}^2W_{k-2} + W_{k-1}^2W_k) =\\
&= W_k^2W_{k+2}W_{k-2}A_n^4 + W_{k-1}W_k^2W_{k+1}A_n(A_{n+2}A_{n-1}^2 + A_{n-2}A_{n+1}^2).
\end{aligned} \tag{31}$$

Согласно (24) и (27) первые слагаемые в обеих частях последнего равенства можно записать как

$$W_k^4 A_{n-2} A_n^2 A_{n+2} = aW_k^4 A_n^2 A_{n+1} A_{n-1} + bW_k^4 A_n^4,$$
$$W_k^2 W_{k+2} W_{k-2} A_n^4 = aW_k^2 A_n^4 W_{k+1} W_{k-1} + bW_k^4 A_n^4.$$

Поэтому (31) равносильно тому, что

$$A_{n-1} A_n^2 A_{n+1} W_k (aW_k^3 + W_{k+1}^2 W_{k-2} + W_{k-1}^2 W_k) =$$
$$= W_{k-1} W_k^2 W_{k+1} A_n (aA_n^3 + A_{n+2} A_{n-1}^2 + A_{n-2} A_{n+1}^2).$$

Это равенство выполняется согласно (28), (29). Соотношения (25) доказаны.

3. Докажем равенства (26). В силу (21) их достаточно проверить при $k \geqslant 0$. Для этого используем индукцию по $k = 0, 1, \ldots$

База индукции. Согласно (20) уравнения (26) выполняются при $k = 0, 1$.

Шаг индукции от k к $k+1$ ($k \geqslant 1$). Нужно доказать, что

$$A_{n+k+2} A_{n-k-1} = -a^{-1/2} W_{k+2} W_{k+1} A_{n+2} A_{n-1} + a^{-1/2} W_{k+3} W_k A_{n+1} A_n. \tag{32}$$

Умножим (32) на $aA_{n+k+1} A_{n-k}$, учтем (26) и то, что согласно (25)

$$A_{n+k+2} A_{n-k} = A_{(n+1)+(k+1)} A_{(n+1)-(k+1)} = W_{k+1}^2 A_{n+2} A_n - W_k W_{k+2} A_{n+1}^2,$$
$$A_{n+k+1} A_{n-k-1} = A_{n+(k+1)} A_{n-(k+1)} = W_{k+1}^2 A_{n+1} A_{n-1} - W_k W_{k+2} A_n^2.$$

В итоге получаем эквивалентное соотношение

$$a(W_{k+1}^2 A_{n+2} A_n - W_k W_{k+2} A_{n+1}^2)(W_{k+1}^2 A_{n+1} A_{n-1} - W_k W_{k+2} A_n^2) =$$
$$= (W_{k+2} W_{k+1} A_{n+2} A_{n-1} - W_{k+3} W_k A_{n+1} A_n) \times$$
$$\times (W_{k+1} W_k A_{n+2} A_{n-1} - W_{k+2} W_{k-1} A_{n+1} A_n),$$

которое после раскрытия скобок и элементарных преобразований принимает вид

$$A_{n-1} A_n A_{n+1} A_{n+2} W_{k+1} (aW_{k+1}^3 + W_k^2 W_{k+3} + W_{k-1} W_{k+2}^2) =$$
$$= W_k W_{k+1}^2 W_{k+2} (aA_{n+1}^3 A_{n-1} + aA_{n+2} A_n^3 + A_{n-1}^2 A_{n+2}^2) +$$
$$+ A_{n+1}^2 A_n^2 W_k W_{k+2} (W_{k-1} W_{k+3} - aW_k W_{k+2}). \tag{33}$$

Учитывая, что

$$W_{k-1} W_{k+3} - aW_k W_{k+2} = bW_{k+1}^2,$$
$$aA_{n+1}^3 A_{n-1} + bA_{n+1}^2 A_n^2 = A_{n+1}^2 (aA_{n+1} A_{n-1} + bA_n^2) = A_{n+1}^2 A_{n+2} A_{n-2},$$

нетрудно заметить, что (33) равносильно равенству

$$A_{n-1} A_n A_{n+1} A_{n+2} W_{k+1} (aW_{k+1}^3 + W_k^2 W_{k+3} + W_{k-1} W_{k+2}^2) =$$
$$= W_k W_{k+1}^2 W_{k+2} A_{n+2} (aA_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2}).$$

Последнее выполнено в силу (28), (29). Равенства (26) доказаны. ▲

Т е о р е м а 2. *Пусть* $\alpha_j \in \mathbb{F} \setminus \{0\}$, $j = -2, -1, \ldots, 3$, *причем* $\Delta_1 \neq 0$, *где*

$$\Delta_1 = \begin{vmatrix} \alpha_2 \alpha_0 & \alpha_1^2 \\ \alpha_1 \alpha_{-1} & \alpha_0^2 \end{vmatrix} = \alpha_2 \alpha_0^3 - \alpha_{-1} \alpha_1^3.$$

Тогда существует единственная последовательность $A\colon \mathbb{Z} \to \mathbb{F}$, *удовлетворяющая неравенствам* (4) *и начальным условиям*

$$A_j = \alpha_j, \quad -2 \leqslant j \leqslant 3. \tag{34}$$

Доказательство. Искомая последовательность A должна удовлетворять равенству

$$D_A \begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ \alpha_3\alpha_{-1} & \alpha_2\alpha_0 & \alpha_1^2 \\ \alpha_2\alpha_{-2} & \alpha_1\alpha_{-1} & \alpha_0^2 \end{vmatrix} =$$
$$= \Delta_1 A_{n+2}A_{n-2} - \Delta_2 A_{n+1}A_{n-1} + \Delta_3 A_n^2 = 0,$$

где $\Delta_1, \Delta_2, \Delta_3$ – соответствующие миноры второго порядка. Так как $\Delta_1 \neq 0$, то выполняется уравнение (24), в котором $a = \Delta_2/\Delta_1$, $b = -\Delta_3/\Delta_1$. Отметим, что a и b не могут одновременно обращаться в нуль (иначе $A_{n+2}A_{n-2} = 0$, а это противоречит начальным условиям (34)). Поэтому возможны три случая.

1. Пусть $a = 0$, т.е.

$$A_{n+2}A_{n-2} = bA_n^2.$$

Тогда

$$b = \frac{\alpha_2\alpha_{-2}}{\alpha_0^2}, \quad \alpha_3\alpha_{-1}\alpha_0^2 = \alpha_1^2\alpha_2\alpha_{-2} \text{ (так как } \Delta_2 = 0).$$

Положим

$$A_{2k} = \alpha_0 \left(\frac{\alpha_0}{\alpha_{-2}}\right)^k \left(\frac{\alpha_2\alpha_{-2}}{\alpha_0^2}\right)^{k(k+1)/2},$$
$$A_{2k+1} = \alpha_1 \left(\frac{\alpha_1}{\alpha_{-1}}\right)^k \left(\frac{\alpha_3\alpha_{-1}}{\alpha_1^2}\right)^{k(k+1)/2}.$$

Тогда $A_{n+2}A_{n-2} = bA_n^2$, и выполняются начальные условия (25). Нетрудно также проверить, что выполняются (1), (2) с $N_0 = N_1 = 2$.

2. Пусть $b = 0$, т.е.

$$A_{n+2}A_{n-2} = aA_{n+1}A_{n-1}.$$

Тогда

$$a = \frac{\alpha_2\alpha_{-2}}{\alpha_1\alpha_{-1}}, \quad \alpha_3\alpha_{-1}^2\alpha_1 = \alpha_2^2\alpha_{-2}\alpha_0.$$

Положим

$$A_n = \left(\frac{\alpha_2\alpha_{-2}}{\alpha_1\alpha_{-1}}\right)^{n(n-1)/6} \left(\frac{\alpha_2}{\alpha_{-1}}\right)^{n/3} f_n, \quad f_n = \begin{cases} \alpha_0, & n \equiv 0 \pmod 3, \\ \alpha_1\alpha_{-1}^{1/3}\alpha_2^{-1/3}, & n \equiv 1 \pmod 3, \\ \alpha_1^{1/3}\alpha_{-1}\alpha_{-2}^{-1/3}, & n \equiv 2 \pmod 3. \end{cases}$$

Последовательность A_n определена “формально”, но корректно (если отдельно рассмотреть случаи, когда $n \equiv 0, 1, 2 \pmod 3$, то в каждом из них все степени, входящие в определение A_n, оказываются целыми). Кроме того, $A_{n+2}A_{n-2} = aA_{n+1}A_{n-1}$ и выполняются начальные условия (34). Нетрудно также проверить, что выполняются разложения (1), (2), где $N_0 = N_1 = 2$.

3. Пусть $ab \neq 0$. Начнем вычислять элементы последовательности A по формулам

$$A_{n+2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n-2}} \quad \text{при } n \geqslant 2,$$
$$A_{n-2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n+2}} \quad \text{при } n \leqslant -1.$$

Возможны два варианта.

3.1. Все полученные члены оказались ненулевыми. Тогда A – последовательность без нулей, удовлетворяющая (24). Согласно лемме 7 выполняются (25), (26). Поэтому $R_j(A) \leqslant 2$, $j = 0, 1$.

3.2. Существует номер m, такой что $A_m = 0$. Не умаляя общности, рассмотрим случай, когда $m > 0$. Пусть m – наименьшее натуральное, такое что $A_m = 0$. Тогда $m \geqslant 4$ и $A_n \neq 0$ при $-2 \leqslant n \leqslant m-1$. Элемент A_{m+1} найдем из соотношения

$$A_{m+1}A_{m-3} = aA_mA_{m-2} + bA_{m-1}^2 \quad \Longrightarrow \quad A_{m+1} = \frac{bA_{m-1}^2}{A_{m-3}}.$$

Ясно, что $A_{m+1} \neq 0$. Рассмотрим последовательность $B_n = A_{m-n}$. Тогда

$$B_{-1} = A_{m+1}, \quad B_0 = 0, \quad B_j = A_{m-j} \text{ при } j = 1, 2, 3, 4.$$

Согласно следствию 1 существует ровно одна последовательность B, удовлетворяющая указанным выше начальным условиям, такая что $R_j(B) \leqslant 2$, $j = 0, 1$. Положим теперь $\widetilde{A}_n = B_{m-n}$. Тогда

$$\widetilde{A}_n = A_n \text{ при } m-4 \leqslant n \leqslant m+1, \quad R_j(\widetilde{A}) \leqslant 2,\ j = 0, 1. \tag{35}$$

Докажем, что $\widetilde{A}_n = A_n$ при $-2 \leqslant n \leqslant m+1$. Так как $R_0(\widetilde{A}) \leqslant 2$, то выполняется разложение вида (1). Выбирая в нем $m = 0, 1, 2$, получаем три соотношения, левые части которых линейно зависимы над $\mathbb{F}$. Поэтому существует тройка $(\widetilde{\Delta}_1, \widetilde{\Delta}_2, \widetilde{\Delta}_3) \in \in \mathbb{F}^3 \setminus \{0\}$, такая что

$$\widetilde{\Delta}_1\widetilde{A}_{n+2}\widetilde{A}_{n-2} = \widetilde{\Delta}_2\widetilde{A}_{n+1}A_{n-1} + \widetilde{\Delta}_3\widetilde{A}_n^2.$$

Выбирая в последнем соотношении $n = m-1$ и $n = m-2$ и учитывая (35), имеем

$$\widetilde{\Delta}_1A_{m+1}A_{m-3} = \widetilde{\Delta}_3A_{m-1}^2, \quad \widetilde{\Delta}_2A_{m-1}A_{m-3} + \widetilde{\Delta}_3A_{m-2}^2 = 0.$$

Сравнивая эти соотношения с (24), в котором $n = m-1$ и $n = m-2$, приходим к выводу, что $a = \widetilde{\Delta}_2/\widetilde{\Delta}_1$, $b = \widetilde{\Delta}_3/\widetilde{\Delta}_1$, т.е. $\widetilde{A}$ удовлетворяет уравнению (24). Поэтому $\widetilde{A}_n = A_n$ при $-2 \leqslant n \leqslant m+1$. Значит, $\widetilde{A}$ – искомая последовательность. ▲

§ 4. Построение асимметричных криптосистем

Всюду в этом параграфе мы считаем, что A – последовательность из теоремы 1, причем $\alpha = 1$. Тогда последовательность A – нечетная, т.е. $A_{-n} = -A_n$.

Через S обозначаем последовательность, состоящую из четверок

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2}), \quad n \in \mathbb{Z}.$$

4.1. Алгоритм "быстрого" вычисления четверок $S(n)$. Полагая $n = m + k$ в соотношениях (6), (7), получаем формулы

$$A_{m+2k} = A_m^{-1}(A_k^2A_{m+k+1}A_{m+k-1} - A_{k+1}A_{k-1}A_{m+k}^2), \tag{36}$$

$$A_{m+2k+1} = A_m^{-1}(A_k A_{k+1} A_{m+k+2} A_{m+k-1} - A_{k+2} A_{k-1} A_{m+k} A_{m+k+1}). \qquad (37)$$

Лемма 8. *Зная начальные данные* $(\beta, \gamma, \mathbb{F})$, *четверки* $S(n)$, $S(\ell)$, $S(n+\ell)$ *и номер* ℓ (*номер* n *неизвестен*), *можно вычислить четверку* $S(n+2\ell)$, *используя* $O(1)$ *элементарных операций в поле* $\mathbb{F}$.

Доказательство. Не умаляя общности, можно считать, что $\ell \in \mathbb{N}$. Если $\ell = 1$, то доказательство тривиально (достаточно использовать формулы (9), (10)).

Пусть $\ell > 1$. Нам известны члены последовательности A с номерами

$$n-1,\ n,\ n+1,\ n+2;\ \ell-1,\ \ell,\ \ell+1,\ \ell+2;\ n+\ell-1,\ n+\ell,\ n+\ell+1,\ n+\ell+2.$$

Нужно найти члены с номерами $n+2\ell-1, n+2\ell, n+2\ell+1, n+2\ell+2$. Вычислим $A_{\ell-2}$, используя равенство (6) (или (7) при $A_{\ell+2} = 0$), в котором $k = 2$, $n = \ell$.

1. Пусть $A_n \neq 0$. Тогда элементы $A_{n+2\ell}$, $A_{n+2\ell+2}$ находятся из равенства (36), в котором $m = n$ и $k = \ell, \ell+1$, а элементы $A_{n+2\ell\pm1}$ – из (37), в котором $m = n$ и $k = \ell-1, \ell$.

2. Пусть $A_n = 0$. Тогда $A_{n\pm1} \neq 0$ согласно лемме 3 а). Используя (9), (10), вычислим $A_{\ell+3}$. После этого элементы $A_{n+2\ell+1}$ и $A_{n+2\ell+2}$ находим из (36) и (37), в которых $m = n-1$, $k = \ell+1$, а элементы $A_{n+2\ell-1}$ и $A_{n+2\ell}$ – из (36) и (37), в которых $m = n+1$, $k = \ell-1$. ▲

С помощью леммы 8 стандартным образом (по аналогии с бинарным алгоритмом возведения в степень) строится алгоритм "быстрого" вычисления $S(n+k)$ при заданных $S(n)$ и k (номер n неизвестен). Он совпадает с алгоритмом 1 из [15], поэтому его описание мы опускаем. В итоге приходим к следующему результату.

Следствие 5. *Пусть дано поле* $\mathbb{F}$, *начальные данные* β, γ, *номер* $k \in \mathbb{N}$ *и четверка* $S(n)$ (*номер* n *неизвестен*). *Существует алгоритм вычисления четверки* $S(n+k)$, *сложность которого равна сложности выполнения* $O(\ln k)$ *элементарных операций в поле* $\mathbb{F}$.

4.2. Аналог алгоритма Диффи – Хеллмана. Абоненты B_1, B_2, используя открытый канал связи, выбирают поле $\mathbb{F}$ и начальные данные β, γ. После этого они вырабатывают общий секретный ключ $K \in \mathbb{F}^4$, используя следующий алгоритм.

1. Абонент B_1 выбирает $k_1 \in \mathbb{N}$, вычисляет $S(k_1)$, используя алгоритм 1, и посылает абоненту B_2 сообщение $S(k_1)$ (номер k_1 хранится в секрете);
2. Абонент B_2 выбирает $k_2 \in \mathbb{N}$, вычисляет $S(k_2)$ и посылает абоненту B_1 сообщение $S(k_2)$ (номер k_2 хранится в секрете);
3. Абонент B_2 (абонент B_1), зная номер k_2 (номер k_1) и четверку $S(k_1)$ (четверку $S(k_2)$), вычисляет $S(k_1+k_2)$, используя алгоритм из следствия 5.

Общим секретом является $K = S(k_1+k_2)$.

Пассивный противник знает четверки $S(k_1)$ и $S(k_2)$. Для того чтобы найти секретный ключ $S(k_1+k_2)$, ему достаточно определить номер k_1 (или номер k_2). Для этого нужно решить задачу определения номера k по заданному элементу $S(k)$. Она представляет собой задачу дискретного логарифмирования в группе $(S, +)$, где $S(n) + S(m) = S(n+m)$.

4.3. Аналог алгоритма Эль-Гамаля. Пусть поле $\mathbb{F}$, начальные данные $\beta, \gamma \in \mathbb{F}$ и целое число n – это *общий параметр* всех пользователей. *Секретным ключом абонента* B является некое $k \in \mathbb{N}$, а *открытым ключом* – четверка $S(k)$.

Алгоритм шифрования сообщения $x = x_{-1}x_0x_1x_2 \in \mathbb{F}^4$, отправляемого абоненту B:

1. Выбираем сеансовый ключ $r \in \mathbb{N}$;

2. Вычисляем четверки $S(n+r)$ и $S(n+k+r)$. Для этого можно использовать алгоритм из следствия 5, так как нам известны номера r, n и четверка $S(k)$;
3. Если хотя бы один элемент из $A_{n+k+r+j}$, $j=-1,0,1,2$, равен 0, то возвращаемся к шагу 1;
4. Вычисляем $y=y_{-1}y_0y_1y_2\in\mathbb{F}^4$ по формулам $y_j=x_j\cdot A_{n+k+r+j}$, $j=-1,0,1,2$;
5. Высылаем абоненту B шифротекст $(S(n+r),y)$.

Алгоритм дешифрования шифротекста $(S(n+r),y)$ абонентом B:

1. Абонент B вычисляет $S(n+k+r)$, используя алгоритм из следствия 5 (напомним, что B знает четверку $S(n+r)$ и номер k);
2. Находит открытый текст $x=x_{-1}x_0x_1x_2$ по формулам $x_j=y_j\cdot A^{-1}_{n+k+r+j}$, $j=-1,0,1,2$.

Корректность алгоритма дешифровки очевидна.

Замечание 4. Аналогичным образом можно построить алгоритм электронной цифровой подписи (наподобие ГОСТ 34.10-2012 или FIPS-186-4), использующий последовательность из теоремы 1 вместо группы точек на эллиптической кривой.

§ 5. Заключение

По-видимому, криптостойкость приведенных выше алгоритмов определяется сложностью решения ЗДЛ (задача дискретного логарифмирования) в группе $(S,+)$. Автору не известны методы ее решения, которые более эффективны, нежели алгоритм полного перебора или алгоритм Гельфонда (алгоритм больших и малых шагов). Очевидно, что сложность решения этой задачи зависит от периода ω последовательности A (ω – порядок группы S). Согласно лемме 5 имеем $\omega\leqslant|\mathbb{F}|^4$. Открытыми являются вопросы о существовании последовательностей с $\omega\approx|\mathbb{F}|^4$ и об алгоритмах вычисления периода (кроме известных универсальных). Если предположить, что $\mathbb{F}=\mathbb{Z}_p$, $\omega\approx|\mathbb{F}|^4$, то атака на криптосистемы из пп. 4.2, 4.3, основанная на методе Гельфонда, потребует выполнения порядка $\sqrt{\omega}\approx|\mathbb{Z}_p|^2=p^2$ элементарных операций в $\mathbb{Z}_p$. Выбирая $p\approx 2^{64}$, получаем алгоритмы, криптостойкость которых сравнима с соответствующими алгоритмами, использующими группу точек на эллиптической кривой над полем $\mathbb{Z}_q$ с $q\approx 2^{256}$. Разумеется, все это верно при выполнении двух условий: 1) мы умеем находить последовательности с периодом порядка $|\mathbb{F}|^4$; 2) не известны субэкспоненциальные алгоритмы решения ЗДЛ в группе $(S,+)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Авдеева М.О., Быковский В.А.* Гиперэллиптические системы последовательностей и функций // Дальневост. матем. журн. 2016. Т. 16. № 2. С. 115–122. https://www.mathnet.ru/dvmg326
2. *Илларионов А.А.* Гиперэллиптические системы последовательностей ранга 4 // Матем. сб. 2019. Т. 210. № 9. С. 59–88. https://doi.org/10.4213/sm9050
3. *Robinson R.M.* Periodicity of Somos Sequences // Proc. Amer. Math. Soc. 1992. V. 116. № 3. P. 613–619. https://doi.org/10.2307/2159426
4. *Shipsey R.* Elliptic Divisibility Sequences. PhD Thesis. Goldsmiths College, Univ. London, 2000.
5. *Fomin S., Zelevinsky A.* The Laurent Phenomenon // Adv. Appl. Math. 2002. V. 28. № 2. P. 119–144. https://doi.org/10.1006/aama.2001.0770
6. *Swart C.S.* Elliptic Curves and Related Sequences. PhD Thesis. Royal Holloway, Univ. London, 2003.
7. *Hone A.N.W.* Elliptic Curves and Quadratic Recurrence Sequences // Bull. Lond. Math. Soc. 2005. V. 37. № 2. P. 161–171. https://doi.org/10.1112/S0024609304004163

8. *van der Poorten A.J., Swart C.S.* Recurrence Relations for Elliptic Sequences: Every Somos 4 Is a Somos k // Bull. Lond. Math. Soc. 2006. V. 38. № 4. P. 546–554. https://doi.org/10.1112/S0024609306018534
9. *Hone A.N.W.* Sigma Function Solution of the Initial Value Problem for Somos 5 Sequences // Trans. Amer. Math. Soc. 2007. V. 359. № 10. P. 5019–5034. https://doi.org/10.1090/S0002-9947-07-04215-8
10. *Hone A.N.W., Swart C.* Integrality and the Laurent Phenomenon for Somos 4 and Somos 5 Sequences // Math. Proc. Cambridge Philos. Soc. 2008. V. 145. № 1. P. 65–85. https://doi.org/10.1017/S030500410800114X
11. *Hone A.N.W.* Analytic Solutions and Integrability for Bilinear Recurrences of Order Six // Appl. Anal. 2010. V. 89. № 4. P. 473–492. https://doi.org/10.1080/00036810903329977
12. *Fedorov Yu.N., Hone A.N.W.* Sigma-Function Solution to the General Somos-6 Recurrence via Hyperelliptic Prym Varieties // J. Integrable Syst. 2016. V. 1. № 1. Art. xyw012 (34 pp.). https://doi.org/10.1093/integr/xyw012
13. *Быковский В.А., Устинов А.В.* Сомос-4 и эллиптические системы последовательностей // ДАН. 2016. Т. 471. № 1. С. 7–10. https://doi.org/10.7868/S0869565216310030
14. *Shor P.W.* Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proc. 35th Annu. Symp. on Foundations of Computer Science. Santa Fe, NM, USA. Nov. 20–22, 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700
15. *Илларионов А.А.* Асимметричные криптосистемы и гиперэллиптические последовательности // Дальневост. матем. журн. 2019. Т. 19. № 2. С. 185–196. https://www.mathnet.ru/dvmg407
16. *Устинов А.В.* Элементарный подход к изучению последовательностей Сомоса // Тр. МИАН. 2019. Т. 305. С. 330–343. https://doi.org/10.4213/tm3990
17. *Ward M.* Memoir on Elliptic Divisibility Sequences // Amer. J. Math. 1948. V. 70. № 1. P. 31–74. https://doi.org/10.2307/2371930

Илларионов Андрей Анатольевич
Национальный исследовательский университет
"Высшая школа экономики", Москва
Хабаровское отделение
Института прикладной математики
ДВО РАН, Хабаровск
illar_a@list.ru

Поступила в редакцию
19.01.2023
После доработки
11.05.2023
Принята к публикации
11.05.2023

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*
по контракту с ООО «Объединённая редакция»

Москва
ООО «Объединённая редакция»