

ISSN 0555-2923

РОССИЙСКАЯ АКАДЕМИЯ НАУК

---

# Проблемы передачи информации



НАУКА  
— 1727 —

том 60 вып. 1

2024

РОССИЙСКАЯ АКАДЕМИЯ НАУК  
ПРОБЛЕМЫ  
ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан  
в январе 1965 г.

ISSN: 0555-2923

Выходит  
4 раза в год

Том 60, 2024

Вып. 1

Январь–Февраль–Март

Москва

---

СО Д Е Р Ж А Н И Е

Обращение главного редактора ..... 3

Теория информации

Гутьеррес-Гутьеррес Х., Барасойн-Эчепаре И., Саррага-Родригес М., Инсаusti Ш.  
Вычисление фундаментальных пределов сжатия данных для некоторых нестационарных источников векторных процессов авторегрессии со скользящим средним.... 4

Теория кодирования

Бассальго Л.А., Зиновьев В.А., Лебедев В.С. Конструкции недвоичных кодов, лежащих на границе Джонсона..... 17

Воробьев И.В., Лебедев А.В., Лебедев В.С. Исправление одной ошибки в асимметричном канале с обратной связью..... 26

Квантовая связь и квантовые вычисления

Морозов А.А. Об измерении топологического заряда энионов ..... 33

Большие системы

Бланк М.Л., Поляков М.О. Элементарное решение задачи справедливого деления .... 41

## CONTENTS

Editor-in-Chief Address .....	3
-------------------------------	---

### Information Theory

<b>Gutiérrez-Gutiérrez, J., Barasoain-Echepare, Í., Zárrega-Rodríguez, M., and Insausti, X.,</b> Computation of the Fundamental Limits of Data Compression for Certain Nonstationary ARMA Vector Sources .....	4
---	---

### Coding Theory

<b>Bassalygo, L.A., Zinoviev, V.A., and Lebedev, V.S.,</b> Constructions of Nonbinary Codes Meeting the Johnson Bound .....	17
<b>Vorobyev, I.V., Lebedev, A.V., and Lebedev, V.S.,</b> Correcting a Single Error in an Asymmetric Feedback Channel .....	26

### Quantum Communications and Computing

<b>Morozov, A.A.,</b> On Measuring the Topological Charge of Anyons .....	33
---	----

### Large Systems

<b>Blank, M.L. and Polyakov, M.O.,</b> Elementary Solution to the Fair Division Problem.....	41
--	----

ОБРАЩЕНИЕ ГЛАВНОГО РЕДАКТОРА

DOI: 10.31857/S0555292324010017, EDN: NCLRDR

Дорогие читатели!

В качестве недавно назначенного главного редактора журнала «Проблемы передачи информации» я рад продолжить наследие этого уважаемого издания, который был в авангарде теории информации и математики с момента его создания в 1965 году. Для меня большая честь опереться на прочный фундамент, заложенный моими предшественниками, и развивать журнал в наше время, которое можно назвать эпохой инноваций в области передачи и обработки информации.

Жизненно важная роль информации как организующего принципа всей деятельности человека сегодня ощущается сильнее, чем когда-либо прежде, а проблемы передачи, хранения, обработки и распространения информации становятся все более сложными и разнообразными. В результате потребность в специализированных периодических изданиях, описывающих новейшие исследования в этой области, как никогда велика.

«Проблемы передачи информации» всегда был теоретическим журналом, публикующим оригинальные исследовательские статьи по широкому кругу тем, связанных с передачей и обработкой информации. Мы также рады видеть на своих страницах и обзорные статьи, дающие всесторонний анализ открытых проблем и перспективных направлений. Мы расширяем тематику журнала, включая в нее новые актуальные направления, такие как квантовая связь и вычисления, биоинформатика и теория искусственного интеллекта. Мы также будем продолжать публиковать статьи по важным темам в областях теории информации, проводной и беспроводной связи, моделирования каналов и сетей, обработки сигналов, обработки изображений, компьютерного зрения и т. д.

Двигаясь вперед, мы продолжим поддерживать самые высокие стандарты качества во всех аспектах нашей деятельности. Мы будем стремиться реагировать на потребности наших читателей, авторов и рецензентов, а также способствовать развитию активного сообщества ученых, инженеров и исследователей.

Я хотел бы выразить глубочайшую благодарность покидающему свой пост главному редактору и редколлегии, чье руководство и видение сыграли важную роль в успехе журнала. Я также выражаю искреннюю благодарность рецензентам и авторам за неоценимый вклад в развитие журнала. С нетерпением жду возможности работать со всеми вами в ближайшие годы.

Искренне ваш,  
*Е.М. Хоров*

УДК 621.391 : 519.72

© 2024 г. Х. Гутьеррес-Гутьеррес, И. Барасоайн-Эчепаре,  
М. Саррага-Родригес, Ш. Инсаusti

## ВЫЧИСЛЕНИЕ ФУНДАМЕНТАЛЬНЫХ ПРЕДЕЛОВ СЖАТИЯ ДАННЫХ ДЛЯ НЕКОТОРЫХ НЕСТАЦИОНАРНЫХ ИСТОЧНИКОВ ВЕКТОРНЫХ ПРОЦЕССОВ АВТОРЕГРЕССИИ СО СКОЛЬЗЯЩИМ СРЕДНИМ<sup>1</sup>

Для определенных нестационарных источников вещественных гауссовских векторных процессов авторегрессии со скользящим средним (ARMA-процессов) вычисляются скорость создания дифференциальной энтропии и скорость как функция искажения.

*Ключевые слова:* векторная авторегрессия со скользящим средним (ARMA), сжатие данных, скорость создания дифференциальной энтропии, скорость как функция искажения.

DOI: 10.31857/S0555292324010029, EDN: OZSXLJ

### § 1. Введение

В работе [1] Шеннон ввел два фундаментальных предела (термин, предложенный Вайнером в [2]) для сжатия данных: энтропия источника (аналогом которой для непрерывных источников является скорость создания дифференциальной энтропии [3]) и скорость как функция искажения. Однако для векторных источников в литературе было получено очень мало выражений в замкнутом виде для этих фундаментальных пределов. Наиболее примечательным исключением является замкнутое выражение, полученное Томсом и Бергером в [4] для некоторых нестационарных вещественных гауссовских векторных источников с авторегрессией. В настоящей статье мы распространим их результат на векторные ARMA-источники. Мы также получим выражение в замкнутом виде для скорости создания дифференциальной энтропии таких векторных ARMA-источников. Для вычисления этих двух величин мы сперва докажем два новых математических результата, касающихся автокорреляционных матриц векторных ARMA-процессов. Хотя в литературе существуют и другие теоремы об автокорреляционных матрицах векторных ARMA-процессов (см., например, [5]), их условия трудно проверяемы на практике. Основное преимущество наших новых результатов заключается в том, что их условия легко проверить с помощью хорошо известных численных методов.

Дальнейшая часть статьи имеет следующую структуру. В § 2 получены два новых результата о векторных ARMA-процессах. В § 3 эти результаты применяются для вычисления двух фундаментальных пределов сжатия данных для некоторых нестационарных векторных ARMA-источников.

<sup>1</sup> Работа выполнена при частичной финансовой поддержке Министерства науки и инноваций Испании в рамках проекта MADDIE (номер проекта PID2022-137099NB-C44).

## § 2. Два новых результата о векторных ARMA-процессах

**2.1. Обозначения и определения.** В этом пункте приведем обозначения для блочно-теплицевых матриц, которые будут использоваться далее по всей статье, а также напомним три известных определения, касающиеся стохастических векторных процессов.

Для непрерывной  $2\pi$ -периодической функции

$$F: \mathbb{R} \rightarrow \mathbb{C}^{N \times N}$$

через  $T_n(F)$  обозначим блочно-теплицеву матрицу с  $n \times n$  блоками размера  $N \times N$  вида

$$[T_n(F)]_{j,k} = F_{j-k}, \quad j, k \in \{1, \dots, n\},$$

где  $\{F_k\}_{k \in \mathbb{Z}}$  – последовательность коэффициентов Фурье функции  $F$ . Если  $F$  имеет вид

$$F(\omega) = I_N + \sum_{k=1}^p e^{-k\omega i} F_{-k}, \quad \forall \omega \in \mathbb{R},$$

для некоторого  $p \in \mathbb{N}$ , то через  $\Psi_p(F)$  обозначается ее сопровождающая матрица

$$\Psi_p(F) = \left( \begin{array}{ccc|c} -F_{-1} & \dots & -F_{-(p-1)} & -F_{-p} \\ \hline & I_{(p-1)N} & & 0_{(p-1)N \times N} \end{array} \right),$$

где  $I_m$  – единичная матрица размера  $m \times m$ , а  $0_{m \times n}$  – нулевая матрица размера  $m \times n$ .

Всюду далее для матрицы  $A \in \mathbb{C}^{n \times n}$  через  $\rho(A)$  будем обозначать ее спектральный радиус (т.е. максимальный модуль ее собственных значений), а через  $\sigma_1(A)$  и  $\sigma_n(A)$  – ее наибольшее и наименьшее сингулярные числа соответственно. Если матрица  $A$  эрмитова, то через  $\lambda_1(A)$  и  $\lambda_n(A)$  будем обозначать ее наибольшее и наименьшее собственные значения соответственно.

Теперь напомним понятие асимптотически стационарного процесса в широком смысле (AWSS-процесса), введенное для скалярных процессов в [6, с. 225] и обобщенное на векторные процессы в [7, определение 7.1 и теорема 4.3].

**Определение 1.** Пусть функция  $X: \mathbb{R} \rightarrow \mathbb{C}^{N \times N}$  непрерывна и  $2\pi$ -периодична. Случайный  $N$ -мерный процесс  $\{x_n\}$  называется AWSS-процессом с (асимптотической) спектральной плотностью мощности (СПМ)  $X$ , если он имеет постоянное среднее, множество  $\{\|\mathbf{E}(x_{n:1}x_{n:1}^*)\|_2\}$  ограничено и

$$\lim_{n \rightarrow \infty} \frac{\|\mathbf{E}(x_{n:1}x_{n:1}^*) - T_n(X)\|_F}{\sqrt{n}} = 0, \quad (1)$$

где

$$x_{n:1} = \begin{pmatrix} x_n \\ x_{n-1} \\ \vdots \\ x_1 \end{pmatrix}, \quad \forall n \in \mathbb{N},$$

через  $*$  обозначено эрмитово сопряжение,  $\mathbf{E}$  – математическое ожидание,  $\|\cdot\|_2$  – спектральная норма, а  $\|\cdot\|_F$  – норма Фробениуса.

Следует отметить, что векторный WSS-процесс  $\{x_n\}$  с непрерывной СПМ  $X$  является AWSS-процессом с СПМ  $X$ , поскольку в силу того, что

$$\{\mathbf{E}(x_{n:1}x_{n:1}^*)\} = \{T_n(X)\},$$

равенство (1) выполняется и  $\{\|\mathbf{E}(x_{n:1}x_{n:1}^*)\|_2\}$  ограничено (см., например, [7, теорема 4.3]).

Теперь напомним понятие (одностороннего) векторного ARMA-процесса.

**Определение 2.** ARMA-процессом называется  $N$ -мерный процесс  $\{x_n\}$  с нулевым средним, такой что

$$x_n = \sum_{k=0}^{n-1} B_{-k}w_{n-k} - \sum_{\ell=1}^{n-1} A_{-\ell}x_{n-\ell}, \quad \forall n \in \mathbb{N}, \quad (2)$$

где

$$\begin{aligned} A_{-\ell} &\in \mathbb{C}^{N \times N}, \quad \forall \ell \in \mathbb{N}, \\ B_{-k} &\in \mathbb{C}^{N \times N}, \quad \forall k \in \mathbb{N} \cup \{0\}, \end{aligned}$$

а  $\{w_n\}$  –  $N$ -мерный процесс с нулевым средним с

$$\mathbf{E}(w_j w_h^*) = \delta_{j,h} W, \quad \forall j, h \in \mathbb{N},$$

где  $\delta$  – символ Кронекера, а  $W$  – положительно определенная матрица размера  $N \times N$  (т.е. процесс  $\{w_n\}$  – векторный белый шум).

Если  $\det(B_0) \neq 0$ , то без ограничения общности можно считать, что  $B_0 = I_N$  (см. Приложение А). Этот факт хорошо известен в скалярном случае, т.е. для  $N = 1$  (см., например, [8]).

Заметим, что уравнение (2) можно переписать в виде

$$\sum_{k=0}^{n-1} A_{-k}x_{n-k} = \sum_{k=0}^{n-1} B_{-k}w_{n-k}, \quad \forall n \in \mathbb{N},$$

где  $A_0 = I_N$ . Предположим, что

$$\sum_{k=0}^{\infty} \|A_{-k}\|_F < \infty \quad \text{и} \quad \sum_{k=0}^{\infty} \|B_{-k}\|_F < \infty,$$

тогда из [7, Приложение В] получаем, что

$$T_n(A)x_{n:1} = T_n(B)w_{n:1}, \quad \forall n \in \mathbb{N},$$

где

$$A(\omega) = I_N + \sum_{k=1}^{\infty} e^{-k\omega i} A_{-k}$$

и

$$B(\omega) = \sum_{k=0}^{\infty} e^{-k\omega i} B_{-k}$$

для всех  $\omega \in \mathbb{R}$ . Таким образом,  $\{\mathbf{E}(x_{n:1}x_{n:1}^*)\}$  можно выразить через блочно-теплицевы матрицы как

$$\begin{aligned}
\{\mathbf{E}(x_{n:1}x_{n:1}^*)\} &= \{(T_n(A))^{-1}T_n(A)\mathbf{E}(x_{n:1}x_{n:1}^*)(T_n(A))^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}\mathbf{E}(T_n(A)x_{n:1}x_{n:1}^*(T_n(A))^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}\mathbf{E}(T_n(A)x_{n:1}(T_n(A)x_{n:1})^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}\mathbf{E}(T_n(B)w_{n:1}(T_n(B)w_{n:1})^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}\mathbf{E}(T_n(B)w_{n:1}w_{n:1}^*(T_n(B))^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}T_n(B)\mathbf{E}(w_{n:1}w_{n:1}^*)(T_n(B))^*((T_n(A))^*)^{-1}\} = \\
&= \{(T_n(A))^{-1}T_n(B)T_n(W)(T_n(B))^*((T_n(A))^{-1})^*\}, \tag{3}
\end{aligned}$$

поскольку

$$\det(T_n(A)) = 1 \neq 0, \forall n \in \mathbb{N}.$$

Следует отметить, что блочно-теплицева матрица  $T_n(W)$  является блочно-диагональной матрицей с блоками размера  $N \times N$  на главной диагонали, равными  $W$ . Если  $N = 1$ , то  $W$  – дисперсия шума, обычно обозначаемая через  $\sigma^2$ .

Теперь можно напомнить понятие векторного ARMA( $p, q$ )-процесса.

**Определение 3.** Пусть процесс  $\{x_n\}$  такой, как в определении 2, где  $\mathbf{B}_0 = I_N$ . Если существуют  $p, q \in \mathbb{N}$ , такие что

$$\mathbf{A}_{-\ell} = 0_{N \times N}, \quad \forall \ell > p$$

и

$$\mathbf{B}_{-k} = 0_{N \times N}, \quad \forall k > q,$$

то  $\{x_n\}$  называется векторным ARMA( $p, q$ )-процессом. Заметим, что последовательность его автокорреляционных матриц  $\{\mathbf{E}(x_{n:1}x_{n:1}^*)\}$  задается уравнением (3), где

$$A(\omega) = I_N + \sum_{k=1}^p e^{-k\omega i} \mathbf{A}_{-k}$$

и

$$B(\omega) = I_N + \sum_{k=1}^q e^{-k\omega i} \mathbf{B}_{-k}.$$

Скалярные ARMA( $p, q$ )-модели часто используются в сжатии сигналов (см., например, [9]).

## 2.2. Об автокорреляционных матрицах некоторых векторных ARMA-процессов.

Первый из наших результатов дает достаточное условие, при котором векторный ARMA( $p, q$ )-процесс является AWSS-процессом.

**Теорема 1.** Пусть  $\{x_n\}$  – процесс из определения 3. Если  $\rho(\Psi_p(A)) < 1$ , то

1. Множество  $\{\|\mathbf{E}(x_{n:1}x_{n:1}^*) - T_n(X)\|_F\}$ , где

$$X(\omega) = (A(\omega))^{-1}B(\omega)W(B(\omega))^*((A(\omega))^{-1})^*$$

для всех  $\omega \in \mathbb{R}$ , ограничено;

2.  $\{x_n\}$  является AWSS-процессом с СПМ  $X$ .

Доказательство. 1. Так как  $\rho(\Psi_p(A)) < 1$ , то в силу [10, теорема 6] имеем  $\det(A(\omega)) \neq 0$  для всех  $\omega \in \mathbb{R}$ , и множество  $\{\|(T_n(A))^{-1}\|_2\}$  ограничено. Из (3) и [7, лемма 4.2] получаем

$$\begin{aligned}
& \|\mathbf{E}(x_{n:1}x_{n:1}^*) - T_n(A^{-1}BW B^*(A^{-1})^*)\|_F = \\
& = \|(T_n(A))^{-1}T_n(B)T_n(W)(T_n(B))^*((T_n(A))^{-1})^* - T_n(A^{-1}BW B^*(A^{-1})^*)\|_F \leq \\
& \leq \|(T_n(A))^{-1}\|_2 \times \\
& \times \|T_n(B)T_n(W)(T_n(B))^*((T_n(A))^{-1})^* - T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*)\|_F \leq \\
& \leq \|(T_n(A))^{-1}\|_2 \left( \|T_n(BW)(T_n(B))^*((T_n(A))^*)^{-1} - T_n(BW B^*(A^{-1})^*)\|_F + \right. \\
& \left. + \|T_n(BW B^*(A^{-1})^*) - T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*)\|_F \right) \leq \|(T_n(A))^{-1}\|_2 \times \\
& \times \left( \|((T_n(A))^*)^{-1}\|_2 \|T_n(BW)(T_n(B))^* - T_n(BW B^*(A^*)^{-1})(T_n(A))^*\|_F + \right. \\
& \left. + \|T_n(BW B^*(A^{-1})^*) - T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*)\|_F \right) \leq \\
& \leq \|(T_n(A))^{-1}\|_2 \left( \|((T_n(A))^{-1})^*\|_2 \left( \|T_n(BW)T_n(B^*) - T_n(BW B^*)\|_F + \right. \right. \\
& \left. \left. + \|T_n(BW B^*) - T_n(BW B^*(A^*)^{-1})T_n(A^*)\|_F \right) + \right. \\
& \left. + \|T_n(BW B^*(A^{-1})^*) - T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*)\|_F \right) = \\
& = \|(T_n(A))^{-1}\|_2 \left( \|(T_n(A))^{-1}\|_2 \left( \|T_n(BW)T_n(B^*) - T_n(BW B^*)\|_F + \right. \right. \\
& \left. \left. + \|T_n(BW B^*(A^*)^{-1})T_n(A^*) - T_n(BW B^*(A^*)^{-1}A^*)\|_F \right) + \right. \\
& \left. + \|T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*) - T_n(AA^{-1}BW B^*(A^{-1})^*)\|_F \right)
\end{aligned}$$

для всех  $n \in \mathbb{N}$ . Для завершения доказательства остается показать, что множества

$$\begin{aligned}
& \left\{ \|T_n(BW)T_n(B^*) - T_n(BW B^*)\|_F \right\}, \\
& \left\{ \|T_n(BW B^*(A^*)^{-1})T_n(A^*) - T_n(BW B^*(A^*)^{-1}A^*)\|_F \right\}, \\
& \left\{ \|T_n(A)T_n(A^{-1}BW B^*(A^{-1})^*) - T_n(AA^{-1}BW B^*(A^{-1})^*)\|_F \right\}
\end{aligned}$$

ограничены. Это следует из [11, лемма 2] и того факта, что  $A$ ,  $A^*$  и  $B^*$  – тригонометрические многочлены.

2. Это является прямым следствием утверждения 1 и [10, теорема 8].  $\blacktriangle$

В теореме 1 мы доказали, что  $\rho(\Psi_p(A)) < 1$  является достаточным условием для того, чтобы векторный ARMA( $p, q$ )-процесс был AWSS-процессом. В [5, теорема 8] было получено другое достаточное условие, а именно:

$$\inf_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)) > 0 \quad \text{и} \quad \inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0.$$

В Приложении В мы покажем, что эти условия равносильны. Однако основным преимуществом нового условия  $\rho(\Psi_p(A)) < 1$  является то, что его выполнение легко проверять, используя, например, степенной метод – классический численный метод для нахождения спектрального радиуса матрицы. Напротив того, проверка условия

$$\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0,$$

приведенного в [5, теорема 8], представляет собой в общем случае трудноразрешимую задачу, поскольку для этого требуется вычислить наименьшее сингулярное чис-

ло бесконечного количества матриц. Кроме того, в теореме 1 мы также установили, что скорость сходимости последовательности

$$\left\{ \frac{\|\mathbf{E}(x_{n:1}x_{n:1}^*) - T_n(X)\|_F}{\sqrt{n}} \right\}$$

равна  $O\left(\frac{1}{\sqrt{n}}\right)$ .

Наш второй результат касается собственных значений автокорреляционных матриц некоторых векторных ARMA( $p, q$ )-процессов.

**Теорема 2.** Пусть  $\{x_n\}$  – процесс из определения 3.

1. Если  $\rho(\Psi_p(A)) < 1$ , то

$$\sup_{n \in \mathbb{N}} \lambda_1(\mathbf{E}(x_{n:1}x_{n:1}^*)) < \infty;$$

2. Если  $\rho(\Psi_q(B)) < 1$ , то

$$0 < \inf_{n \in \mathbb{N}} \lambda_{nN}(\mathbf{E}(x_{n:1}x_{n:1}^*)).$$

**Доказательство.** 1. По теореме 1 процесс  $\{x_n\}$  является AWSS-процессом, и следовательно, множество  $\{\|\mathbf{E}(x_{n:1}x_{n:1}^*)\|_2\}$  ограничено. Так как  $\mathbf{E}(x_{n:1}x_{n:1}^*)$  положительно полуопределена для всех  $n \in \mathbb{N}$ , то

$$\|\mathbf{E}(x_{n:1}x_{n:1}^*)\|_2 = \lambda_1(\mathbf{E}(x_{n:1}x_{n:1}^*))$$

для всех  $n \in \mathbb{N}$ .

2. Согласно [10, теорема 6] множество  $\{\|(T_n(B))^{-1}\|_2\}$  ограничено. Применяя равенство (3) и [7, теорема 4.3], получаем

$$\begin{aligned} \lambda_{nN}(\mathbf{E}(x_{n:1}x_{n:1}^*)) &= \sigma_{nN}(\mathbf{E}(x_{n:1}x_{n:1}^*)) = \\ &= \frac{1}{\sigma_1((\mathbf{E}(x_{n:1}x_{n:1}^*))^{-1})} = \frac{1}{\|(\mathbf{E}(x_{n:1}x_{n:1}^*))^{-1}\|_2} = \\ &= \frac{1}{\|(T_n(A))^*((T_n(B))^*)^{-1}(T_n(W))^{-1}(T_n(B))^{-1}T_n(A)\|_2} \geq \\ &\geq \frac{1}{\|T_n(A)\|_2 \|((T_n(B))^{-1})^*\|_2 \|(T_n(W))^{-1}\|_2 \|(T_n(B))^{-1}\|_2 \|T_n(A)\|_2} = \\ &= \frac{1}{\|T_n(A)\|_2^2 \|(T_n(B))^{-1}\|_2^2 \|T_n(W^{-1})\|_2} = \\ &= \frac{1}{\|T_n(A)\|_2^2 \|(T_n(B))^{-1}\|_2^2 \|W^{-1}\|_2} = \\ &= \frac{\lambda_N(W)}{\|T_n(A)\|_2^2 \|(T_n(B))^{-1}\|_2^2} \geq \\ &\geq \frac{\lambda_N(W)}{\left(\sup_{m \in \mathbb{N}} \|T_m(A)\|_2\right)^2 \left(\sup_{m \in \mathbb{N}} \|(T_m(B))^{-1}\|_2\right)^2}, \quad \forall n \in \mathbb{N}. \end{aligned}$$

Следовательно,

$$\inf_{n \in \mathbb{N}} \lambda_{nN}(\mathbf{E}(x_{n:1}x_{n:1}^*)) \geq \frac{\lambda_N(W)}{\left(\sup_{n \in \mathbb{N}} \|T_n(A)\|_2\right)^2 \left(\sup_{n \in \mathbb{N}} \|(T_n(B))^{-1}\|_2\right)^2} > 0. \quad \blacktriangle$$

### § 3. Вычисление двух фундаментальных пределов теории информации для некоторых нестационарных векторных ARMA-источников

В работе [1] Шеннон ввел три фундаментальных предела (термин, предложенный Вайнером в [2]) теории информации: энтропия источника (для непрерывных источников названная в [3] скоростью создания дифференциальной энтропии), скорость как функция искажения и пропускная способность канала. Первые два относятся к сжатию данных, а третий – к передаче информации. Используя математические результаты, полученные в предыдущем параграфе, мы теперь вычислим два фундаментальных предела сжатия данных для некоторых определенных нестационарных векторных ARMA-источников.

**3.1. Скорость создания дифференциальной энтропии.** Формула для скорости создания дифференциальной энтропии вещественного стационарного гауссовского скалярного источника была получена Колмогоровым в [12, формула (16)]. Мы обобщим эту формулу на случай вещественных гауссовских векторных AWSS-источников.

*Теорема 3. Пусть  $\{x_n\}$  –  $N$ -мерный AWSS-процесс с СПМ  $X$ . Предположим, что  $\{x_n\}$  – вещественный гауссовский процесс с нулевым средним. Тогда если*

$$\inf_{n \in \mathbb{N}} \lambda_{nN}(\mathbf{E}(x_{n:1} x_{n:1}^\top)) > 0,$$

то

$$\lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) = \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln(\det(X(\omega))) d\omega,$$

где  $^\top$  обозначает транспонирование, а через  $h$  обозначена дифференциальная энтропия (в натуральных единицах).

*Доказательство.* Согласно [3, формула (8.44)] дифференциальная энтропия (в натуральных единицах) вещественного гауссовского векторного процесса  $x_{n:1}$  с нулевым средним имеет вид

$$h(x_{n:1}) = \frac{1}{2} \ln \left( (2\pi e)^{nN} \det(\mathbf{E}(x_{n:1} x_{n:1}^\top)) \right)$$

для всех  $n \in \mathbb{N}$ . Следовательно, применяя [7, теорема 6.6] и [13, предложение 2], имеем

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) &= \lim_{n \rightarrow \infty} \frac{1}{2n} \ln \left( (2\pi e)^{nN} \det(\mathbf{E}(x_{n:1} x_{n:1}^\top)) \right) = \\ &= \lim_{n \rightarrow \infty} \frac{1}{2n} \left( \ln(2\pi e)^{nN} + \ln(\det(\mathbf{E}(x_{n:1} x_{n:1}^\top))) \right) = \\ &= \lim_{n \rightarrow \infty} \left( \frac{N}{2} \ln(2\pi e) + \frac{1}{2n} \ln(\det(\mathbf{E}(x_{n:1} x_{n:1}^\top))) \right) = \\ &= \frac{N}{2} \ln(2\pi e) + \lim_{n \rightarrow \infty} \frac{1}{2n} \ln(\det(\mathbf{E}(x_{n:1} x_{n:1}^\top))) = \\ &= \frac{N}{2} \ln(2\pi e) + \lim_{n \rightarrow \infty} \frac{1}{2n} \ln \left( \prod_{k=1}^{nN} \lambda_k(\mathbf{E}(x_{n:1} x_{n:1}^\top)) \right) = \\ &= \frac{N}{2} \ln(2\pi e) + \frac{1}{2} \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^{nN} \ln(\lambda_k(\mathbf{E}(x_{n:1} x_{n:1}^\top))) = \end{aligned}$$

$$\begin{aligned}
&= \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \sum_{k=1}^N \ln(\lambda_k(X(\omega))) d\omega = \\
&= \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln(\det(X(\omega))) d\omega. \quad \blacktriangle
\end{aligned}$$

Теперь мы можем вычислить скорость создания дифференциальной энтропии для некоторых нестационарных векторных ARMA-источников.

*Следствие 1. Пусть  $\{x_n\}$  – процесс из определения 3. Предположим, что  $\{x_n\}$  – вещественный гауссовский процесс. Если  $\rho(\Psi_p(A)) < 1$  и  $\rho(\Psi_q(B)) < 1$ , то*

$$\lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) = \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln \left( \left| \frac{\det(B(\omega))}{\det(A(\omega))} \right|^2 \det(W) \right) d\omega.$$

Доказательство. Объединяя теоремы 1–3, получаем

$$\begin{aligned}
&\lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) = \\
&= \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln \left( \det((A(\omega))^{-1} B(\omega) W (B(\omega))^* ((A(\omega))^{-1})^*) \right) d\omega. \quad \blacktriangle
\end{aligned}$$

Заметим, что для векторных ARMA-источников условие

$$\inf_{n \in \mathbb{N}} \lambda_{nN}(\mathbf{E}(x_{n:1} x_{n:1}^\top)) > 0$$

теоремы 3 заменено на условие, которое можно проверить:  $\rho(\Psi_q(B)) < 1$ . Теперь докажем, что для векторного WSS-источника с непрерывной СПМ  $X$  трудно проверяемое на практике условие теоремы 3 можно заменить на следующее:

$$\det(X(\omega)) \neq 0 \quad \forall \omega \in \mathbb{R}.$$

*Следствие 2. Пусть  $\{x_n\}$  –  $N$ -мерный WSS-процесс с непрерывной СПМ  $X$ . Предположим, что  $\{x_n\}$  – вещественный гауссовский процесс с нулевым средним. Если  $\det(X(\omega)) \neq 0$  для всех  $\omega \in \mathbb{R}$ , то*

$$\lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) = \frac{N}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln(\det(X(\omega))) d\omega. \quad (4)$$

Доказательство. Из [13, предложение 3] имеем, что  $X(\omega)$  положительно полуопределена для всех  $\omega \in \mathbb{R}$ , и следовательно,

$$\lambda_N(X(\omega)) \geq 0, \quad \forall \omega \in \mathbb{R}.$$

Значит, так как

$$\det(X(\omega)) \neq 0, \quad \forall \omega \in \mathbb{R},$$

то

$$\lambda_N(X(\omega)) > 0, \quad \forall \omega \in \mathbb{R}.$$

Отсюда, используя [13, предложение 3], получаем

$$\inf_{n \in \mathbb{N}} \lambda_{nN}(\mathbf{E}(x_{n:1} x_{n:1}^\top)) = \inf_{n \in \mathbb{N}} \lambda_{nN}(T_n(X)) = \min_{\omega \in [0, 2\pi]} \lambda_N(X(\omega)) > 0.$$

Таким образом, применяя теорему 3, получаем равенство (4).  $\blacktriangle$

Выбирая  $N = 1$  в следствии 2, получаем формулу скорости создания дифференциальной энтропии (в натуральных единицах) для вещественного стационарного гауссовского скалярного источника с нулевым средним:

$$\lim_{n \rightarrow \infty} \frac{1}{n} h(x_{n:1}) = \frac{1}{2} \ln(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \ln(X(\omega)) d\omega. \quad (5)$$

Доказательство формулы (5) приведено также в [6, с. 161–162], но, к сожалению, там оно содержит две ошибки. Поделив равенство (5) на  $\ln 2$ , приходим к формуле для скорости создания дифференциальной энтропии (в битах), полученной Колмогоровым (см. [3, формула (12.40)]):

$$\lim_{n \rightarrow \infty} \frac{1}{n} h_2(x_{n:1}) = \frac{1}{2} \log_2(2\pi e) + \frac{1}{4\pi} \int_0^{2\pi} \log_2(X(\omega)) d\omega, \quad (6)$$

где через  $h_2$  обозначена дифференциальная энтропия в битах. Мы даем ссылку именно на книгу [3], поскольку оригинальная формула, приведенная Колмогоровым в [12, формула (16)], содержит ошибку. Отметим, что доказательство формулы (6) не содержится ни в [3], ни в [12].

**3.2. Скорость как функция искажения.** В [4, теорема 1] Томс и Бергер привели формулу скорости как функции искажения для некоторых нестационарных вещественных гауссовских векторных источников с авторегрессией, но доказательство этой формулы ими не приведено. Здесь мы обобщаем эту формулу на векторные ARMA-источники.

*Теорема 4. Пусть  $\{x_n\}$  – процесс из определения 3. Предположим, что  $\{x_n\}$  – вещественный гауссовский процесс. Пусть*

$$\rho(\Psi_p(A)) < 1$$

*и*

$$\det(B(\omega)) \neq 0 \quad \text{для всех } \omega \in \mathbb{R}.$$

*Пусть*

$$X(\omega) = (A(\omega))^{-1} B(\omega) W(B(\omega))^* ((A(\omega))^{-1})^*$$

*для всех  $\omega \in \mathbb{R}$ . Если  $D \in \left(0, \frac{\text{tr}(X_0)}{N}\right)$ , то*

$$R(D) = \frac{1}{4\pi N} \int_0^{2\pi} \sum_{k=1}^N \max \left\{ 0, \ln \frac{\lambda_k(X(\omega))}{\theta} \right\} d\omega, \quad (7)$$

*где  $\theta$  – вещественное число, такое что*

$$D = \frac{1}{2\pi N} \int_0^{2\pi} \sum_{k=1}^N \min \{ \theta, \lambda_k(X(\omega)) \} d\omega. \quad (8)$$

**Доказательство.** Применяя теорему 1, получаем, что  $\{x_n\}$  – AWSS-процесс с СПМ  $X$ . Так как матрица  $\mathbf{E}(x_{n:1}x_{n:1}^\top)$  положительно полуопределена для всех  $n \in \mathbb{N}$ , из [13, предложение 2] следует, что  $X(\omega)$  положительно полуопределена для всех  $\omega \in \mathbb{R}$ . Имеем

$$\det(X(\omega)) = \left| \frac{\det(B(\omega))}{\det(A(\omega))} \right|^2 \det(W) \neq 0, \quad \forall \omega \in \mathbb{R},$$

и из равенства (3) получаем

$$\det(\mathbf{E}(x_{n:1}x_{n:1}^\top)) = \left| \frac{\det(T_n(B))}{\det(T_n(A))} \right|^2 \det(T_n(W)) = (\det(W))^n \neq 0, \quad \forall n \in \mathbb{N}.$$

Так как  $\mathbf{E}(x_{n:1}x_{n:1}^\top)$  положительно определена для всех  $n \in \mathbb{N}$  и  $X(\omega)$  положительно определена для всех  $\omega \in \mathbb{R}$ , то из [14, теорема 1] следует равенство (7).  $\blacktriangle$

Поскольку

$$\left\{ \lambda_k((X(\omega))^{-1}) : k \in \{1, \dots, N\} \right\} = \left\{ \frac{1}{\lambda_k(X(\omega))} : k \in \{1, \dots, N\} \right\}, \quad \forall \omega \in \mathbb{R},$$

формулы (7) и (8) можно переписать в виде

$$R(D) = \frac{1}{4\pi N} \int_0^{2\pi} \sum_{k=1}^N \max\{0, -\ln(\theta \lambda_k((X(\omega))^{-1}))\} d\omega$$

и

$$D = \frac{1}{2\pi N} \int_0^{2\pi} \sum_{k=1}^N \min\left\{ \theta, \frac{1}{\lambda_k((X(\omega))^{-1})} \right\} d\omega$$

соответственно. Выбирая  $B(\omega) = I_N$ , получаем формулу скорости как функции искажения для векторных источников с авторегрессией, приведенную Томсом и Бергером в [4, формулы (8), (9)]:

$$R(D) = \frac{1}{4\pi N} \int_0^{2\pi} \sum_{k=1}^N \max\{0, -\ln(\theta \lambda_k((A(\omega))^* W^{-1} A(\omega)))\} d\omega$$

и

$$D = \frac{1}{2\pi N} \int_0^{2\pi} \sum_{k=1}^N \min\left\{ \theta, \frac{1}{\lambda_k((A(\omega))^* W^{-1} A(\omega))} \right\} d\omega.$$

Наконец, следует отметить, что условия, требуемые в следствии 1, являются более ограничительными, чем условия в теореме 4, поскольку при  $\rho(\Psi_q(B)) < 1$  из [10, теорема 6] следует, что  $\det(B(\omega)) \neq 0$  для всех  $\omega \in \mathbb{R}$ .

## ПРИЛОЖЕНИЕ А

Здесь мы покажем, почему без ограничения общности можно считать, что если  $\det(B_0) \neq 0$  в определении 2, то  $B_0 = I_N$ .

Доказательство. Так как  $\det(\mathbf{B}_0) \neq 0$ , то равенство (2) можно переписать в виде

$$\begin{aligned} x_n &= \sum_{k=0}^{n-1} \mathbf{B}_{-k} \mathbf{B}_0^{-1} \mathbf{B}_0 w_{n-k} - \sum_{\ell=1}^{n-1} \mathbf{A}_{-\ell} x_{n-\ell} = \\ &= \sum_{k=0}^{n-1} \widehat{\mathbf{B}}_{-k} \widehat{w}_{n-k} - \sum_{\ell=1}^{n-1} \mathbf{A}_{-\ell} x_{n-\ell}, \quad \forall n \in \mathbb{N}, \end{aligned}$$

где  $\widehat{\mathbf{B}}_0 = I_N$ ,  $\widehat{\mathbf{B}}_{-k} = \mathbf{B}_{-k} \mathbf{B}_0^{-1}$  и  $\widehat{w}_k = \mathbf{B}_0 w_k$  для всех  $k \in \mathbb{N}$ . Тогда

$$\mathbf{E}(\widehat{w}_k) = \mathbf{E}(\mathbf{B}_0 w_k) = \mathbf{B}_0 \mathbf{E}(w_k) = \mathbf{B}_0 0_{N \times 1} = 0_{N \times 1}, \quad \forall k \in \mathbb{N},$$

т.е.  $\{\widehat{w}_n\}$  является процессом с нулевым средним. Далее,

$$\begin{aligned} \mathbf{E}(\widehat{w}_j \widehat{w}_h) &= \mathbf{E}(\mathbf{B}_0 w_j (\mathbf{B}_0 w_h)^*) = \mathbf{E}(\mathbf{B}_0 w_j w_h^* \mathbf{B}_0^*) = \mathbf{B}_0 \mathbf{E}(w_j w_h^*) \mathbf{B}_0^* = \\ &= \mathbf{B}_0 (\delta_{j,h} W) \mathbf{B}_0^* = \delta_{j,h} \mathbf{B}_0 W \mathbf{B}_0^* \end{aligned}$$

для всех  $j, h \in \mathbb{N}$ . Для завершения доказательства остается лишь показать, что матрица  $\mathbf{B}_0 W \mathbf{B}_0^*$  положительно определена. Если  $u \in \mathbb{C}^{N \times 1} \setminus 0_{N \times 1}$ , то  $\mathbf{B}_0^* u \neq 0_{N \times 1}$ , поскольку

$$\det(\mathbf{B}_0^*) = \overline{\det(\mathbf{B}_0)} \neq 0.$$

Так как  $W$  положительно определена, то

$$u^* \mathbf{B}_0 W \mathbf{B}_0^* u = (\mathbf{B}_0^* u)^* W \mathbf{B}_0^* u > 0. \quad \blacktriangle$$

## ПРИЛОЖЕНИЕ В

Здесь мы докажем, что условие теоремы 1 равносильно условию, приведенному в [5, теорема 8], а именно  $\rho(\Psi_p(A)) < 1$  равносильно тому, что

$$\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0 \quad \text{и} \quad \inf_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)) > 0.$$

Доказательство. Разобьем доказательство на три шага.

Шаг 1: Докажем, что

$$\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0$$

тогда и только тогда, когда множество  $\{\|(T_n(A))^{-1}\|_2\}$  ограничено.

С одной стороны, если  $\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0$ , то

$$0 \leq \|(T_n(A))^{-1}\|_2 = \sigma_1((T_n(A))^{-1}) = \frac{1}{\sigma_{nN}(T_n(A))} \leq \frac{1}{\inf_{m \in \mathbb{N}} \sigma_{mN}(T_m(A))} < \infty$$

для всех  $n \in \mathbb{N}$ . С другой стороны, если  $\{\|(T_n(A))^{-1}\|_2\}$  ограничено, то

$$\sigma_{nN}(T_n(A)) = \frac{1}{\sigma_1((T_n(A))^{-1})} = \frac{1}{\|(T_n(A))^{-1}\|_2} \geq \frac{1}{\sup_{m \in \mathbb{N}} \|(T_m(A))^{-1}\|_2}$$

для всех  $n \in \mathbb{N}$ , и следовательно,

$$\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) \geq \frac{1}{\sup_{n \in \mathbb{N}} \|(T_n(A))^{-1}\|_2} > 0.$$

**Шаг 2:** Покажем, что если  $\det(A(\omega)) \neq 0$  для всех  $\omega \in \mathbb{R}$ , то выполнено условие

$$\inf_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)) > 0.$$

Так как матрица  $(A(\omega))^* A(\omega)$  эрмитова, то применяя [15, следствие VI.1.6], получаем, что

$$\inf_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)) = \min_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)).$$

Следовательно, для завершения доказательства этого шага осталось лишь доказать, что  $\lambda_N((A(\omega))^* A(\omega)) > 0$  для всех  $\omega \in \mathbb{R}$ . С одной стороны, так как  $(A(\omega))^* A(\omega)$  положительно полуопределена, то  $\lambda_N((A(\omega))^* A(\omega)) \geq 0$  для всех  $\omega \in \mathbb{R}$ . С другой стороны, так как

$$\det((A(\omega))^* A(\omega)) = |\det(A(\omega))|^2 \neq 0,$$

то  $\lambda_N((A(\omega))^* A(\omega)) \neq 0$  для всех  $\omega \in \mathbb{R}$ .

**Шаг 3:** Докажем, что  $\rho(\Psi_p(A)) < 1$  тогда и только тогда, когда выполнены условия

$$\inf_{n \in \mathbb{N}} \sigma_{nN}(T_n(A)) > 0 \quad \text{и} \quad \inf_{\omega \in [0, 2\pi]} \lambda_N((A(\omega))^* A(\omega)) > 0.$$

Это непосредственно вытекает из шагов 1, 2 и утверждения [10, теорема 6].  $\blacktriangle$

## СПИСОК ЛИТЕРАТУРЫ

1. Shannon C.E. A Mathematical Theory of Communication // Bell Syst. Tech. J. 1948. V. 27. № 3. P. 379–423. <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>
2. Wyner A. Fundamental Limits in Information Theory // Proc. IEEE. 1981. V. 69. № 2. P. 239–251. <https://doi.org/10.1109/PROC.1981.11956>
3. Cover T.M., Thomas J.A. Elements of Information Theory. Hoboken, NJ: Wiley, 2006.
4. Toms W., Berger T. Information Rates of Stochastically Driven Dynamic Systems // IEEE Trans. Inform. Theory. 1971. V. 17. № 1. P. 113–114. <https://doi.org/10.1109/TIT.1971.1054569>
5. Gutiérrez-Gutiérrez J., Crespo P.M. Asymptotically Equivalent Sequences of Matrices and Multivariate ARMA Processes // IEEE Trans. Inform. Theory. 2011. V. 57. № 8. P. 5444–5454. <https://doi.org/10.1109/TIT.2011.2159042>
6. Gray R.M. Toeplitz and Circulant Matrices: A Review // Found. Trends Commun. Inform. Theory. 2006. V. 2. № 3. P. 155–239. <https://doi.org/10.1561/0100000006>
7. Gutiérrez-Gutiérrez J., Crespo P.M. Block Toeplitz Matrices: Asymptotic Results and Applications // Found. Trends Commun. Inform. Theory. 2011. V. 8. № 3. P. 179–257. <https://doi.org/10.1561/0100000006>
8. Ephraim Y., Lev-Ari H., Gray R.M. Asymptotic Minimum Discrimination Information Measure for Asymptotically Weakly Stationary Processes // IEEE Trans. Inform. Theory. 1988. V. 34. № 5. P. 1033–1040. <https://doi.org/10.1109/18.21226>
9. Gersho A., Gray R.M. Vector Quantization and Signal Compression. New York: Springer, 2012.

10. *Gutiérrez-Gutiérrez J., Barasoain-Echepare Í., Zárraga-Rodríguez M., Insausti X.* Necessary and Sufficient Conditions for AR Vector Processes to Be Stationary: Applications in Information Theory and in Statistical Signal Processing // *Appl. Math. Comput.* 2023. V. 445, Article 127824 (14 pp.). <https://doi.org/10.1016/j.amc.2022.127824>
11. *Gutiérrez-Gutiérrez J., Zárraga-Rodríguez M., Insausti X.* On the Asymptotic Optimality of a Low-Complexity Coding Strategy for WSS, MA, and AR Vector Sources // *Entropy*. 2020. V. 22. № 12, Article 1378 (20 pp.). <https://doi.org/10.3390/e22121378>
12. *Kolmogorov A.* On the Shannon Theory of Information Transmission in the Case of Continuous Signals // *IRE Trans. Inform. Theory*. 1956. V. 2. № 4. P. 102–108. <https://doi.org/10.1109/TIT.1956.1056823>
13. *Gutiérrez-Gutiérrez J.* A Modified Version of the Pisarenko Method to Estimate the Power Spectral Density of Any Asymptotically Wide Sense Stationary Vector Process // *Appl. Math. Comput.* 2019. V. 362, Article 124526 (11 pp.). <https://doi.org/10.1016/j.amc.2019.06.040>
14. *Gutiérrez-Gutiérrez J., Zárraga-Rodríguez M., Crespo P.M., Insausti X.* Rate Distortion Function of Gaussian Asymptotically WSS Vector Processes // *Entropy*. 2018. V. 20. № 9, Article 719 (12 pp.). <https://doi.org/10.3390/e20090719>
15. *Bhatia R.* *Matrix Analysis*. New York: Springer, 1997.

*Гутьеррес-Гутьеррес Хесус* (Gutiérrez-Gutiérrez, Jesús)  
*Барасоайн-Эчепаре Иньиго*<sup>✉</sup> (Barasoain-Echepare, Íñigo)  
*Саррага-Родригес Марта* (Zárraga-Rodríguez, Marta)  
*Инсаусти Шавьер* (Insausti, Xabier)  
 Инженерная школа Теснун, Университет Наварры,  
 Сан-Себастьян, Испания  
<sup>✉</sup>[ibarasoaine@tecnun.es](mailto:ibarasoaine@tecnun.es)

Поступила в редакцию  
 30.11.2023  
 После доработки  
 26.03.2024  
 Принята к публикации  
 09.04.2024

УДК 621.391 : 519.725

© 2024 г. Л.А. Бассальго, В.А. Зиновьев, В.С. Лебедев

**КОНСТРУКЦИИ НЕДВОИЧНЫХ КОДОВ, ЛЕЖАЩИХ  
НА ГРАНИЦЕ ДЖОНСОНА**

Предложено несколько конструкций недвоичных равновесных кодов, лежащих на границе Джонсона.

*Ключевые слова:* недвоичный равновесный код, граница Джонсона, посимвольно равномерно код, эквидистантный код.

**DOI:** 10.31857/S0555292324010030, **EDN:** URTWNL

**§ 1. Введение**

Пусть  $C$  –  $q$ -ичный равновесный код над алфавитом  $\{0, 1, \dots, q - 1\}$  длины  $n$  мощности  $N$  ( $N = |C|$ ) с весом кодовых слов  $w$  и расстоянием  $d$ . Такой код назовем  $(n, N, w, d)_q$ -кодом. Мощность  $N$  такого  $(n, N, w, d)_q$ -кода удовлетворяет следующей обобщенной границе Джонсона [1]:

$$N \leq \frac{(q - 1)dn}{qw^2 - (q - 1)(2w - d)n}, \tag{1}$$

если знаменатель положителен.

Напомним (см. [2]), что равновесный код достигает границы (1) тогда и только тогда, когда он эквидистантен и посимвольно равномерен. Посимвольно равномерным называется код, матрица которого размера  $N \times n$  содержит каждый ненулевой символ в каждом столбце одно и то же число раз независимо от выбора символа и выбора столбца.

Всюду в дальнейшем будем считать, что каждый ненулевой символ в каждом столбце встречается  $t$  раз,  $t > 0$ , а следовательно, нулевой символ в каждом столбце встречается

$$m = N - (q - 1)t$$

раз,  $m > 0$ .

Отметим, что при  $m \neq t$  эквидистантный посимвольно равномерный код является равновесным, но при  $m = t$  это не так: например, код  $\{(00), (11), (22)\}$  является эквидистантным и посимвольно равномерным, но не равновесным.

Равновесный эквидистантный посимвольно равномерный код будем кратко называть РЭПР-кодом. Несложно вычислить (см., например, [2]), что параметры всякого  $(n, N, w, d)_q$ -РЭПР-кода при заданных  $q, t, m$  и  $n$  связаны следующими соотношениями:

$$N = (q - 1)t + m, \quad w = \frac{(N - m)n}{N}, \quad d = \frac{(N - m)(N + m - t)n}{N(N - 1)}. \tag{2}$$

Прежде чем перейти к изложению конструкции, отметим, что для любых заданных  $q$ ,  $t$  и  $m$  существует некоторый РЭПР-код, но, к сожалению, слишком большой длины.

**Предложение 1.** *При заданных  $q$ ,  $t$  и  $m$  существует РЭПР-код длины*

$$n = \frac{N!}{m!(t!)^{q-1}(q-1)!}.$$

**Доказательство.** Соответствующая матрица кода размера  $N \times n$  состоит из столбцов, каждый из которых содержит  $m$  нулей и по  $t$  раз каждый ненулевой символ. Выберем в столбце  $m$  позиций для нулевых символов (таких выборов всего  $\binom{N}{m}$ ), а оставшееся множество из

$$N - m = (q - 1)t$$

позиций разобьем на  $q - 1$  подмножеств мощности  $t$ . Число таких неупорядоченных разбиений равно

$$\frac{(N - m)!}{(t!)^{q-1}(q-1)!}.$$

В матрицу кодовых слов при фиксированном выборе  $m$  позиций для нулевого символа запишем все  $\frac{(N - m)!}{(t!)^{q-1}(q-1)!}$  столбцов неупорядоченных разбиений, и каждый такой столбец заполним ненулевыми кодовыми символами так, что на всех  $t$  позициях, соответствующих фиксированному элементу разбиения, стоит один и тот же ненулевой символ, а на позициях разных элементов разбиения эти символы различны. Число столбцов в такой матрице равно

$$\binom{N}{m} \frac{(N - m)!}{(t!)^{q-1}(q-1)!} = \frac{N!}{m!(t!)^{q-1}(q-1)!}.$$

Очевидно, что эта матрица задает равновесный эквидистантный посимвольно равномерный код. ▲

## § 2. Каскадная конструкция

Естественно желание использовать для построения РЭПР-кодов каскадную конструкцию. Пусть имеется  $(q_1, t_1, m_1, n_1)$ -РЭПР-код (далее будем называть его внешним кодом) и  $(q_2, t_2, m_2, n_2)$ -РЭПР-код (называемый далее внутренним кодом),

$$N_2 = (q_2 - 1)t_2 + m_2 = q_1 - 1.$$

Стандартная каскадная конструкция состоит в замене нулевого символа внешнего кода на нулевое слово длины  $n_2$ , а каждого фиксированного ненулевого символа внешнего кода – на фиксированное слово внутреннего кода. Очевидно, что полученный таким образом каскадный код будет посимвольно равномерным с параметрами

$$q_3 = q_2, \quad t_3 = t_1 t_2, \quad m_3 = m_1 + t_1 m_2, \quad n_3 = n_1 n_2 \quad (3)$$

и равновесным ( $w_3 = w_1 w_2$ ), однако такой код может быть не эквидистантным. Для того чтобы он был эквидистантным, необходимо и достаточно выполнение по крайней мере одного из двух следующих дополнительных условий:

а) на внешний код: число  $\xi(x, y)$  координат, в которых любые два слова  $x, y$  внешнего кода равны нулю, не зависит от выбора этих двух слов (положим это число равным  $\xi$ ,  $\xi = \frac{m_1(m_1 - 1)n_1}{N_1(N_1 - 1)}$ );

б) на внутренний код:  $w_2 = d_2$ , что эквивалентно равенству  $m_2 = t_2 - 1$ .

Эти условия вытекают из вычисления расстояния между двумя словами  $x, y$  каскадного кода:

$$\begin{aligned} d_3(x, y) &= (d_1 - 2(n_1 - w_1 - \xi(x, y)))d_2 + 2(n_1 - w_1 - \xi(x, y))w_2 = \\ &= d_1d_2 + 2(n_1 - w_1 - \xi(x, y))(w_2 - d_2). \end{aligned}$$

Внешние  $(q_1, t_1, m_1, n_1)$ -РЭПР-коды со свойством а) были введены в [3], где было доказано, что их существование эквивалентно существованию  $m_1$ -квазиразрешимых схем, и были построены семейства таких кодов. Отметим, что не всякий РЭПР-код удовлетворяет условию а). Таковым, к примеру, является РЭПР-код с параметрами

$$q = 4, \quad N = 9, \quad n = 18, \quad m = 3, \quad t = 2,$$

столбцы которого образованы циклическими сдвигами двух столбцов-генераторов

$$(0\ 3\ 2\ 1\ 0\ 1\ 2\ 3\ 0)^T \quad \text{и} \quad (2\ 1\ 1\ 0\ 0\ 3\ 0\ 2\ 3)^T.$$

Внутренние  $(q_2, t_2, m_2, n_2)$ -РЭПР-коды со свойством б) – это коды, лежащие на границе Плоткина, из которых удалено нулевое слово (мощность такого кода  $N_2 = \frac{(q_2 - 1)n_2}{q_2d_2 - (q_2 - 1)n_2}$ ).

Таким образом, если внутренний код удовлетворяет условию б), то при любом внешнем РЭПР-коде каскадный код является РЭПР-кодом с расстоянием  $d_3 = d_1d_2$ . Если внутренний код не удовлетворяет условию б), то внешний код должен удовлетворять условию а), и тогда

$$d_3 = d_1d_2 + 2(n_1 - w_1 - \xi)(w_2 - d_2).$$

Очевидно, что  $N_3 = N_1$ , а параметры  $d_3$  и  $w_3$  каскадного кода легко вычисляются исходя из (2) и (3).

Приведем теперь примеры каскадных конструкций.

**Пример 1.** Выберем в качестве внешнего кода  $(q_1, t_1 = 2, m_1 = 1, n_1 = 2q_1 - 1)$ -РЭПР-код, а в качестве внутреннего – РЭПР-код из предложения 2 работы [4] с параметрами

$$N_2 = p^2, \quad q_2 = (p^2 - p)/2 + 1, \quad t_2 = 2, \quad m_2 = p, \quad n_2 = p(p + 1)/2,$$

где  $p$  – степень простого числа. В результате получим РЭПР-код с параметрами

$$q_3 = (p^2 - p)/2 + 1, \quad t_3 = 4, \quad m_3 = 1 + 2p, \quad n_3 = (2p^2 + 1)p(p + 1)/2.$$

Такой внешний код существует при любых  $q_1$  (см. [5]) и удовлетворяет условию а), как и любой РЭПР-код при  $m = 1$ . Так как в каскадной конструкции  $N_2 = q_1 - 1$ , то в данном примере надо выбрать  $q_1 = p^2 + 1$ .

Согласно формуле перехода от параметров РЭПР-кода к привычным кодовым параметрам построенный каскадный РЭПР-код является кодом над алфавитом размера  $q_3 = (p^2 - p)/2 + 1$ , мощности  $N_3 = 2p^2 + 1$ , длины  $n_3 = (2p^2 + 1)p(p + 1)/2$ , с весом кодовых слов  $w_3 = p^2(p^2 - 1)$  и расстоянием  $d_3 = (p^2 - 1)(p^2 + p - 1)$ .

Например, выбрав  $p = 3$ , получим четверичный код мощности 19, длины 114, с весом кодовых слов 72 и расстоянием 88.

**Пример 2.** Выберем в качестве внешнего кода  $(q_1, t_1, m_1 = 1, n_1 = (q_1 - 1)t_1 + 1)$ -РЭПР-код, а в качестве внутреннего – РЭПР-код из предложения 1 с параметрами

$$\left( q_2 = q, t_2 = 1, m_2, n_2 = \begin{pmatrix} q_2 - 1 + m_2 \\ m_2 \end{pmatrix} \right).$$

Так как  $N_2 = (q_2 - 1) + m_2 = q_1 - 1$ , то в данном примере надо выбрать  $m_2 = q_1 - q$ . Получим РЭПР-код с параметрами

$$\left( q_3 = q, t_3 = t_1, m_3 = 1 + t_1(q_1 - q), n_3 = [(q_1 - 1)t_1 + 1] \binom{q_1 - 1}{q_1 - q} \right).$$

Тогда согласно формуле перехода от параметров РЭПР-кода к привычным кодовым параметрам построенный каскадный РЭПР-код является кодом над алфавитом размера  $q$ , мощности  $(q_1 - 1)t_1 + 1$ , длины

$$[(q_1 - 1)t_1 + 1] \binom{q_1 - 1}{q_1 - q},$$

с весом кодовых слов

$$(q - 1)t_1 \binom{q_1 - 1}{q - 1}$$

и расстоянием

$$[(2q_1 - q - 2)t_1 + 2] \binom{q_1 - 2}{q - 2}.$$

Использованный в этом примере внешний код приведен в [6], где показано, что он эквивалентен почти разрешимой блок-схеме.

Например, выбрав в качестве внешнего кода  $(6, 5, 1, 26)$ -РЭПР-код, а в качестве внутреннего  $(4, 1, 2, 10)$ -РЭПР-код из предложения 1, получим четверичный РЭПР-код мощности 26, длины 260, с весом 150 и расстоянием 192.

Прежде чем привести еще один пример каскадной конструкции, мы ее слегка модифицируем – допустим в качестве внешнего кода код, лежащий на границе Плоткина, т.е. используем эквидистантный посимвольно равномерный, но не равновесный код. Внутренний код остается прежним, но теперь каждому символу внешнего кода (включая нулевой) мы ставим в соответствие одно из слов внутреннего кода. Очевидно, что при такой модифицированной каскадной конструкции полученный код будет посимвольно равномерным с параметрами

$$q_3 = q_2, \quad t_3 = t_1 t_2, \quad m_3 = t_1 m_2, \quad n_3 = n_1 n_2, \quad (4)$$

так как  $m_1 = t_1$ , равновесным ( $w_3 = n_1 w_2$ ) и эквидистантным ( $d_3 = d_1 d_2$ ).

Так как  $N_1 = q_1 t_1$ ,  $N_2 = q_1$ , то

$$N_3 = (q_2 - 1)t_1 t_2 + t_1 m_2 = [(q_2 - 1)t_2 + m_2]t_1 = N_2 t_1 = q_1 t_1 = N_1.$$

Пример 3. Пусть внешний код лежит на границе Плоткина с параметрами  $(q_1, t_1, m_1 = t_1, n_1)$  (см. [5, 7]), а в качестве внутреннего выберем РЭПР-код из предложения 1 с параметрами

$$\left( q_2 = q, t_2 = 1, m_2, n_2 = \binom{q_2 - 1 + m_2}{m_2} \right).$$

Так как  $N_2 = q_2 - 1 + m_2 = q_1$ , то в данном примере надо выбрать  $m_2 = q_1 - q + 1$ . В результате получим РЭПР-код с параметрами

$$\left( q_3 = q, t_3 = t_1, m_3 = t_1(q_1 - q + 1), n_3 = n_1 \binom{q_1}{q - 1} \right).$$

Согласно формуле перехода от параметров РЭПР-кода к привычным кодовым параметрам построенный каскадный РЭПР-код является кодом над алфавитом раз-

мера  $q$ , мощности  $q_1 t_1$ , длины

$$n_1 \binom{q_1}{q-1},$$

с весом кодовых слов

$$n_1 \binom{q_1 - 1}{q-2}$$

и расстоянием

$$n_1 \binom{q_1 - 1}{q-2} \frac{(2q_1 - q)t_1}{q_1 t_1 - 1}.$$

Например, выбрав в качестве внешнего  $(7, 7, 7, 8)$ -РЭПР-код (см. [7]), а в качестве внутреннего  $(4, 1, 4, 35)$ -РЭПР-код из предложения 1, получим четверичный РЭПР-код мощности 49, длины 280, с весом 120 и расстоянием 175.

Теперь приведем две конструкции, использующие блок-схемы.

### § 3. Конструкция А

Блок-схема  $B(v, k, \lambda)$  называется *разрешимой* и обозначается через  $\text{RB}(v, k, \lambda)$ , если она перестановкой строк и столбцов может быть приведена к следующему виду:

$$A = [A_1 | A_2 | \dots | A_r],$$

где каждая подматрица  $A_j$  размера  $v \times \frac{v}{k}$  состоит из строк веса 1. Разрешимая блок-схема  $\text{RB}(v, k, \lambda)$  называется *аффинно разрешимой* и обозначается через  $\text{ARB}(v, k, \lambda)$ , если скалярное произведение любых двух столбцов из различных подматриц  $A_j, A_{j'}$ ,  $j \neq j'$ , равно  $\mu$ . Согласно теореме Боуза (см. [8, гл. II, теорема 8.7]) параметры аффинно разрешимой блок-схемы можно записать в следующем виде:

$$k = t\mu, \quad v = t^2\mu, \quad \lambda = \frac{t\mu - 1}{t - 1},$$

где  $t \geq 2$ . Отсюда мы видим, что  $\lambda = k(k-1)/(v-k)$ , и следовательно, аффинно разрешимая схема является частным случаем блок-схемы  $B(v, k, \lambda)$ , в котором

$$\lambda = \frac{k(k-1)}{v-k}.$$

Построение троичного кода из аффинно разрешимой схемы весьма просто – выбираем любые два столбца из любых двух различных подматриц схемы и превращаем эти два столбца в столбец троичного кода по следующему правилу:

$$(1, 1) \rightarrow 0, \quad (0, 0) \rightarrow 0, \quad (1, 0) \rightarrow 1, \quad (0, 1) \rightarrow 2.$$

Результат такого преобразования подытоживает следующее

**Утверждение 1.** *Любая аффинно разрешимая схема  $\text{ARB}(v, k, \lambda)$  порождает троичный равновесный эквидистантный код, лежащий на границе Джонсона (1), с параметрами*

$$q = 3, \quad N = v, \\ n = \left(\frac{v}{k}\right)^2 \binom{r}{2} = \frac{v^3(v-1)(k-1)}{2k(v-k)^2},$$

$$w = 2 \binom{\frac{v}{k} - 1}{2} \binom{r}{2} = \frac{v(v-1)(k-1)}{v-k},$$

$$\begin{aligned} d &= \lambda(r-\lambda) \left( 2 + 2 \binom{\frac{v}{k} - 1}{2} \right) + \binom{r-\lambda}{2} \left( 2 \binom{\frac{v}{k} - 1}{2} + 2 \binom{\frac{v}{k} - 2}{2} \right) = \\ &= \frac{(k-1)(2v^2 - 3vk + 3k^2)}{v-k}. \end{aligned}$$

**Доказательство.** Здесь пояснения требуют лишь левые равенства, ибо правые равенства следуют из того факта, что для аффинно разрешимой схемы

$$\lambda = \frac{k(k-1)}{v-k}, \quad r = \frac{k(v-1)}{v-k} \quad \text{и} \quad r - \lambda = k.$$

Вычисление веса  $w$  кодового слова очевидно, так как имеется всего  $r$  подматриц, и вклад любых двух подматриц в вес фиксированного слова равен  $2 \binom{\frac{v}{k} - 1}{2}$ , ибо каждая строка любой подматрицы содержит ровно одну единицу, а длина каждой строки подматрицы равна  $v/k$ .

Рассмотрим теперь две фиксированные строки матрицы  $\text{ARB}(v, k, \lambda)$  и вычислим вклад каждой пары подматриц в расстояние трюичного кода между соответствующими кодовыми словами. Имеется ровно  $\lambda$  подматриц, в которых фиксированные две строки подматриц одинаковы, и  $r - \lambda$  подматриц, в которых они различны. Пары подматриц первого типа не вносят вклада в расстояние. Рассмотрим теперь две фиксированные строки подматрицы первого типа и подматрицы второго типа: их вклад в расстояние равен

$$2 + 2 \binom{\frac{v}{k} - 1}{2}.$$

Осталось заметить, что вклад в расстояние двух подматриц второго типа равен

$$2 \binom{\frac{v}{k} - 1}{2} + 2 \binom{\frac{v}{k} - 2}{2}. \quad \blacktriangle$$

#### § 4. Конструкция В

Еще одно семейство недвоичных эквидистантных равновесных кодов, лежащих на границе Джонсона, строится с использованием идеи одновременного построения блок-схем для всех символов. Используя метод построения блок-схемы из [9], удастся разбить кодовую матрицу размера  $N \times n$  на  $q$  блок-схем (т.е. для каждого символа  $i$  замена этого символа на единицу, а всех остальных символов на ноль приводит к блок-схеме).

Пусть  $v = p^s$ , где  $p$  – нечетное простое,  $s = 1, 2, \dots$ , и  $k < v$ . Опишем построение блок-схемы из работы [9]: выбираются  $k$  различных элементов  $A = \{\alpha_1, \dots, \alpha_k\}$  поля  $\mathbb{F}_v$  и образуются  $(v-1)/2$  блоков-генераторов

$$B_j = \beta_j \times A = (\beta_j \alpha_1, \beta_j \alpha_2, \dots, \beta_j \alpha_k), \quad j = 1, 2, \dots, (v-1)/2$$

(здесь  $\beta_j$  – различные ненулевые элементы поля, такие что  $\beta_j \neq -\beta_j$ , т.е. из каждой пары  $\beta_j, -\beta_j$  выбирается один элемент и всего выбрано  $(v-1)/2$  таких элементов поля). Затем из каждого блока-генератора  $B_j$ ,  $j = 1, 2, \dots, (v-1)/2$ , порождаются  $v$  блоков

$$\beta + B_j = (\beta + \beta_j \alpha_1, \beta + \beta_j \alpha_2, \dots, \beta + \beta_j \alpha_k)$$

для всех  $\beta \in \mathbb{F}_v$  (здесь знак  $+$  обозначает сложение вектора с элементом). Таким образом, каждый блок-генератор порождает  $v$  блоков, и всего получаем  $v(v-1)/2$

блоков, каждый из которых содержит  $k$  элементов поля. Теорема из [9] утверждает, что полученные таким образом  $v(v-1)/2$  блоков представляют собой  $B(v, k, \lambda)$ -схему с параметром

$$\lambda = \frac{k(k-1)}{2}$$

(соответственно,  $b = v(v-1)/2$ ,  $r = k(v-1)/2$ ). Построение  $q$ -ичного кода из такой  $B(v, k, \lambda)$ -схемы совсем просто.

**Утверждение 2.** Пусть  $v = p^s$ , где  $p$  – нечетное простое, и пусть натуральные числа  $s, k'$  таковы, что  $(q-1)k' < v$ . Тогда в явном виде строится  $q$ -ичный равновесный эквидистантный код, лежащий на границе Джонсона (1), с параметрами

$$\begin{aligned} N &= v, \\ n &= \frac{v(v-1)}{2}, \\ w &= \frac{(q-1)k'(v-1)}{2}, \\ d &= (q-1)k' \left( v - \frac{qk'}{2} \right). \end{aligned}$$

**Доказательство.** Покажем, что этот код порождается блок-схемой

$$B(v, (q-1)k', \lambda = (q-1)k'[(q-1)k' - 1]/2),$$

описанной в работе [9]. Положим  $k = (q-1)k'$  и разобьем множество элементов  $A = \{\alpha_1, \dots, \alpha_k\}$  на  $q-1$  подмножеств  $A_1, A_2, \dots, A_{q-1}$  мощности  $k'$ . В каждом блоке, который по построению имеет вид  $\beta + \beta_j \times A$ , все элементы поля  $\mathbb{F}_v$  вида  $\beta + \beta_j \times A_i$  заменим на символ  $q$ -ичного кода  $i$ ,  $i = 1, 2, \dots, q-1$ . Очевидно, что такой  $q$ -ичный код имеет параметры

$$N = v, \quad n = v(v-1)/2, \quad w = k(v-1)/2.$$

Он эквидистантен, ибо у любых двух кодовых слов число покоординатно совпадающих ненулевых символов равно  $k'(k'-1)/2$  для любого ненулевого символа, а число покоординатно совпадающих нулевых символов равно

$$v(v-1)/2 - 2r + \lambda,$$

где

$$r = (q-1)k'(v-1)/2, \quad \lambda = (q-1)k'[(q-1)k' - 1]/2,$$

и следовательно, расстояние эквидистантного кода равно

$$\begin{aligned} d &= -(q-1)k'(k'-1)/2 + (q-1)k'(v-1) - (q-1)k'[(q-1)k' - 1]/2 = \\ &= (q-1)k'(v - qk'/2). \end{aligned}$$

Так как код равносимвольный и эквидистантный, то он лежит на границе Джонсона, что, впрочем, нетрудно проверить и непосредственно.  $\blacktriangle$

## § 5. Примеры

Приведем теперь примеры применения конструкций А и В.

Пример 4 (конструкция А). Схема Адамара с параметрами

$$v = 4\ell, \quad k = 2\ell, \quad \lambda = 2\ell - 1, \quad \mu = \ell$$

является аффинно разрешимой схемой.

Так как  $k = 2\mu = v/2$  и  $k - \mu = v - \mu - 2(k - \mu) = \ell$ , то получаем троичные коды с параметрами

$$q = 3, \quad n = 4(4\ell - 1)(2\ell - 1), \quad N = 4\ell, \\ w = 2(4\ell - 1)(2\ell - 1), \quad d = 10\ell(2\ell - 1).$$

Очевидно, что таким же способом, как построен троичный код, можно построить четверичный код, превращая пару  $(1, 1)$  в символ 3. Но требование, чтобы полученный четверичный код лежал на границе Джонсона, не порождает новый код, а приводит к коду, который является четырехкратным повторением четверичного кода, построенного в [10].

Пример 5 (конструкция В). Выбрав  $v = 19$ ,  $q = 4$ ,  $k' = 4$ , получим четверичный код мощности 19, длины 171, с весом кодовых слов 108 и расстоянием 132. Параметры  $t = 4$ ,  $m = 7$  этого кода совпадают с параметрами четверичного кода в примере 1, но длина кода в примере 1 равна 114. Минимальная длина РЭПР-кода при  $q = 4$ ,  $t = 4$ ,  $m = 7$  ограничена снизу величиной 57 (см. [4, предложение 4]).

Если взять  $q = 3$ ,  $t = 7$ ,  $m = 5$ , то длина кода из конструкции В равна 171, но уже не может быть уменьшена, поскольку из (2) имеем

$$d = (7 \times 17)n / (19 \times 9),$$

а расстояние кода является целым числом.

Отметим, что связь разрешимых блок-схем с оптимальными недвоичными равновесными кодами также исследуется в работе [11], где авторы используют транспонированную (в отличие от данной статьи) матрицу инцидентности блок-схем для построения кодовой матрицы.

Авторы весьма благодарны рецензенту, привлечшему их внимание к каскадной конструкции.

## СПИСОК ЛИТЕРАТУРЫ

1. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. <http://www.mathnet.ru/ppi762>
2. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Симметричные блок-схемы и оптимальные эквидистантные коды // Пробл. передачи информ. 2020. Т. 56. № 3. С. 50–58. <https://doi.org/10.31857/S055529232003002X>
3. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Об  $m$ -квазиразрешимых блок-схемах и  $q$ -ичных равновесных кодах // Пробл. передачи информ. 2018. Т. 54. № 3. С. 54–61. <http://www.mathnet.ru/ppi2272>
4. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Слабо разрешимые блок-схемы и недвоичные коды, лежащие на границе Джонсона // Пробл. передачи информ. 2022. Т. 58. № 1. С. 3–15. <https://doi.org/10.31857/S0555292322010016>
5. *Семаков Н.В., Зиновьев В.А.* Эквидистантные  $q$ -ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы // Пробл. передачи информ. 1968. Т. 4. № 2. С. 3–10. <http://www.mathnet.ru/ppi1845>
6. *Бассалыго Л.А., Зиновьев В.А.* Замечание об уравновешенных неполных блок-схемах, почти разрешимых блок-схемах и  $q$ -ичных равновесных кодах // Пробл. передачи информ. 2017. Т. 53. № 1. С. 56–59. <https://www.mathnet.ru/ppi2227>

7. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87. <https://www.mathnet.ru/ppi1804>
8. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge: Cambridge Univ. Press, 1999.
9. *Ramanujacharyulu C.* A New General Series of Balanced Incomplete Block Designs // Proc. Amer. Math. Soc. 1966. V. 17. № 5. P. 1064–1068. <https://doi.org/10.2307/2036090>
10. *Sinha K., Sinha N.* A Class of Optimal Quaternary Codes // Ars Combin. 2010. V. 94. P. 61–64.
11. *Shi M., Xia Y., Krotov D.S.* A Family of Diameter Perfect Constant-Weight Codes from Steiner Systems // J. Combin. Theory Ser. A. 2003. V. 200. Paper No. 105790 (20 pp.). <https://doi.org/10.1016/j.jcta.2023.105790>

*Бассалыго Леонид Александрович*  
*Зиновьев Виктор Александрович*  
*Лебедев Владимир Сергеевич*  
Институт проблем передачи информации  
им. А.А. Харкевича РАН, Москва  
[bass@iitp.ru](mailto:bass@iitp.ru)  
[vazinov@iitp.ru](mailto:vazinov@iitp.ru)  
[lebedev37@mail.ru](mailto:lebedev37@mail.ru)

Поступила в редакцию  
21.09.2023  
После доработки  
18.03.2024  
Принята к публикации  
19.03.2024

УДК 621.391 : 519.725

© 2024 г. И.В. Воробьев<sup>1</sup>, А.В. Лебедев, В.С. Лебедев**ИСПРАВЛЕНИЕ ОДНОЙ ОШИБКИ  
В АСИММЕТРИЧНОМ КАНАЛЕ С ОБРАТНОЙ СВЯЗЬЮ**

Доказывается новая нижняя оценка мощности кода с полной обратной связью, исправляющего одну ошибку в двоичном асимметричном канале. Также представлена верхняя граница мощности кода, близкая к новой нижней границе.

*Ключевые слова:* асимметричный канал, обратная связь, кодовая конструкция.

**DOI:** 10.31857/S0555292324010042, **EDN:** EUSSZN

**§ 1. Введение**

В данной статье изучается двоичный асимметричный канал с мгновенной бесшумной обратной связью. Нами рассматривается комбинаторная модель асимметричного канала, в котором при передаче кодового слова длины  $n$  происходит не более одной ошибки.

В рассматриваемом нами асимметричном канале, также известном как  $Z$ -канал, при передаче символа 1 может произойти ошибка и на выходе канала будет получен символ 0, при этом символ 0 всегда передается безошибочно. Наличие полной обратной связи означает, что после передачи каждого символа кодер получает информацию о том, какой символ был принят декодером. Изучению двоичного асимметричного канала посвящено значительное количество работ. В работе [1] были предложены коды Варшамова – Тененгольца, позволяющие исправлять одну ошибку в асимметричном канале без обратной связи. В работах [2, 3] Варшамов показал, что для исправления  $t$  ошибок без обратной связи необходимо и достаточно, чтобы кодовые слова находились друг от друга на асимметричном расстоянии не менее  $2t + 1$ , где асимметричное расстояние между словами  $\mathbf{x}, \mathbf{y}$  определяется как

$$p(\mathbf{x}, \mathbf{y}) = |\mathbf{x} - \mathbf{y}| + ||\mathbf{x}| - |\mathbf{y}||$$

(где  $|\mathbf{x}|$  – число единиц в слове  $\mathbf{x}$ , часто называемое весом слова). Бассальго в работе [4] вывел из этого, что мощность кода  $M$  для длины сообщения  $n$  в асимметричном канале не может превышать мощность кода в симметричном канале более чем в  $t + 1$  раз. Таким образом, асимптотическая скорость кода без обратной связи ( $R = \lim_{n \rightarrow \infty} \frac{\log M}{n}$ ), исправляющего  $t$  ошибок в асимметричном канале, ровно такая же, как и скорость кода, исправляющего  $t$  ошибок в симметричном канале. При наличии обратной связи и линейном числе ошибок асимптотическая скорость для симметричного и асимметричного каналов уже будет различаться [5, 6].

<sup>1</sup> Работа выполнена при частичной финансовой поддержке Российского научного фонда (номер проекта 22-41-02028).

При фиксированном числе ошибок  $t$  максимальное число передаваемых сообщений  $M$  с полной обратной связью асимптотически эквивалентно  $2^{n+t} t! n^{-t}$ . Это утверждение было доказано для  $t = 1$  в [7] и для произвольного  $t$  в [8,9]. Позднее было показано, что такого же асимптотического результата можно добиться, используя обратную связь лишь один раз. Это было доказано для двоичного симметричного канала в [10] и для произвольного дискретного канала в [11].

Для оптимальной мощности кода любой длины, исправляющего одну ошибку в двоичном симметричном канале при наличии полной обратной связи, известен точный ответ [12]. Более того, в [13] показано, что можно построить код такой же мощности, использующий обратную связь только два раза. В случае же асимметричного канала точный ответ для одной ошибки до сих пор не получен. Известны только асимптотические результаты и таблицы оптимальных кодов для небольших длин (см. [7,13]).

В работе [7] доказано, что для передачи с полной обратной связью  $M = 2^\ell$  сообщений достаточно длины кода

$$n = \ell - 1 + \lceil \log(\ell + 3) \rceil.$$

Выражая число сообщений через длину, получаем, что возможна передача

$$M = \frac{2^{n+1}}{n - \log n(1 + o(1))} = \frac{2^{n+1}}{n} \left( 1 + \frac{\log n}{n} + o\left(\frac{\log n}{n}\right) \right) \quad (1)$$

сообщений.

В работе [14] нами был построен рекурсивный алгоритм, позволяющий получать оптимальные коды с полной обратной связью, исправляющие одну ошибку. Также была предложена модификация этого рекурсивного алгоритма, позволяющая относительно легко получать оценки мощностей кодов большой длины. В данной статье мы применяем упомянутый алгоритм для получения новой нижней оценки мощности кода, превосходящей результат (1). Также мы доказываем верхнюю границу мощности кода, близкую к новой нижней границе.

## § 2. Определения и обозначения

Рассмотрим канал с двоичным алфавитом  $\{0, 1\}$  на входе и на выходе. Кодер передает сообщение  $\mathbf{x} \in \{0, 1\}^n$ , декодер получает сообщение  $\mathbf{y} \in \{0, 1\}^n$ . Ошибкой будем называть замену символа 1 из последовательности  $\mathbf{x}$  на символ 0 (а нулевой символ всегда передается безошибочно). Символом  $[M]$  будем обозначать множество  $\{1, 2, \dots, M\}$ .

В данной статье рассматривается передача данных по каналу с полной обратной связью. Кодер передает сообщение  $m \in [M]$ . Первый передаваемый символ  $x_1$  зависит только от сообщения  $m$ . После передачи каждого символа  $x_i$  кодер получает обратную связь о принятом символе  $y_i$ . Перед отправкой следующего символа кодер учитывает в своей стратегии информацию о полученных символах. Таким образом, второй передаваемый символ  $x_2$  зависит не только от сообщения  $m$ , но и от принятого символа  $y_1$ , и так далее.

Определим облако  $V(m)$  для сообщения  $m$  как множество последовательностей  $\mathbf{y}$ , которые могут быть получены на выходе канала с не более чем одной ошибкой при передаче этого сообщения. Каждое облако  $V(m)$  содержит последовательность, которая будет передана в том случае, если в канале не происходит ошибок. Назовем эту последовательность корневой. Отметим, что размер облака всегда превосходит вес корневой последовательности на 1.

Будем называть набор непересекающихся облаков  $V(m)$ ,  $m \in [M]$ , кодом  $\mathcal{C}$  мощности  $M$ , исправляющим одну ошибку. Точки пространства, не принадлежащие ни

одному облаку, будем называть свободными; количество таких точек будет обозначаться через  $F$ .

### § 3. Основной результат

Всюду далее под кодом будем понимать код с полной обратной связью, исправляющий одну ошибку в асимметричном канале.

При доказательстве основного результата мы будем опираться на следующее утверждение, доказанное в [14].

**Предложение 1.** *Если существует код длины  $n$  и мощности  $M$ , имеющий  $F$  свободных точек,  $F \geq M$ , то тогда существует код длины  $n + 1$  и мощности  $2M$ , имеющий  $2F - M$  свободных точек.*

Последовательное применение предложения 1 дает следующий результат.

**Предложение 2.** *Пусть существует код длины  $k$  и мощности  $M_0$ , имеющий  $F$  свободных точек. Тогда для любого  $N \leq 2F/M_0 - 1$  существует код длины  $n = k + N$  и мощности  $M = M_0 \cdot 2^N$ .*

В зависимости от того, какой начальный код длины  $k$  используется в предложении 2, будут получаться коды с разными параметрами. В теореме 2 работы [14] показано, что применяя предложение 2 к тривиальному коду, состоящему из одного нулевого слова, мы повторяем результат (1).

В следующей теореме мы улучшаем этот результат, применяя предложение 2 к более сложному коду.

**Теорема 1.** *Существует код длины  $n$  и мощности*

$$M = \frac{2^{n+1}}{n - \alpha\sqrt{n}(1 + o(1))} = \frac{2^{n+1}}{n} \left( 1 + \frac{\alpha}{\sqrt{n}} + o\left(\frac{1}{\sqrt{n}}\right) \right) \quad \text{при } n \rightarrow \infty,$$

где  $\alpha > 0,4499$ .

**Доказательство.** Построим код длины  $k$  и мощности

$$M_0 = \sum_{w=0}^s \binom{k - \lceil \log k \rceil}{w}$$

с одной обратной связью, исправляющий одну ошибку. Код строится следующим образом. Каждому сообщению поставим в соответствие двоичную последовательность длины  $r = k - \lceil \log k \rceil$ , имеющую вес не более  $s$ . При передаче сообщения на первых  $r$  символах передается соответствующая двоичная последовательность, последующие  $\lceil \log k \rceil$  символов используются для исправления возможной ошибки. В случае, если ошибки не было, передается нулевое слово, в противном случае передается номер позиции, в которой произошла ошибка. Так как возможных позиций строго меньше чем  $k$ , то нам хватает длины кода для передачи нужной информации.

Пусть  $s = \lfloor r/2 - C\sqrt{r} \rfloor$ , где  $C$  – некая константа, которая будет оптимизирована в дальнейшем. Подсчитаем количество свободных точек в коде. Каждому сообщению соответствует корневое слово веса  $w \leq s$ , состоящее из последовательности веса  $w$  на первых  $r = k - \lceil \log k \rceil$  символах, дополненной последовательностью из  $\lceil \log k \rceil$  нулей. Поэтому соответствующее облако состоит из  $w + 1$  точек. Таким образом, количество свободных точек вычисляется по формуле

$$F = 2^k - \sum_{w=0}^s \binom{r}{w} (w + 1).$$

Преобразуем выражение для мощности кода:

$$M_0 = \sum_{w=0}^s \binom{r}{w} = 1 + \sum_{w=1}^s \left( \binom{r-1}{w} + \binom{r-1}{w-1} \right) = \quad (2)$$

$$= \sum_{w=1}^{s+1} \binom{r-1}{w-1} + \sum_{w=1}^s \binom{r-1}{w-1} = 2 \sum_{w=1}^s \binom{r-1}{w-1} + \binom{r-1}{s}. \quad (3)$$

Теперь преобразуем выражение для количества свободных точек:

$$\begin{aligned} F &= 2^k - \sum_{w=0}^s \binom{r}{w} (w+1) = 2^k - \sum_{w=0}^s \binom{r}{w} w - \sum_{w=0}^s \binom{r}{w} = \\ &= 2^k - r \sum_{w=1}^s \binom{r-1}{w-1} - M_0 = \\ &= 2^k - M_0 - r \left( M_0 - \binom{r-1}{s} \right) \cdot \frac{1}{2} = \\ &= 2^k - M_0 - rM_0/2 + \frac{r}{2} \binom{r-1}{s} = \\ &= 2^k - M_0 - rM_0/2 + \frac{r-s}{2} \binom{r}{s}. \end{aligned} \quad (4)$$

Применяя  $N$  раз предложение 2, где

$$N = 2F/M_0 - 1, \quad (5)$$

получаем новый код. Длина нового кода  $n = k + N$ , а его мощность

$$M = M_0 \cdot 2^N = M_0 \frac{2^{n+1}}{2^{k+1}}. \quad (6)$$

Дальнейшие вычисления направлены на установление зависимости мощности  $M$  кода от его длины  $n$ .

Воспользуемся следующей асимптотической формулой для  $M_0$ :

$$M_0 = \sum_{w=0}^s \binom{r}{w} = 2^r (\Phi(-2C) + o(1)) \quad \text{при } r \rightarrow \infty, \quad (7)$$

где

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{x^2}{2}} dx$$

– функция распределения стандартного нормального распределения  $\mathcal{N}(0, 1)$ . Эта формула легко выводится из центральной предельной теоремы, примененной к биномиальной случайной величине  $\xi$  с параметрами  $r$  и  $1/2$ .

Действительно, если поделить  $M_0$  на  $2^r$ , то мы получим вероятность того, что биномиальная случайная величина  $\xi$  с параметрами  $r$  и  $1/2$  принимает значение не более  $s$ . Из центральной предельной теоремы следует, что

$$\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \xrightarrow{d} \mathcal{N}(0, 1).$$

Имеем

$$M_0 = 2^r \mathbf{P}(\xi \leq s) = 2^r \mathbf{P}\left(\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \leq \frac{s - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}}\right). \quad (8)$$

Заметим, что

$$\mathbf{E}\xi = \frac{r}{2}, \quad \mathbf{D}\xi = \frac{r}{4}, \quad s = \lfloor r/2 - C\sqrt{r} \rfloor,$$

и поэтому

$$M_0 = 2^r \mathbf{P}\left(\frac{\xi - \mathbf{E}\xi}{\sqrt{\mathbf{D}\xi}} \leq \frac{-2C\sqrt{r}}{\sqrt{r}}(1 + o(1))\right) = 2^r(\Phi(-2C) + o(1)). \quad (9)$$

Для биномиального коэффициента воспользуемся известной формулой, которую можно найти, например, в [15]:

$$\binom{r}{s} = 2^r \frac{e^{-2C^2}}{\sqrt{\pi r/2}}(1 + o(1)). \quad (10)$$

Подставляя в формулу (5) выражения (7), (10) и (4), получаем следующее:

$$N = 2^{k+1}/M_0 - 3 - r + \frac{r-s}{\sqrt{r}} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{\pi/2}}(1 + o(1)) = \quad (11)$$

$$= 2^{k+1}/M_0 - k + \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)). \quad (12)$$

Отсюда

$$\frac{2^{k+1}}{M_0} = N + k - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)), \quad (13)$$

а значит, с учетом формулы (6) верно следующее равенство:

$$M = \frac{2^{n+1}}{n - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1))}. \quad (14)$$

Подставим в формулу (13) выражение (9) для  $M_0$ :

$$\frac{2^{k+1}}{2^r \Phi(-2C)}(1 + o(1)) = n - \sqrt{k} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1)), \quad (15)$$

т.е.

$$\frac{2k}{\Phi(-2C)}(1 + o(1)) = n,$$

$$k = \frac{n\Phi(-2C)}{2}(1 + o(1)).$$

Подставляя это выражение в формулу (14) для  $M$ , получаем

$$M = \frac{2^{n+1}}{n - \sqrt{n} \frac{\sqrt{\Phi(-2C)}}{\sqrt{2}} \frac{e^{-2C^2}}{\Phi(-2C)\sqrt{2\pi}}(1 + o(1))} = \frac{2^{n+1}}{n - \alpha\sqrt{n}(1 + o(1))},$$

где

$$\alpha = \frac{e^{-2C^2}}{2\sqrt{\Phi(-2C)\pi}}.$$

Максимальное значение  $\alpha$  достигается при  $C \approx 0,306$  и превышает 0,4499. ▲

#### § 4. Верхняя граница

Докажем верхнюю границу мощности кода.

Теорема 2. *Мощность кода длины  $n$  не превосходит*

$$\frac{2^{n+1}}{n - 2\sqrt{n \ln n}(1 + o(1))} = \frac{2^{n+1}}{n} \left( 1 + \frac{2\sqrt{\ln n}}{\sqrt{n}} + o\left(\frac{\sqrt{\ln n}}{\sqrt{n}}\right) \right).$$

Доказательство. Пусть передается  $M$  сообщений, каждому из которых соответствует корневое сообщение веса  $w_i$ ,  $1 \leq i \leq M$ . Размер облака с корневым сообщением веса  $w$  равен  $w + 1$ , поэтому

$$\sum_{i=1}^M (w_i + 1) \leq 2^n.$$

Рассмотрим отдельно слова веса меньше  $T = \frac{n}{2} - \sqrt{n \ln n}$  и слова веса не менее  $T$ . Пусть в первой группе  $M_0$  слов, а во второй –  $M_1$ . Количество слов  $M_0$  в первой группе можно оценить с помощью неравенства Хёфдинга [16], примененного к случайной величине  $\xi$ , имеющей распределение  $\text{Bin}(n, 1/2)$ :

$$\mathbf{P}(\xi \leq T) \leq e^{-2 \ln n} = n^{-2}.$$

Отсюда следует, что  $M_0 \leq 2^n \cdot n^{-2}$ .

Для оценки  $M_1$  заметим, что  $M_1(T + 1) \leq 2^n$ , а значит,

$$M_1 \leq \frac{2^{n+1}}{n - 2\sqrt{n \ln n}}.$$

Таким образом, общее количество сообщений не превосходит

$$M \leq \frac{2^{n+1}}{n - 2\sqrt{n \ln n}(1 + o(1))}. \quad \blacktriangle$$

Таким образом, мы видим, что нижняя и верхняя границы достаточно близки, а именно второй член известен с точностью до умножения на  $O(\sqrt{\ln n})$ . Однако в отличие от симметричного канала точную формулу для мощности кода получить не удается.

#### СПИСОК ЛИТЕРАТУРЫ

1. Варшамов Р.Р., Тененгольц Г.М. Код, исправляющий одиночные несимметрические ошибки // *АиТ*. 1965. Т. 26. № 2. С. 288–292. <http://www.mathnet.ru/at11293>
2. Варшамов Р.Р. К теории несимметрических кодов // *Докл. АН СССР*. 1965. Т. 164. № 4. С. 757–760. <http://www.mathnet.ru/dan31642>
3. Варшамов Р.Р. О некоторых особенностях линейных кодов, корректирующих несимметрические ошибки // *Докл. АН СССР*. 1964. Т. 157. № 3. С. 546–548. <https://www.mathnet.ru/dan29877>

4. *Бассальго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. <http://www.mathnet.ru/ppi762>
5. *Deppe C., Lebedev V., Maringer G., Polyanskii N.* Coding with Noiseless Feedback over the Z-Channel // IEEE Trans. Inform. Theory. 2022. V. 68. № 6. P. 3731–3739. <https://doi.org/10.1109/TIT.2022.3148446>
6. *Lebedev A., Lebedev V., Polyanskii N.* Two-Stage Coding over the Z-Channel // IEEE Trans. Inform. Theory. 2022. V. 68. № 4. P. 2290–2299. <https://doi.org/10.1109/TIT.2022.3141082>
7. *Cicalese F., Mundici D.* Optimal Coding with One Asymmetric Error: Below the Sphere Packing Bound // Computing and Combinatorics (Proc. 6th Annu. Int. Conf. COCOON 2000. Sydney, Australia. July 26–28, 2000). Lect. Notes Comput. Sci. V. 1858. Berlin: Springer, 2000. P. 159–169. [https://doi.org/10.1007/3-540-44968-X\\_16](https://doi.org/10.1007/3-540-44968-X_16)
8. *Dumitriu I., Spencer J.* A Halfliar’s Game // Theoret. Comput. Sci. 2004. V. 313. № 3. P. 353–369. <https://doi.org/10.1016/j.tcs.2002.09.001>
9. *Spencer J., Yan C.H.* The Halfie Problem // J. Combin. Theory Ser. A. 2003. V. 103. № 1. P. 69–89. [https://doi.org/10.1016/S0097-3165\(03\)00068-2](https://doi.org/10.1016/S0097-3165(03)00068-2)
10. *Бассальго Л.А.* Недвоичные коды, исправляющие ошибки при наличии одноразовой безошибочной обратной связи // Пробл. передачи информ. 2005. Т. 41. № 2. С. 63–67. <http://www.mathnet.ru/ppi96>
11. *Dumitriu I., Spencer J.* The Two-Batch Liar Game over an Arbitrary Channel // SIAM J. Discrete Math. 2005. V. 19. № 4. P. 1056–1064. <https://doi.org/10.1137/040617510>
12. *Pelc A.* Solution of Ulam’s Problem on Searching with a Lie // J. Combin. Theory Ser. A. 1987. V. 44. № 1. P. 129–140. [https://doi.org/10.1016/0097-3165\(87\)90065-3](https://doi.org/10.1016/0097-3165(87)90065-3)
13. *Воробьев И.В., Денне К., Лебедев А.В., Лебедев В.С.* Исправление одной ошибки в каналах с обратной связью // Пробл. передачи информ. 2022. Т. 58. № 4. С. 38–49. <https://doi.org/10.31857/S0555292322040040>
14. *Vorobyev I., Lebedev A., Lebedev V.* Correcting Errors in Asymmetric and Generalized Asymmetric Channels with Feedback // Proc. XVIII Int. Symp. “Problems of Redundancy in Information and Control Systems” (REDUNDANCY’2023). Moscow, Russia. Oct. 24–27, 2023. P. 163–167. <https://doi.org/10.1109/Redundancy59964.2023.10330199>
15. *Spencer J., Florescu L.* Asymptopia. Providence, RI: Amer. Math. Soc., 2014.
16. *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.

*Воробьев Илья Викторович*  
 Технический университет Мюнхена, Германия  
 vorobyev.i.v@yandex.ru  
*Лебедев Алексей Владимирович*  
*Лебедев Владимир Сергеевич*  
 Институт проблем передачи информации  
 им. А.А. Харкевича РАН, Москва  
 al\_lebed95@mail.ru  
 lebedev37@mail.ru

Поступила в редакцию  
 28.12.2023  
 После доработки  
 03.04.2024  
 Принята к публикации  
 03.04.2024

УДК 621.391 : 530.145 : 515.162.8

© 2024 г. А.А. Морозов

ОБ ИЗМЕРЕНИИ ТОПОЛОГИЧЕСКОГО ЗАРЯДА ЭНИОНОВ<sup>1</sup>

Обсуждается принцип измерения топологического заряда или представления, в котором находится набор энионов. Описывается метод измерения и исследуется, как он работает для различных значений параметров теории. Также предлагается способ, с помощью которого этот метод можно сделать более эффективным.

*Ключевые слова:* топологический квантовый компьютер, теория узлов, квантовые измерения.

**DOI:** 10.31857/S0555292324010054, **EDN:** JDBCMW

## § 1. Введение

Топологический квантовый компьютер – это перспективная модель квантового компьютера, которая, как ожидается, будет иметь малую вероятность ошибок по построению [1–3]. Модели такого квантового компьютера основаны на перемещении квазичастиц, называемых энионами. Эти частицы могут существовать в некоторых эффективных двумерных теориях и имеют статистику, отличную от фермионов и бозонов. А именно, перемена их местами порождает нетривиальный и в общем случае неабелев оператор.

Энионы описываются эффективной теорией Черна – Саймонса

$$S_{CS} = \frac{k}{4\pi} \int_{S^3} A \wedge dA + \frac{2}{3} A \wedge A \wedge A. \quad (1)$$

Эта теория калибровочно-инвариантна, при этом обычно рассматривается калибровочная группа  $SU(N)$ . Энионы в такой теории могут преобразовываться в разных представлениях, которые также называют топологическим зарядом.

Квантовые вычисления в модели топологического квантового компьютера осуществляются посредством перемещения энионов, нетривиальные операции при этом получаются посредством сплетения их траекторий (см. рис. 1). Базовый алгоритм устроен следующим образом. Во-первых, пара или несколько пар энионов рождаются, затем их траектории сплетаются, и наконец, мы пытаемся аннигилировать пары энионов, и в зависимости от конечного состояния системы они могут аннигилировать или не аннигилировать. Если энионы аннигилировали, то их траектории образуют узел или зацепление, а амплитуда вероятности такого процесса равна полиному соответствующего узла [4–6]. Сплетение траекторий соответствует квантовой  $\mathcal{R}$ -матрице, которая определяет элементарную операцию в топологическом квантовом компьютере.

<sup>1</sup> Исследование выполнено при поддержке гранта Российского научного фонда № 23-71-10058.

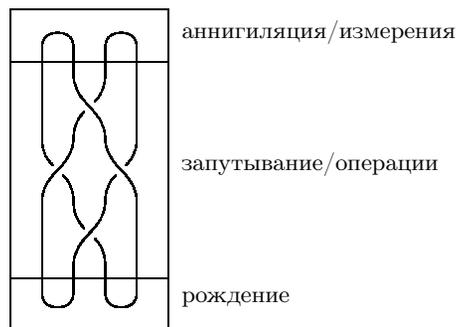


Рис. 1. Базовый квантовый алгоритм для топологического квантового компьютера. Пары энионов рождаются, сплетаются и аннигилируют. Двухмостовое зацепление, изображенное на рисунке, соответствует одно-кубитным операциям

Простейшее описание кубита [5–7] состоит из двух пар энионов, чьи траектории составляют двухмостовой узел. С точки зрения теории представлений вся коса, включающая в себя четыре эниона, находится в тривиальном представлении калибровочной группы, так как квантовые  $\mathcal{R}$ -матрицы не меняют неприводимое представление, в котором находится вся коса любой ширины (подробнее см. в [8–10]). Однако в произведении представлений, связанных с энионами в косе, может быть несколько тривиальных представлений. Если все энионы находятся в фундаментальном представлении группы  $SU(N)$  (энионы, летящие во встречном направлении, при этом соответствуют антифундаментальному представлению), пространство тривиальных представлений окажется двумерным. Эти тривиальные представления соответствуют различным представлениям, в которых находятся отдельные пары энионов, а не вся коса.

Существуют также другие подходы к построению топологического квантового компьютера. В работе [11] вместо группы кос, рассматриваемой в данной статье, изучается подход, связанный с алгеброй Темперли – Либа. Эта алгебра тесно связана с группой  $SU(2)$  и дает альтернативный подход к вычислению полиномов Джонса. Эти отличия, однако, несущественны в контексте задачи, рассматриваемой в данной статье.

В рамках разработки инструментария для обращения с энионами важна задача измерения состояния кубита без его разрушения. В топологическом квантовом компьютере мы можем измерить неприводимое представление, в котором находится коса, состоящая из траекторий энионов. Такое представление также называется топологическим зарядом энионов. Эта процедура в дальнейшем может быть использована для построения многокубитных операций в топологическом квантовом компьютере [7].

В данной статье обсуждается метод измерения неприводимого представления, известного также как топологический заряд эниона, и исследуется, как можно сделать это измерение более точным.

## § 2. Метод измерения

Способ измерения представления, в котором находится какая-либо коса, состоит в оплетении дополнительной нити вокруг измеряемой косы. Другими словами, мы создаем дополнительную пару вспомогательных энионов и сплетаем один из них с исследуемой косой, затем мы измеряем вероятность аннигиляции этой вспомо-

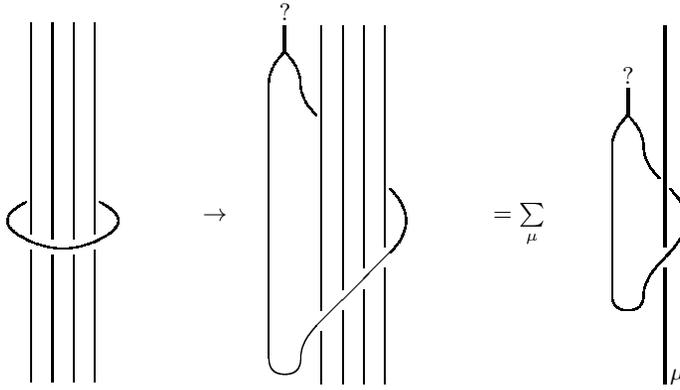


Рис. 2. Процедура измерения с помощью пары вспомогательных энионов. В зависимости от вероятности их аннигиляции мы можем найти представление  $\mu$ , в котором находится коса

гательной пары энионов (см. рис. 2). В зависимости от представления, в котором находится измеряемая коса, эта вероятность будет различной.

Согласно работе [9] вместо косы мы можем рассмотреть одну нить, но в старшем неприводимом представлении. Более того, представление, в котором находится коса, остается неизменным. В данной статье мы рассмотрим случай  $N = 2$  и косы, состоящей из двух энионов в фундаментальном представлении. В этом случае коса может быть в тривиальном или же в симметрическом представлении:

$$[1] \otimes [1] = \emptyset + [2], \quad \mu \in \{\emptyset, [2]\}. \quad (2)$$

Теперь, используя подходы, рассмотренные в [9, 12, 13], опишем операторы, которые возникают в таких косах.

### § 3. $\mathcal{R}$ -матрицы

Мы рассмотрим трехнитевые косы, как показано на рис. 3. Такие косы состоят из двух нитей в фундаментальном представлении (эти нити соответствуют вспомогательным энионам) и одной нити в неизвестном представлении, которое мы хотим измерить (оно может быть тривиальным или же симметрическим). Случай тривиального представления очень простой. Тривиальное представление взаимодействует тривиально со всеми другими представлениями. Это означает, что состояние первой пары нитей остается неизменным, и соответственно, вероятность успешной их аннигиляции равна 1.

Теперь обсудим случай симметрического представления. Так как изначально мы создали пару энионов в тривиальном представлении, а также есть дополнительная нить, которая несет на себе симметрическое представление [2], вся коса также находится в представлении [2]. Тем не менее в такой косе пространство таких представлений двумерно. Это можно увидеть из следующего разложения:

$$[1] \otimes [1] \otimes [2] = ([2] + \emptyset) \otimes [2] = ([4] + [2] + \emptyset) + [2]. \quad (3)$$

Одно из симметрических представлений появляется, когда первая пара нитей находится в тривиальном представлении, а другое – в симметрическом представлении. Вся коса в этом секторе описывается матрицей  $B$  размера  $2 \times 2$ , которая описывает, как пара симметрических представлений в начале преобразуется в пару представлений в конце. Так как мы знаем, что состояние в начале отвечает тривиальному

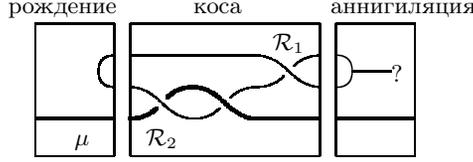


Рис. 3. Коса, которую нужно рассмотреть для описания взаимодействия между жирной нитью, которая соответствует изучаемому представлению  $\mu$ , и вспомогательными энионами. Коса состоит из  $\mathcal{R}$ -матриц различных типов – матрица  $\mathcal{R}_1$  соответствует пересечению между первыми двумя нитями, а матрица  $\mathcal{R}_2$  – пересечению между второй парой нитей

представлению по построению, элемент  $B[1, 1]$  описывает амплитуду вероятности аннигиляции, а  $B[1, 2]$  – не аннигиляции вспомогательной пары энионов.

Для построения матрицы  $B$  нужно описать  $\mathcal{R}$ -матрицы, возникающие в такой косе. Они описываются с использованием переменной  $q$ , которая строится из уровня  $k$  теории Черна – Саймонса и квантовых чисел  $[n]_q$ , которые являются функциями  $q$ :

$$q = e^{\frac{2\pi i}{k+2}}, \quad [n]_q = \frac{q^n - q^{-n}}{q - q^{-1}}. \quad (4)$$

Также важно отметить, что физическая теория Черна – Саймонса соответствует целым значениям  $k$ . Более того, как обсуждалось в работе [6],  $k \geq 6$ . С помощью методов, описанных в [9, 12, 13], можно построить матрицу  $\mathcal{R}_2^2$ , возникающую в косе, представленной на рис. 3:

$$\mathcal{R}_2^2 = \begin{pmatrix} \frac{q^2[6]_q}{[2]_q[3]_q} & \sqrt{\frac{[4]_q q^4 - q^{-2}}{[2]_q [3]_q}} \\ \sqrt{\frac{[4]_q q^4 - q^{-2}}{[2]_q [3]_q}} & \frac{[6]_q}{[2]_q[3]_q} \end{pmatrix}. \quad (5)$$

Это означает, что амплитуда вероятности получения тривиального или симметрического представления в произведении двух нитей в конце процесса, и соответственно, амплитуда вероятности энионов аннигиляции или не аннигиляции равна

$$\begin{aligned} A_\emptyset &= \frac{q^2[6]_q}{[2]_q[3]_q}, \\ A_2 &= \sqrt{\frac{[4]_q q^4 - q^{-2}}{[2]_q [3]_q}}. \end{aligned} \quad (6)$$

Если подставить в эти выражения  $q = e^{i\varphi}$ , они превратятся в

$$\begin{aligned} A_\emptyset &= \frac{\sin 6\varphi \sin \varphi}{\sin 2\varphi \sin 3\varphi} e^{2i\varphi}, \\ A_2 &= \sqrt{2 \cos 2\varphi} 2e^{i\varphi} \sin \varphi = \sqrt{4 \cos 2\varphi (1 - \cos 2\varphi)} e^{i\varphi}. \end{aligned} \quad (7)$$

На рис. 4 приведены графики вероятности того, что пара энионов находится в том или ином представлении.

При  $k = 10$ ,  $\varphi = 2\pi/(k + 2) = \pi/6$  вероятность того, что вспомогательная пара энионов не аннигилирует, равна 1, если измеряемая коса находится в симметрическом представлении. Это оптимальное значение параметров теории для измерения

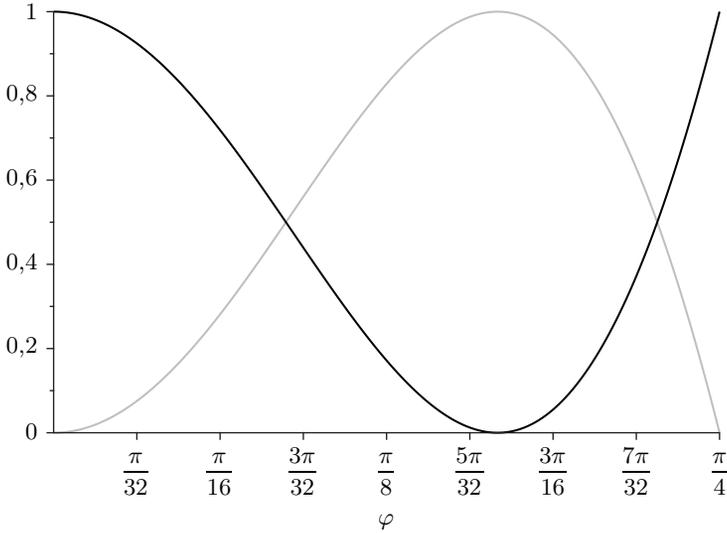


Рис. 4. Вероятности того, что пара вспомогательных энионов находится в симметрическом или тривиальном представлении в зависимости от значения  $\varphi$ . Черная кривая описывает вероятность измерения тривиального представления, серая кривая – симметрического представления

представления или топологического заряда. В этой точке вспомогательные энионы аннигилируют, только если измеряемое представление тривиально, и не аннигилируют, если это представление симметрическое. Для других значений параметров представление по-прежнему можно измерить, потому что измеряемое представление не изменяется при измерении, и соответственно, мы можем сделать столько измерений, сколько нам нужно, но для  $k = 10$  эта процедура оказывается самой простой.

#### § 4. Измерение с помощью нескольких сплетений

Мы можем модифицировать алгоритм измерения так, чтобы он лучше работал для других значений параметра  $k$ . Для этого вместо одного сплетения вспомогательного эниона с изучаемой косой можно оплести его несколько раз, и только потом попытаться аннигилировать его со вторым вспомогательным энионом, как показано на рис. 5. Если представление  $\mu$ , в котором находится измеряемая нить, тривиально, то взаимодействие между этой нитью и измеряющим энионом по-прежнему отсутствует. Это означает, что для любого числа сплетений вероятность аннигиляции в конце петли равна 1.

Если измеряемое представление – симметрическое, то  $2b$  сплетений описываются степенью  $b$  матрицы (5). Матричный элемент, соответствующий не аннигиляции, равен

$$A_2 = \sqrt{\frac{[4]_q}{[2]_q} q^b (q^{3b} - q^{-3b})} { [3]_q } } . \quad (8)$$

Если подставить значение  $q = e^{i\varphi}$  в эту формулу, получим следующее:

$$A_2 = \sqrt{8 \cos 2\varphi} \frac{e^{ib\varphi} \sin \varphi \sin 3b\varphi}{\sin 3\varphi} \quad (9)$$

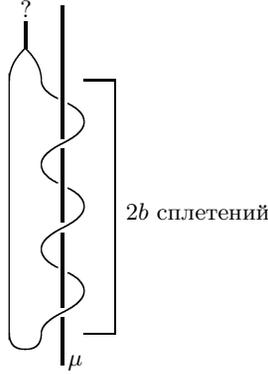


Рис. 5. Модифицированная процедура измерения с несколькими сплетениями одного из вспомогательных энионов с измеряемой косой. На рисунке изображен случай с  $2b = 6$  сплетениями

Вероятность не аннигиляции максимальна как функция  $b$  при

$$3b\varphi = \frac{\pi}{2} + \pi n. \quad (10)$$

Так как мы хотим, чтобы и  $b$ , и  $k$  были целыми, существует две серии значений  $k$ , удовлетворяющих этому соотношению:

$$\begin{cases} \frac{6b\pi}{k+2} = \frac{\pi}{2} \implies k = 12b - 2, \\ \frac{6b\pi}{k+2} = \frac{3\pi}{2} \implies k = 4b - 2. \end{cases} \quad (11)$$

Все остальные серии, возникающие из формулы (10), являются подмножеством этих двух серий. Более того, первая из этих серий также является подмножеством второй. По этой причине мы будем рассматривать только вторую серию решений  $k = 4b - 2$ . Теперь найдем вероятность не аннигиляции вспомогательных энионов для этой серии. После подстановки значений  $k$  и  $\varphi = \pi/2b$  в (9) получим

$$\begin{aligned} P_2 &= |A_2|^2 = 8 \cos \pi/b \left( \frac{\sin \pi/2b \sin 3\pi/2}{\sin 3\pi/2b} \right)^2 = \\ &= 8 \cos \pi/b \frac{1}{(\cos \pi/b + 2 \cos^2(\pi/2b))^2} = 8 \cos \pi/b \frac{1}{(2 \cos \pi/b + 1)^2}. \end{aligned} \quad (12)$$

Существует два значения  $b$ , для которых эта вероятность равна нулю, а именно  $b = 1$  и  $2$ ; также для  $b = 3, k = 10$  эта вероятность равна 1. После этого производная вероятности отрицательна, а значит, эта вероятность монотонно убывает. Но предел вероятности при  $b \rightarrow \infty$  равен  $8/9 \approx 0,89$ . Таким образом, при  $k = 4b - 2, b \geq 3$  вероятность того, что вспомогательные энионы не будут аннигилировать, выше чем  $8/9 \approx 0,89$ . Это означает, что мы можем отличить тривиальное представление от симметрического в измеряемой косе с вероятностью почти 90%. Эту вероятность также можно увеличить с помощью дополнительных измерений.

## § 5. Заключение

В данной статье мы обсудили возможность измерения топологического заряда нескольких энионов, которые лежат вместе. Основная идея состоит в том, что из-за топологических свойств энионов топологический заряд, связанный с квантовыми состояниями топологического квантового компьютера, может быть измерен, не изменяя само состояние. Мы показали, что наилучшая теория для таких измерений – это  $SU(2)$ -теория Черна – Саймонса уровня  $k = 10$ . Мы также предложили модификацию алгоритма измерения, которая упрощает измерение топологического заряда для теорий с уровнем  $k = 4b - 2$ .

Также возможно рассмотреть и более сложные конфигурации для измерения. Вспомогательные энионы могут быть запутаны с измеряемой косою, в том числе с включением пересечений траекторий вспомогательных энионов, что потенциально может сделать процедуру измерения еще более эффективной. Также возможно использовать вспомогательные энионы в старших представлениях. Возможно, рассмотрение таких энионов потребует, если мы хотим различать больше представлений в измеряемой косою и делать это эффективно с помощью малого числа измерений. Наконец, интересно обобщить этот подход на случай группы  $SU(N)$ . Как нам кажется, это можно сделать напрямую с использованием методов, описанных в [9, 12–15].

Алгоритм измерения может быть применен к квантовым алгоритмам, особенно при рассмотрении квантовых компьютеров, основанных на измерениях или при желании ввести непрямые измерения в квантовые алгоритмы.

Автор благодарен С. Миронову и А. Пополитову за плодотворные обсуждения.

## СПИСОК ЛИТЕРАТУРЫ

1. *Кутаев А.Ю.* Квантовые вычисления: алгоритмы и исправление ошибок // УМН. 1997. Т. 52. № 6 (318). С. 53–112. <https://doi.org/10.4213/rm892>
2. *Nayak C., Simon S.H., Stern A., Freedman M., Das Sarma S.* Non-Abelian Anyons and Topological Quantum Computation // Rev. Mod. Phys. 2008. V. 80. № 3. P. 1083–1159. <https://doi.org/10.1103/RevModPhys.80.1083>
3. *Rowell E.C.* Braids, Motions and Topological Quantum Computing. <https://arxiv.org/abs/2208.11762> [quant-ph], 2022.
4. *Melnikov D., Mironov A., Mironov S., Morozov A., Morozov An.* Towards Topological Quantum Computer // Nucl. Phys. B. 2018. V. 926. P. 491–508. <https://doi.org/10.1016/j.nuclphysb.2017.11.016>
5. *Kolganov N., Morozov An.* Quantum  $\mathcal{R}$ -Matrices as Universal Qubit Gates // Письма в ЖЭТФ. 2020. Т. 111. № 9. С. 623–624. <https://doi.org/10.31857/S1234567820090086>
6. *Kolganov N., Mironov S., Morozov An.* Large  $k$  Topological Quantum Computer // Nucl. Phys. B. 2023. V. 987. P. 116072 (17 pp.). <https://doi.org/10.1016/j.nuclphysb.2023.116072>
7. *Levaillant C., Bauer B., Freedman M., Wang Z., Bonderson P.* Universal Gates via Fusion and Measurement Operations on  $SU(2)_4$  Anyons // Phys. Rev. A. 2015. V. 92. № 1. P. 012301 (17 pp.). <https://doi.org/10.1103/PhysRevA.92.012301>
8. *Mironov A., Morozov A., Morozov An.* Character Expansion for HOMFLY Polynomials. II. Fundamental Representation. Up to Five Strands in Braid // J. High Energ. Phys. 2012. V. 2012. № 3. Article No. 34. [https://doi.org/10.1007/JHEP03\(2012\)034](https://doi.org/10.1007/JHEP03(2012)034)
9. *Анохина А.С., Морозов А.А.* Процедура каблирования для раскрашенных полиномов ХОМФЛИ // ТМФ. 2014. Т. 178. № 1. С. 3–68. <https://doi.org/10.4213/tmf8588>
10. *Anokhina A., Mironov A., Morozov A., Morozov An.* Colored HOMFLY Polynomials as Multiple Sums over Paths or Standard Young Tableaux // Adv. High Energy Phys. 2013. V. 2013. Article ID 931830 (12 pp.). <https://doi.org/10.1155/2013/931830>

11. *Aharonov D., Jones V., Landau Z.* A Polynomial Quantum Algorithm for Approximating the Jones Polynomial // Proc. 38th Annu. ACM Symp. on Theory of Computing (STOC'06). Seattle, WA, USA. May 21–23, 2006. New York, NY, USA: ACM, 2006. P. 427–436. <https://doi.org/10.1145/1132516.1132579>
12. *Dhara S., Mironov A., Morozov A., Morozov An., Ramadevi P., Singh V.K., Sleptsov A.* Multi-colored Links from 3-Strand Braids Carrying Arbitrary Symmetric Representations // Ann. Henri Poincaré. 2019. V. 20. № 12. P. 4033–4054. <https://doi.org/10.1007/s00023-019-00841-z>
13. *Bai C., Jiang J., Liang J., Mironov A., Morozov A., Morozov An., Sleptsov A.* Quantum Racah Matrices up to Level 3 and Multicolored Link up to Invariants // J. Geom. Phys. 2018. V. 132. P. 155–180. <https://doi.org/10.1016/j.geomphys.2018.05.020>
14. *Mironov A., Morozov A., Morozov An., Ramadevi P., Singh V.K., Sleptsov A.* Tabulating Knot Polynomials for Arborescent Knots // J. Phys. A: Math. Theor. 2017. V. 50. № 8. P. 085201 (22 pp.). <https://doi.org/10.1088/1751-8121/aa5574>
15. *Mironov A., Morozov A., Morozov An., Ramadevi P., Singh V.K.* Colored HOMFLY Polynomials of Knots Presented as Double Fat Diagrams // J. High Energ. Phys. 2015. V. 2015. № 7. Article No. 109 (68 pp.). [https://doi.org/10.1007/JHEP07\(2015\)109](https://doi.org/10.1007/JHEP07(2015)109)

*Морозов Андрей Алексеевич*  
 НИЦ “Курчатовский институт”, Москва  
 Институт проблем передачи информации  
 им. А.А. Харкевича РАН, Москва  
[andrey.morozov@itep.ru](mailto:andrey.morozov@itep.ru)

Поступила в редакцию  
 26.03.2024  
 После доработки  
 13.05.2024  
 Принята к публикации  
 17.05.2024

УДК 621.391 : 517.938 : 330.4

© 2024 г. М.Л. Бланк, М.О. Поляков

**ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ЗАДАЧИ СПРАВЕДЛИВОГО ДЕЛЕНИЯ**

Предлагается новый и сравнительно элементарный подход для решения задачи справедливого деления непрерывного ресурса (измеримого пространства, пирога и т.п.) между несколькими участниками, критерии выбора которых описываются зарядами (мерами со знаком). Постановка задачи с зарядами рассматривается впервые. Задача сводится к анализу свойств траекторий специально построенной динамической системы, действующей на пространстве конечных измеримых разбиений. Доказана экспоненциально быстрая сходимости к предельному решению как для случая мер, так и для случая зарядов.

*Ключевые слова:* справедливое деление, математическая экономика, многокритериальная оптимизация, счетно-аддитивные меры/заряды, динамические системы.

**DOI:** 10.31857/S0555292324010066, **EDN:** KJGZYI

**§ 1. Введение**

Проблемы, связанные с “оптимальным” делением ресурсов при заданной системе ограничений, являются одними из самых базовых задач математической экономики. Принципиальная их сложность определяется большим количеством (как правило) конфликтующих критериев “оптимальности” деления. Простейшим примером здесь является вопрос о делении сильно неоднородного пирога (клада, квартиры и т.п.) между несколькими участниками, оценки которых получаемых ими частей могут принципиально отличаться между собой.

Таким образом, задача справедливого деления относится к классу задач многокритериальной оптимизации, однако эта задача имеет несколько важных особенностей. Главная из них состоит в том, что вместо поиска “оптимального” (в том или ином смысле) решения (которое может и не существовать) предлагается поиск допустимого решения. Последняя постановка в большинстве случаев оказывается значительно проще. В некотором смысле этот подход является далеким обобщением поиска базовой точки (одной из вершин симплекса) в классической задаче линейного программирования.

Задача справедливого деления в простейшем случае формулируется следующим образом. Пусть нам нужно поделить пирог на  $r$  человек так, чтобы каждый считал, что его не обделили. При этом пирог сильно неоднороден, а у каждого из участников имеются собственные критерии сравнения различных кусков пирога. Например, кому-то больше нравится кусок с клубникой, а кто-то замечает, что левая сторона пирога слегка подгорела, и т.п. Возникает вопрос, всегда ли можно это сделать? Несмотря на кажущуюся “школьность”, эта задача оказывается очень сложной, и в различных постановках ей посвящено огромное количество публикаций (обзоры известных результатов можно найти, например, в [1–4]).

Первые строгие математические результаты для случая, когда критерии участников определяются неатомарными счетно-аддитивными мерами, были получены в 1961 г. Дубинсом и Спаньером [5], которые, опираясь на результаты Ляпунова [6] и Халмоша [7] о свойстве выпуклости для векторных мер, доказали, что для любого набора критериев участников дележа (представляемых неатомарными мерами) пирог можно разрезать “честно”. В 1980 году У. Стромквист [8] доказал, что это можно сделать ровно за  $r - 1$  разрезов. Однако это доказательство (как, впрочем, и результат [5]) не конструктивно, и явный алгоритм подобного деления известен только при  $r < 4$ . Существенно позже, в 1999 году, Ф.Е. Су [9] разработал принципиально другой комбинаторно-топологический подход для решения этой задачи, основанный на итерационном экспоненциально быстро сходящемся алгоритме.

Поскольку нас будет интересовать подход к задаче справедливого деления с точки зрения абстрактной теории меры, то мы не рассматриваем многочисленные важные и интересные геометрические аспекты этой задачи, такие как представление ресурса как подмножества евклидова пространства, возможности разбиения гиперплоскостями или ограничение разбиений только на связные множества. Читатель может найти ссылки на соответствующие результаты в указанных выше обзорах.

До недавнего времени считалось, что конечного алгоритма решения задачи справедливого деления (при некоторых “естественных” технических предположениях<sup>1</sup>) не существует (см., например, [10]). Однако в 2016 году Х. Азиз и С. Маккензи [11] предложили конечный алгоритм. Этот алгоритм технически весьма сложен, а оценка  $r^{r^{r^{r^{r^r}}}}$  необходимого для конструкции решения числа шагов астрономически велика даже при небольшом числе участников.

В реальной жизни критерии участников, естественно, могут оказаться гораздо более сложными и не сводящимися к классическим мерам. Полного исследования функционалов, допускающих решение задачи справедливого деления, на сегодняшний день нет. Единственное продвижение здесь относится к ситуации, когда выбираются не “лучшие”, а худшие части. Формально в терминах мер это означает, что соответствующий критерий равен некоторой мере со знаком минус. Версия конечного алгоритма Азиза – Маккензи для этого случая предложена в [12]. Как ни странно, комбинация этих вариантов – ситуация, когда критерии описываются зарядами (мерами со знаком), – в математической литературе не исследована<sup>2</sup>. Возможное объяснение состоит в том, что авторам не удалось согласовать в одном алгоритме противоречия, возникающие в подходах с положительными и отрицательными мерами.

В настоящей статье предлагается достаточно простой экспоненциально быстро сходящийся алгоритм решения задачи справедливого деления для случая, когда критерии участников описываются неатомарными счетно-аддитивными зарядами.

В силу неатомарности рассматриваемых функционалов различные части измеримого пространства в целом (одновременно для всех участников) выглядят однородными. Поэтому, на первый взгляд, наше решение выглядит несколько парадоксально. Его идея состоит в последовательном выделении дизъюнктивных частей пространства, на каждой из которых удается предъявить точное решение. Суммарная мера остатка оказывается экспоненциально малой (относительно номера шага процесса деления), что гарантирует экспоненциально быструю сходимость процесса.

Статья организована следующим образом. В § 2 приводится формальная математическая постановка задачи, после чего приводятся факты, на которых основан приведенный алгоритм, а также демонстрируются основные идеи его построения на случаях с малым количеством участников. В последних двух параграфах описы-

<sup>1</sup> Ресурс представлен единичным отрезком, а элементы разбиения являются интервалами.

<sup>2</sup> Как указал нам рецензент, частный пример для трех участников рассматривался в работе [13].

вается алгоритм построения сильного решения для мер и его обобщение на случай зарядов.

## § 2. Постановка задачи. Сильное и слабое решения

Пусть  $(M, \Sigma)$  – измеримое пространство, т.е. пара, состоящая из множества  $M$  и  $\sigma$ -алгебры его измеримых подмножеств  $\Sigma$ . Зафиксируем натуральное число  $r$ , набор  $\{\mu_i\}_{i=1}^r$  функционалов  $\mu_i: \Sigma \rightarrow \mathbb{R}$  и измеримое разбиение  $\mathcal{F} := \{F_i\}_{i=1}^r$  множества  $M$ .

Определение 1. В задаче о справедливом делении назовем разбиение  $\mathcal{F}$

- *слабым* решением, если

$$\mu_i(F_i) \geq \frac{1}{r} \sum_{j=1}^r \mu_i(F_j)$$

для любого  $i$ ;

- *сильным* решением, если

$$\mu_i(F_i) \geq \mu_i(F_j)$$

для любых  $i, j$ .

Слабое решение задачи соответствует случаю, когда  $i$ -й участник относительно функционала  $\mu_i$  получил в среднем не меньше, чем остальные. Сильное решение соответствует случаю, когда каждый считает, что остальные участники получили не больше, чем он сам.

Отметим, что в литературе по экономике слабое решение часто называют термином “proportional”, а сильное решение – термином “envy-free”. В математическом контексте наша терминология (впервые предложенная М. Бланком в [14]) представляется более удобной и адекватной. Идейно эта терминология восходит к классическим понятиям слабых и сильных решений в теории дифференциальных уравнений.

*Лемма 1. Пусть  $\mathcal{M}$  – класс функционалов, для которого задача о справедливом делении имеет решение. Тогда для любого  $r$  и любого  $\mu \in \mathcal{M}$  существует такое разбиение  $M$  на  $r$  измеримых подмножеств  $\{F_i\}_{i=1}^r$ , что  $\mu(F_i) = \mu(F_j) \forall i, j$ .*

*Доказательство.* Для существования любого из вышеперечисленных решений задачи о справедливом делении необходимым требованием является наличие соответствующего решения для случая, когда все функционалы  $\mu_i$  совпадают и равны  $\mu$ . В этом случае условия слабого и сильного решения выглядят следующим образом:

- $\mu(F_i) \geq \frac{1}{r} \sum_{j=1}^r \mu(F_j) \forall i$ ;
- $\mu(F_i) \geq \mu(F_j) \forall i, j$ .

Из каждого из этих условий следует, что  $\mu(F_i) = \mu(F_j)$  для любых  $i, j$ . Таким образом, найдется измеримое разбиение множества  $M$  на  $r$  частей  $F_i$ , равных относительно функционала  $\mu$ . ▲

Важным вопросом является достаточность этого условия при разных типах постановки задачи. Полный ответ на этот вопрос остается открытым, но следующая теорема дает наиболее полное на сегодняшний день его решение.

*Теорема 1. Для любых неатомарных счетно-аддитивных зарядов  $\{\psi_i\}_{i=1}^r$  имеется явный конструктивный алгоритм построения сильного решения задачи о справедливом делении.*

Доказательством этого результата является предлагаемая ниже элементарная конструкция построения сильного решения для случая неатомарных счетно-аддитивных зарядов.

### § 3. Технические средства

Основным утверждением, которое мы будем использовать при построении решения для зарядов, является разложение Хана – Жордана заряда  $\psi$  на множестве  $M$ , согласно которому имеется такое измеримое разбиение  $M = A^+ \cup A^-$ , что:

- $\psi(a) \geq 0$  для любого множества  $a \subset A^+$ ;
- $\psi(b) \leq 0$  для любого множества  $b \subset A^-$ .

Иначе говоря,  $\psi = \mu^+ - \mu^-$ , где  $\mu^\pm$  – счетно-аддитивные меры, являющиеся ограничениями заряда  $\psi$  на множества  $A^\pm$  соответственно.

**Определение 2.** Заряд  $\psi$  назовем *неатомарным*, если соответствующие ему меры  $\mu^+$  и  $\mu^-$  являются неатомарными.

Также в дальнейшем нам понадобится следующее важное утверждение, доказанное А.А. Ляпуновым для случая векторных мер (см. [6, 7]).

**Теорема 2.** Для любой счетно-аддитивной неатомарной меры  $\mu$  на  $(M, \Sigma)$  множество значений меры  $\mu$  на  $\sigma$ -алгебре  $\Sigma$  выпукло.

**Следствие 1.** Для любой счетно-аддитивной неатомарной меры  $\mu$  на  $(M, \Sigma)$ , любого измеримого множества  $A \subset M$  и любого числа  $\delta \in [0, \mu(A)]$  найдется измеримое подмножество  $B \subseteq A$  с  $\mu(B) = \delta$ .

Последнее утверждение (на которое иногда ссылаются как на теорему В. Серпинского, 1922 г.) говорит о существовании множества любой заданной меры. В рамках рассматриваемого подхода мы предполагаем, что такое подмножество может быть предъявлено явно.

### § 4. Сильное решение для случая $r \in \{2, 3\}$ мер

**Определение 3.** Для разбиения  $\mathcal{F} = \{F_i\}_{i=1}^r$  будем говорить, что множество  $A$  сопоставляется  $j$ -му участнику, если  $F_j = A$ .

Начнем с построения сильного решения задачи для неатомарных счетно-аддитивных мер в простейшей ситуации двух участников процесса деления,  $r = 2$  (алгоритм “Cut and choose”).

По следствию 1 в  $M$  имеется подмножество  $A_1$  половинной  $\mu_1$ -меры. Тогда при  $A_2 := M \setminus A_1$  выполняется

$$\mu_1(A_2) = \mu_1(M \setminus A_1) = \mu_1(M) - \frac{1}{2}\mu_1(M) = \frac{1}{2}\mu_1(M).$$

Получаем разбиение  $M$  на две части, равные по мере  $\mu_1$ . Тогда, если второму участнику сопоставить большую (либо равную) относительно меры  $\mu_2$  часть (обозначенную через  $A_2$ ), а оставшуюся часть (обозначенную через  $A_1$ ) сопоставить первому, то получим сильное решение нашей задачи. Действительно,

$$\begin{aligned} \mu_1(A_1) = \mu_1(A_2) &\implies \mu_1(A_1) \geq \mu_1(A_2), \\ \mu_2(A_2) &\geq \mu_2(A_1). \end{aligned}$$

На первый взгляд кажется, что эта схема последовательного “деления пополам” легко продолжается и на большее число участников, скажем,  $r = 3$ . Точнее, первый участник делит  $M$  на  $r$  равных с его точки зрения частей, а остальные участники

упорядочивают это разбиение каждый в соответствии со своей мерой. Далее, все “спорные” элементы разбиения делятся между парами претендующих на них участников. Фактически к этому алгоритму сводится целый ряд публикаций, популяризирующих задачу справедливого деления. Алгоритм деления конечен и предельно прост, однако его детальный анализ показывает, что в результате будет получено только слабое решение, поскольку может оказаться, что участник, не участвующий в каком то из “делений пополам”, получит долю строго меньшую, чем один из других участников (см., например, [10]).

В дальнейшем нам понадобится следующее техническое утверждение<sup>3</sup>.

*Лемма 2.* Пусть  $\mu$  – счетно-аддитивный функционал,  $M = \bigsqcup_{i=1}^{\infty} H_i$ , и на каждом множестве  $H_i$  есть сильное решение  $\mathcal{F}_i = \{F_{j,i}\}_{j=1}^n$ . Тогда разбиение  $\mathcal{F} = \{F_j\}_{j=1}^n$  является сильным решением на  $M$ , где  $F_j = \bigsqcup_{i=1}^{\infty} F_{j,i}$ .

*Доказательство.* Во-первых,  $\mathcal{F}$  действительно является разбиением  $M$ :

$$\bigsqcup_{j=1}^n F_j = \bigsqcup_{j=1}^n \bigsqcup_{i=1}^{\infty} F_{j,i} = \bigsqcup_{i=1}^{\infty} \bigsqcup_{j=1}^n F_{j,i} = \bigsqcup_{i=1}^{\infty} H_i = M.$$

Во-вторых, так как  $\mu_j(F_{j,i}) \geq \mu_j(F_{k,i}) \forall i, j, k$ , то

$$\mu_j(F_j) = \mu_j\left(\bigsqcup_{i=1}^{\infty} F_{j,i}\right) = \sum_{i=1}^{\infty} \mu_j(F_{j,i}) \geq \sum_{i=1}^{\infty} \mu_j(F_{k,i}) = \mu_j\left(\bigsqcup_{i=1}^{\infty} F_{k,i}\right) = \mu_j(F_k).$$

Значит,  $\mathcal{F}$  является сильным решением.  $\blacktriangle$

Используя этот результат, разберем построение сильного решения для случая  $r = 3$ .

Аналогично случаю  $r = 2$  разделим сначала  $M$  на  $r = 3$  равных по мере  $\mu_1$  части  $A_1, A_2$  и  $A_3$ . Для этого по следствию 1 мы можем выбрать в  $M$  такое подмножество  $A_1$ , что  $\mu_1(A_1) = \frac{1}{3}\mu_1(M)$ , а так как

$$\mu_1(M \setminus A_1) = \mu_1(M) - \frac{1}{3}\mu_1(M) = \frac{2}{3}\mu_1(M),$$

то найдется такое  $A_2 \subset M \setminus A_1$ , что  $\mu_1(A_2) = \frac{1}{3}\mu_1(M)$ .

Полагая  $A_3 := M \setminus (A_1 \cup A_2)$ , получаем

$$\begin{aligned} \mu_1(A_3) &= \mu_1(M \setminus (A_1 \cup A_2)) = \mu_1(M \setminus A_1) - \mu_1(A_2) = \\ &= \frac{2}{3}\mu_1(M) - \frac{1}{3}\mu_1(M) = \frac{1}{3}\mu_1(M). \end{aligned}$$

Упорядочим эти множества относительно второй меры. Без ограничения общности положим  $\mu_2(A_1) \geq \mu_2(A_2) \geq \mu_2(A_3)$ . Так как  $\mu_2(A_1) \geq \mu_2(A_2)$ , то найдется такое  $A' \subset A_1$ , что  $\mu_2(A') = \mu_2(A_2)$ . Поэтому

$$\mu_1(A') \leq \mu_1(A_1) = \mu_1(A_2) = \mu_1(A_3).$$

Мы хотим разделить множества  $A', A_2$  и  $A_3$  между участниками. Сопоставим третьему участнику наибольшее относительно его меры из этих множеств. Если

<sup>3</sup> Здесь и далее  $\sqcup$  обозначает объединение непересекающихся множеств.

это  $A'$ , то тогда, сопоставив первому  $A_3$ , а второму  $A_2$ , получим сильное решение на  $M' := A' \cup A_2 \cup A_3$ . Действительно,

$$\begin{aligned}\mu_1(A') &\leq \mu_1(A_2) = \mu_1(A_3), \\ \mu_2(A') &= \mu_2(A_2) \geq \mu_2(A_3).\end{aligned}$$

Если  $\mu_3(A_2)$  – наибольшее, то эти неравенства доказывают, что если сопоставить первому участнику  $A_3$ , а второму  $A'$ , то полученное разбиение окажется сильным решением.

Наконец, если  $\mu_3(A_3)$  – наибольшее, то для получения сильного решения надо сопоставить  $A_2$  первому участнику, а  $A'$  – второму.

Далее, будем искать сильное решение на оставшейся части  $M_1 = M \setminus M'$ . Так как  $M' = A' \cup A_2 \cup A_3$ , то  $M_1 \subset A_1$ , а значит,

$$\mu_1(M_1) \leq \mu_1(A_1) = \frac{1}{3}\mu_1(M).$$

Заметим, что нумерация мер была абсолютно произвольной, а значит, наш алгоритм позволяет за один шаг уменьшить любую из мер  $\{\mu_i\}$  оставшейся части более чем в 3 раза. Получается, что любая из этих мер остатка экспоненциально убывает. Поэтому в пределе мы получим разбиение  $M$  на счетное число частей, на которых есть сильное решение, а в остатке получится множество  $M_\infty$ , нулевое по каждой мере (каждое разбиение  $M_\infty$  – сильное решение). Значит, по лемме 2 мы получаем сильное решение на  $M$ .

**Определение 4.** Последовательность множеств  $\{A_n\}$  назовем *сходящейся*, если верхний предел последовательности

$$\bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} A_k$$

совпадает с нижним

$$\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} A_k.$$

Строгое описание построения последовательности множеств, сходящейся к сильному решению, будет дано при описании алгоритма построения решения для общего случая  $r \geq 3$  участников.

Приведенный выше элементарный алгоритм построения сильного решения для случая  $r = 3$  не удастся обобщить для большего числа участников. В первую очередь дело в том, что в процессе перераспределения частей  $A_i$  между собой может возникать заикливание. Поэтому, оставляя в силе индукционную схему процесса деления, мы предлагаем иную, несколько более сложную конструкцию (см. следующий параграф).

Также стоит заметить, что даже если мы умеем решать задачу для мер, остается еще важная ситуация, когда функционалы являются зарядами. Обсудим возможные подходы к решению этой задачи. Начнем с ситуации, когда рассматриваемые заряды строго отрицательны, т.е. взятые с обратным знаком  $\{-\mu_i\}$  являются счетно-аддитивными мерами.

На первый взгляд кажется, что если эти меры являются вероятностными<sup>4</sup>, то рассматриваемая постановка сводится к предыдущей заменой  $\{\mu_i\}$  на набор поло-

<sup>4</sup> Мера  $\mu$  на  $(M, \Sigma)$  называется вероятностной, если  $\mu(M) = 1$ .

жительных функционалов  $\{1 - \mu_i\}$ . Однако функционалы  $1 - \mu_i$  не аддитивны, что означает, что они не являются мерами.

Действительно, если бы функционал  $\varphi = 1 - \mu$  был бы аддитивен, то

$$\begin{aligned}\varphi(A \sqcup B) &= \varphi(A) + \varphi(B) = (1 - \mu(A)) + (1 - \mu(B)) = 2 - \mu(A) - \mu(B), \\ \varphi(A \sqcup B) &= 1 - \mu(A \sqcup B) = 1 - \mu(A) - \mu(B).\end{aligned}$$

Приходим к противоречию:

$$2 - \mu(A) - \mu(B) = 1 - \mu(A) - \mu(B).$$

Поэтому даже для случая строго отрицательных зарядов необходима специальная конструкция процесса построения сильного решения, которая будет описана в § 6.

### § 5. Построение сильного решения для случая $r > 3$ мер

Частным случаем теоремы 1 является ситуация, когда функционалы  $\{\mu_i\}_{i=1}^r$  являются мерами. Ниже мы сформулируем и докажем это утверждение.

*Теорема 3. Для любых неатомарных счетно-аддитивных мер  $\{\mu_i\}_{i=1}^r$  имеется явный конструктивный алгоритм построения сильного решения задачи о справедливом делении.*

*Определение 5. Для дизъюнктного<sup>5</sup> набора множеств  $\{A_i\}_{i=1}^r$  предпочтением  $k$ -го участника<sup>6</sup> назовем такой индекс  $j$ , что  $\mu_k(A_j) \geq \mu_k(A_i)$  для любого  $i$ .*

*Лемма 3. Для заданного набора мер  $\{\mu_i\}_{i=1}^r$  и любого индекса  $k$  из произвольного измеримого множества  $S \subset \Sigma$  можно выделить его подмножество  $H \subset S$  “большой” меры*

$$\mu_k(H) \geq \frac{1}{2^{r-1}} \mu_k(S),$$

*на котором существует сильное решение задачи о справедливом делении.*

*Доказательство.* Для удобства перенумеруем меры  $\{\mu_i\}$  так, чтобы мера  $\mu_k$  имела индекс 1.

На первом шаге разделим  $S$  на  $2^{r-1}$  частей  $A_1^1, \dots, A_{2^{r-1}}^1$  равных по мере  $\mu_1$ . Для этого мы последовательно будем рассматривать в  $S$  подмножества  $A_i^1$ . Во-первых, по следствию 1 существует такое множество  $A_1^1$ , что

$$\mu_1(A_1^1) = \frac{1}{2^{r-1}} \mu_1(S).$$

Далее, на  $t$ -м шаге в  $S \setminus \bigcup_{i=1}^{t-1} A_i^1$  найдется такое подмножество  $A_t^1$ , что

$$\mu_1(A_t^1) = \frac{1}{2^{r-1}} \mu_1(S),$$

так как

$$\mu_1\left(S \setminus \bigcup_{i=1}^t A_i^1\right) = \frac{2^{r-1} - t}{2^{r-1}} \mu_1(S).$$

<sup>5</sup> Множества  $\{A_i\}$  называются дизъюнктными, если они попарно не пересекаются.

<sup>6</sup> Как нам указал рецензент, похожая конструкция предпочтений была описана в работе [15], где было проанализировано несколько примеров для 3 и 4 участников.

Заметим, что за  $2^{r-1} - 1$  шагов мы получим искомое разбиение, так как если

$$A_{2^{r-1}} = S \setminus \bigcup_{i=1}^{2^{r-1}-1} A_i^1,$$

то

$$\mu_1 \left( S \setminus \bigcup_{i=1}^{2^{r-1}-1} A_i^1 \right) = \frac{2^{r-1} - (2^{r-1} - 1)}{2^{r-1}} \mu_1(S) = \frac{1}{2^{r-1}} \mu_1(S).$$

Обозначим полученные на  $t$ -м шаге множества через  $A_1^t, \dots, A_{2^{r-1}}^t$ . Каждый наш следующий шаг (на котором мы будем выделять некоторые предпочтения участников) будет состоять в изменении текущего набора множеств. Пусть  $K_i^t$  – набор выделенных предпочтений  $i$ -го участника на  $t$ -м шаге. На первом шаге  $K_1^1 = \{1, \dots, 2^{r-1}\}$  (все  $A_i^1$  являются его предпочтениями), а остальные  $K_i^1$  оставим пустыми.

Далее на  $t$ -м шаге мы делаем следующее.

Упорядочим все множества  $A_1^{t-1}, \dots, A_{2^{r-1}}^{t-1}$  по мере  $\mu_t$  и рассмотрим  $2^{r-t}$  наибольших среди них:

$$\mu_1(A_{k_1}^{t-1}) \geq \mu_1(A_{k_2}^{t-1}) \geq \dots \geq \mu_1(A_{k_{2^{r-t}}}^{t-1}).$$

Тогда в каждом множестве  $A_{k_i}^{t-1}$  найдется подмножество

$$A'_{k_i} \subset A_{k_i}^{t-1} : \mu_t(A'_{k_i}) = \mu_t(A_{k_{2^{r-t}}}^{t-1}).$$

Новый набор  $A_i^t$  – это набор  $A_i^{t-1}$ , в котором элементы  $A_{k_i}^{t-1}$  заменены на  $A'_{k_i}$ . Набор новых выделенных предпочтений  $K_i^t$  таков, что  $K_t^t = \{k_1, \dots, k_{2^{r-t}}\}$ , а  $K_i^t = K_i^{t-1} \setminus K_t^t$  при  $i \neq t$  (в частности,  $K_i^t = \emptyset$  при  $i > t$ ).

Проверим индукцией по  $t$ , что на каждом шаге выполняются следующие свойства:

1. Множества  $K_i^t$  дизъюнктные;
2.  $|K_j^t| \geq 2^{r-t}$  при  $j \leq t$ ;
3. Для любого  $j$  и  $k \in K_j^t$  верно, что  $A_k^t$  – предпочтение  $j$ -го участника.

Проверим базу индукции:

1.  $K_1^1 = \{1, \dots, 2^{r-1}\}$ , а остальные  $K_i^1$  пустые, что означает, что они дизъюнктны;
2. Для  $j = 1$  имеем  $|K_j^1| = |K_1^1| = 2^{r-1}$ ;
3. При  $j = 1$  для любого  $k$  верно, что  $A_k^1$  – предпочтение 1-го участника по построению. При  $j \neq 1$  имеем  $K_j^1 = \emptyset$ .

Доказательство шага индукции:

1. При  $j > t$  множества  $K_j^t$  пустые, а значит, с ними никто пересекаться не может. При  $s, k < t$  множества  $K_s^t = K_s^{t-1} \setminus K_t^t$  и  $K_k^t = K_k^{t-1} \setminus K_t^t$  не пересекаются, так как  $K_s^{t-1}$  и  $K_k^{t-1}$  не пересекались по предположению индукции. Для  $j = t$  и  $s < t$  множества  $K_t^t$  и  $K_s^t = K_s^{t-1} \setminus K_t^t$  не пересекаются. Это означает, что  $K_i^t$  не пересекаются.
2.  $|K_t^t| \geq 2^{r-t}$ , так как  $|K_t^t| = 2^{r-t}$ , а для  $j \leq t-1$

$$|K_j^t| = |K_j^{t-1} \setminus K_t^t| \geq |K_j^{t-1}| - |K_t^t| \geq 2^{r-(t-1)} - 2^{r-t} = 2^{r-t}$$

(по предположению индукции  $|K_j^{t-1}| \geq 2^{r-(t-1)}$  при  $j \leq t-1$ ).

3. Для любого  $j \leq t-1$  имеем  $K_j^t = K_j^{t-1} \setminus K_t^t$ . По предположению индукции  $A_i^{t-1}$  с индексами, лежащими в  $K_j^{t-1}$ , были предпочтениями  $j$ -го участника. Далее,  $t$ -й шаг состоит в изменении множеств с индексами, лежащими в  $K_t^t$ , каждое из них заменяется на некоторое подмножество, а значит, его мера  $\mu_j$  уменьшается. Получается, что множества с индексами из  $K_j^t = K_j^{t-1} \setminus K_t^t$  остались предпочтениями  $j$ -го участника. Для  $k \in K_t^t$  имеем  $\mu_t(A_k^t) = \mu_t(A_{k_{2^{r-1}}}^{t-1})$ , а значит, так как  $\mu_t(A_{k_{2^{r-1}}}^{t-1})$  по построению – наибольшее из значений  $\mu_t(A_i^t)$ , то  $A_k^t$  – предпочтение  $j$ -го участника.

В итоге на  $r$ -м шаге  $|K_i^r| \geq 2^{r-r} = 1$  для любого  $i$ , и следовательно, у каждого участника будет ровно по одному предпочтению, которые не совпадают между собой из-за дизъюнктивности  $\{K_i^r\}$ . Сопоставим  $i$ -му участнику его предпочтение  $F_i$ .

При этом первому сопоставлено такое множество  $F_1$ , что

$$\mu_1(F_1) = \frac{1}{2^{r-1}} \mu_1(S),$$

так как по построению мы убираем из выделенных предпочтений первого участника те, что мы изменили.

Это означает, что множество  $H = \bigsqcup_{i=1}^r F_i$  является искомым, так как

$$\mu_1(H) \geq \mu_1(F_1) = \frac{1}{2^{r-1}} \mu_1(S),$$

а также  $\mu_i(F_i) \geq \mu_i(F_j)$  для любых  $i$  и  $j$ , так как  $F_i$  – предпочтение  $i$ -го участника.  $\blacktriangle$

**Определение 6.** Полученное в лемме 3 множество  $H$  будем называть  $\mu_k$ -удовлетворяющим подмножеством  $S$ .

Построим новую последовательность множеств  $\{H_i\}$  по следующим правилам:

- $H_1$  –  $\mu_1$ -удовлетворяющее подмножество  $M = M_0$ ;
- Если  $k \bmod r \neq 0$ , то  $t = k \bmod r$ , в противном случае  $t = r$ ;
- $H_k$  –  $\mu_t$ -удовлетворяющее подмножество  $M \setminus \bigcup_{i=1}^{k-1} H_i$ ;
- $M_s = M \setminus \bigcup_{i=1}^{sr} H_i$ .

Определим также усредненную меру

$$\mu(A) = \frac{1}{r} \sum_{i=1}^r \mu_i(A).$$

Иначе говоря, мы по очереди для каждой меры выделяем множества, которые не меньше  $1/2^{r-1}$  очередной меры остатка  $M \setminus \bigcup_{i=1}^{k-1} H_i$ . Действительно,

$$\mu_t(H_k) \geq 2^{-(r-1)} \mu_t \left( M \setminus \bigcup_{i=1}^{k-1} H_i \right).$$

**Лемма 4.** *Справедливо неравенство*

$$\mu(M_s) \leq \frac{2^{r-1} - 1}{2^{r-1}} \mu(M_{s-1}).$$

Доказательство. Для любого  $j$  имеем

$$\begin{aligned}
\mu_j \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \right) &= \mu_j(H_{(s-1)r+j}) + \mu_j \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \setminus H_{(s-1)r+j} \right) \geq \\
&\geq 2^{-(r-1)} \mu_j \left( M \setminus \bigcup_{i=1}^{(s-1)r+j-1} H_i \right) + \mu_j \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \setminus H_{(s-1)r+j} \right) \geq \\
&\geq 2^{-(r-1)} \left( \mu_j \left( M_{s-1} \setminus \bigcup_{i=(s-1)r+1}^{(s-1)r+j-1} H_i \right) + \mu_j \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \setminus H_{(s-1)r+j} \right) \right) \geq \\
&\geq 2^{-(r-1)} \mu_j \left( \left( M_{s-1} \setminus \bigcup_{i=(s-1)r+1}^{(s-1)r+j-1} H_i \right) \cup \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \setminus H_{(s-1)r+j} \right) \right) = \\
&= 2^{-(r-1)} \mu_j \left( M_{s-1} \cup \left( \bigcup_{i=(s-1)r+j+1}^{sr} H_i \right) \right) \geq 2^{-(r-1)} \mu_j(M_{s-1}).
\end{aligned}$$

Следовательно,

$$\begin{aligned}
\mu_j(M_s) &= \mu_j \left( M_{s-1} \setminus \bigcup_{i=(s-1)r+1}^{sr} H_i \right) = \mu_j(M_{s-1}) - \mu_j \left( \bigcup_{i=(s-1)r+1}^{sr} H_i \right) \leq \\
&\leq \frac{2^{r-1} - 1}{2^{r-1}} \mu_j(M_{s-1}).
\end{aligned}$$

Таким образом,

$$\sum_{j=1}^r \mu_j(M_s) \leq \frac{2^{r-1} - 1}{2^{r-1}} \sum_{j=1}^r \mu_j(M_{s-1}).$$

Окончательно получаем

$$\mu(M_s) \leq \frac{2^{r-1} - 1}{2^{r-1}} \mu(M_{s-1}). \quad \blacktriangle$$

Следствие 2. *Справедливо неравенство*

$$\mu(M_s) \leq \left( \frac{2^{r-1} - 1}{2^{r-1}} \right)^s \mu(M).$$

Следствие 3. *Пусть*

$$M_\infty = M \setminus \bigcup_{i=1}^{\infty} H_i,$$

тогда  $\mu_j(M_\infty) = 0$  для любого  $j$ .

Доказательство. Устремим в следствии 2 параметр  $s$  к бесконечности. Поскольку

$$\frac{2^{r-1} - 1}{2^{r-1}} < 1,$$

то  $\mu(M_\infty) \leq 0$ , а из неотрицательности меры  $\mu$  следует, что  $\mu(M_\infty) = 0$ . Так как

$$\mu(M_\infty) = \sum_{j=1}^n \mu_j(M_\infty),$$

то получаем требуемое утверждение.  $\blacktriangle$

Таким образом, мы представили  $M$  в следующем виде:  $M = \bigsqcup_{i=0}^{\infty} H_i$ , где на каждом  $H_i$  имеется сильное решение  $\mathcal{F}_i = \{F_{j,i}\}_{j=1}^n$ . (На  $M_\infty$  есть сильное решение, при котором первой мере сопоставлено  $M_\infty$ , а остальным – пустое множество, поэтому будем считать, что  $M_\infty = H_0$ .) Это означает, что по лемме 2 существует сильное решение на  $M$ .

Для каждой меры  $\mu_j$  рассмотрим последовательность множеств

$$N_{j,k} = \bigsqcup_{i=0}^{kr} F_{j,i}.$$

Лемма 5. *Последовательность множеств  $N_{j,k}$  сходится по  $k$ , причем предел последовательности  $N_{j,k}$  равен*

$$\bigcup_{k=1}^{\infty} N_{j,k} =: N_j^\infty.$$

Доказательство. Так как  $N_{j,k} \subset N_{j,k+1}$ , то

$$\bigcup_{k=n}^{\infty} N_{j,k} = \bigcup_{k=1}^{\infty} N_{j,k} = N_j^\infty.$$

Это означает, что верхний предел  $N_{j,k}$  удовлетворяет соотношению

$$\bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} N_{j,k} = \bigcap_{n=1}^{\infty} N_j^\infty = N_j^\infty.$$

С другой стороны,

$$\bigcap_{k=n}^{\infty} N_{j,k} = N_{j,n}.$$

Следовательно, нижний предел

$$\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} N_{j,k} = \bigcup_{n=1}^{\infty} N_{j,n} = N_j^\infty,$$

что и требовалось доказать.  $\blacktriangle$

Лемма 6.  $\{N_j^\infty\}_{j=1}^r$  – сильное решение на  $M$ .

Доказательство. Поскольку множества  $F_{j,i}$  не пересекаются при разных  $j$ , то  $N_j^\infty \cap N_l^\infty = \emptyset$  при  $j \neq l$ .

С другой стороны,

$$\bigcup_{j=1}^r N_j^\infty = \bigcup_{j=1}^r \bigcup_{k=1}^{\infty} N_{j,k} = \bigcup_{j=1}^r \bigcup_{k=1}^{\infty} \bigsqcup_{i=0}^{kr} F_{j,i} = \bigcup_{j=1}^r \bigcup_{i=0}^{\infty} F_{j,i} = \bigcup_{i=0}^{\infty} H_i = M.$$

Поэтому  $M = \bigsqcup_{j=1}^r N_j^\infty$ .

Так как по лемме 2 выполняется

$$N_j^\infty = \bigcup_{k=1}^{\infty} N_{j,k},$$

то  $\mu_j(N_j^\infty) \geq \mu_j(N_l^\infty)$  при всех  $j, l$ , что завершает доказательство.  $\blacktriangle$

## § 6. Построение сильного решения для зарядов

Перейдем к случаю неатомарных счетно-аддитивных зарядов  $\{\psi_i\}_{i=1}^r$ .

Для каждого заряда  $\psi_i$  рассмотрим соответствующие ему множества  $A_i^+$  и  $A_i^-$  из разложения Хана – Жордана. Тогда пересечения наборов множеств  $\{A_i^+, A_i^-\}$  разбивают все множество  $M$  на  $2^r$  частей, ограничение  $\psi_i$  на каждой из которых является либо мерой, либо минус мерой.

Поэтому по лемме 2 нам достаточно научиться решать задачу на каждой из этих  $2^r$  частей. Согласно предыдущему параграфу задача уже решена для тех частей, где все ограничения на нее зарядов положительны.

Обозначим полученные части через  $X_1, \dots, X_{2^r}$  и рассмотрим одну из этих частей, которую мы для простоты обозначим через  $X$ .

**Определение 7.** Обозначим через  $I^+$  ( $I^-$ ) множество индексов  $i$ , для которых ограничение заряда  $\psi_i$  на  $X$  является мерой (минус мерой).

Возможны два случая:  $I^+ \neq \emptyset$  и  $I^+ = \emptyset$ . Рассмотрим сначала первый из них.

**Лемма 7.** Если  $I^+ \neq \emptyset$ , то на  $X$  есть сильное решение.

**Доказательство.** По теореме 3 на множестве  $X$  существует сильное решение  $\mathcal{F}^+ := \{F_i\}_{i \in I^+}$  для мер  $\{\psi_i\}_{i \in I^+}$ . Дополним набор  $\mathcal{F}^+$  до набора  $\mathcal{F} := \{F_i\}_{i=1}^r$  множествами  $F_i = \emptyset$  для  $i \in I^-$ .

Тогда для  $i \in I^-$  и любого  $j$  выполнено

$$\psi_i(F_i) = \psi_i(\emptyset) = 0 \geq \psi_i(F_j),$$

так как на рассматриваемом множестве  $i$ -я мера со знаком отрицательна.

Если  $i \in I^+$  и  $j \in I^+$ , то  $\psi_i(F_i) \geq \psi_i(F_j)$ , так как  $\mathcal{F}^+$  – сильное решение для положительных мер. Если же  $i \in I^+$  и  $j \in I^-$ , то

$$\psi_i(F_i) \geq 0 = \psi_i(\emptyset) = \psi_i(F_j). \quad \blacktriangle$$

Осталось построить сильное решение на множестве, ограничение любого рассматриваемого заряда на которое является минус мерой. Для этого надо заметить, что задача поиска сильного решения для минус мер равносильна поиску следующего разбиения.

**Определение 8.** В задаче о справедливом делении с набором мер  $\{\mu_i\}_{i=1}^r$  разбиение  $\mathcal{F}$  назовем *джентльменским* решением, если

$$\mu_i(F_i) \leq \mu_i(F_j)$$

для любых  $i, j$ .

Отметим, что поскольку выполнен переход к минус мере, то знак неравенства изменен на противоположный по сравнению с определением 1.

В литературе по экономике эту постановку часто называют “chore division”. Нетрудно понять, что с точки зрения решения задачи о справедливом делении с набором строго отрицательных зарядов  $\{\psi_i = -\mu_i\}_{i=1}^r$  эти две постановки эквивалентны.

Аналогично лемме 2 доказывается следующий ее вариант.

Лемма 8. Пусть  $\mu$  – счетно-аддитивный функционал,  $M = \bigsqcup_{i=1}^{\infty} H_i$  и на каждом множестве  $H_i$  есть джентльменское решение  $\mathcal{F}_i = \{F_{j,i}\}_{j=1}^n$ . Тогда разбиение  $\mathcal{F} = \{F_j\}_{j=1}^n$ , где  $F_j = \bigsqcup_{i=1}^{\infty} F_{j,i}$ , является сильным решением на  $M$ .

Доказательство. Так как  $\mu_j(F_{j,i}) \leq \mu_j(F_{k,i})$  для любых  $i, j, k$ , то

$$\mu_j(F_j) = \mu_j\left(\bigsqcup_{i=1}^{\infty} F_{j,i}\right) = \sum_{i=1}^{\infty} \mu_j(F_{j,i}) \leq \sum_{i=1}^{\infty} \mu_j(F_{k,i}) = \mu_j\left(\bigsqcup_{i=1}^{\infty} F_{k,i}\right) = \mu_j(F_k). \quad \blacktriangle$$

Пусть множество  $S \in \Sigma$  удовлетворяет условию  $\prod_{i=1}^r \mu_i(S) \neq 0$ .

Лемма 9. Найдутся множества  $R^1, \dots, R^r, \bigsqcup_i R^i \subset S$ , и такая перенумерация мер  $\mu_{l_1}, \dots, \mu_{l_r}$ , что для любого  $k$  выполнено

$$\mu_{l_k}(R^k) = \frac{1}{r} \mu_{l_k}(S),$$

а для  $j > k$  выполнено

$$\mu_{l_j}(R^k) \leq \frac{1}{r} \mu_{l_k}(S).$$

Доказательство. Будем последовательно строить этот набор множеств. На первом шаге мы рассмотрим такое  $R_1^1 \subset S$ , что

$$\mu_1(R_1^1) = \frac{1}{r} \mu_1(S).$$

Далее, если на  $t$ -м шаге

$$\mu_t(R_{t-1}^1) > \frac{1}{r} \mu_t(S),$$

то  $R_t^1$  – такое подмножество  $R_{t-1}^1$ , что  $\mu_t(R_t^1) = \frac{1}{r} \mu_t(S)$ , а в противном случае  $R_t^1 = R_{t-1}^1$ .

В конце  $r$ -го шага мы получим множество  $R^1 = R_r^1$ . Через  $l_1$  обозначим тот номер шага, после которого мы больше не изменяли  $R_{l_1}^1$ . Тогда по построению  $\mu_{l_1}$  и  $R^1$  удовлетворяют следующим условиям:

$$\mu_{l_1}(R^1) = \frac{1}{r} \mu_{l_1}(S), \quad \mu_j(R^1) \leq \frac{1}{r} \mu_j(S), \quad j \neq l_1.$$

Теперь на  $k$ -м шаге аналогичным образом будем из множества  $S \setminus \bigsqcup_{i=1}^{k-1} R^i$  для всех мер, кроме  $\mu_{l_1}, \dots, \mu_{l_{k-1}}$ , выделять  $R^k$  и меру  $\mu_{l_k}$ , такую что

$$\mu_{l_k}(R^k) = \frac{1}{r} \mu_{l_k}(S)$$

и

$$\mu_j(R^k) \leq \frac{1}{r} \mu_j(S) \quad \text{для всех } j \notin \{l_1, \dots, l_k\}.$$

Нам надо лишь проверить, что мы можем сделать первое действие  $k$ -го шага, т.е. по какой-то мере  $\mu_j$  для  $j \notin \{l_1, \dots, l_{k-1}\}$  мера остатка не меньше  $\frac{1}{r} \mu_j(S)$ .

По построению

$$\mu_j(R^i) \leq \frac{1}{r} \mu_j(S)$$

для любого  $j \notin \{l_1, \dots, l_{k-1}\}$ . Следовательно,

$$\mu_j \left( S \setminus \bigsqcup_{i=1}^{k-1} R^i \right) = \mu_j(S) - \sum_{i=1}^{k-1} \mu_j(R^i) \geq \mu_j(S) \left( 1 - \frac{k-1}{r} \right).$$

Поэтому для  $k \leq r$  мы можем сделать этот шаг, и в результате получим искомое упорядочение мер  $\mu_i$  и множества  $R^i$ .  $\blacktriangle$

**Определение 9.** В случае джентльменского решения для дизъюнктного набора множеств  $\{A_i\}_{i=1}^r$  предпочтением  $k$ -го участника назовем такой индекс  $j$ , что

$$\mu_k(A_j) \leq \mu_k(A_i) \quad \forall i.$$

**Лемма 10.** Для заданного набора мер  $\{\mu_i\}_{i=1}^r$  из любого множества  $S \subset M$  можно выделить такое подмножество  $H$ , что если  $\{\mu_i\}_{i=1}^r$  – упорядочение мер для  $S$  из леммы 9, то

$$\mu_{l_1}(H) \geq \frac{1}{2^{r-1}} \mu_{l_1}(S)$$

и на  $H$  имеется джентльменское решение.

**Доказательство.** Для простоты записи будем нумеровать меры  $\mu_i$ , а не  $\mu_{l_i}$ , запомнив, что нумерация не произвольная, так как она зависит от множества, которое мы делим.

Сначала разделим  $R^1$  на  $2^{r-1}$  частей, равных по мере  $\mu_1$ . Обозначим полученные элементы разбиения на  $t$ -м шаге через  $A_1^t, \dots, A_{2^{r-1}}^t$ , а выделенные предпочтения  $i$ -го участника на  $t$ -м шаге – множествами  $K_i^t$ . На первом шаге положим  $K_1^1 := \{1, \dots, 2^{r-1}\}$  (все  $A_i^1$  являются его предпочтениями), а остальные  $K_i^1$  оставим пустыми.

Далее на  $t$ -м шаге мы делаем следующее.

Упорядочим все множества  $A_1^{t-1}, \dots, A_{2^{r-1}}^{t-1}$  по мере  $\mu_t$  и рассмотрим любые  $2^{r-t}$  наименьших среди них:

$$\mu_1(A_{k_1}^{t-1}) \leq \mu_1(A_{k_2}^{t-1}) \leq \dots \leq \mu_1(A_{k_{2^{r-t}}}^{t-1}).$$

Мы хотим отделить от  $R^t$  такой набор множеств  $C_1^{t-1}, \dots, C_{2^{r-t}}^{t-1}$ , что  $\forall i$

$$\mu_t(C_i^{t-1}) = \mu_t(A_{k_{2^{r-t}}}^{t-1}) - \mu_t(A_{k_i}^{t-1}).$$

Тогда новый набор  $A_i^t$  является “отредактированным” набором  $A_i^{t-1}$ , в котором элементы  $A_{k_i}^{t-1}$  заменены на  $A_{k_i}^{t-1} \sqcup C_i^{t-1}$ . Набор новых выделенных предпочтений  $K_i^t$  таков, что  $K_t^t = \{k_1, \dots, k_{2^{r+1-t}}\}$ , а для  $i \neq t$  имеем  $K_i^t = K_i^{t-1} \setminus K_t^t$  (в частности,  $K_i^t = \emptyset$  для  $i > t$ ).

Заметим, что мы можем сделать этот шаг, если

$$\sum_{i=1}^{2^{r-t}} \mu_t(C_i^{t-1}) \leq \mu_t(R^t).$$

Далее, имеем

$$\begin{aligned} \sum_{i=1}^{2^{r-t}} \mu_t(C_i^{t-1}) &= \sum_{i=1}^{2^{r-t}} \left( \mu_t(A_{k_{2^{r-t}}}^{t-1}) - \mu_t(A_{k_i}^{t-1}) \right) \leq 2^{r-t} \mu_t(A_{k_{2^{r-t}}}^{t-1}) \leq \\ &\leq \frac{2^{r-t}}{2^{r-1} - 2^{r-t}} \sum_{i=2^{r-t}+1}^{2^{r-1}} \mu_t(A_{k_i}^{t-1}). \end{aligned}$$

Так как все множества  $A_i^{t-1}$  содержатся в объединении  $R^1, \dots, R^{t-1}$ , то

$$\mu_t \left( \bigsqcup_{i=1}^{2^{r-1}} A_i^{t-1} \right) \leq \sum_{j=1}^{t-1} \mu_t(R^j) \leq \frac{t-1}{r} \mu_t(S).$$

Последнее неравенство следует из построения  $R^i$ .

Таким образом,

$$\sum_{i=2^{r-t}+1}^{2^{r-1}} \mu_t(A_{k_i}^{t-1}) \leq \mu_t \left( \bigsqcup_{i=1}^{2^{r-1}} A_i^{t-1} \right) \leq \frac{t-1}{r} \mu_t(S).$$

Поскольку  $\frac{t-1}{2^{t-1}-1} \leq 1$  при  $t \geq 2$ , то

$$\begin{aligned} \frac{2^{r-t}}{2^{r-1} - 2^{r-t}} \sum_{i=2^{r-t}+1}^{2^{r-1}} \mu_t(A_{k_i}^{t-1}) &\leq \frac{2^{r-t}}{2^{r-1} - 2^{r-t}} \frac{t-1}{r} \mu_t(S) = \\ &= \frac{t-1}{(2^{t-1}-1)r} \mu_t(S) \leq \frac{1}{r} \mu_t(S) = \mu_t(R^t). \end{aligned}$$

Аналогично предыдущей рассмотренной ситуации индукцией по  $t$  доказываются следующие утверждения:

1. Множества  $K_i^t$  дизъюнктивны;
2.  $|K_j^t| \geq 2^{r-t}$  при  $j \leq t$ ;

а для доказательства пункта 3 нам понадобится следующее рассуждение:

3. Для любого  $j$  и  $k \in K_j^t$  верно, что  $A_k^t$  – предпочтение  $j$ -й меры. Необходимо лишь отметить, что изменение частей происходит путем их объединения, а значит, части ни по какой мере не уменьшаются, а потому не могут стать предпочтениями, если они ими не были исходно. Кроме того, по построению множество  $K_t^t$  состоит только из предпочтений  $t$ -й меры.

На  $r$ -м шаге у каждого участника будет хотя бы  $2^{r-r} = 1$  предпочтений, не совпадающих между собой. Сопоставим каждому участнику свое предпочтение  $F_i$ . Заметим, что при этом первому участнику сопоставлено такое множество  $F_1$ , что  $\mu_1(F_1) = 1/2^{r-1} \mu_1(R^1)$ , так как по построению мы убираем из выделенных предпочтений первого участника те, что мы изменили.

Также надо заметить, что  $\mu_1(F_1) \leq \mu_1(F_j)$  для любого  $j$ , так как исходные множества  $A_i^1$  только увеличивались. Поэтому

$$\begin{aligned} \mu_1(H) &= \mu_1 \left( \bigsqcup_{j=1}^r F_j \right) = \sum_{j=1}^r \mu_1(F_j) \geq \sum_{j=1}^r \mu_1(F_1) = r \mu_1(F_1) = r \frac{1}{2^{r-1}} \mu_1(R^1) = \\ &= r \frac{1}{2^{r-1}} \frac{1}{r} \mu_1(S) = 2^{-(r-1)} \mu_1(S). \end{aligned}$$

Таким образом, разбиение  $H = \bigsqcup_{i=1}^r F_i$  удовлетворяет всем требуемым условиям.  $\blacktriangle$

**Теорема 4.** *Для неатомарных счетно-аддитивных мер  $\{\mu_i\}_{i=1}^r$  найдется джентльменское деление.*

**Доказательство.** Докажем индукцией по количеству участников, что существует джентльменское деление  $M$ .

Проверим базу индукции  $r = 1$ . Для одного участника существует единственное разбиение с  $F_1 = M$ , и оно, очевидно, джентльменское.

Проверим шаг индукции.

**Определение 10.** Множество  $H$ , полученное в лемме 10, назовем  $\mu_{h_1}$ -удовлетворяющим подмножеством  $S$ .

Определим по индукции последовательность множеств  $H_i$ :

- $H_1$  –  $\mu_{h_1}$ -удовлетворяющее подмножество  $M = M_0$ ;
- $H_k$  –  $\mu_{h_k}$ -удовлетворяющее подмножество  $M \setminus \bigcup_{i=1}^{k-1} H_i$ ;
- $M_\infty = M \setminus \bigcup_{i=1}^{\infty} H_i$ .

Все индексы  $h_1, h_2, \dots$  принадлежат конечному множеству  $\{1, \dots, r\}$ . Это значит, что один из них повторяется бесконечно много раз, обозначим его через  $\ell$ .

**Лемма 11.** *Пусть  $k_1 < k_2 < \dots$  – набор всех индексов  $i$ , при которых  $h_i = \ell$ . Тогда*

$$\mu_\ell \left( M \setminus \bigcup_{i=1}^{k_{i+1}} H_i \right) \leq \left( \frac{2^{r-1} - 1}{2^{r-1}} \right)^{i+1} \mu_\ell(M).$$

**Доказательство.** Имеем

$$\begin{aligned} \mu_\ell \left( \bigcup_{i=k_i+1}^{k_{i+1}} H_i \right) &= \mu_\ell(H_{k_{i+1}}) + \mu_\ell \left( \bigcup_{i=k_i+1}^{k_{i+1}} H_i \setminus H_{k_{i+1}} \right) \geq \\ &\geq 2^{-(r-1)} \mu_\ell \left( M \setminus \bigcup_{i=1}^{k_{i+1}-1} H_i \right) + \mu_\ell \left( \bigcup_{i=k_i+1}^{k_{i+1}} H_i \setminus H_{k_{i+1}} \right) \geq \\ &\geq 2^{-(r-1)} \left( \mu_\ell \left( M \setminus \bigcup_{i=1}^{k_{i+1}-1} H_i \right) + \mu_\ell \left( \bigcup_{i=k_i+1}^{k_{i+1}} H_i \setminus H_{k_{i+1}} \right) \right) \geq \\ &\geq 2^{-(r-1)} \mu_\ell \left( M \setminus \bigcup_{i=1}^{k_i} H_i \right). \end{aligned}$$

Следовательно,

$$\mu_\ell \left( M \setminus \bigcup_{i=1}^{k_{i+1}} H_i \right) \leq \frac{2^{r-1} - 1}{2^{r-1}} \mu_\ell \left( M \setminus \bigcup_{i=1}^{k_i} H_i \right).$$

Окончательно получаем

$$\mu_\ell \left( M \setminus \bigcup_{i=1}^{k_{i+1}} H_i \right) \leq \left( \frac{2^{r-1} - 1}{2^{r-1}} \right)^{i+1} \mu_\ell(M). \quad \blacktriangle$$

Следствие 4. Переходя к пределу в лемме 11 по числу рассматриваемых индексов  $i$ , получаем  $\mu_\ell(M_\infty) = 0$ .

По предположению индукции для мер с индексами  $i \in \{1, 2 \dots r\} \setminus \ell$  имеется джентльменское решение  $\mathcal{F}^* = \{F_i\}$  на  $M_\infty$ . Тогда при  $F_\ell = \emptyset$  разбиение

$$\mathcal{F} := \{F_i\}_{i=1}^r$$

на  $M_\infty$  является джентльменским решением для всех  $r$  мер.

Действительно, так как  $\mathcal{F}^*$  – джентльменское решение для мер с индексами  $i \in \{1, 2 \dots r\} \setminus \ell$ , то нам надо проверить только неравенства, содержащие условия, связанные с  $\ell$ -м участником:

$$\begin{aligned} \mu_i(F_i) &\geq 0 = \mu_i(\emptyset) = \mu_i(F_\ell), \\ \mu_\ell(F_\ell) &= \mu_\ell(\emptyset) = 0 = \mu_\ell(M_\infty) \geq \mu_\ell(F_i). \end{aligned}$$

Получаем

$$M = M_\infty \sqcup \left( \bigsqcup_{i=1}^{\infty} H_i \right),$$

причем на каждом элементе разбиения имеется джентльменское решение. Это означает, что по лемме 8 существует искомое разбиение.  $\blacktriangle$

По настоятельной просьбе анонимного рецензента привести простой понятный пример в малой размерности для двух участников мы разберем эту простейшую ситуацию детально. Заметим, во-первых, что ни размерность, ни геометрия в рассматриваемой постановке никакого значения не имеют, а во-вторых, для двух участников сильное решение для зарядов можно получить методом “Cut and choose”. Тем не менее, возможно, существенно более сложная конструкция при формальной реализации алгоритма, описанного в § 6, для  $r = 2$  поможет для понимания общей ситуации при  $r > 2$ .

По заданным зарядам  $\psi_1, \psi_2$  построим два разбиения пространства

$$M = M_1^+ \sqcup M_1^- = M_2^+ \sqcup M_2^-,$$

соответствующие положительным и отрицательным частям зарядов  $\psi_1, \psi_2$ . Положим

$$\begin{aligned} M^{++} &:= M_1^+ \cap M_2^+, & M^{+-} &:= M_1^+ \cap M_2^-, \\ M^{-+} &:= M_1^- \cap M_2^+, & M^{--} &:= M_1^- \cap M_2^-. \end{aligned}$$

Заметим, что

$$\{M^{++}, M^{+-}, M^{-+}, M^{--}\}$$

– это вновь разбиение  $M$ . Согласно построению сильного решения для зарядов части  $M^{++}$  и  $M^{--}$  делятся между участниками “пополам”, часть  $M^{+-}$  целиком отдается первому участнику, а часть  $M^{-+}$  целиком отдается второму.

На этом процесс построения сильного решения для двух участников заканчивается, поскольку необходимость в итерационной схеме возникает только при  $r > 2$ .

## § 7. Заключение

В настоящей статье предложен простой экспоненциально быстро сходящийся алгоритм построения сильного решения задачи справедливого деления для случая индивидуальных критериев, описываемых неатомарными зарядами. Как уже было

отмечено в § 1, имеются публикации [11, 12], в которых описываются конечные алгоритмы решения этой задачи для случаев строго положительных и строго отрицательных мер соответственно (пусть и с астрономической оценкой числа необходимых операций). К сожалению, эти публикации написаны с не вполне математическим уровнем строгости (приводимые в них доказательства скорее являются подробными описаниями блок-схемы программы), а сами алгоритмы настолько сложны, что проверка адекватности их работы представляется затруднительной. По-видимому, здесь необходимо что-то вроде доказательств с использованием компьютера (computer-assisted proof). Во всяком случае, проверить их “вручную” даже для небольшого числа участников нам не удалось. Тем не менее, если эти алгоритмы действительно работают, то их сочетание с описанной в § 6 схемой разбиения пространства на носители положительных и отрицательных частей зарядов и работой с их комбинациями приводит к конечному алгоритму построения сильного решения.

Отметим, что несмотря на кажущуюся похожесть рассматриваемой задачи справедливого деления с более известной постановкой многокритериальной оптимизации по Парето они принципиально различны. Под оптимальностью по Парето понимается такое состояние системы, при котором ни один ее показатель не может быть улучшен без ухудшения какого-либо другого показателя. Нетрудно понять, что любое оптимальное по Парето состояние оказывается сильным решением задачи справедливого деления, однако последняя постановка является значительно более гибкой и позволяет исследовать более широкий класс систем.

#### СПИСОК ЛИТЕРАТУРЫ

1. *Brams S.J., Jones M.A., Klamler C.* Better Ways to Cut a Cake // *Notices Amer. Math. Soc.* 2006. V. 53. № 11. P. 1314–1321.
2. *Moulin H.* Fair Division and Collective Welfare. Cambridge: MIT Press, 2003.
3. *Brams S.J.* Mathematics and Democracy: Designing Better Voting and Fair Division Procedures. Princeton, NJ: Princeton Univ. Press, 2008.
4. *Barbanel J.B., Brams S.J., Stromquist W.* Cutting a Pie Is Not a Piece of Cake // *Amer. Math. Monthly.* 2009. V. 116. № 6. P. 496–514. <https://doi.org/10.1080/00029890.2009.11920966>
5. *Dubins L.E., Spanier E.H.* How to Cut a Cake Fairly // *Amer. Math. Monthly.* 1961. V. 68. № 1. Part 1. P. 1–17. <https://doi.org/10.1080/00029890.1961.11989615>
6. *Ляпунов А.А.* О вполне аддитивных вектор-функциях // *Изв. АН СССР. Сер. матем.* 1940. Т. 4. № 6. С. 465–478. <https://www.mathnet.ru/rus/im3907>
7. *Halmos P.R.* The Range of a Vector Measure // *Bull. Amer. Math. Soc.* 1948. V. 54. № 4. P. 416–421. <https://doi.org/10.1090/S0002-9904-1948-09020-6>
8. *Stromquist W.* How to Cut a Cake Fairly // *Amer. Math. Monthly.* 1980. V. 87. № 8. P. 640–644. <https://doi.org/10.1080/00029890.1980.11995109>
9. *Su F.E.* Rental Harmony: Sperner’s Lemma in Fair Division // *Amer. Math. Monthly.* 1999. V. 106. № 10. P. 930–942. <https://doi.org/10.2307/2589747>
10. *Stromquist W.* Envy-free Cake Divisions Cannot Be Found by Finite Protocols // *Electron. J. Combin.* 2008. V. 15. № 1. Research Paper R11 (10 pp.). <https://doi.org/10.37236/735>
11. *Aziz H., Mackenzie S.* A Discrete and Bounded Envy-free Cake Cutting Protocol for Any Number of Agents // *Proc. 2016 IEEE 57th Annu. Symp. on Foundations of Computer Science (FOCS’2016)*. New Brunswick, NJ, USA. Oct. 9–11, 2016. Los Alamitos, CA: IEEE Comp. Soc., 2016. P. 416–427. <https://doi.org/10.1109/FOCS.2016.52>
12. *Dehghani S., Farhadi A., HajiAghayi M.T., Yami H.* Envy-free Chore Division for an Arbitrary Number of Agents // *Proc. 29th Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA’2018)*. New Orleans, LA, USA. Jan. 7–10, 2018. Philadelphia, PA: SIAM, 2018. P. 2564–2583. <https://doi.org/10.1137/1.9781611975031.164>
13. *Segal-Halevi E.* Fairly Dividing a Cake after Some Parts Were Burnt in the Oven. <https://arxiv.org/abs/1704.00726v5> [math.CO], 2018.

14. *Бланк М.Л.* Как делить неделимое // Докл. Акад. наук. 2016. Т. 471. № 6. С. 635–639. <https://doi.org/10.7868/S0869565216360044>
15. *Segal-Halevi E., Hassidim A., Aumann Y.* Waste Makes Haste: Bounded Time Algorithms for Envy-free Cake Cutting with Free Disposal // ACM Trans. Algorithms. 2016. V. 13. № 1. Art. 12 (32 pp.). <https://doi.org/10.1145/2988232>

*Бланк Михаил Львович*

Институт проблем передачи информации

им. А.А. Харкевича РАН, Москва

Национальный исследовательский университет

“Высшая школа экономики”, Москва

Высшая школа современной математики МФТИ, Москва

[blank@iitp.ru](mailto:blank@iitp.ru)

*Поляков Максим Олегович*

Институт проблем передачи информации

им. А.А. Харкевича РАН, Москва

Национальный исследовательский университет

“Высшая школа экономики”, Москва

[pmahol73@gmail.com](mailto:pmahol73@gmail.com)

Поступила в редакцию

18.01.2024

После доработки

23.05.2024

Принята к публикации

23.05.2024

**Р е д к о л л е г и я :**

**Главный редактор Е.М. ХОРОВ**

**А.М. БАРГ, Л.А. БАССАЛЫГО, В.А. ЗИНОВЬЕВ, В.В. ЗЯБЛОВ,  
И.А. ИБРАГИМОВ, Н.А. КУЗНЕЦОВ (зам. главного редактора),  
Д.Ю. НОГИН (ответственный секретарь), В.М. ТИХОМИРОВ,  
Ю.Н. ТЮРИН, Б.С. ЦЫБАКОВ**

Зав. редакцией *С.В. ЗОЛОТАЙКИНА*

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*

**Москва  
ФГБУ Издательство «Наука»**