РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

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

Том 58, 2022 **Вып. 4**

Октябрь–Ноябрь–Декабрь

М о с к в а

С О Д Е Р Ж А Н И Е

Теория информации

Теория кодирования

Методы обработки сигналов

Большие системы

CONTENTS

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.72

© 2022 г. **С. Гуй, И. Хуан**[1]

ЗАМЕЧАНИЯ ОБ ОБРАТНЫХ НЕРАВЕНСТВАХ ПИНСКЕРА

Предлагается простой подход к обратным неравенствам Пинскера, недавно полученным О. Бинеттом. Более конкретно, приводятся прямые доказательства оптимальных вариационных границ на f-дивергенцию с возможными ограничениями на экстремальные значения относительной информации. Предлагаемые рассуждения близки по духу к рассуждениям Сасона и Верду.

Ключевые слова: дивергенция Кульбака – Лейблера, полная вариация, обратные неравенства Пинскера, f-дивергенция, выпуклость, точные неравенства, экстремизатор.

DOI: 10.31857/S0555292322040015, **EDN:** EBBEJG

§ 1. Введение

Через $\mathcal{P}(\mathcal{X})$ обозначим класс всех распределений вероятностей на дискретном пространстве $\mathcal{X}$. Для заданной выпуклой функции $f\colon [0,\infty) \to (-\infty,\infty]$, такой что $f(1) = 0$, f-дивергенция между распределениями $P, Q \in \mathcal{P}(\mathcal{X})$ при условии $P \ll Q$ определяется как

$$D_f(P \,\|\, Q) = \mathbf{E}_Q\left[f\left(\frac{dP}{dQ}\right)\right].$$

Напомним определение полной вариации

$$|P - Q| = \sup_A |P(A) - Q(A)|$$

и неравенство Пинскера

$$|P - Q| \leqslant \sqrt{\frac{D_{\mathrm{KL}}(P \,\|\, Q)}{2}}.$$

Здесь дивергенция Кульбака – Лейблера D_{KL} соответствует дивергенции D_f при $f(x) = x \log x$.

В этой заметке нас будут интересовать некоторые обратные неравенства Пинскера. Точнее, мы хотим установить верхние границы на f-дивергенцию при дополнительных ограничениях. Подобные верхние границы называются *вариационными*, если в них участвует полная вариация.

[1] Работа выполнена при частичной финансовой поддержке Национального фонда естественных наук Китая (грант № 11801274). Статья завершена во время визита, финансируемого программой № 202006865011 для аспирантов/приглашенных ученых Китайского совета по стипендиям, в Лабораторию анализа, геометрии и приложений (LAGA) Университета Сорбонна Париж-Север.

Пусть $\delta \geqslant 0$ и $0 \leqslant m \leqslant 1 \leqslant M < \infty$. Набор (δ, m, M) представляет собой заданные параметры ограничений. Рассмотрим следующие три класса $\mathcal{P}(\mathcal{X})$-пар (P, Q):

$$\mathcal{A}(\delta, m, M) = \left\{(P, Q) :\ P \ll Q,\ |P - Q| = \delta,\ \inf \frac{dP}{dQ} = m,\ \sup \frac{dP}{dQ} = M\right\},$$

$$\mathcal{B}(m, M) = \bigcup_{\delta \geqslant 0} \mathcal{A}(\delta, m, M),$$

$$\mathcal{C}(\delta) = \bigcup_{0 \leqslant m \leqslant 1 \leqslant M < \infty} \mathcal{A}(\delta, m, M).$$

Следующие верхние границы получены в [1].

Теорема 1 (Бинетт, 2019). *Пусть $\delta \geqslant 0$ и $0 \leqslant m \leqslant 1 \leqslant M < \infty$. Тогда*

$$D_f(P \,\|\, Q) \leqslant \frac{(M-1)f(m) + (1-m)f(M)}{M - m}, \quad (P, Q) \in \mathcal{B}(m, M), \tag{1.1}$$

$$D_f(P \,\|\, Q) \leqslant \delta\left(\frac{f(m)}{1-m} + \frac{f(M)}{M-1}\right), \quad (P, Q) \in \mathcal{A}(\delta, m, M), \tag{1.2}$$

$$D_f(P \,\|\, Q) \leqslant \delta\left(f(0) + \lim_{M' \to \infty} \frac{f(M')}{M' - 1}\right), \quad (P, Q) \in \mathcal{C}(\delta). \tag{1.3}$$

Замечание 1. Мы используем следующие соглашения:

(i) Правая часть (1.1) считается равной 0 при $M = m$;

(ii) Правая часть (1.2) считается равной 0, когда $m = 1$ или $M = 1$ (заметим, что в этих крайних случаях $\delta = 0$).

Все три неравенства точны, что показано с помощью построенных в [1] примеров распределений, на которых достигается экстремум. Дополнительные сведения об этих неравенствах см. в [1, раздел 1]. О некоторых связанных с этим верхних границах на f-дивергенцию см. в [2, 3].

Цель настоящей заметки – предложить относительно более простой подход к доказательству теоремы 1. Наши аргументы близки по духу к рассуждениям Сасона и Верду в [4].

§ 2. Доказательство теоремы 1

Пусть $\kappa = \dfrac{dP}{dQ}$ и, таким образом, $\mathbf{E}_Q(\kappa) = 1$. В силу выпуклости f имеем

$$f(\kappa) \leqslant \frac{f(M) - f(m)}{M - m}(\kappa - m) + f(m).$$

Применяя к этому $\mathbf{E}_Q$, получаем (1.1). Далее, снова благодаря выпуклости f и с учетом условия $f(1) = 0$ имеем

$$f(\kappa) = f(\kappa)\big(\mathbf{1}_{\kappa \leqslant 1} + \mathbf{1}_{\kappa \geqslant 1}\big) \leqslant \frac{f(m)}{1-m}(1-\kappa)\mathbf{1}_{\kappa \leqslant 1} + \frac{f(M)}{M-1}(\kappa - 1)\mathbf{1}_{\kappa \geqslant 1}. \tag{2.1}$$

Применяя $\mathbf{E}_Q$ к этому неравенству и используя тот факт, что

$$\mathbf{E}_Q\big((1-\kappa)\mathbf{1}_{\kappa \leqslant 1}\big) = \mathbf{E}_Q\big((\kappa - 1)\mathbf{1}_{\kappa \geqslant 1}\big) = \delta, \tag{2.2}$$

получаем (1.2). Доказательство неравенства (1.3) можно получить аналогично, замечая, что

$$f(\kappa) \leqslant f(0)(1-\kappa)\mathbf{1}_{\kappa\leqslant 1} + \left(\lim_{M'\to\infty} \frac{f(M')}{M'-1}\right)(\kappa-1)\mathbf{1}_{\kappa\geqslant 1}.$$

Замечание 2. Наш вывод границы (1.1) упрощает непрямое доказательство следствия 2 в [1]. Более того, условие $f(1) = 0$ мы здесь не используем. Впрочем, само по себе неравенство (1.1) инвариантно относительно замены $f \mapsto f + \mathrm{const}$.

Замечание 3. Наше доказательство неравенства (1.1) также обосновывает его предельную версию:

$$D_f(P\,\|\,Q) \leqslant f(m) + (1-m)\left(\lim_{M'\to\infty} \frac{f(M')}{M'-m}\right), \quad (P,Q) \in \mathcal{B}(m,\infty).$$

Замечание 4. Трюк с разложением в (2.1) взят из доказательства теоремы 23 в [4] (см. также [1]). Равенства (2.2) можно найти, например, в [4, теорема 12].

Второй автор выражает благодарность проф. Ян Яну (Нанкинский научно-технологический университет) за полезные обсуждения в области теории информации и ее приложений в теории обучения.

Авторы заявляют об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Binette O.* A Note on Reverse Pinsker Inequalities // IEEE Trans. Inform. Theory. 2019. V. 65. № 7. P. 4094–4096. https://doi.org/10.1109/TIT.2019.2896192
2. *Прелов В.В.* О максимальных значениях f-дивергенции и дивергенции Реньи при заданном вариационном расстоянии // Пробл. передачи информ. 2020. Т. 56. № 1. С. 3–15. https://doi.org/10.31857/S0555292320010015
3. *Прелов В.В.* О максимуме f-дивергенции вероятностных распределений при заданной величине их склеивания // Пробл. передачи информ. 2021. Т. 57. № 4. С. 24–33. https://doi.org/10.31857/S0555292321040021
4. *Sason I., Verdú S.* f-Divergence Inequalities // IEEE Trans. Inform. Theory. 2016. V. 62. № 11. P. 5973–6006. https://doi.org/10.1109/TIT.2016.2603151

Сяюнь Гуй (Xiayun Gui)
Школа транспортной инженерии,
Восточно-китайский университет Цзяотун,
Наньчан, провинция Цзянси, КНР
453421770@qq.com
И Хуан✉ (Yi C. Huang)
Университет Сорбонна Париж-Север, Институт Галилея,
Лаборатория анализа, геометрии и приложений,
CNRS (UMR 7539), Вильтанёз, Франция
Школа математических наук,
Нанкинский нормальный университет, Нанкин, КНР
✉Yi.Huang.Analysis@gmail.com
ORCID: 0000-0002-1297-7674

Поступила в редакцию
24.06.2022
После доработки
23.09.2022
Принята к публикации
24.09.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.72

© 2022 г. **В.В. Прелов**

СКЛЕИВАНИЕ НЕСКОЛЬКИХ СЛУЧАЙНЫХ ВЕЛИЧИН

Рассматривается задача нахождения условий, при которых возможно α-склеивание нескольких случайных величин $X_1, X_2, \dots, X_k$ с конечным или счетным множеством значений, имеющих заданные распределения вероятностей, т.е. возможность построения совместного распределения этих случайных величин, такого что $\Pr\{X_1 = X_2 = \ldots = X_k\} = \alpha$.

Ключевые слова: склеивание дискретных распределений вероятностей, максимальное склеивание, вероятность ошибки.

DOI: 10.31857/S0555292322040027, **EDN:** EBJQOY

Пусть $X_1, X_2, \dots, X_k$, $k \geqslant 2$, – дискретные случайные величины, принимающие значения в одном и том же конечном или счетном множестве I с распределениями вероятностей

$$P_{X_1} = \big\{p_i^{(1)},\, i \in I\big\}, \quad P_{X_2} = \big\{p_i^{(2)},\, i \in I\big\}, \quad \dots, \quad P_{X_k} = \big\{p_i^{(k)},\, i \in I\big\}$$

соответственно. В дальнейшем без ограничения общности будем считать, что $I = \{1, 2, \dots, n\}$, $n \geqslant 2$, или $I = \{1, 2, \dots\}$ в конечномерном или счетномерном случаях соответственно. Для заданного числа α, $0 \leqslant \alpha \leqslant 1$, назовем *$\alpha$-склеиванием* случайных величин $X_1, X_2, \dots, X_k$ (или их распределений вероятностей $P_{X_1}, P_{X_2}, \dots, P_{X_k}$) совместное распределение

$$P_{X_1 X_2 \dots X_k} = \{p_{i_1 i_2 \dots i_k},\, i_j \in I,\, j = 1, 2, \dots, k\}$$

этих случайных величин, такое что $\Pr\{X_1 = X_2 = \ldots = X_k\} = \alpha$. *Максимальным склеиванием* случайных величин $X_1, X_2, \dots, X_k$ называется их α-склеивание при максимально возможном $\alpha = \alpha_{\max}$.

Ранее рассматривался лишь случай $k = 2$, т.е. случай склеивания двух дискретных случайных величин. Понятие α-склеивания для этого случая было введено в работе автора [1], а понятие максимального склеивания было введено ранее (см., например, работы [2–4] и библиографию в них), где, в частности, приведены примеры использования этого понятия в некоторых задачах теории информации и теории вероятностей. В [1] были получены необходимые и достаточные условия существования α-склеивания двух случайных величин X и Y с распределениями вероятностей $P_X = \{p_i,\, i \in I\}$ и $P_Y = \{q_i,\, i \in I\}$ соответственно. А именно, было показано, что следующие неравенства для α являются необходимыми и достаточными условиями для существования α-склеивания этих случайных величин:

$$\alpha_{\min} \leqslant \alpha \leqslant \alpha_{\max}, \tag{1}$$

где

$$\alpha_{\max} = \sum_{i \in I} \min\{p_i, q_i\} \tag{2}$$

и

$$\alpha_{\min} = \max\Big\{ \max_{i \in I}(p_i + q_i) - 1,\, 0 \Big\}. \tag{3}$$

Этот результат об условиях существования α-склеивания был использован в [1] для решения одной экстремальной задачи о нахождении явного выражения для минимума информационной дивергенции двух случайных величин при условии, что заданы распределение вероятностей одной из них и величина их склеивания.

Основная цель данной статьи – установить условия, при которых существует α-склеивание нескольких случайных величин $X_1, X_2, \ldots, X_k$, $k \geqslant 3$, с заданными распределениями вероятностей $P_{X_j} = \big\{p_i^{(j)},\, i \in I\big\}$, $j = 1, 2, \ldots, k$. Здесь мы устанавливаем как необходимое, так и достаточное условия для существования α-склеивания, которые, вообще говоря, различны.

Для формулировки основного утверждения введем необходимые нам величины. Для целого $k \geqslant 2$ положим

$$m_i = \min\Big\{p_i^{(1)}, p_i^{(2)}, \ldots, p_i^{(k)}\Big\}, \quad i \in I, \tag{4}$$

$$\alpha_* = \max\left\{ \max_{i \in I} \sum_{j=1}^{k} p_i^{(j)} - (k-1), 0 \right\}, \tag{5}$$

$$\alpha^* = \inf_{A \in I} \left| \sum_{i \in A} m_i - \sum_{i \in I \setminus A} m_i \right|, \tag{6}$$

где m_i, $i \in I$, определены в (4). Основной результат статьи представляет

Т е о р е м а. *Для любых дискретных случайных величин $X_1, X_2, \ldots, X_k$, $k \geqslant 3$, с распределениями вероятностей $P_{X_j} = \big\{p_i^{(j)},\, i \in I\big\}$, $j = 1, 2, \ldots, k$, и любого α, $0 \leqslant \alpha \leqslant 1$, справедливы следующие утверждения*:

- *Для максимального α-склеивания случайных величин $X_1, X_2, \ldots, X_k$ имеет место равенство*

  $$\alpha_{\max} = \sum_{i \in I} m_i, \tag{7}$$

  где m_i, $i \in I$, определены в (4);
- *Если существует α-склеивание случайных величин $X_1, X_2, \ldots, X_k$, то α удовлетворяет неравенствам*

  $$\alpha_* \leqslant \alpha \leqslant \alpha_{\max}, \tag{8}$$

  где α_* определено в (5);
- *Если α удовлетворяет неравенствам*

  $$\alpha^* \leqslant \alpha \leqslant \alpha_{\max}, \text{ если } I \text{ конечно}, \quad \text{и} \quad \alpha^* < \alpha \leqslant \alpha_{\max}, \text{ если } I \text{ счетно}, \tag{9}$$

  где α^* определено в (6), *то существует α-склеивание случайных величин X_1, $X_2, \ldots, X_k$*;

- *Если существуют непересекающиеся подмножества A, B и C множества I, такие что $A \cup B \cup C = I$ и*

$$\sum_{i\in A} m_i \leqslant 2\sum_{i\in B} m_i \quad \text{и} \quad \sum_{i\in B} m_i = \sum_{i\in C} m_i, \tag{10}$$

то α-склеивание случайных величин $X_1, X_2, \ldots, X_k$ возможно при любых $\alpha \in \in [0, \alpha_{\max}]$.

Следствие. *Если случайные величины $X_1, X_2, \ldots, X_k$ имеют равномерные распределения на одном и том же конечном множестве I, то их α-склеивание возможно при всех $\alpha \in [0, 1]$.*

Прежде чем привести доказательство этой теоремы, заметим, что необходимое условие существования α-склеивания (8) в случае $k = 2$ является и достаточным, как было установлено в [1]. Заметим также, что во многих частных случаях существует α-склеивание при всех $\alpha \in [0, \alpha_{\max}]$, поскольку выполняется условие (10).

Доказательство теоремы разобьем на несколько шагов.

1. Вначале покажем, что для величины $\alpha_{\max}$ максимального склеивания случайных величин $X_1, X_2, \ldots, X_k$ с распределениями вероятностей $P_{X_j} = \{p_i^{(j)}, i \in I\}$, $j = 1, 2, \ldots, k$, справедливо равенство (7). Прежде всего, очевидно, что

$$\alpha_{\max} \leqslant \sum_{i\in I} m_i,$$

так как

$$\Pr\{X_1 = X_2 = \ldots = X_k\} = \sum_{i\in I} \Pr\{X_1 = X_2 = \ldots = X_k = i\} \leqslant$$
$$\leqslant \sum_{i\in I} \min\{\Pr\{X_1 = i\}, \Pr\{X_2 = i\}, \ldots, \Pr\{X_k = i\}\} = \sum_{i\in I} m_i.$$

Поэтому нужно лишь доказать, что существуют случайные величины $X_1, X_2, \ldots, X_k$ с заданными распределениями вероятностей $P_{X_j} = \{p_i^{(j)}, i \in I\}$, $j = 1, 2, \ldots, k$, такие что их совместное распределение удовлетворяет условию

$$\Pr\{X_1 = X_2 = \ldots = X_k\} = \sum_{i\in I} m_i.$$

Предположим вначале, что $\sum\limits_{i\in I} m_i = 1$. В этом случае очевидно, что все распределения $P_{X_j} = \{p_i^{(j)},\ i \in I\}$, $j = 1, 2, \ldots, k$, одинаковы, так что $p_i^{(j)} = m_i$ при всех $i \in I$ и $j = 1, 2, \ldots, k$, а тогда справедливость равенства (7) следует из того, что совместное распределение случайных величин $X_1, X_2, \ldots, X_k$, для которого $\Pr\{X_1 = X_2 = \ldots = X_k\} = \sum\limits_{i\in I} m_i$, может быть задано равенствами

$$\Pr\{X_1 = X_2 = \ldots = X_k = i\} = m_i, \quad i \in I,$$

а остальные вероятности этого совместного распределения равны нулю.

Если же $\sum\limits_{i\in A} m_i < 1$, то совместное распределение случайных величин X_1, X_2, $\ldots, X_k$, для которого $\Pr\{X_1 = X_2 = \ldots = X_k\} = \sum\limits_{i\in I} m_i$, может быть определено следующим образом. Введем в рассмотрение независимые случайные величины $U, Y, Z_1, Z_2, \ldots, Z_k$, имеющие следующие распределения вероятностей:

- Случайная величина U принимает два значения 0 и 1 с вероятностями

$$\Pr\{U=0\}=\sum_{i\in I} m_i, \quad \Pr\{U=1\}=1-\sum_{i\in I} m_i; \tag{11}$$

- Случайная величина Y принимает значения в множестве I с вероятностями

$$\Pr\{Y=i\}=\frac{m_i}{\sum\limits_{i\in I} m_i}, \quad i\in I; \tag{12}$$

- Случайные величины Z_j, $j=1,2,\ldots,k$, принимают значения в множестве I с вероятностями

$$\Pr\{Z_j=i\}=\frac{p_i^{(j)}-m_i}{1-\sum\limits_{i\in I} m_i}, \quad i\in I, \quad j=1,2,\ldots,k. \tag{13}$$

Определим теперь случайные величины $X_1, X_2, \ldots, X_k$ следующим образом:

$$\begin{cases} X_1=X_2=\ldots=X_k=Y, & \text{если } U=0,\\ X_j=Z_j,\ j=1,2,\ldots,k, & \text{если } U=1. \end{cases} \tag{14}$$

Из (11)–(14) легко следует, что так определенные случайные величины $X_1, X_2, \ldots, X_k$ имеют заданные распределения вероятностей $\{p_i^{(j)},\ i\in I\}$, $j=1,2,\ldots,k$, а их совместное распределение таково, что $\Pr\{X_1=X_2=\ldots=X_k\}=\sum\limits_{i\in I} m_i$. Действительно,

$$\begin{aligned}
&\Pr\{X_1=X_2=\ldots=X_k\}=\sum_{i\in I}\Pr\{X_1=X_2=\ldots=X_k=i\}=\\
&=\sum_{i\in I}\Big[\Pr\{U=0\}\Pr\{X_1=X_2=\ldots=X_k=i\,|\,U=0\}+\\
&+\Pr\{U=1\}\Pr\{X_1=X_2=\ldots=X_k=i\,|\,U=1\}\Big]=\\
&=\sum_{i\in I}\left[\left(\sum_{i\in I} m_i\right)\Pr\{Y=i\}+\left(1-\sum_{i\in I} m_i\right)\prod_{j=1}^{k}\Pr\{Z_j=i\}\right]=\sum_{i\in I} m_i,
\end{aligned}$$

поскольку из (13) и (4) следует, что $\prod\limits_{j=1}^{k}\Pr\{Z_j=i\}=0$ при любом $i\in I$. Аналогично доказывается, что эти случайные величины $X_1, X_2, \ldots, X_k$ имеют заданные распределения вероятностей $\big\{p_i^{(j)},\ i\in I\big\}$, $j=1,2,\ldots,k$.

2. Докажем теперь необходимое условие существования α-склеивания (8). Для любых $j=1,2,\ldots,k$ и $i\in I$, очевидно, имеем

$$\begin{aligned}
&\Pr\{X_j=i\}\leqslant\Pr\{X_1=X_2=\ldots=X_k=i\}+\Pr\{\exists\ell,\ \ell\neq j:\ X_\ell\neq i\}\leqslant\\
&\leqslant\alpha+\sum_{\ell:\,\ell\neq j}\Pr\{X_\ell\neq i\}=\alpha+(k-1)-\sum_{\ell:\,\ell\neq j}\Pr\{X_\ell=i\},
\end{aligned}$$

т.е.

$$\alpha\geqslant\sum_{j=1}^{k} p_i^{(j)}-(k-1),$$

и так как это условие должно выполняться при любом $i \in I$, то

$$\alpha \geqslant \max_{i \in I} \left(\sum_{j=1}^{k} p_i^{(j)} \right) - (k-1),$$

а значит, необходимое условие (8) доказано.

3. Докажем теперь, что α-склеивание случайных величин $X_1, X_2, \ldots, X_k$ существует при любых α, удовлетворяющих условию (9). Согласно доказанному выше существует максимальное склеивание этих случайных величин с $\alpha = \alpha_{\max} = \sum\limits_{i \in I} m_i$, где величины m_i, $i \in I$, определены в (4). Пусть $P_{X_1 X_2 \ldots X_k} = \{p_{i_1 i_2 \ldots i_k}\}$, где

$$p_{i_1 i_2 \ldots i_k} = \Pr\{X_1 = i_1, X_2 = i_2 \ldots, X_k = i_k\}, \quad i_j \in I, \quad j = 1, 2, \ldots, k,$$

– совместное распределение случайных величин $X_1, X_2, \ldots, X_k$, осуществляющее это максимальное склеивание. Покажем теперь, что в случае, когда имеются хотя бы две отличных от нуля компоненты этого совместного распределения $m_i = p_{ii\ldots i}$ и $m_j = p_{jj\ldots j}$, $i \neq j$, то существует α-склеивание случайных величин $X_1, X_2, \ldots, X_k$ при любом $\alpha \in \left[\alpha_{\max} - 2\min\{m_i, m_j\},\, \alpha_{\max}\right]$.

Для этого рассмотрим новое совместное распределение

$$P'_{X_1 X_2 \ldots X_k}(x) = \{p'_{i_1 i_2 \ldots i_k}(x)\}$$

этих случайных величин, зависящее от параметра x, компоненты которого задаются равенствами

$$\begin{aligned}
&p'_{ii\ldots ii}(x) = p_{ii\ldots ii} - kx, && p'_{jj\ldots jj}(x) = p_{jj\ldots jj} - kx,\\
&p'_{ji\ldots ii}(x) = p_{ji\ldots ii} + x, && p'_{ij\ldots jj}(x) = p_{ij\ldots jj} + x,\\
&p'_{iji\ldots i}(x) = p_{iji\ldots i} + x, && p'_{jij\ldots j}(x) = p_{jij\ldots j} + x,\\
&\ldots\ldots\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots\ldots\ldots\\
&p'_{ii\ldots ji}(x) = p_{ii\ldots ji} + x, && p'_{jj\ldots ij}(x) = p_{jj\ldots ij} + x,\\
&p'_{ii\ldots ij}(x) = p_{ii\ldots ij} + x, && p'_{jj\ldots ji}(x) = p_{jj\ldots ji} + x,
\end{aligned} \tag{15}$$

а остальные компоненты распределения $P'_{X_1 X_2 \ldots X_k}(x)$ равны соответствующим компонентам распределения $P_{X_1 X_2 \ldots X_k}$, т.е. $p'_{i_1 i_2 \ldots i_k}(x) = p_{i_1 i_2 \ldots i_k}$ для всех компонент $p'_{i_1 i_2 \ldots i_k}(x)$, кроме заданных в (15). Заметим, что параметр x в (15) может принимать любые значения из интервала $\left[0,\, \min\{m_i, m_j\}/k\right]$, а распределение $P'_{X_1 X_2 \ldots X_k}(x)$ задает $(\alpha_{\max} - 2kx)$-склеивание заданных случайных величин $X_1, X_2, \ldots, X_k$. Поэтому существует их α-склеивание при любых $\alpha \in \left[\alpha_{\max} - 2\min\{m_i, m_j\},\, \alpha_{\max}\right]$.

Теперь заметим, что в случае, когда это совместное распределение $P'_{X_1 X_2 \ldots X_k}(x)$ снова имеет хотя бы две отличные от нуля компоненты $p'_{rr\ldots r}$ и $p'_{ss\ldots s}$, $r \neq s$, то снова с помощью аналогичной процедуры можно расширить интервал возможных значений существования α-склеивания случайных величин и т.д. Отсюда легко следует, что с помощью подобных процедур можно расширить интервал возможных значений α-склеивания случайных величин $X_1, X_2, \ldots, X_k$ до $\left[\alpha_{\max} - 2\sum\limits_{i \in A} m_i,\, \alpha_{\max}\right]$, где A – любое подмножество множества I, такое что

$$\sum_{i \in A} m_i \leqslant \sum_{i \in I \setminus A} m_i.$$

А из этого утверждения очевидно следует и существование любого α-склеивания этих случайных величин из интервалов, указанных в (9).

4. Докажем, наконец, что в случае выполнения условия (10) существует α-склеивание заданных случайных величин $X_1, X_2, \ldots, X_k$ при любом $\alpha \in [0, \alpha_{\max}]$. Предположим, что существует некоторое $\widehat{\alpha}$-склеивание $X_1, X_2, \ldots, X_k$, задаваемое совместным распределением $P_{X_1X_2\ldots X_k} = \{p_{i_1i_2\ldots i_k}\}$, у которого хотя бы две его компоненты $\beta = p_{ii\ldots i}$ и $\gamma = p_{i_1i_2\ldots i_k}$ строго положительны, где все индексы i_j второй из этих компонент отличны от i, т.е. $i_j \neq i$, $j = 1, 2, \ldots, k$, и хотя бы два из этих индексов i_j различны. Покажем, что в этом случае существует α-склеивание $X_1, X_2, \ldots, X_k$ при любом $\alpha \in \bigl[\widehat{\alpha} - \min\{\beta, \gamma\},\, \widehat{\alpha}\bigr]$.

Чтобы доказать это утверждение, рассмотрим новое совместное распределение $\widehat{P}_{X_1X_2\ldots X_k} = \{\widehat{p}_{i_1i_2\ldots i_k}\}$ этих случайных величин, зависящее от параметра x, компоненты которого задаются равенствами

$$\begin{aligned}
&\widehat{p}_{ii\ldots ii}(x) = p_{ii\ldots ii} - kx, && \widehat{p}_{i_1i_2\ldots i_{k-1}i_k}(x) = p_{i_1i_2\ldots i_{k-1}i_k} - kx,\\
&\widehat{p}_{i_1i\ldots ii}(x) = p_{i_1i\ldots ii} + x, && \widehat{p}_{ii_2\ldots i_{k-1}i_k}(x) = p_{ii_2\ldots i_{k-1}i_k} + x,\\
&\widehat{p}_{ii_2i\ldots i}(x) = p_{ii_2i\ldots i} + x, && \widehat{p}_{i_1ii_3\ldots i_k}(x) = p_{i_1ii_3\ldots i_k} + x,\\
&\ldots\ldots\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots\ldots\ldots\\
&\widehat{p}_{ii\ldots i_{k-1}i}(x) = p_{ii\ldots i_{k-1}i} + x, && \widehat{p}_{i_1i_2\ldots ii_k}(x) = p_{i_1i_2\ldots ii_k} + x,\\
&\widehat{p}_{ii\ldots ii_k}(x) = p_{ii\ldots ii_k} + x, && \widehat{p}_{i_1i_2\ldots i_{k-1}i}(x) = p_{i_1i_2\ldots i_{k-1}i} + x,
\end{aligned} \tag{16}$$

а остальные компоненты распределения $\widehat{P}_{X_1X_2\ldots X_k}(x)$ равны соответствующим компонентам распределения $P_{X_1X_2\ldots X_k}$, т.е. $\widehat{p}_{i_1i_2\ldots i_k}(x) = p_{i_1i_2\ldots i_k}$ для всех компонент $\widehat{p}_{i_1i_2\ldots i_k}(x)$, кроме заданных в (16). Параметр x в (16) может принимать любые значения из интервала $\bigl[0,\, \min\{\beta, \gamma\}/k\bigr]$. Легко убедиться, что распределение $\widehat{P}_{X_1X_2\ldots X_k}(x)$ задает $(\widehat{\alpha} - kx)$-склеивание заданных случайных величин $X_1, X_2, \ldots, X_k$, а значит, существует их α-склеивание при любых $\alpha \in \bigl[\widehat{\alpha} - \min\{\beta, \gamma\},\, \widehat{\alpha}\bigr]$.

Предположим теперь, что выполнено условие (10). Тогда, начиная с совместного распределения $P_{X_1X_2\ldots X_k}$ случайных величин $X_1, X_2, \ldots, X_k$, задающего их максимальное склеивание, и последовательно применяя метод расширения интервала существования α-склеивания, описанный выше в п. 3, к элементам из множеств B и C, мы можем утверждать, что существует α-склеивание $X_1, X_2, \ldots, X_k$ при любом $\alpha \in \bigl[\alpha_{\max} - 2\sum\limits_{i\in B} m_i,\, \alpha_{\max}\bigr]$. При этом заметим, что совместное распределение $P_{X_1X_2\ldots X_k} = \{p_{i_1i_2\ldots i_k}\}$ случайных величин $X_1, X_2, \ldots, X_k$, осуществляющее $\bigl(\alpha_{\max} - 2\sum\limits_{i\in B} m_i\bigr)$-склеивание, обладает следующим свойством: суммарное количество его компонент $p_{i_1i_2\ldots i_k}$, все индексы которых отличны от любого из индексов компонент $p_{ii\ldots i}$ при всех $i \in A$, не меньше $2\sum\limits_{i\in B} m_i$. Кроме того, у всех таких компонент $p_{i_1i_2\ldots i_k}$ имеются хотя бы два различных индекса i_j, $j = 1, 2, \ldots, k$. Это утверждение немедленно следует из свойств совместных распределений, задаваемых равенствами (15). Поэтому, применяя последовательно метод расширения интервала α-склеивания случайных величин $X_1, X_2, \ldots, X_k$, описанный в начале этого пункта (см. (16)), к элементам множества A и элементам, все индексы которых отличны от любого из индексов компонент $p_{ii\ldots i}$ при всех $i \in A$, описанных выше, приходим к выводу, что ввиду условия

$$\sum_{i\in A} m_i \leqslant 2\sum_{i\in B} m_i$$

интервал существования α-склеивания случайных величин $X_1, X_2, \ldots, X_k$ можно расширить до $\bigl[0, \alpha_{\max}\bigr]$.

На этом доказательство теоремы заканчивается. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Прелов В.В.* Склеивание вероятностных распределений и экстремальная задача для дивергенции // Пробл. передачи информ. 2015. Т. 51. № 2. С. 114–121. http://mi.mathnet.ru/ppi2174
2. *Zhang Z.* Estimating Mutual Information via Kolmogorov Distance // IEEE Trans. Inform. Theory. 2007. V. 53. № 9. P. 3280–3282. https://doi.org/10.1109/TIT.2007.903122
3. *Sason I.* Entropy Bounds for Discrete Random Variables via Maximal Coupling // IEEE Trans. Inform. Theory. 2013. V. 59. № 11. P. 7118–7131. https://doi.org/10.1109/TIT.2013.2274515
4. *Strassen V.* The Existence of Probability Measures with Given Marginals // Ann. Math. Statist. 1965. V. 36. № 2. P. 423–439. https://doi.org/10.1214/aoms/1177700153

Прелов Вячеслав Валерьевич
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
prelov@iitp.ru

Поступила в редакцию
25.10.2022
После доработки
03.11.2022
Принята к публикации
03.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.725

© 2022 г. **М. Вильянуэва[1], В.А. Зиновьев[2], Д.В. Зиновьев[2]**

ОБ ОДНОМ МЕТОДЕ ПОСТРОЕНИЯ МАТРИЦ АДАМАРА

Используя каскадную конструкцию q-ичных кодов, построены коды над $\mathbb{Z}_q$ в метрике Ли, которые после отображения в двоичный алфавит (которое в случае алфавита $\mathbb{Z}_4$ является отображением Грея) становятся кодами Адамара, в частности, матрицами Адамара. Наша конструкция позволяет увеличить ранг и размерность ядра получаемого таким образом кода Адамара. С помощью компьютера построены новые неэквивалентные матрицы Адамара порядка 32, 48 и 64 с разными фиксированными значениями их рангов и размерности ядер из диапазонов возможных значений. Оказалось, что в специальном случае наша конструкция совпадает с кронекеровской (или конструкцией Сильвестра) и может считаться вариантом известной в настоящее время [1] модифицированной конструкции Сильвестра, которая использует одну матрицу Адамара порядка m и m (не обязательно различных) матриц Адамара порядка k. Мы обобщаем здесь эту модифицированную конструкцию, предложив новую более общую конструкцию типа Сильвестра, основанную уже на двух семействах (не обязательно различных) матриц Адамара, а именно на k матрицах порядка m и m матрицах порядка k. Получающаяся матрица Адамара имеет порядок mk, как и в конструкции в [1].

Ключевые слова: матрица Адамара, код Адамара, обобщенная каскадная конструкция, код в метрике Ли, кронекеровское произведение, конструкция Сильвестра, ранг матрицы Адамара, размерность ядра матрицы Адамара, неэквивалентные матрицы Адамара.

DOI: 10.31857/S0555292322040039, **EDN:** EBOXEM

§ 1. Введение

Пусть $E_q = \{0, 1, \ldots, q-1\}$ – алфавит размера q. Произвольное подмножество $C \subseteq E_q^n$ называется q-ичным кодом и обозначается через $(n, N, d)_q$, где n – *длина* кода, N – число его кодовых слов (или *мощность*), и d – его *минимальное расстояние* (*Хэмминга*), т.е.

$$d = d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y},\ \boldsymbol{x}, \boldsymbol{y} \in C\},$$

где для $\boldsymbol{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, \ldots, y_n)$ из множества E^n

$$d(\boldsymbol{x}, \boldsymbol{y}) = |\{j : x_j \neq y_j,\ j = 1, \ldots, n\}|.$$

[1] Работа выполнена при поддержке Национального гранта правительства Испании PID2019-104664GB-I00 (AEI, 10.13039/501100011033).

[2] Исследования были выполнены в ИППИ им. А.А. Харкевича РАН в рамках проводимых фундаментальных исследований по теме “Математические теории корректирующих кодов”, а также поддержаны грантом Национального научного фонда Болгарии (номер проекта 20-51-18002).

Для случая, когда q – степень простого числа, а E – конечное поле порядка q, обозначаемое через $\mathbb{F}_q$, q-ичный $(n, N = q^k, d)_q$-код C является линейным пространством размерности k над $\mathbb{F}_q$, и для него используется стандартное обозначение $[n, k, d]_q$.

Для двоичных кодов принято обозначение (n, N, d) и $[n, k, d]$ (т.е. q опускается).

Расстоянием Ли $d_L(i, j)$ между символами i и j из E называется минимальная разность между этими символами по модулю q:

$$d_L(i, j) = \min\big\{|j - i|, q - |j - i|\big\}.$$

Это расстояние симметрично, т.е. $d_L(i, j) = d_L(j, i)$, и продолжается на векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ из E^n стандартным образом:

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} d_L(x_i, y_i).$$

Минимальное расстояние q-ичного кода $\mathcal{C}$ в метрике Ли определяется как

$$d_L = \min\{d_L(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y},\ \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}\}.$$

В случае, когда E – кольцо $\mathbb{Z}_q$, назовем q-ичный код $\mathbb{Z}_q$-*аддитивным*, или $\mathbb{Z}_q$-*линейным*, если он при этом является подгруппой группы $E^n = \mathbb{Z}_q^n$. В противном случае будем называть его нелинейным $\mathbb{Z}_q$-кодом, либо просто $\mathbb{Z}_q$-кодом.

Заметим, что в случае, когда $q = 2$, $\mathbb{Z}_q$-аддитивный код является линейным двоичным кодом, а в случае $q = 4$ – линейным четверичным или линейным $\mathbb{Z}_4$-кодом. В этой статье мы рассматриваем алфавит $E = \mathbb{Z}_q$.

Произвольный, не обязательно линейный, $\mathbb{Z}_q$-код можно рассматривать как двоичный код, получаемый с помощью отображения Грея. В работе [2] отображение Грея из $\mathbb{Z}_4$ на $\mathbb{Z}_2^2$ определено как

$$\varphi(0) = (0, 0), \quad \varphi(1) = (0, 1), \quad \varphi(2) = (1, 1), \quad \varphi(3) = (1, 0).$$

Существуют различные обобщения отображения Грея, действующие из $\mathbb{Z}_{2^s}$ в пространство $\mathbb{Z}_2^{2^{s-1}}$ (см. [3–6]). В работе Карле [3] отображение

$$\varphi\colon \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$$

определено как

$$\varphi(u) = (u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-2})Y, \tag{1}$$

где $u \in \mathbb{Z}_{2^s}$, $[u_0, u_1, \ldots, u_{s-1}]_2$ – двоичное представление числа u, т.е.

$$u = \sum_{i=0}^{s-1} 2^i u_i, \quad u_i \in \{0, 1\},$$

а Y – матрица размера $(s-1) \times 2^{s-1}$, столбцами которой являются элементы $\mathbb{Z}_2^{s-1}$. Заметим, что $(u_{s-1}, \ldots, u_{s-1})$ и $(u_0, \ldots, u_{s-2})Y$ являются двоичными векторами длины 2^{s-1} и что строки матрицы Y вместе со строкой, состоящей из одних единиц, образуют базис кода Рида – Маллера первого порядка.

В работе [7] показано, что обобщение Карле является специальным случаем обобщения, рассмотренного в работе [6], для которого имеет место равенство

$$\sum_{i=0}^{s-1} \lambda_i \varphi(2^i) = \varphi\Big(\sum_{i=0}^{s-1} \lambda_i 2^i\Big), \quad \lambda_i \in \{0, 1\}.$$

Далее, доопределим отображение для векторов

$$\Phi\colon \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$$

как покомпонентное отображение Грея φ. В этой статье мы используем новое отображение Грея, являющееся обобщением отображения Грея, рассмотренного в [6]. Новое отображение Грея определено на словах, являющихся строками матриц Адамара, для любого натурального числа q, такого что существует матрица Адамара порядка $q/2$.

Помимо фундаментальных кодовых параметров, двумя другими важными параметрами произвольных двоичных кодов являются *ранг* и *размерность ядра* кода. Рангом двоичного кода C является размерность его линейной оболочки $\langle C\rangle$. Ядро двоичного кода C длины n, введенное в [8] и обозначаемое через $\ker(C)$, образовано векторами, стабилизирующими код C:

$$\ker(C) = \{\boldsymbol{x} \in \mathbb{Z}_2^n : \boldsymbol{x} + C = C\}. \tag{2}$$

Если код C содержит нулевой вектор, т.е. вектор из одних нулей, то $\ker(C)$ является линейным подкодом C. Заметим, что если код C линейный, то $\ker(C) = C = \langle C\rangle$. Обозначим ранг двоичного кода C через $\mathrm{rank}(C)$, а размерность ядра – через $\dim(\ker(C))$.

Для кодов, содержащих нулевой вектор, ранг и размерность ядра могут быть использованы как достаточное условие неэквивалентности этих кодов, так как очевидно, что эквивалентные коды имеют одинаковый ранг и размерность ядра.

Матрица Адамара H порядка n – это квадратная матрица размера $n \times n$, состоящая из элементов $+1$ и -1, такая что выполнено условие $HH^T = nI$, где I – (двоичная) диагональная матрица размера $n \times n$, а H^T – транспонированная матрица H. Как известно [9], матрица Адамара H порядка n существует для n, равных 1, 2, либо кратных 4. Две матрицы Адамара эквивалентны, если одна переводится в другую перестановкой строк и/или столбцов и умножением строк и/или столбцов на строку/столбец, состоящий из одних элементов -1.

Поэтому всегда можно считать, что первая строка и первый столбец матрицы H состоят из элементов $+1$, получая таким образом эквивалентную матрицу, которую будем называть *нормализованной*. Если заменить $+1$ на 0, а -1 на 1, и добавить дополнительные строки (т.е. полученные заменой нулей на единицы и, наоборот, единиц на нули), то получим двоичный $(n, 2n, n/2)$-код, который будем называть (двоичным) кодом Адамара и обозначать через H_n (см. [9]). Мы всегда предполагаем, что матрица Адамара нормализована, и таким образом, соответствующий код Адамара содержит нулевое слово.

Пусть H – матрица Адамара порядка n. Обозначим через j_m столбец длины m, состоящий из одних единиц. Применяя перестановки строк и столбцов и умножая столбцы и строки матрицы H на -1, любые четыре столбца матрицы H можно (единственным образом) привести к следующему виду:

$$\begin{bmatrix}
j_a & j_a & j_a & j_a \\
j_a & j_a & -j_a & -j_a \\
j_a & -j_a & j_a & -j_a \\
j_a & -j_a & -j_a & j_a \\
j_b & j_b & j_b & -j_b \\
j_b & j_b & -j_b & j_b \\
j_b & -j_b & j_b & j_b \\
j_b & -j_b & -j_b & -j_b
\end{bmatrix}$$

Таблица 1

Число матриц Адамара различных типов порядка $n \leqslant 32$

Тип	Порядок							
	4	8	12	16	20	24	28	32
0	1	1	0	5	0	58	0	13680757
1	0	0	1	0	3	1	486	26369
2	0	0	0	0	0	1	1	2900
3	0	0	0	0	0	0	0	1

Таблица 2

Размерность ядра и ранг кода Адамара длины $n = 32$

$\dim(\ker(C))$	$\operatorname{rank}(C)$										
	6	7	8	9	10	11	12	13	14	15	16
6	$*$										
4		$*$									
3		$*$	$*$	$*$	$*$						
2			$\circ$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$
1			$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$

для некоторых натуральных чисел a, b, таких что $a + b = n/4$ и $0 \leqslant b \leqslant \lfloor n/8 \rfloor$. Следуя [10], будем говорить, что произвольный набор из четырех столбцов, который может быть приведен к такому виду, имеет тип b. Очевидно, что перестановки и смены знака строк и столбцов подматрицы из четырех столбцов не меняют тип. Матрица Адамара имеет тип b (где $0 \leqslant b \leqslant \lfloor n/8 \rfloor$), если у нее имеется набор из четырех столбцов типа b и нет набора из четырех столбцов типа, меньшего чем b.

Все матрицы Адамара порядка $n \leqslant 32$ классифицированы согласно своему типу. В частности, пользуясь соответствующей таблицей работы [11] и результатами для $n = 32$ из работ [11, 12], получается классификация, приведенная в табл. 1.

Заметим, что линейные коды Адамара являются кодами Рида – Маллера первого порядка, или, что эквивалентно, кодами, дуальными к расширенным кодам Хэмминга.

$\mathbb{Z}_{2^s}$-аддитивный код (т.е. код над $\mathbb{Z}_{2^s}$), образ которого под действием отображения Грея Φ является кодом Адамара, будем называть $\mathbb{Z}_{2^s}$-аддитивным кодом Адамара, а его образ под действием Φ будем называть $\mathbb{Z}_{2^s}$-линейным кодом Адамара. В работах [7, 13, 14] рассматривалось отображение Φ Карле [3] и изучались ранг, размерность ядра и эквивалентность $\mathbb{Z}_{2^s}$-линейных кодов Адамара. В работах [15, 16] приведены оценки на возможные значения ранга и размерности ядра кодов Адамара. Кроме того, приведены конструкции кодов Адамара для различных рангов и размерностей ядер. В частности, в работе [15] показано, что в дополнение к линейным кодам Адамара существует код Адамара длины $n = 2^t$, $t > 4$, с размерностью ядра k и рангом r для всех значений r, таких что

$$\begin{cases} t + 2 \leqslant r \leqslant 2^{t+1-k} + k - 1, & \text{если } 3 \leqslant k \leqslant t - 1, \\ t + 3 \leqslant r \leqslant 2^{t-1}, & \text{если } 1 \leqslant k \leqslant 2. \end{cases} \tag{3}$$

Например, в табл. 2 и 3 приведены все возможные значения этих параметров r и k (помеченные символами $*$, $\diamond$ и $\circ$, значение которых объясняется в § 4) для случаев $t = 5$ и $t = 6$ соответственно. В случае $t = 4$ существуют ровно пять неэквивалентных кодов Адамара [9, с. 266]. Один из них – линейный код Адамара с рангом и размерностью ядра, равными 5, и по одному коду Адамара для каждого из значений параметров $(r, k) \in \{(6, 3), (7, 2), (8, 2), (8, 1)\}$.

Таблица 3

Размерность ядра и ранг кода Адамара длины $n = 64$

$\dim(\ker(C))$	$\operatorname{rank}(C)$													
	7	8	9	10	11	12	13	...	17	18	19	20	...	32
7	*													
5		*												
4		*	*	*	○									
3		○	*	*	*	*	*	...	*	○				
2			◇	◇	◇	◇	◇	...	◇	◇	◇	◇	...	◇
1			◇	◇	◇	◇	◇	...	◇	◇	◇	◇	...	◇

Таблица 4

Размерность ядра и ранг кода Адамара длины $n = 48$

$\dim(\ker(C))$	$\operatorname{rank}(C)$					
	13	14	15	16	...	24
3	*	○				
2	◇	◇	◇	◇	...	◇
1	*	*	○	○	...	○

В [16] доказано существование кодов Адамара длины $n = 2^t \cdot s$ ($s \neq 1$ нечетное) ранга r и размерности ядра k для всех $r \in \{4s + t - 3, \ldots, n/2\}$ и $k \in \{1, \ldots, t - 1\}$ при условии существования кода Адамара длины $4s$. Кроме того, там же доказано, что существование кода Адамара длины $4s$, где $s \neq 1$ – нечетное число, влечет существование кода Адамара длины $n = 2^t s$ ($t \geqslant 3$) с размерностью ядра k и рангом r для всех значений r, таких что

$$4s + t - 3 \leqslant r \leqslant \begin{cases} 2^{t+1-k}s + k - 1, & \text{если } 3 \leqslant k \leqslant t - 1, \\ 2^{t-1}s, & \text{если } 1 \leqslant k \leqslant 2. \end{cases} \tag{4}$$

Например, для длины $n = 48$ в табл. 4 приведены все возможные значения для ранга и размерности ядра (помеченные символами $*$, $\diamond$ и $\circ$, значение которых объясняется в § 4). Нахождение точной нижней границы для ранга является открытой проблемой. Однако для случая, когда размерность ядра равна $t-1$ или $t-2$, точная нижняя оценка равна $4s + t - 3$. В работе [16] установлено, что для того чтобы доказать точность этой нижней границы, достаточно показать несуществование кодов Адамара с $k = 1$ и $r < 4s + t - 3$. Наименьшая длина, для которой это неизвестно, – это $n = 48$, где $k = 1$ и $r < 13$.

Цель настоящей статьи – описать новую общую конструкцию двоичных кодов (или матриц) Адамара, которые могут быть представлены как $\mathbb{Z}_q$-коды. Построение основано на обобщенной каскадной конструкции и на результатах и идеях работ [17–19]. Для случая $q = 4$ наша конструкция дает $\mathbb{Z}_4$-коды произвольной длины n (при условии существования матрицы Адамара порядка n) с минимальным расстоянием Ли, равным n, которые после применения известного отображения Грея дают двоичные коды Адамара длины $2n$. Для кодов Адамара длины 16, 32, 48 и 64 мы приводим примеры конструкции кодов Адамара почти для всех возможных значений ранга и размерности ядра, а также приводим новые нижние оценки числа таких неэквивалентных кодов с фиксированным рангом и размерностью ядра. Оказалось, что в специальном случае наша конструкция совпадает с кронекеровской (или конструкцией Сильвестра), и может считаться вариантом известной в настоящее время [1] модифицированной конструкции Сильвестра, которая использует одну матрицу Адамара порядка m, а также m (не обязательно различных) матриц Адамара порядка k.

Здесь мы обобщаем эту модифицированную конструкцию, предложив новую более общую конструкцию типа Сильвестра, основанную уже на двух семействах (не обязательно различных) матриц Адамара, а именно на k матрицах порядка m и m матрицах порядка k. Результирующая матрица Адамара имеет порядок mk, как и в конструкции из [1].

§ 2. Построение $\mathbb{Z}_q$-кодов в метрике Ли

Для независимости изложения вкратце повторим конструкцию q-ичных кодов в метрике Ли, введенную в [20, 21]. Пусть имеется алфавит $E = \{0, 1, \ldots, q-1\}$ размера q. Пронумеруем элементы алфавита: $E = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Предположим, что q можно представить в виде произведения $q = q_1 q_2 \ldots q_s$, где все q_i – произвольные натуральные числа, упорядоченные произвольным образом. Это разложение на множители мы используем для нумерации элементов алфавита E. Определим числа

$$Q_j = \frac{q}{q_1 q_2 \ldots q_j}, \quad j = 1, \ldots, s.$$

Сначала разобьем E на q_1 подмножеств E_i размера Q_1:

$$E = E_0 \cup \ldots \cup E_{q_1-1}, \quad E_i = \{i + j \cdot q_1 : \ j = 0, \ldots, Q_1 - 1\}.$$

Затем сделаем то же самое для каждого множества E_i:

$$E_i = E_{i,0} \cup E_{i,1} \cup \ldots \cup E_{i,q_2-1},$$

где

$$E_{i,j} = \{i + j \cdot q_1 + k \cdot q_1 q_2 : \ k = 0, \ldots, Q_2 - 1\},$$

и так далее. Эта процедура повторяется s шагов, в результате которых получаем подмножества $E_{i_1,\ldots,i_{s-1}}$ размера $Q_{s-1} = q_s$, такие что

$$E = \bigcup_{i_1=0}^{q_1-1} \ldots \bigcup_{i_{s-1}=0}^{q_{s-1}-1} E_{i_1,\ldots,i_{s-1}}, \tag{5}$$

где каждое множество $E_{i_1,\ldots,i_{s-1}}$ содержит q_s элементов. Каждому элементу a из алфавита E размера q с разложением $q = q_1 q_2 \ldots q_s$ приписывается номер, а именно его вектор индексов $L(a) = (i_1, i_2, \ldots, i_{s-1}, i_s)$, если элемент a принадлежит подмножеству $E_{i_1,\ldots,i_{s-1}}$ и имеет индекс i_s в множестве $E_{i_1,\ldots,i_{s-1}}$, где элементы $E_{i_1,\ldots,i_{s-1}}$ упорядочены по возрастанию.

Таким образом, каждому элементу из E ставится в соответствие его номер, представляющий собой целочисленный вектор $L(a) = (i_1, \ldots, i_s)$ длины s, удовлетворяющий следующему свойству: *j-й индекс i_j принадлежит множеству* $\{0, 1, \ldots, q_j - 1\}$. Определим обратное отображение:

$$L^{-1}(i_1, i_2, \ldots, i_s) = a.$$

Легко видеть, что вектор $L(a)$ является $(q_1, \ldots, q_s)$-разложением числа a, а именно

$$L(a) = (i_1, i_2, \ldots, i_s), \quad a = L^{-1}(i_1, i_2, \ldots, i_s),$$

где

$$a = \sum_{j=1}^{s} i_j \cdot q_1 \ldots q_{j-1} \quad \text{и} \quad q_0 = 1.$$

Конструкция. Пусть задано множество $E = \{0, 1, \ldots, q-1\}$ размера q, где q представимо в виде произведения s натуральных чисел $q = q_1 q_2 \ldots q_s$. Предположим, что имеется s кодов A_j (одной и той же длины), $j = 1, \ldots, j$, где код A_j над алфавитом $E_{q_j} = \{0, 1, \ldots, q_j - 1\}$ размера q_j имеет параметры $(n, N_j, d_j)_{q_j}$. Из каждого кода A_j, $j = 1, \ldots, s$, выберем по произвольному кодовому слову $\boldsymbol{a}^{(j)} = (a_1^{(j)}, \ldots, a_n^{(j)})$. Для каждого i, $i = 1, \ldots, n$, построим вектор $\boldsymbol{b}_i = (a_i^{(1)}, \ldots, a_i^{(s)})$ из i-х координат s векторов $\boldsymbol{a}^{(j)}$, $j = 1, \ldots, s$. Очевидно, что элемент j-й позиции этого вектора $\boldsymbol{b}_i$ принадлежит алфавиту размера q_j, поскольку это как раз алфавит кода A_j. Отсюда следует, что любой такой вектор является вектором индексов $L(a)$ некоторого элемента a_i из множества E, который имеет такой номер, т.е. $L(a_i) = (a_i^{(1)}, \ldots, a_i^{(s)})$. Зададим кодовое слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ над E нового результирующего кода $\mathcal{C}$, заменяя каждый i-й вектор $\boldsymbol{b}_i$ элементом $c_i = L^{-1}(\boldsymbol{b}_i)$, индексный вектор которого $L(c_i)$ совпадает с вектором $\boldsymbol{b}_i$, т.е. $L(c_i) = \boldsymbol{b}_i$. Это означает, что на i-й позиции кодового слова $\boldsymbol{c} = (c_1, \ldots, c_n)$ стоит элемент c_i, т.е. что $c_i = L^{-1}(\boldsymbol{b}_i)$. Когда все кодовые слова $\boldsymbol{a}^{(j)}$ пробегают все внешние коды A_j для всех $j = 1, \ldots, s$, соответствующие кодовые слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ пробегают весь код $\mathcal{C}$.

Теорема 1 [20, 21]. *Пусть задано множество $E = \{0, 1, \ldots, q-1\}$ размера q, где q представимо в виде произведения s натуральных чисел $q = q_1 q_2 \ldots q_s$. Предположим, что имеются s внешних q_j-ичных кодов A_j, $j = 1, \ldots, s$, с параметрами $(n, N_j, d_j)_{q_j}$. Тогда описанная выше конструкция приводит к q-ичному коду C над алфавитом E с параметрами*

$$n, \quad N = \prod_{j=1}^{s} N_j, \quad d_L = \min\{d_1, q_1 d_2, q_1 q_2 d_3, \ldots, q_1 q_2 \ldots q_{s-1} d_s\}.$$

В следующем параграфе мы представим общую конструкцию кодов в метрике Ли над алфавитом $\mathbb{Z}_q$, которые под действием отображения Грея становятся двоичными $(n, 2n, n/2)$-кодами Адамара.

§ 3. Построение $\mathbb{Z}_q$-кодов Адамара

В работах [20,21] было замечено, что при существовании двоичного кода Адамара длины n теорема 1 порождает q-ичный код Адамара той же длины n в метрике Ли над алфавитом $\mathbb{Z}_4$, из которого под действием отображения Грея получается двоичный код Адамара (в метрике Хэмминга) длины $2n$. Объясним этот результат как начальный шаг к пояснению более общей конструкции.

Пусть $E = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$, а значит, $q_1 = q_2 = 2$. Произвольному элементу a из E поставим в соответствие вектор индексов $L(a) = (i_1, i_2)$, являющийся двоичным представлением числа a, т.е. $a = i_1 + 2\, i_2$, где $i_1, i_2 \in \mathbb{Z}_2$. Пусть n – некоторое натуральное число, такое что существует двоичный $(n, 2n, n/2)$-код Адамара H_n, и пусть A_1 – тривиальный $(n, 2, n)$-код, состоящий из пары дополнительных векторов длины n. Пусть $\boldsymbol{h} = (h_1, \ldots, h_n)$ – произвольное кодовое слово кода H_n, а $\boldsymbol{a} = (a_1, \ldots, a_n)$ – одно из двух кодовых слов кода A_1. Для такой пары выбранных слов поставим в соответствие слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{h}) = (c_1, c_2, \ldots, c_n)$ нового кода, где $c_i = L^{-1}(a_i, h_i)$ – элемент из $\mathbb{Z}_4$. Таким образом мы получаем новый код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ с параметрами $(n, 4n, d_L = n)_4$, где d_L – расстояние Ли, а значит, отображение Грея порождает двоичный $(2n, 4n, n)$-код Адамара H_{2n} [20, 21].

Теорема 2 [20,21]. *Пусть H_n – двоичный $(n, 2n, n/2)$-код Адамара. Тогда конструкция, приведенная в теореме* 1, *дает код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ с параметрами $(n, 4n, d_L = n)_4$, который под действием отображения Грея индуцирует двоичный $(2n, 4n, n)$-код Адамара H_{2n}.*

Новый код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ сохраняет ряд свойств изначального кода Адамара H_n. Необходимо отметить, что в работе [22] были классифицированы все линейные $\mathbb{Z}_2\mathbb{Z}_4$-коды Адамара. Цель настоящей статьи – показать, какие коды могут быть получены общей конструкцией, приведенной в теореме 1 для произвольного $q > 4$. В частности, главной целью является изучение значений q, для которых существуют $\mathbb{Z}_q$-коды Адамара. Однако поясним сначала, что подразумевается под $\mathbb{Z}_q$-кодом Адамара, или, что эквивалентно, кодом Адамара над $\mathbb{Z}_q$.

Поскольку отображение Грея существует только для случая $q = 4$, нам придется для случаев $q > 4$ использовать другие отображения множества E в двоичные векторы. Как мы уже упоминали ранее, одно из таких возможных отображений было предложено Карле [3]. В частности, для $q = 2^s$ элементы алфавита E отображаются в кодовые слова линейного $[q/2, q, q/4]$-кода Адамара $H_{q/2}$, и таким образом, конструкцию можно рассматривать как каскадный код второго порядка с кодом Адамара в качестве внутреннего кода [17]. В работе [6] Кротов слегка обобщил отображение Грея – Карле, предложив использовать в качестве внутреннего кода произвольный код Адамара. Мы модифицируем оба отображения, используя идеи обобщенной каскадной конструкции [17, 19].

Пусть q – целое число, такое что существует двоичный код Адамара $H_{q/2}$. Предположим, что элементы $\mathbb{Z}_q$ пронумерованы в соответствии с разложением числа q, а именно пусть $q = q_1 \cdot q_2$, где $q_1 = q/2$ и $q_2 = 2$. Таким образом, произвольному $a \in \mathbb{Z}_q$ ставим в соответствие вектор индексов $L(a) = (i_1, i_2)$, где $i_1 \in \mathbb{Z}_{q/2}$ и $i_2 \in \mathbb{Z}_2$, причем

$$\{0, 1\} = \mathbb{Z}_2 \subset \mathbb{Z}_{q/2} \subset \mathbb{Z}_q = \{0, 1, \ldots, q-1\}.$$

Предположим, что $H_{q/2}$ – двоичный $(q/2, q, q/4)$-код Адамара, кодовые слова которого $\boldsymbol{h}_i$, $i = 0, 1, \ldots, q-1$, пронумерованы таким образом, что для произвольного $i = 0, 1, \ldots, q/2 - 1$ имеет место следующее равенство:

$$d_H(\boldsymbol{h}_i, \boldsymbol{h}_{i+q/2}) = q/2. \tag{6}$$

Для произвольного элемента $a \in \mathbb{Z}_q$ с вектором индексов $L(a) = (i_1, i_2)$ определим следующее отображение $\Phi(a, H_{q/2})$ (являющееся переформулировкой отображений из [3, 6]) в множество кодовых слов кода Адамара $H_{q/2}$:

$$\boldsymbol{h}_a = \Phi(a, H_{q/2}) = \boldsymbol{h}_{i_1 + i_2 q/2} = \boldsymbol{h}_{i_1} + i_2(1, 1, \ldots, 1). \tag{7}$$

Это отображение может быть естественным образом продолжено на векторы $\boldsymbol{u} = (u_1, \ldots, u_m)$ над $\mathbb{Z}_q$, отображающиеся в двоичные векторы длины $qm/2$:

$$\boldsymbol{c} = \Phi(\boldsymbol{u}, H_{q/2}) = (\boldsymbol{h}_{u_1}, \ldots, \boldsymbol{h}_{u_m}), \tag{8}$$

а также для множеств U векторов над алфавитом $\mathbb{Z}_q$:

$$\Phi(U, H_{q/2}) = \{\Phi(\boldsymbol{u}, H_{q/2}) : \boldsymbol{u} \in U\}. \tag{9}$$

Определение 1. Будем называть $\mathbb{Z}_q$-код $\mathcal{C}$ длины m и мощности $N = qm$ *$\mathbb{Z}_q$-кодом Адамара*, если его образ $C = \Phi(\mathcal{C}, H_{q/2})$ является двоичным $(qm/2, qm, qm/4)$-кодом Адамара $H_{qm/2}$.

Теорема 3. *Пусть q и m – натуральные числа, такие что существуют матрицы Адамара $H_{q/2}$ и H_m порядков $q/2$ и m. Тогда конструкция, заданная в теореме* 1, *дает $\mathbb{Z}_q$-код Адамара $\mathcal{C}$ длины m, такой что его образ $C = \Phi(\mathcal{C}, H_{q/2})$, заданный отображениями* (7)–(9), *представляет собой двоичный $(qm/2, qm, qm/4)$-код Адамара $H_{qm/2}$.*

Доказательство. В качестве кода $A_1 = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{q/2-1}\}$ возьмем тривиальный $(m, q/2, m)_{q/2}$-код U, состоящий из $q/2$ кодовых слов $\boldsymbol{a}_i$ над алфавитом $\mathbb{Z}_{q/2}$. В качестве кода A_2 возьмем $(m, 2m, m/2)$-код Адамара $H_m = \{\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{2m-1}\}$. По построению, приведенному в теореме 1, получаем $\mathbb{Z}_q$-код $\mathcal{C}$ длины m и мощности qm с минимальным расстоянием Ли

$$d_L = \min\{m, 2 \cdot m/2\} = m.$$

Мы утверждаем, что $\mathcal{C}$ является $\mathbb{Z}_q$-кодом Адамара. Чтобы убедиться в этом, возьмем произвольный двоичный $(q/2, q, q/4)$-код Адамара $H_{q/2}$ с кодовыми словами $\{\boldsymbol{h}_0, \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{q-1}\}$, пронумерованными так, что для произвольного i, $i = 0, 1, \ldots, q/2-1$, кодовые слова $\boldsymbol{h}_i$ и $\boldsymbol{h}_{i+q/2}$ находятся на расстоянии Хэмминга $q/2$. Рассмотрим двоичный код $C = \Phi(\mathcal{C}, H_{q/2})$. Ясно, что длина кода C равна $n = qm/2$, а его мощность $N = qm$. Необходимо проверить, что минимальное расстояние (Хэмминга) составляет $qm/4$. Рассмотрим два кодовых слова $\boldsymbol{c}_1 = \Phi(\boldsymbol{v}_1, H_{q/2})$ и $\boldsymbol{c}_2 = \Phi(\boldsymbol{v}_2, H_{q/2})$ кода C. Предположим, что $\boldsymbol{v}_1$ получено из кодовых слов $\boldsymbol{a}_{i_1} \in A_1$ и $\boldsymbol{b}_{j_1} \in H_m$, а $\boldsymbol{v}_2$ – из кодовых слов $\boldsymbol{a}_{i_2} \in A_1$ и $\boldsymbol{b}_{j_2} \in H_m$. В соответствии с конструкцией векторы $\boldsymbol{v}_1 = (v_{1,1}, \ldots, v_{1,m})$ и $\boldsymbol{v}_2 = (v_{2,1}, \ldots, v_{2,m})$ представляются в виде

$$\boldsymbol{v}_1 = \boldsymbol{a}_{i_1} + \frac{q}{2}\boldsymbol{b}_{j_1}, \quad \boldsymbol{v}_2 = \boldsymbol{a}_{i_2} + \frac{q}{2}\boldsymbol{b}_{j_2}, \tag{10}$$

где покомпонентное сложение производится в кольце $\mathbb{Z}_q$ и при этом мы полагаем, что $\mathbb{Z}_{q/2} \subset \mathbb{Z}_q$. Необходимо рассмотреть два случая: (i) $\boldsymbol{a}_{i_1} = \boldsymbol{a}_{i_2}$ и (ii) $\boldsymbol{a}_{i_1} \neq \boldsymbol{a}_{i_1}$.

Сначала предположим, что $\boldsymbol{a}_{i_1} = \boldsymbol{a}_{i_2}$. Из этого следует, что $\boldsymbol{b}_{j_1} \neq \boldsymbol{b}_{j_2}$. Значит, эти слова различаются в $m/2$ позициях, из чего, в свою очередь, следует, что слова $\boldsymbol{v}_1$ и $\boldsymbol{v}_2$ находятся на расстоянии $d_H(\boldsymbol{v}_1, \boldsymbol{v}_2) = m/2$. Однако для каждой s-й позиции, в которой они различны (т.е. когда $v_{1,s} \neq v_{2,s}$), в соответствии с (10) имеет место равенство

$$d_L(v_{1,s}, v_{2,s}) = |v_{1,s} - v_{2,s}| = q/2,$$

из чего опять вытекает, что под действием отображения $\Phi(\mathcal{C}, H_{q/2})$ согласно условию (6) каждая такая позиция увеличивает расстояние Хэмминга ровно на $q/2$ (а не на $q/4$). Следовательно, общий вклад в расстояние Хэмминга будет $m/2 \cdot q/2$, из чего следует, что в этом случае $d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) = qm/4$.

Теперь предположим, что $\boldsymbol{a}_{i_1} \neq \boldsymbol{a}_{i_2}$. Из этого следует, что $d_H(\boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}) = m$. Поскольку для любой пары кодовых слов $\boldsymbol{b}_i, \boldsymbol{b}_j \in H_{q/2}$ выполнено условие $d_H(\boldsymbol{b}_i, \boldsymbol{b}_j) \geqslant$ $\geqslant q/4$, из этого также следует, что $d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) = qm/4$. Таким образом, получаем, что результирующий код $C = \Phi(\mathcal{C}, H_{q/2})$ имеет минимальное расстояние Хэмминга $d_H(C) = qm/4$, откуда (учитывая его длину $m\,q/2$ и мощность $m\,q$) заключаем, что результирующий код C – это двоичный код Адамара $H_{qm/2}$. ▲

Определение 2. Для заданных натуральных чисел $q \geqslant 2$ и $m \geqslant 4$, двоичного вектора $\boldsymbol{a} = (a_1, \ldots, a_m)$ и вектора $\boldsymbol{v} = (v_1, \ldots, v_m)$ длины m над алфавитом $\mathbb{Z}_{q/2}$ обозначим через $\Psi(\boldsymbol{v}, \boldsymbol{a})$ следующее отображение этой пары векторов в вектор $\boldsymbol{u}$ длины m над алфавитом $\mathbb{Z}_q$:

$$\boldsymbol{u} = \Psi(\boldsymbol{v}, \boldsymbol{a}) = \Big(v_1 + a_1\frac{q}{2},\ v_2 + a_2\frac{q}{2},\ \ldots,\ v_m + a_m\frac{q}{2}\Big),$$

где покомпонентное сложение производится в кольце $\mathbb{Z}_q$ и мы предполагаем, что $\mathbb{Z}_{q/2} \subset \mathbb{Z}_q$. Пусть теперь $\boldsymbol{v}$ пробегает некоторое множество V, а $\boldsymbol{a}$ – некоторое множество A, тогда определим соответствующее множество результирующих векторов над алфавитом $\mathbb{Z}_q$:

$$\mathcal{C} = \Psi(V, A) = \{\Psi(\boldsymbol{v}, \boldsymbol{a}) :\ \boldsymbol{v} \in V,\ \boldsymbol{a} \in A\}. \tag{11}$$

Теперь опишем обобщенную конструкцию $\mathbb{Z}_q$-кодов Адамара. Рассмотрим множество

$$S_H(q/2) = \{H_{q/2}(i) : \ i = 1, \ldots, s_{q/2}\},$$

состоящее из $s_{q/2}$ различных двоичных $(q/2, q, q/4)$-кодов Адамара $H_{q/2}(i)$. Предположим, что кодовые слова каждого из кодов $H_{q/2}(i)$ пронумерованы:

$$H_{q/2}(i) = \{\boldsymbol{h}_0^{(i)}, \boldsymbol{h}_1^{(i)}, \ldots, \boldsymbol{h}_{q-1}^{(i)}\},$$

причем таким образом, что для произвольного i и произвольного $j = 0, 1, \ldots, q/2-1$ кодовые слова $\boldsymbol{h}_j^{(i)}$ и $\boldsymbol{h}_{j+q/2}^{(i)}$ находятся на расстоянии $q/2$ друг от друга, т.е. выполнено условие (6). Обобщим отображение, заданное формулой (8).

Определение 3. Пусть $S_H(q/2)$ – множество, состоящее из $s_{q/2}$ различных кодов Адамара

$$H_{q/2}(i) = \{\boldsymbol{h}_0^{(i)}, \boldsymbol{h}_1^{(i)}, \ldots, \boldsymbol{h}_{q-1}^{(i)}\}, \quad i = 1, \ldots, s_{q/2},$$

с нумерацией кодовых слов, удовлетворяющих условию (6). Пусть $\boldsymbol{f} = (f_1, \ldots, f_m)$ – произвольный вектор длины m над алфавитом $\{1, 2, \ldots, s_{q/2}\}$, а $\boldsymbol{u} = (u_1, \ldots, u_m)$ – произвольный вектор длины m над алфавитом $\mathbb{Z}_q$. Определим следующее отображение $\Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2))$ из векторов $\boldsymbol{f}$ и $\boldsymbol{u}$ в двоичный вектор $\boldsymbol{c}$ длины $n = qm/2$:

$$\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2)) = \left(\boldsymbol{h}_{u_1}^{(f_1)}, \boldsymbol{h}_{u_2}^{(f_2)}, \ldots, \boldsymbol{h}_{u_m}^{(f_m)}\right). \tag{12}$$

Соответственно, обозначим через $\Phi(U, \boldsymbol{f}, S_H(q/2))$ отображение из множества U таких векторов $\boldsymbol{u}$ длины m над алфавитом $\mathbb{Z}_q$ в множество C двоичных векторов $\boldsymbol{c}$:

$$C = \Phi(U, \boldsymbol{f}, S_H(q/2)) = \{\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2)) : \ \boldsymbol{u} \in U\}. \tag{13}$$

Следующее утверждение является обобщением теоремы 3.

Теорема 4. *Пусть $q \geqslant 4$ и $m \geqslant 2$ – произвольные натуральные числа, для которых существуют матрицы Адамара порядков $q/2$ и m. Пусть $S_H(q/2)$ – множество, состоящее из $s_{q/2}$ различных кодов Адамара $H_{q/2}(i)$, $i = 1, \ldots, s_{q/2}$. Тогда для произвольного $(m, 2m, m/2)$-кода Адамара H_m, тривиального $(m, q/2, m)_{q/2}$-кода V и произвольного вектора $\boldsymbol{f} = (f_1, \ldots, f_m)$ длины m над алфавитом $\{1, 2, \ldots, s_{q/2}\}$ результирующий двоичный код*

$$C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(q/2)), \quad \textit{где } \mathcal{C} = \Psi(V, H_m), \tag{14}$$

является двоичным $(qm/2, qm, qm/4)$-кодом Адамара $H_{qm/2}$.

Доказательство. В соответствии с определением отображения Φ кодовые слова $\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2))$ кода C имеет следующую блоковую структуру: $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$, где $\boldsymbol{c}_i$ – подвектор длины $q/2$, являющийся некоторым кодовым словом $\boldsymbol{h}_j^{(f_i)}$ кода Адамара $H_{q/2}(f_i)$, где f_i – элемент, стоящей на i-й позиции вектора $\boldsymbol{f}$. Таким образом, произвольное кодовое слово $\boldsymbol{c}$ кода C имеет в качестве i-го блока некоторое слово кода $H_{q/2}(f_i)$. Поскольку все коды $H_{q/2}(i)$ имеют одинаковое минимальное расстояние, а нумерация их кодовых слов удовлетворяет условию (6), то вклад в расстояние (Хэмминга) между различными кодовыми словами $\boldsymbol{c}$ и $\boldsymbol{c}'$ не зависит от индекса f_i. Таким образом, утверждение теоремы вытекает из предыдущей теоремы 3. ▲

§ 4. Примеры построения кодов Адамара

Для заданного множества $S_H(n) = \{H_n(i) : i = 1, \ldots, s_n\}$ двоичных $(n, 2n, n/2)$-кодов Адамара обозначим через $r_n(i)$ двоичный ранг кода $H_n(i)$, а через $k_n(i)$ – размерность ядра кода $H_n(i)$. Представляет интерес следующий вопрос: *знаем ли мы ранг и размерность ядра кодов Адамара, построенных конструкцией, введенной в теореме* 4? Ясно, что для того чтобы ранг был как можно больше, необходимо выбрать коды V_i с попарно различными столбцами, а в качестве векторов f_i – векторы с различными компонентами. Для того чтобы размерность ядра была большой, необходимо уменьшить число различных столбцов в кодах V_i и число различных компонент в векторах f_i. Примеры, приведенные в данном параграфе для случаев $n = 16$, 32, 48, 64, демонстрируют сложность данного вопроса.

Пример 1. Пусть $q = 8$ и $m = 4$. Пусть множество

$$S_H(4) = \{H_4(1), H_4(2), H_4(3)\}$$

состоит, например, из трех (т.е. $s_4 = 3$) различных кодов Адамара длины 4, где каждый код $H_4(i)$ задается множеством слов, образующих матрицу Адамара порядка 4, в объединении с множеством их дополнительных слов, которое обозначается через $\bar{H}$:

$$H_4(1) = \{(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1)\} \cup \bar{H},$$
$$H_4(2) = \{(0,0,0,0), (0,1,1,0), (0,1,0,1), (0,0,1,1)\} \cup \bar{H},$$
$$H_4(3) = \{(0,0,0,0), (1,1,0,0), (0,1,1,0), (0,1,0,1)\} \cup \bar{H}.$$

Пусть V_i – следующие тривиальные $(4,4,4)_4$-коды над алфавитом $\mathbb{Z}_4$, $i = 0, \ldots, 4$:

$$V_0 = \{(k,k,k,k) : k \in \{0,1,2,3\}\},$$
$$V_1 = \{(0,0,0,0), (1,1,1,2), (3,2,2,1), (2,3,3,3)\},$$
$$V_2 = \{(0,0,0,0), (1,3,2,1), (3,2,1,2), (2,1,3,3)\},$$
$$V_3 = \{(0,0,0,0), (1,1,1,1), (3,2,2,3), (2,3,3,2)\},$$
$$V_4 = \{(0,0,0,0), (1,2,2,3), (2,3,1,2), (3,1,3,1)\}.$$

В качестве вектора $\boldsymbol{f}$ можно взять один из $3^4 = 81$ векторов длины 4 над алфавитом $\{1,2,3\}$. В качестве кода Адамара H_4 длины $m = 4$ выберем, например, $H_4 = H_4(2)$. Тогда можно построить $\mathbb{Z}_8$-код Адамара $\mathcal{C}$ длины 4 с $|H_4| \cdot |V_i| = 8 \cdot 4 = 32$ кодовыми словами, полагая $\mathcal{C} = \Psi(V_i, H_4)$, что дает $(16, 32, 8)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$. С помощью системы компьютерной алгебры Magma [23] мы проверили, что все такие коды Адамара длины 16 являются либо линейными (с рангом и размерностью ядра, равными 5), либо нелинейными с рангом 6 и размерностью ядра 3. Кроме того, для длины 16 известно, что с точностью до эквивалентности существует ровно один код для каждого такого параметра. Следовательно, возможными значениями для параметров (r,k) являются $\{(5,5), (6,3)\}$, и не существует кодов с размерностью ядра 2 или 1. Другими словами, мы можем получить коды Адамара для всех возможных пар значений (r,k), таких что $k \geqslant 3$. Интересный факт был получен из результатов компьютерных вычислений. Было замечено, что для любого кода V_i, $i = 0, \ldots, 4$, получающийся $(16, 32, 8)$-код Адамара является линейным, если и только если используемый вектор $\boldsymbol{f} = (f_1, f_2, f_3, f_4)$ удовлетворяет следующему условию:

$$f_1 + f_2 + f_3 + f_4 \equiv 0 \pmod 2,$$

и соответственно является нелинейным в противном случае. Более того, если теперь вместо $H_4 = H_4(2)$ выбрать другую матрицу – $H_4 = H_4(1)$ либо $H_4 = H_4(3)$, то результат не меняется.

Таблица 5

Число неэквивалентных $(32, 64, 16)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$ относительно общего числа

k	r										
	6	7	8	9	10	11	12	13	14	15	16
6	1/3										
4		1/38									
3		1/40	1/23	5/120	3/32						

Пример 2. Пусть $q = 16$ и $m = 4$. В качестве кода Адамара H_4 длины 4 возьмем код из примера 1. Пусть V – следующий тривиальный $(4, 8, 4)_8$-код над алфавитом $\mathbb{Z}_8$:

$$V = \{(0,0,0,0), (1,2,3,4), (2,3,4,5), (3,4,5,6), (4,5,6,7), (5,6,7,1), (6,7,1,2), (7,1,2,3)\}.$$

На основе этих кодов с помощью нашей конструкции можно построить $\mathbb{Z}_{16}$-код Адамара $\mathcal{C} = \Psi(V, H_4)$ длины 4 и мощности $|H_4| \cdot |V| = 8 \cdot 8 = 64$. В качестве различных кодов Адамара длины 8 выберем следующие четыре кода Адамара

$$S_H(8) = \{H_8(1), H_8(2), H_8(3), H_8(4)\}$$

(т.е. $s_8 = 4$), которые мы задаем половиной кодовых слов (так как вторая, обозначенная через $\bar{H}$, однозначно определяется первой):

$$H_8(1) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (0,0,0,0,1,1,1,1) \\ (0,0,1,1,0,0,1,1) \\ (0,0,1,1,1,1,0,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,0,1,0,1,0,1) \\ (0,1,0,1,1,0,1,0) \\ (0,1,1,0,0,1,1,0) \\ (0,1,1,0,1,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(2) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (1,1,1,0,1,0,0,0) \\ (1,0,1,1,0,1,0,0) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (1,0,0,0,1,1,0,1) \\ (1,1,0,0,0,1,1,0) \\ (1,0,1,0,0,0,1,1) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(3) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (1,1,1,0,1,0,0,0) \\ (0,1,0,0,1,0,1,1) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,1,1,0,0,1,0) \\ (1,1,0,0,0,1,1,0) \\ (0,1,0,1,1,1,0,0) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(4) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (0,0,0,1,0,1,1,1) \\ (0,1,0,0,1,0,1,1) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,1,1,0,0,1,0) \\ (0,0,1,1,1,0,0,1) \\ (1,0,1,0,0,0,1,1) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H}.$$

Используя все возможные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4\}$, получаем 256 различных $(32, 64, 16)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$. Все эти коды имеют тип 0. Можно получить коды Адамара для всех возможных значений параметров (r, k) при условии, что $k \geqslant 3$, т.е. всех пар параметров с символом $*$ в табл. 2. С помощью системы компьютерной алгебры Magma [23] мы получили коды Адамара длины 32, параметры (r, k) которых приведены в табл. 5. В таблице указано число неэквивалентных кодов Адамара относительно общего числа различных кодов для всех возможных пар (r, k). Кроме того, табл. 6 показывает значения $\boldsymbol{f}$ для соответствующих неэквивалентных кодов.

Таблица 6

Значения векторов $\boldsymbol{f}$ для неэквивалентных $(32, 64, 16)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$

r	k	$\boldsymbol{f}$
6	6	$(2,2,2,2)$
7	4	$(4,2,2,2)$
7	3	$(3,2,2,2)$
8	3	$(3,2,2,1)$
9	3	$(1,1,1,1)$, $(2,2,1,1)$, $(1,3,1,1)$, $(2,2,2,1)$, $(4,3,2,1)$
10	3	$(2,1,1,1)$, $(1,2,1,1)$, $(3,2,1,1)$

Пример 3. Пусть $q = 8$ и $m = 8$. Пусть H_8 – код Адамара $H_8(1)$, заданный в примере 2, а $S_H(4)$ – множество из трех кодов, заданных в примере 1. Рассматривая тривиальный код

$$V = \{(0,0,0,0,0,0,0,0), (1,3,3,2,1,3,1,2), (3,1,2,1,3,2,2,1), (2,2,1,3,2,1,3,3)\},$$

можно построить $3^8 = 6561$ различных $(32, 64, 16)$-кодов Адамара: один линейный (при выборе $\boldsymbol{f} = (1,1,1,1,1,1,1,1)$) и два неэквивалентных (например, когда $\boldsymbol{f} = (1,1,1,1,1,1,1,2)$ и $\boldsymbol{f} = (1,1,1,1,1,1,2,2)$) кода типа 0 ранга 7 с ядром размерности 4. Таким образом, мы строим коды для всех возможных пар (r, k), таких что $k \geqslant 4$. Кроме того, мы получаем коды, не эквивалентные кодам из примера 2.

Пример 4. Пусть $q = 32$ и $m = 4$. Пусть H_4 будет тем же кодом Адамара, что и в примере 1, а V_i, $i \in \{1, 2\}$, – следующие тривиальные $(4, 16, 4)_{16}$-коды над алфавитом $\mathbb{Z}_{16}$:

$$V_1 = \{(k,k,k,k) : \ k \in \{0, \ldots, 15\}\}$$

и

$$V_2 = \{(k,k,k,k) : \ k \in \{0, \ldots, 7, 10, \ldots 15\}\} \cup \{(8,9,8,9), (9,8,9,8)\}.$$

С этими исходными кодами мы можем построить $\mathbb{Z}_{32}$-коды $\mathcal{C}$ длины 4 мощности $|H_4| \cdot |V_i| = 8 \cdot 16 = 128$, полагая $\mathcal{C} = \Psi(V_i, H_4)$, $i \in \{1, 2\}$. Пусть

$$S_H(16) = \{H_{16}(1), H_{16}(2), H_{16}(3), H_{16}(4), H_{16}(5)\}$$

– множество из пяти попарно неэквивалентных кода Адамара длины 16, приведенных в [23], которые были описаны в 1933 г. в работе [24] (см. также [25, 26]). Рассматривая различные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4, 5\}$, получаем 625 различных $(64, 128, 32)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$. В табл. 7 для данных тривиальных кодов V_1 и V_2 приводится число неэквивалентных кодов Адамара в зависимости от ранга и размерности ядра. Заметим, что можно получить коды Адамара для всех возможных пар (r, k), таких что $k \geqslant 3$, за исключением случаев $(11, 4)$, $(8, 3)$, и $(18, 3)$ (т.е. для пар (r, k), обозначенных символом $*$ в табл. 3). Выбирая максимальное значение для каждой пары (r, k), мы получаем по крайней мере 137 неэквивалентных кодов. И наконец, в табл. 8 приведены значения векторов $\boldsymbol{f}$, для которых мы можем построить коды Адамара для каждой из возможных пар параметров (r, k), используя коды V_1 и V_2.

Пример 5. Пусть $q = 8$ и $m = 12$. Пусть $S_H(4)$ – такое же множество, как в примере 1, с $s_4 = 3$ различными кодами Адамара длины 4. Пусть V_0 – тривиальный $(12, 4, 12)_4$-код над алфавитом $\mathbb{Z}_4$:

$$V_0 = \{(k,k,k,k,k,k,k,k,k,k,k,k) : \ k \in \{0,1,2,3\}\}.$$

Таблица 7

Неэквивалентные $(64, 128, 32)$-коды $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с использованием кодов V_1 и V_2

k	r													
	7	8	9	10	11	12	13	14	15	16	17	18	...	32
7	1-0													
5		1-0												
4		0-1	1-0	1-0	0-0									
3		0-0	0-1	4-1	0-6	6-2	6-13	9-12	12-6	6-29	23-49	0-0		

Таблица 8

Значения векторов $\boldsymbol{f}$ для некоторых неэквивалентных $(64, 128, 32)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с использованием кодов V_1 и V_2

r	k	$\boldsymbol{f}$ с использ. V_1	$\boldsymbol{f}$ с использ. V_2
7	7	$(1,1,1,1)$	
8	5	$(4,4,4,4)$	
8	4		$(1,1,1,1)$
8	3		
9	4	$(5,5,5,5)$	
9	3		$(4,4,4,4)$
10	4	$(3,3,3,3)$	
10	3	$(2,1,1,1)$	$(5,5,5,5)$

r	k	$\boldsymbol{f}$ с использ. V_1	$\boldsymbol{f}$ с использ. V_2
11	4		
11	3		$(2,1,1,1)$
12	3	$(4,1,1,1)$	$(4,1,4,1)$
13	3	$(5,1,1,1)$	$(4,1,1,1)$
14	3	$(3,1,1,1)$	$(5,2,1,1)$
15	3	$(4,2,1,1)$	$(3,1,1,1)$
16	3	$(4,3,1,1)$	$(4,2,1,1)$
17	3	$(3,2,1,1)$	$(3,2,1,1)$

В качестве кода Адамара H_{12} длины $m = 12$ выбираем следующий код:

$$H_{12} = \left\{ \begin{array}{l} (0,0,0,0,0,0,0,0,0,0,0,0) \\ (0,0,0,0,0,0,1,1,1,1,1,1) \\ (0,0,0,1,1,1,0,0,0,1,1,1) \\ (0,0,1,0,1,1,0,1,1,0,0,1) \\ (0,0,1,1,0,1,1,0,1,0,1,0) \\ (0,0,1,1,1,0,1,1,0,1,0,0) \\ (0,1,1,1,0,0,0,0,1,1,0,1) \\ (0,1,0,0,1,1,1,0,1,1,0,0) \\ (0,1,0,1,1,0,0,1,1,0,1,0) \\ (0,1,1,0,1,0,1,0,0,0,1,1) \\ (0,1,1,0,0,1,0,1,0,1,1,0) \\ (0,1,0,1,0,1,1,1,0,0,0,1) \end{array} \right\} \cup \bar{H},$$

который получен из строк двоичной матрицы Адамара порядка 12 и ее дополнения, обозначенного через $\bar{H}$. Теперь можно построить $\mathbb{Z}_8$-коды Адамара $\mathcal{C}$ длины 12 мощности $|H_{12}| \cdot |V_0| = 24 \cdot 4 = 96$, полагая $\mathcal{C} = \Psi(V_0, H_{12})$. Рассматривая различные векторы $\boldsymbol{f}$ длины 12 над алфавитом $\{1, 2, 3\}$, мы получаем $3^{12} = 531441$ различных $(48, 96, 24)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$.

В табл. 9 приведено число таких кодов в зависимости от ранга и размерности ядра, а также все различные векторы $\boldsymbol{f}$, для которых получаются неэквивалентные коды с этими параметрами. Заметим, что мы можем построить коды Адамара только для параметров $(13, 3)$, $(13, 1)$ и $(14, 1)$, т.е. для пар, обозначенных символом $*$ в табл. 4. Такие же результаты получаются при других выборах тривиальных $(12, 4, 12)_4$-кодов V_i над алфавитом $\mathbb{Z}_4$.

Пример 6. Пусть $q = 24$ и $m = 4$. Пусть H_4 – код Адамара $H_4(1)$ из примера 1, а V – следующий тривиальный $(4, 12, 4)_{12}$-код над алфавитом $\mathbb{Z}_{12}$:

$$V = \{(0,0,0,0), (1,2,3,4), (2,3,4,5), (3,4,5,6), (4,5,6,7), (5,6,7,8),$$
$$(6,7,8,9), (7,8,9,10), (8,9,10,11), (9,10,11,1), (10,11,1,2), (11,1,2,3)\}.$$

Таблица 9

Векторы $\boldsymbol{f}$ для неэквивалентных $(48, 96, 24)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$

r	k	$\boldsymbol{f}$	Число кодов
13	3	$(1,1,1,1,1,1,1,1,1,1,1,1,1)$	4097
13	1	$(2,2,1,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,2,2,1,1,1,1,1,1,1)$ $(2,2,2,2,2,1,2,1,1,1,1,1,1)$	261624
14	1	$(2,1,1,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,2,1,1,1,1,1,1,1,1)$	265720

Для этих значений q и m можно построить $\mathbb{Z}_{24}$-коды $\mathcal{C}$ длины 4 мощности $|H_4|\cdot|V| = 8 \cdot 12 = 96$, полагая $\mathcal{C} = \Psi(V, H_4)$. Пусть

$$S_H(12) = \{H_{12}, \pi_1(H_{12}), \ldots, \pi_4(H_{12})\}$$

– множество из пяти различных кодов Адамара длины 12, полученных из кода H_{12}, приведенного в примере 5, и следующих четырех случайных перестановок множества $\{0, 1, \ldots, 11\}$:

$$\pi_1 = (2, 9, 8, 4, 3),$$
$$\pi_2 = (2, 11, 8, 10, 9, 7, 6, 5, 4, 3),$$
$$\pi_3 = (1, 3)(5, 6)(9, 11, 10),$$
$$\pi_4 = (1, 2, 3, 4)(5, 10, 9, 8, 7, 6).$$

Выбирая различные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4, 5\}$, получаем $5^4 = 625$ различных $(48, 96, 24)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(12))$. Все такие коды имеют ранг 13 и размерность ядра 3. Кроме того, все эти $(48, 96, 24)$-коды Адамара попарно не эквивалентны.

§ 5. Случай $m = 2$

В предыдущих примерах в случаях, когда m равно степени двойки, мы всегда получали коды с размерностью ядра $k \geqslant \log_2 m + 1$. В данном параграфе мы рассмотрим случай $m = 2$ и покажем, что для этого случая можно получить коды с меньшим ядром, вплоть до размерности 2. Заметим, что коды с размерностью ядра 1 получить невозможно. Кроме того, мы покажем, что если исходные коды Адамара из множества $S_H(q/2)$ не эквивалентны, то и результирующие коды Адамара не эквивалентны.

Пример 7. Пусть $q = 16$ и $m = 2$. Пусть $H_2 = \{(0\,0), (0\,1), (1\,0), (1\,1)\}$, и пусть $V_1 = \{(0\,0), (1\,2), (2\,3), \ldots, (6\,7), (7\,1)\}$ – тривиальный код над алфавитом $\mathbb{Z}_8$. Пусть $S_H(8)$ – множество из трех (эквивалентных) кодов Адамара длины 8. При этих параметрах исходных кодов можно построить $\mathbb{Z}_{16}$-коды Адамара $\mathcal{C}$ длины 2, что дает результирующие $(16, 32, 8)$-коды Адамара вида $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$ со следующими параметрами (r, k):

$$(r, k) \in \{(5, 5), (6, 3), (7, 2), (8, 2)\},$$

т.е. все возможные неэквивалентные коды с ядрами размерности $k \geqslant 2$. Заметим, что в примере 1 мы получаем все неэквивалентные $(16, 32, 8)$-коды Адамара с ядрами размерности $k \geqslant 3$.

Напомним несколько простых свойств ядра (см. (2)) двоичного кода H. Если код H содержит нулевое слово и $\boldsymbol{x} \in \ker(H)$, то очевидно, что

$$\ker(H + \boldsymbol{x}) = \ker(H) \quad \text{и} \quad \ker(\pi(H)) = \pi(\ker(H)), \tag{15}$$

где π – некоторая перестановка координат. Напомним, что два двоичных кода H и H' длины n эквивалентны, если существуют некоторая перестановка координат π и кодовое слово $\boldsymbol{h} \in H'$, такие что

$$\pi(H) = H' + \boldsymbol{h}. \tag{16}$$

Определим стабилизатор ядра как

$$\mathrm{PAut}(H) = \{\pi : \ \pi(H) = H\}.$$

Тогда справедлива следующая

Лемма 1. *Предположим, что два двоичных кода H и H', содержащие нулевой вектор, эквивалентны, т.е. выполняется равенство* (16) *для некоторых π и $\boldsymbol{h} \in H'$. Если в дополнении к этому имеет место условие* $\ker(H) = \ker(H')$, *то тогда* $\pi \in \mathrm{PAut}(\ker(H))$.

Доказательство. Действительно, рассматривая ядра обеих сторон равенства (16) и принимая во внимание первое равенство в (15), получаем, что

$$\ker(\pi(H)) = \ker(H' + \boldsymbol{h}) = \ker(H').$$

Из второго равенства в (15) получаем, что $\pi(\ker(H)) = \ker(H')$. По предположению $\ker(H) = \ker(H')$, откуда и вытекает утверждение леммы. ▲

Рассмотрим теперь для случая $m = 2$ конструкцию, описанную в теореме 4. Тривиальный $(2, q/2, 2)_{q/2}$-код V можно задать перестановкой τ на множестве $\{0, 1, \ldots, q/2 - 1\}$ с помощью выражения

$$V = \{(i, \tau(i)) : \ i = 0, 1, \ldots, q/2 - 1\}.$$

При этом рассматриваются только те перестановки, для которых $\tau(0) = 0$. Предположим, что H_1 и H_1' – две двоичные матрицы Адамара с нулевым вектором и нулевым столбцом, такие что $H_1 \cup \bar{H}_1$ и $H_1' \cup \bar{H}_1'$ являются $(q/2, q, q/4)$-кодами Адамара. Пусть $P = P(\tau)$ – перестановочная матрица, индуцированная перестановкой τ. Тогда результирующий код Адамара $C = C(H_1, H_1', \tau)$ длины q представляется в следующем виде:

$$C = \begin{bmatrix} H_1 & PH_1' \\ H_1 & P\bar{H}_1' \\ \bar{H}_1 & PH_1' \\ \bar{H}_1 & P\bar{H}_1' \end{bmatrix}. \tag{17}$$

Из построения кода следует, что $\ker(C)$ содержит вектор из всех единиц $(1, \ldots, 1)$, а также вектор $(0, \ldots, 0, 1, \ldots, 1)$ веса $q/2$. Предположим, что $\ker(C)$ содержит эти два вектора, т.е. размерность ядра не меньше двух. Для двух пар матриц $\{H_1, H_1'\}$ и $\{H_2, H_2'\}$ скажем, что они эквивалентны, и обозначим это через $\{H_1, H_1'\} \approx \{H_2, H_2'\}$, если имеет место одно из следующих двух условий:

(i) матрица H_1 эквивалентна H_2, а матрица H_1' эквивалентна H_2', либо

(ii) H_1' эквивалентна H_2, а H_1 эквивалентна H_2'.

Лемма 2. *Предположим, что коды $C_1 = C_1(H_1, H_1', \tau_1)$ и $C_2 = C_1(H_2, H_2', \tau_2)$ построены конструкцией, заданной в теореме* 4, *и имеют вид* (17). *Предположим,*

что $\ker(C_1) = \ker(C_2)$ *и эти ядра имеют размерность* 2. *Тогда, если две пары матриц* $\{H_1, H_1'\}$ *и* $\{H_2, H_2'\}$ *не эквивалентны, то соответствующие результирующие коды* C_1 *и* C_2 (*с размерностью ядра* 2) *также не эквивалентны.*

Доказательство. Поскольку размерность $\ker(C_1)$ равна 2, то очевидно, что

$$\ker(C_1) = \ker(C_2) = \{(\mathbf{0},\mathbf{0}), (\mathbf{0},\mathbf{1}), (\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{1})\},$$

где $\mathbf{0} = (0,\ldots,0)$, и $\mathbf{1} = (1,\ldots,1)$ – векторы длины $q/2$. Предположим, что коды C_1 и C_2 эквивалентны, тогда существуют перестановка π и кодовое слово $\boldsymbol{c} \in C_2$, такие что $\pi(C_1) = C_2 + \boldsymbol{c}$. Без ограничения общности можно предположить, что $\boldsymbol{c} = (\boldsymbol{c}_2, \boldsymbol{c}_2')$, где $\boldsymbol{c}_2 \in H_2$ и $\boldsymbol{c}_2' \in H_2'$ (в противном случае можно добавить соответствующий вектор из $\ker(C_2)$). По лемме 1

$$\pi \in \mathrm{PAut}(\{(\mathbf{0},\mathbf{0}), (\mathbf{0},\mathbf{1}), (\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{1})\}),$$

откуда следует, что $\pi = \xi * (\pi_1 \times \pi_2)$, где перестановки π_1, π_2 переставляют $q/2$ координатных позиций исходных кодов, а ξ меняет местами первые $q/2$ координатных позиций со вторыми. Таким образом, имеем

$$\pi(C_1) = \begin{bmatrix} \pi_1(H_1) & \pi_2(P_1H_1') \\ \pi_1(H_1) & \pi_2(P_1\bar{H}_1') \\ \pi_1(\bar{H}_1) & \pi_2(P_1H_1') \\ \pi_1(\bar{H}_1) & \pi_2(P_1\bar{H}_1') \end{bmatrix} \quad \text{или} \quad \pi(C_1) = \begin{bmatrix} \pi_2(P_1H_1') & \pi_1(H_1) \\ \pi_2(P_1\bar{H}_1') & \pi_1(H_1) \\ \pi_2(P_1H_1') & \pi_1(\bar{H}_1) \\ \pi_2(P_1\bar{H}_1') & \pi_1(\bar{H}_1) \end{bmatrix} \tag{18}$$

и

$$C_2 + (\boldsymbol{c}_2, \boldsymbol{c}_2') = \begin{bmatrix} H_2 + \boldsymbol{c}_2 & P_2H_2' + \boldsymbol{c}_2' \\ H_2 + \boldsymbol{c}_2 & P_2\bar{H}_2' + \boldsymbol{c}_2' \\ \bar{H}_2 + \boldsymbol{c}_2 & P_2H_2' + \boldsymbol{c}_2' \\ \bar{H}_2 + \boldsymbol{c}_2 & P_2\bar{H}_2' + \boldsymbol{c}_2' \end{bmatrix} = \begin{bmatrix} H_2 + \boldsymbol{c}_2 & P_2(H_2' + \boldsymbol{c}_2') \\ \overline{H_2 + \boldsymbol{c}_2} & P_2(\overline{H_2' + \boldsymbol{c}_2'}) \\ \overline{H_2 + \boldsymbol{c}_2} & P_2(H_2' + \boldsymbol{c}_2') \\ H_2 + \boldsymbol{c}_2 & P_2(\overline{H_2' + \boldsymbol{c}_2'}) \end{bmatrix}. \tag{19}$$

Сравнивая матрицы (18) с (19), заключаем, что либо матрица H_1 эквивалентна H_2, а H_1' эквивалентна H_2', либо H_1' эквивалентна H_2, а H_1 эквивалентна H_2'. ▲

Пример 8. Пусть $q = 48$ и $m = 2$. Определим две перестановки

$$\tau_1 = (1,2,3,\ldots,23),$$
$$\tau_2 = (1,5)(2,10)(3,15)\ldots(19,23),$$

действующие на множестве $\{0,1,\ldots,23\}$, где $\tau_2(i) = 5i \pmod{24}$ для $i = 0,1,\ldots,23$. Пусть H_2 – код Адамара, рассмотренный в примере 7, а $V_1 = V(\tau_1)$ и $V_2 = V(\tau_2)$ – $(2,24,2)_{24}$-коды над алфавитом $\mathbb{Z}_{24}$, где

$$V_i = V(\tau_i) = \{(0,0), (1,\tau_i(1)), \ldots, (23,\tau_i(23))\}$$

для $i = 1,2$. Пусть $S_H(24)$ – множество из всех 60 попарно неэквивалентных кодов Адамара длины 24, указанных в работе [27] (см. также [28]). По лемме 2 получаем $60^2 = 3600$ попарно неэквивалентных матриц Адамара. Число таких матриц в зависимости от значений ранга и размерности ядра указано в табл. 10. Выбирая максимальные значения для каждого из рангов, получаем не менее 3932 неэквивалентных кодов. Все полученные матрицы имеют тип 0 и размерность ядра 2. Учитывая теперь результаты, приведенные в примерах 5, 6 и 8, получаем не менее $7 + 625 + 3931 = 4563$ неэквивалентных кодов Адамара длины 48.

Пример 9. Пусть $q = 32$ и $m = 2$. Пусть H_2 – код из примера 7, а V – код, соответствующий перестановке $\tau = (1,2,\ldots,15)$. Пусть $S_H(16)$ – множество из пяти неэквивалентных кодов Адамара длины 16. По лемме 2 получаем $5^2 = 25$ неэквивалентных матриц Адамара порядка 32. Если добавить к множеству $S_H(16)$ еще

Таблица 10

Неэквивалентные $(48, 96, 24)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(24))$, полученные с помощью кодов V_1 и V_2

r	k	Число неэквивалентных кодов с использованием V_1	Число неэквивалентных кодов с использованием V_2
13	2	1	1 ($k = 3$)
14	2	0	2
15	2	1	7
16	2	2	14
17	2	7	49
18	2	16	68
19	2	72	245
20	2	208	246
21	2	687	693
22	2	1043	964
23	2	1232	1005
24	2	331	306

Таблица 11

Неэквивалентные $(32, 64, 16)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с размерностью ядра 2

k	r							
	9	10	11	12	13	14	15	16
2	1	3	7	14	19	23	10	3

четыре нелинейных кода Адамара, к которым применена случайная перестановка $\pi = (2, 9, 8, 4, 3)(12, 14)(13, 15)$, то получим 80 неэквивалентных матриц Адамара. В табл. 11 показано число таких неэквивалентных матриц Адамара с заданными рангом и размерностью ядра. Таким образом получаем коды с параметрами (r, k), помеченными в табл. 2 символом $\diamond$. Поскольку все они имеют размерность ядра 2, они не эквивалентны кодам, рассмотренным в примерах 2 и 3.

§ 6. Связь с модифицированной конструкцией Сильвестра матриц Адамара

Цель данного параграфа – показать связь нашей конструкции с известной в настоящее время модифицированной конструкцией Сильвестра [1], а затем обобщить эту модифицированную конструкцию. Существует очевидное сходство нашей конструкции и кронекеровского произведения (в частности, обе они имеют блочный тип), которое (для построения матриц Адамара) также называется конструкцией Сильвестра, известной уже с 1867 г. Следующее утверждение устанавливает связь нашей конструкции, введенной в теореме 3, с классической конструкцией Сильвестра. Сначала напомним, что под конструкцией Сильвестра для матриц Адамара из исходных матриц Адамара $H_n = [h_{i,j}]$ и H_m мы подразумеваем матрицу вида $H_{mn} = H_n \otimes H_m$, полученную заменой каждого элемента $h_{i,j}$ на матрицу $h_{i,j}H_m$ (очевидно, что в этом случае $h_{i,j} \in \{\pm 1\}$).

Предложение 1. *Предположим, что выполнены условия теоремы* 3. *Если код A_1 состоит из тривиальных векторов вида $(i, \ldots, i)$, где $i \in \{0, 1, \ldots, q/2 - 1\}$, то получаемая матрица $H_{qm/2}$ совпадает с классической конструкцией Сильвестра при использовании матриц $H_{q/2}$ и H_m.*

Доказательство. Обозначим i-ю строку матрицы Адамара $H_{q/2}$ через $\boldsymbol{r}^{(i)}$, а через $H^{(i)}(A_1)$ – подматрицу, образованную $q/2$ строками результирующей матри-

цы Адамара порядка $qm/2$, полученную нашей конструкцией, когда мы выбираем все N_1 кодовых слов кода A_1 при фиксированном кодовом слове кода A_2, а именно i-й строки $\boldsymbol{r}^{(i)}$ кода $H_{q/2}$. Поскольку $\boldsymbol{r}^{(i)} = (h_{i,1}, h_{i,2}, \ldots, h_{i,q/2})$, то соответствующая подматрица $H^{(i)}(A_1)$ имеет следующий вид:

$$H^{(i)}(A_1) = \boldsymbol{r}^{(i)} \otimes H_m = \begin{bmatrix} h_{i,1}H_m & h_{i,2}H_m & \ldots & h_{i,q/2}H_m \end{bmatrix}$$

(действительно, используемый нами код A_1 не меняет порядок строк матрицы H_m). Выпишем подматрицы $H^{(i)}(A_1)$ друг под другом для всех значений $i = 1, 2, 3, 4$:

$$H = \begin{bmatrix} H^{(1)}(A_1) \\ H^{(2)}(A_1) \\ \vdots \\ H^{(q/2)}(A_1) \end{bmatrix}.$$

В результате мы в точности получаем матрицу Адамара H порядка $mq/2$, полученную, как легко заметить, классической конструкцией Сильвестра из матриц $H_{q/2}$ и H_m. ▲

В работе [1] предложен модифицированный метод Сильвестра построения матриц Адамара. Приведем этот результат. Положим для краткости, что под суммой $a + B$ элемента $a \in \{0, 1\}$ и двоичной матрицы $B = [b_{i,j}]$ понимается двоичная матрица $a + B = [b_{i,j} + a]$.

Теорема 5 [1]. *Пусть заданы m матриц Адамара $B_1, B_2, \ldots, B_m$ порядка k (не обязательно попарно различных) и матрица Адамара $C = [c_{i,j}]$ порядка m, где все матрицы определены над $\{0, 1\}$. Тогда матрица*

$$H = \begin{bmatrix} c_{1,1} + B_1 & c_{1,2} + B_2 & \ldots & c_{1,m} + B_m \\ c_{2,1} + B_1 & c_{2,2} + B_2 & \ldots & c_{2,m} + B_m \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ c_{m,1} + B_1 & c_{m,2} + B_2 & \ldots & c_{m,m} + B_m \end{bmatrix}$$

является матрицей Адамара порядка mk.

Следующий иллюстративный пример нашей конструкции показывает, что конструкция теоремы 4 является модифицированной конструкцией Сильвестра, и для случая $s_{q/2} \leqslant m$ совпадает с конструкцией, предложенной в работе [1], представленной в теореме 5.

Пример 10. Пример конструкции для случая $n = 16$, где $q/2 = m = 4$. Пусть $S_H(4) = \{H_4(i) : i = 1, \ldots, 4\}$, где

$$H_4(1) = \{(0,0,0,0), (0,1,0,1), (0,0,1,1), (0,1,1,0)\},$$
$$H_4(2) = \{(0,0,0,0), (1,0,0,1), (1,0,1,0), (0,0,1,1)\},$$
$$H_4(3) = \{(0,0,0,0), (1,1,0,0), (0,1,0,1), (1,0,0,1)\},$$
$$H_4(4) = \{(0,0,0,0), (1,0,1,0), (0,1,1,0), (1,1,0,0)\}.$$

Выберем $\boldsymbol{f} = (1, 2, 3, 4)$, матрицу Адамара H_4 и тривиальный $(4, 4, 4)_4$-код V над алфавитом $\mathbb{Z}_4$:

$$H_4 = \{(0,0,0,0), (0,0,1,1), (0,1,1,0), (0,1,0,1)\},$$
$$V \ = \{(0,0,0,0), (1,1,3,3), (3,2,2,2), (2,3,1,1)\}.$$

Сначала построим $(4,16,4)_8$-код $\mathcal{C}=\Psi(V,H_4)$ над алфавитом $\mathbb{Z}_8$:

$$\mathcal{C}=\begin{Bmatrix}(0,0,0,0), & (1,1,3,3), & (3,2,2,2), & (2,3,1,1),\\ (0,0,4,4), & (1,1,7,7), & (3,2,6,6), & (2,3,5,5),\\ (0,4,4,0), & (1,5,7,3), & (3,6,6,2), & (2,7,5,1),\\ (0,4,0,4), & (1,5,3,7), & (3,6,2,6), & (2,7,1,5)\end{Bmatrix}.$$

Далее получаем следующую результирующую матрицу $H=\Phi(\mathcal{C},S_H(4))$:

```
0000  0000  0000  0000
0101  1001  1001  1100
0110  1010  0101  0110
0011  0011  1100  1010

0000  0000  1111  1111
0101  1001  0110  0011
0110  1010  1010  1001
0011  0011  0011  0101

0000  1111  1111  0000
0101  0110  0110  1100
0110  0101  1010  0110
0011  1100  0011  1010

0000  1111  0000  1111
0101  0110  1001  0011
0110  0101  0101  1001
0011  1100  1100  0101
```

Легко видеть, что эта матрица может быть построена модифицированной конструкцией Сильвестра при выборе в теореме 5 матриц $B_i=H_4(i)$, $i=1,2,3,4$, и матрицы $C=H_4$.

§ 7. Обобщение модифицированной конструкции Сильвестра матриц Адамара

Теперь наша цель – обобщить модифицированную конструкцию Сильвестра, предложенную в [1] и сформулированную выше в теореме 5. Конструкцию, приведенную в теоремах 4 и 5, можно обобщить, вовлекая в такую конструкцию большее число исходных матриц Адамара. Идея такого усиления основана на том, что в обобщенной каскадной конструкции для каждого кодового слова $\boldsymbol{a}^{(i)}$ кода A_i мощности N_i, $i=1,\ldots,s$, можно выбирать кодовые слова $\boldsymbol{b}$ из N_i различных кодов $A_{i+1}(\boldsymbol{a}^{(i)})$, соответствующему кодовому слову $\boldsymbol{a}^{(i)}$, т.е. каждому слову соответствует свой код (см., например, [19] для кодов в метрике Хэмминга). Для случая $s=2$ и метрики Ли получаем следующее утверждение (где для удобства обозначений полагаем $A_i=H_q(i)$, $B_j=H_m(j)$ и $k=q/2$):

Теорема 6. *Пусть заданы два натуральных числа k и m, такие что существуют матрицы Адамара порядка k и m. Пусть заданы два множества (не обязательно различных) матриц Адамара A_i, $i=1,\ldots,m$, и B_j, $j=1,\ldots,k$, порядков k и m соответственно. Тогда для произвольного тривиального $(m,k,m)_k$-кода V и произвольного вектора $\boldsymbol{f}=(f_1,\ldots,f_m)$ длины m над алфавитом $\{1,2,\ldots,m\}$ матрица C, где*

$$C=\Phi(\mathcal{C},\boldsymbol{f},A_1,\ldots,A_m),\quad \mathcal{C}=\Psi(V,B_1,\ldots,B_k), \tag{20}$$

является матрицей Адамара H_{km} порядка km.

Эту теорему мы не будем доказывать, учитывая, что аналогичный результат для метрики Хэмминга известен [19], а докажем соответствующий результат, сформулированный в терминах модифицированной конструкции Сильвестра. т.е. в терминах теоремы 5 из работы [1].

Для произвольного двоичного вектора $\boldsymbol{a}$ и $e \in \{0,1\}$ для краткости будем обозначать

$$\boldsymbol{a} + e = \boldsymbol{a} + e(1,1,\ldots,1).$$

Новая общая конструкция Сильвестра, которая обобщает известную в настоящее время модифицированную конструкцию Сильвестра [1], представлена в следующей теореме.

Теорема 7. *Пусть задано m (не обязательно различных) матриц Адамара $A_1, A_2, \ldots, A_m$ порядка k и k (не обязательно различных) матриц Адамара $B_1, B_2, \ldots, B_k$ порядка m, где все матрицы определены над алфавитом $\{0,1\}$. Пусть $\boldsymbol{a}_i^{(j)}$, $j = 1,2,\ldots,m$, $i = 1,2,\ldots,k$, обозначает строку с номером i матрицы A_j, пусть*

$$B_u = \left[b_{r,s}^{(u)}\right], \quad u = 1,2,\ldots,k, \quad r,s = 1,2,\ldots,m,$$

и пусть $\boldsymbol{b}_r^{(u)}$ обозначает строку с номером r матрицы B_u. Тогда матрица H

$$H = \left[\begin{array}{cccc}
\boldsymbol{a}_1^{(1)} + b_{1,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{1,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{1,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{1,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{1,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{1,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{1,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{1,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{1,m}^{(k)} \\
\hline
\boldsymbol{a}_1^{(1)} + b_{2,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{2,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{2,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{2,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{2,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{2,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{2,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{2,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{2,m}^{(k)} \\
\hline
\ldots & \ldots & \ldots & \ldots \\
\hline
\boldsymbol{a}_1^{(1)} + b_{m,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{m,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{m,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{m,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{m,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{m,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{m,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{m,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{m,m}^{(k)}
\end{array}\right]$$

является матрицей Адамара порядка mk.

Приведем независимое доказательство этого результата в обозначениях теоремы 7.

Доказательство. Пусть $\boldsymbol{h}_{i_1}$ и $\boldsymbol{h}_{i_2}$ – две различные строки матрицы H. Следует рассмотреть три различных случая.

(i) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{h}_{i_2}$ принадлежат одной и той же i-й полосе матрицы H, образованной векторами $\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}$ и $\boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}$, где $j, j' = 1,2,\ldots,k$ и $i, u = 1,2,\ldots,m$, т.е. $i = i'$ и $j \neq j'$. Так как

$$d(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}) = d(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}),$$

для любых (т.е. равных или неравных) элементов $b_{i,u}^{(j)}$ и $b_{i,u}^{(j')}$, то получаем для этого случая

$$d(\boldsymbol{h}_{i_1}\boldsymbol{h}_{i_2}) = \sum_{u=1}^{m} d(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}) = m \times \sum_{u=1}^{m} d(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}) =$$
$$= m \times \frac{k}{2} = \frac{mk}{2},$$

поскольку $j \neq j'$.

(ii) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{b}_{i_2}$ принадлежат разным i-й и i'-й полосам, соответственно, матрицы H, но имеют одинаковые номера строк $\boldsymbol{a}_j^{(u)}$ и $\boldsymbol{a}_{j'}^{(u)}$ внутри этих полос, т.е. $i \neq i'$ и $j = j'$. Принимая во внимание, что $\boldsymbol{a}_j^{(u)} = \boldsymbol{a}_{j'}^{(u)}$, получаем в этом случае

$$d(\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}) = \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_j^{(u)} + b_{i',u}^{(j)}\big) = k \times \sum_{u=1}^{m} d\big(b_{i,u}^{(j)}, b_{i',u}^{(j)}\big) =$$
$$= k \times d\big(\boldsymbol{b}_i^{(j)}, \boldsymbol{b}_{i'}^{(j)}\big) = k \times \frac{m}{2} = \frac{km}{2}.$$

(iii) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{b}_{i_2}$ принадлежат разным i-й и i'-й полосам, соответственно, матрицы H, и имеют разные номера строк $\boldsymbol{a}_j^{(u)}$ и $\boldsymbol{a}_{j'}^{(u)}$ внутри этих полос, т.е. $i \neq i'$ и $j \neq j'$. Тогда

$$d(\boldsymbol{h}_{i_1}, \boldsymbol{b}_{i_2}) = \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i',u}^{(j')}\big) = m \times \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big) =$$
$$= m \times \frac{k}{2} = \frac{mk}{2}.$$

Действительно, второе равенство имеет место, поскольку для произвольных различных j и j' выполнено равенство

$$d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)} + (1, 1, \ldots, 1)\big) = d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big),$$

из которого следует, что

$$d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i',u}^{(j')}\big) = d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big). \quad \blacktriangle$$

Проиллюстрируем новую конструкцию минимальным нетривиальным примером. Приведенное выше в примере 10 построение матрицы Адамара порядка 16 модифицированной конструкцией Сильвестра может быть обобщено следующим образом.

Пример 11. Пусть $q = m = 4$, и пусть $A_i = H_4(i)$ (как в примере 10), $i = 1, 2, 3, 4$. Пусть задан тривиальный код

$$V = \{(0,0,0,0), (1,1,1,1), (2,2,2,2), (3,3,3,3)\} \tag{21}$$

(отличный от кода в примере 10), и выберем следующие матрицы B_j, $j = 1, 2, 3, 4$:

$B_1 = \{(0,0,0,0), (0,0,1,1), (0,1,1,0), (0,1,0,1)\}$,
$B_2 = \{(0,0,0,0), (1,0,1,0), (1,0,0,1), (0,0,1,1)\}$,
$B_3 = \{(0,0,0,0), (1,1,0,0), (1,0,0,1), (0,1,0,1)\}$,
$B_4 = \{(0,0,0,0), (1,0,1,0), (1,1,0,0), (0,1,1,0)\}$.

Используя код V и матрицы B_1, B_2, B_3, B_4, сначала построим $(4, 16, 4)_8$-код $\mathcal{C} = \Psi(V, B_1, B_2, B_3, B_4)$ над алфавитом $\mathbb{Z}_8$:

$$\mathcal{C} = \begin{Bmatrix} (0,0,0,0), & (1,1,1,1), & (2,2,2,2), & (3,3,1,1), \\ (0,0,4,4), & (5,1,5,1), & (6,6,2,2), & (7,3,7,3), \\ (0,4,4,0), & (5,1,1,5), & (6,2,2,6), & (7,7,3,3), \\ (0,4,0,4), & (1,1,5,5), & (6,2,2,6), & (3,7,7,3) \end{Bmatrix}.$$

Пользуясь нашим отображением (для j-го столбца матрицы $\mathcal{C}$ мы используем код A_j), из кода $\mathcal{C}$ получаем результирующую матрицу Адамара H_{16}. Заметим, что поскольку у всех матриц B_i первая строка нулевая, первая полоса из k строк H_{16} состоит из m матриц $A_1, \ldots, A_m$. Таким образом, матрица H_{16} имеет следующий вид:

```
0000  0000  0000  0000
0101  1001  1100  1010
0011  1010  0101  0110
0110  0011  1001  1100

0000  0000  1111  1111
1010  1001  0011  1010
1100  0101  0101  0110
1001  0011  0110  1100

0000  1111  1111  0000
1010  1001  1100  0101
1100  1010  0101  1001
1001  1100  1001  1100

0000  1111  0000  1111
0101  1001  0011  0101
0011  0101  0101  1001
0110  1100  0110  1100
```

Результирующая матрица Адамара H_{16} нелинейна, хотя соответствующий код Адамара линеен. Легко убедится, что построенная матрица Адамара не может быть получена конструкцией, представленной в теореме 4 при использовании тривиального кода V, заданного в (21).

В заключение мы хотим отметить, что наша конструкция дает два независимых результата: (i) конструкцию q-ичных кодов в метрике Ли (дающие двоичные матрицы Адамара после применения отображения Грея) (ii) построение матриц Адамара с различными рангами и размерностью ядер.

Авторы выражают глубокую благодарность рецензенту, указавшему им на связь с обобщенной конструкцией Сильвестра и на соответствующую работу [1], в которой приведено такое обобщение.

СПИСОК ЛИТЕРАТУРЫ

1. *No J.-S., Song H.-Y.* Generalized Sylvester-Type Hadamard Matrices // Proc. 2000 IEEE Int. Symp. on Information Theory (ISIT'2000). Sorrento, Italy. June 25–30, 2000. P. 472. https://doi.org/10.1109/ISIT.2000.866770
2. *Hammons A.R., Jr., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319. https://doi.org/10.1109/18.312154
3. *Carlet C.* $\mathbb{Z}_{2^k}$-Linear Codes // IEEE Trans. Inform. Theory. 1998. V. 44. № 4. P. 1543–1547. https://doi.org/10.1109/18.681328

4. *Fernández C., Rifà J., Borges J.* Every $\mathbb{Z}_{2k}$-Code is a Binary Propelinear Code // Electron. Notes Discrete Math. 2001. V. 10. P. 100–102. https://doi.org/10.1016/S1571-0653(04)00370-1
5. *Dougherty S.T., Fernández-Córdoba C.* Codes over $\mathbb{Z}_{2^k}$, Gray Map and Self-Dual Codes // Adv. Math. Commun. 2011. V. 5. № 4. P. 571–588. https://doi.org/10.3934/amc.2011.5.571
6. *Krotov D.S.* On $\mathbb{Z}_{2^k}$-Dual Binary Codes // IEEE Trans. Inform. Theory. 2007. V. 53. № 4. P. 1532–1537. https://doi.org/10.1109/TIT.2007.892787
7. *Fernández-Córdoba C., Vela C., Villanueva M.* On $\mathbb{Z}_{2^s}$-Linear Hadamard Codes: Kernel and Partial Classification // Des. Codes Cryptogr. 2019. V. 87. № 2–3. P. 417–435. https://doi.org/10.1007/s10623-018-0546-6
8. *Bauer H., Ganter B., Hergert F.* Algebraic Techniques for Nonlinear Codes // Combinatorica. 1983. V. 3. № 1. P. 21–33. https://doi.org/10.1007/BF02579339
9. *Assmus E.F., Jr., Key J.D.* Designs and Their Codes. Cambridge, UK: Cambridge Univ. Press, 1992.
10. *Kimura H.* Classfication of Hadamard Matrices of Order 28 // Discrete Math. 1994. V. 133. № 1–3. P. 171–180. https://doi.org/10.1016/0012-365X(94)90024-8
11. *Kharaghani H., Tayfeh-Rezaie B.* On the Classification of Hadamard Matrices of Order 32 // J. Combin. Des. 2010. V. 18. № 5. P. 328–336. https://doi.org/10.1002/jcd.20245
12. *Kharaghani H., Tayfeh-Rezaie B.* Hadamard Matrices of Order 32 // J. Combin. Des. 2013. V. 21. № 5. P. 212–221. https://doi.org/10.1002/jcd.21323
13. *Fernández-Córdoba C., Vela C., Villanueva M.* On $\mathbb{Z}_8$-Linear Hadamard Codes: Rank and Classification // IEEE Trans. Inform. Theory. 2020. V. 66. № 2. P. 970–982. https://doi.org/10.1109/TIT.2019.2952599
14. *Fernández-Córdoba C., Vela C., Villanueva M.* Equivalences among $\mathbb{Z}_{2^s}$-Linear Hadamard Codes // Discrete Math. 2020. V. 343. № 3. Art. 111721 (13 pp.). https://doi.org/10.1016/j.disc.2019.111721
15. *Phelps K.T., Rifà J., Villanueva M.* Rank and Kernel of Binary Hadamard Codes // IEEE Trans. Inform. Theory. 2005. V. 51. № 11. P. 3931–3937. https://doi.org/10.1109/TIT.2005.856940
16. *Phelps K.T., Rifà J., Villanueva M.* Hadamard Codes of Length $2^t s$ (s Odd). Rank and Kernel // Proc. 16th Int. Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-16). Las Vegas, NV, USA. Feb. 20–24, 2006. Lect. Notes Comput. Sci. V. 3857. Berlin: Springer, 2006. P. 328–337. https://doi.org/10.1007/11617983_32
17. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670
18. *Ericson T., Zinoviev V.* Spherical Codes Generated by Binary Partitions of Symmetric Pointsets // IEEE Trans. Inform. Theory. 1995. V. 41. № 1. P. 107–129. https://doi.org/10.1109/18.370114
19. *Зиновьев В.А., Зиновьев Д.В.* Структура систем троек Штейнера $S(2^m-1,3,2)$ ранга 2^m-m+2 над $\mathbb{F}_2$ // Пробл. передачи информ. 2013. Т. 49. № 3. С. 40–56. http://mi.mathnet.ru/ppi2115
20. *Zinoviev D.V., Zinoviev V.A.* On Generalized Concatenated Construction of Codes in Metrics Lee L and L_1 // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2018). Svetlogorsk, Kaliningrad region, Russia. Sept. 2–8, 2018. P. 62–65. Available at https://www.dropbox.com/s/h7u89lh8vyirww9.
21. *Зиновьев В.А., Зиновьев Д.В.* Об обобщенной каскадной конструкции кодов в модульной метрике и метрике Ли // Пробл. передачи информ. 2021. Т. 57. № 1. С. 81–95. https://doi.org/10.31857/S0555292321010046
22. *Krotov D.S., Villanueva M.* Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-Linear Hadamard Codes and Their Automorphism Groups // IEEE Trans. Inform. Theory. 2015. V. 61. № 2. P. 887–894. https://doi.org/10.1109/TIT.2014.2379644
23. Handbook of Magma Functions / Bosma W., Cannon J.J., Fieker C., Steel A. (Eds.) Edition 2.26-4, 2021. Available at http://magma.maths.usyd.edu.au/magma/handbook/

24. *Todd J.A.* A Combinatorial Problem // J. Math. Phys. Camb. 1933. V. 12. № 1–4. P. 321–333. https://doi.org/10.1002/sapm1933121321
25. *Hall M., Jr.* Hadamard Matrices of Order 16 // JPL Research Summary № 36-10.1. 1961. P. 21–26.
26. *Hall M., Jr.* Hadamard Matrices of Order 20 // JPL Tech. Rep. № 32-761. 1965.
27. *Kimura H.* New Hadamard Matrix of Order 24 // Graphs Combin. 1989. V. 5. P. 235–242. https://doi.org/10.1007/BF01788676
28. A Library of Hadamard Matrices (online library; maintained by Sloane N.J.A.). http://neilsloane.com/hadamard/

Вильянуэва Мерсе (Villanueva, Mercè)
Независимый университет Барселоны, Беллатерра, Испания
merce.villanueva@uab.cat
Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
07.04.2022
После доработки
18.10.2022
Принята к публикации
18.10.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.72

© 2022 г. **И.В. Воробьев**[1], **К. Деппе**[2], **А.В. Лебедев**[3], **В.С. Лебедев**[3]

ИСПРАВЛЕНИЕ ОДНОЙ ОШИБКИ В КАНАЛАХ С ОБРАТНОЙ СВЯЗЬЮ

Исследуется задача исправления одной ошибки в произвольном дискретном канале без памяти с бесшумной мгновенной обратной связью. Для случая однократной обратной связи предложен способ построения оптимальных стратегий передачи данных. Полученный результат позволяет доказать, что для двоичного канала двух обратных связей достаточно для передачи такого же числа сообщений, как и при полной обратной связи. Также разработанная техника применяется к двоичному асимметричному каналу, для которого строятся стратегии передачи для малых длин.

Ключевые слова: кодирование с обратной связью, симметричный канал, асимметричный канал, граница Хэмминга, задача линейного программирования.

DOI: 10.31857/S0555292322040040, **EDN:** EBRKNL

§ 1. Введение

В данной статье исследуется исправление одной ошибки в произвольном дискретном канале без памяти с бесшумной мгновенной обратной связью. Далее мы будем по умолчанию предполагать все эти условия выполненными – канал без памяти, а обратная связь бесшумная и мгновенная. Наибольшее внимание уделяется двоичным симметричному и асимметричному каналам. В двоичном симметричном канале каждый символ может быть передан неправильно, например, 0 вместо 1 или наоборот. Обычно слово симметричный опускается, и такой канал называется просто двоичным каналом. В двоичном асимметричном канале вместо переданного символа 1 может быть получен 0, но символ 0 всегда передается безошибочно. Рассматривается комбинаторная модель канала с обратной связью и одной ошибкой при передаче символов.

Известно, что задача исправления t ошибок в двоичном канале с полной обратной связью эквивалентна следующей задаче комбинаторного поиска. Требуется найти элемент $x \in \mathcal{M}$ с помощью n вопросов вида: "Лежит ли элемент x в подмножестве A множества $\mathcal{M}$?" Вопросы задаются последовательно, т.е. каждый следующий вопрос может зависеть от ответов на предыдущие. Отвечающий на вопросы оппонент знает x и может солгать не более t раз. Впервые эта задача была сформулирована Реньи [1]. Для линейного числа ошибок в двоичном канале с полной обратной

[1] Работа выполнена при поддержке совместного гранта Российского фонда фундаментальных исследований и Национального научного фонда Болгарии (номер проекта 20-51-18002), Российского фонда фундаментальных исследований (номер проекта 20-01-00559), а также BMBF-NEWCOM (номер гранта 16KIS1005).

[2] Работа выполнена при поддержке грантов BMBF-NEWCOM (номер гранта 16KIS1005) и BMBF-6G-life (номер гранта 16KISK002).

[3] Работа выполнена при поддержке совместного гранта Российского фонда фундаментальных исследований и Национального научного фонда Болгарии (номер проекта 20-51-18002).

связью оптимальная скорость была вычислена Берлекампом [2] и Зигангировым [3]. Эта задача приобрела популярность после того, как в своей автобиографии [4] Улам задал подобный вопрос для $M = 10^6$. Оптимальные стратегии для всех M были найдены в [5] для $t = 1$, в [6] для $t = 2$ и в [7] для $t = 3$. Таблицы оптимальных стратегий были составлены в работе [8] для различных t и $M \leqslant 2^{20}$.

Исправление ошибок в двоичном асимметричном канале с полной обратной связью эквивалентно варианту задачи Улама с полуложью, впервые описанной в [9]. Отличие от оригинальной задачи состоит в том, что лгать можно только в случае, если правильный ответ положительный. Хороший обзор результатов по этой задаче можно найти в книге [10]. Для фиксированного числа ошибок t максимальная мощность множества $\mathcal{M}$ асимптотически эквивалентна $2^{n+t}/\binom{n}{t}$. Это было доказано для $t = 1$ в [11] и для произвольного t в [12, 13].

Отметим, что при фиксированном количестве ошибок даже однократной обратной связи достаточно для передачи асимптотически такого же количества сообщений, как и при полной обратной связи. Это было доказано для недвоичного симметричного канала в работе [14] и для произвольного дискретного канала в [15].

Ключевым результатом настоящей статьи является описание оптимальных стратегий с однократной обратной связью и одной ошибкой для произвольного дискретного канала. Разработанная техника применяется для построения стратегий передачи, исправляющих одну ошибку в двоичном канале с одной или двумя обратными связями, а также для построения стратегий, исправляющих одну ошибку в двоичном асимметричном канале с однократной обратной связью. Наиболее интересным из полученных результатов является, на наш взгляд, построение стратегии с двумя обратными связями, исправляющей одну ошибку в двоичном канале и передающей столько же сообщений, как и полностью адаптивная стратегия.

Оставшаяся часть статьи построена следующим образом. В § 2 приводятся основные определения. В § 3 сформулирована и доказана основная теорема, описывающая структуру оптимальных стратегий с одной ошибкой и однократной обратной связью. В § 4 основная теорема применяется для построения стратегии передачи данных по двоичному каналу с двумя обратными связями, исправляющей одну ошибку и позволяющей передать в точности столько же сообщений, сколько передается при полной обратной связи. В последнем параграфе разработанная техника применяется для поиска хороших стратегий для двоичного асимметричного канала с одной ошибкой и однократной обратной связью.

§ 2. Основные определения

Рассмотрим канал с q-ичным входным алфавитом $\mathcal{X} = \{0, \ldots, q-1\}$ и выходным алфавитом $\mathcal{Y} = \mathcal{X}$. Кодер передает сообщение $\boldsymbol{x} \in \mathcal{X}^n$, декодер получает сообщение $\boldsymbol{y} \in \mathcal{Y}^n$. Префикс длины p вектора $\boldsymbol{y}$ будем обозначать $\boldsymbol{y}_{\overline{p}}$. Ошибкой будем называть замену символа q_1 последовательности $\boldsymbol{x}$ на символ q_2, $q_1 \neq q_2$. Определим двудольный граф ошибок G, левая доля которого соответствует элементам из $\mathcal{X}$, а правая – элементам из $\mathcal{Y}$. Соединим $q_1 \in \mathcal{X}$ и $q_2 \in \mathcal{Y}$, $q_1 \neq q_2$, ребром, если при ошибке символ q_1 может перейти в q_2. Пример такого графа для троичного однонаправленного канала изображен на рис. 1.

В данной статье рассматривается передача данных по каналу с k обратными связями. Пусть длина кодового слова n разбита на $k+1$ частей:

$$n = n_1 + n_2 + \ldots + n_{k+1}.$$

Кодер передает сообщение $m \in [M]$. Первые n_1 передаваемых символов $x_1, \ldots, x_{n_1}$ зависят только от сообщения m. После передачи $N_{i-1} := n_1 + \ldots + n_{i-1}$ символов, $i \geqslant 2$, кодер имеет из канала обратной связи значения принятых символов $\boldsymbol{y}_{\overline{N_{i-1}}}$.

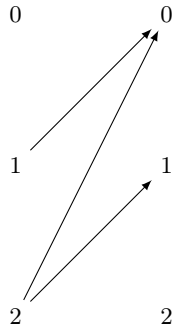

Рис. 1. Граф ошибок для троичного однонаправленного канала

Кодер посылает i-й блок из n_i символов, являющийся функцией от сообщения m и принятых им символов $\boldsymbol{y}_{\overline{N_{i-1}}}$. Случай $k = 0$ соответствует каналу без обратной связи, а случай $k = n - 1$ – каналу с полной обратной связью.

Определим облако $B_t(m)$ ($B(m)$ для $t = 1$) для сообщения m как множество последовательностей $\boldsymbol{y}$, которые могут быть получены на выходе канала с не более чем t ошибками при передаче этого сообщения. Будем называть набор непересекающихся облаков $B_t(m)$, $m \in [M]$, кодом $\mathcal{C}$, исправляющим t ошибок. Точки пространства, не принадлежащие ни одному облаку, будем называть свободными и обозначать через $\mathcal{F}(\mathcal{C})$. Коды, не использующие обратной связи, будем называть неадаптивными.

Отметим, что для симметричного канала без обратной связи облаками являются шары радиуса t в метрике Хэмминга. Для симметричного канала размеры всех облаков одинаковы, однако для произвольного графа ошибок это не так. Для предлагаемых в статье конструкций имеет смысл находить коды с максимальным количеством свободных точек для каждой длины и каждой мощности. Такие коды будем называть F-оптимальными.

В качестве примера опишем структуру облаков для двоичного канала с одной ошибкой и полной обратной связью. Каждое облако $B(m)$ содержит последовательность $\boldsymbol{y}$, которая будет передана в том случае, если в канале нет ошибок. Назовем эту последовательность корневой. Для любой координаты i в облаке присутствует последовательность $\boldsymbol{y}(i)$, которая совпадает с $\boldsymbol{y}$ в первых $i-1$ позициях, отличается в i-й позиции, а в остальных позициях имеет произвольные символы. Отсюда видно, что каждое облако состоит как минимум из $n + 1$ последовательностей. В частности, отсюда следуют граница Хэмминга на максимальное количество передаваемых сообщений.

§ 3. Однократная обратная связь

В этом параграфе предложена стратегия передачи сообщений с одной ошибкой и однократной обратной связью. Разобьем кодовую длину n на две части n_1 и n_2, где $n = n_1 + n_2$. Определим двудольный граф $H = (U \sqcup V, E)$ следующим образом. Левая и правая доли состоят из q^{n_1} вершин, соответствующих множествам входящих и выходящих последовательностей. Вершины u и v соединяются ребром, если последовательность, соответствующая v, может получиться из последовательности, соответствующей u, в результате одной ошибки. Отметим, что мы не соединяем ребрами вершины, соответствующие совпадающим последовательностям (это соответствует случаю, когда ошибки не происходит).

Теорема 1. *Пусть задан граф* $H = (U \sqcup V, E)$. *Стратегия, передающая*

$$M = \sum_{u \in U} M(u) \tag{1}$$

сообщений, существует тогда и только тогда, когда имеются коды $\mathcal{C}(u)$, *описанные выше, удовлетворяющие условию*

$$\sum_{u:\,(u,v)\in E} M(u) \leqslant F(v) \tag{2}$$

для любого $v \in V$.

Доказательство. Опишем произвольную стратегию кодирования. Сначала передается последовательность $\boldsymbol{u}$ длины n_1, которой соответствует вершина u из левой доли U графа H. Пусть количество сообщений, передача которых начинается с последовательности $\boldsymbol{u}$, равно $M(u)$. Рассмотрим случай, когда в первых n_1 символах ошибки не произошло. На оставшихся n_2 символах нам необходимо передать $M(u)$ различных сообщений, причем может произойти одна ошибка. Поэтому необходимо использовать код $\mathcal{C}(u)$ длины n_2 и мощности $M(u)$, исправляющий одну ошибку. Обозначим через $F(u)$ число свободных точек кода $C(u)$.

В том случае, если в первых n_1 символах произошла ошибка и вместо последовательности $\boldsymbol{u}$ была получена $\boldsymbol{v}$, для передачи $M(u)$ сообщений с началом $\boldsymbol{u}$ нужно $M(u)$ точек, причем это должны быть свободные точки кода $\mathcal{C}(v)$.

Таким образом, для каждого сообщения $\boldsymbol{v}$ должен существовать код $\mathcal{C}(v)$, свободные точки которого распределены между последовательностями $\boldsymbol{u}$, из которых можно попасть в последовательность $\boldsymbol{v}$, причем каждой такой последовательности $\boldsymbol{u}$ должно достаться не менее $M(u)$ свободных точек, что возможно тогда и только тогда, когда выполняется условие (2).

Теперь опишем алгоритм декодирования. Пусть последовательность из первых n_1 полученных символов соответствует вершине $v \in V$, последовательность из n_2 последних символов обозначим через $\boldsymbol{a}$. Если $\boldsymbol{a}$ не является свободной точкой кода $\mathcal{C}(v)$, то это значит, что ошибка произошла во второй части сообщения. В этом случае вторая часть сообщения соответствует центру шара, которому принадлежит точка $\boldsymbol{a}$.

Если же последовательность $\boldsymbol{a}$ оказалась свободной точкой кода $\mathcal{C}(v)$, то она относится к какой-то последовательности $\boldsymbol{u}$, из которой может быть получена $\boldsymbol{v}$. Именно эта последовательность $\boldsymbol{u}$ и передавалась на первой стадии кодирования. Вторая часть сообщения восстанавливается исходя из того, какая именно точка $\boldsymbol{a}$ была использована из не менее $M(u)$ точек, относящихся к $\boldsymbol{u}$. ▲

Нам не известен эффективный (полиномиальный от длины кода) способ нахождения оптимального набора кодов, удовлетворяющих (2). Однако даже выбор одинаковых кодов для всех последовательностей $\boldsymbol{u} \in \mathcal{X}^{n_1}$ может дать неплохой результат, как показано в следствии 1.

В качестве примера неоптимальности выбора одинаковых кодов для двоичного канала рассмотрим случай $n_1 = 2, n_2 = 1$. При выборе одинаковых кодов максимальное количество сообщений всегда делится на 2^{n_1}, и в данном случае оно равно 0, так как даже адаптивно на длине 3 нельзя передать больше двух сообщений. При выборе разных кодов можно передать два сообщения.

Следующее утверждение для двоичного симметричного канала будет использовано в дальнейшем для построения оптимальной стратегии с двумя обратными связями.

Следствие 1. *Пусть* $n_2 = 2^k - 1$, $n_1 = n - n_2$, $k \geqslant 1$. *Тогда в симметричном канале с одной ошибкой и однократной обратной связью можно передать*

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor$$

сообщений.

Доказательство. Назначим каждой точке $\boldsymbol{u}$ в качестве кода $\mathcal{C}(u)$ код Хэмминга длины n_2, из которого удалено x слов. Выберем x так, чтобы выполнялись ограничения (2), что эквивалентно неравенству

$$x2^k \geqslant n_1(2^{n_2-k} - x),$$

откуда получаем

$$x \geqslant \frac{n_1 2^{n_2-k}}{n_1 + 2^k}.$$

Тогда можно взять $x = \left\lceil \frac{n_1 2^{n_2-k}}{n_1 + 2^k} \right\rceil$. Количество оставшихся слов в выбранных кодах равно

$$2^{n_2-k} - \left\lceil \frac{n_1 2^{n_2-k}}{n_1 + 2^k} \right\rceil = \left\lfloor \frac{2^{n_2}}{n_1 + 2^k} \right\rfloor = \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor.$$

Суммарное количество передаваемых сообщений равно

$$M_1(n) = 2^{n_1} \left\lfloor \frac{2^{n_2}}{n_1 + n_2 + 1} \right\rfloor. \quad \blacktriangle$$

§ 4. Двоичный симметричный канал с обратной связью

Обозначим через $\mathrm{Alg}_k(n)$ стратегию передачи сообщений по каналу длины n с одной ошибкой и k обратными связями. Опишем алгоритм построения стратегии $\mathrm{Alg}_k(n)$ из $\mathrm{Alg}_{k-1}(n-1)$, который будет использоваться в дальнейшем.

Алгоритм DADA (Double and Delete Algorithm) построения стратегии $\mathrm{Alg}_k(n)$ из $\mathrm{Alg}_{k-1}(n-1)$. Напомним, что каждое облако в двоичном симметричном канале длины $n-1$ содержит корневое сообщение и $n-1$ дополнительных, которые совпадают с корневым в первых $i-1$ символах и отличаются в i-м, $i = 1, 2, \ldots, n-1$. Из каждого облака сообщений длины $n-1$ построим два множества сообщений длины n, дописав слева ко всем сообщениям 0 для первого множества и 1 для второго. Для того чтобы из первого (второго) множества сделать облако на длине n, достаточно добавить любое сообщение, начинающееся на 1 (0). Будем называть такие множества неполными облаками. Далее, из каждой свободной точки сделаем две свободных точки, дописав слева 0 или 1. Потратим все имеющиеся свободные последовательности на то, чтобы какое-то количество неполных облаков превратить в облака. Если число неполных облаков не больше, чем свободных последовательностей длины n, то в конце этой процедуры у нас будет $2M(n-1)$ облаков и какое-то количество свободных точек, где $M(n-1)$ – количество сообщений, передаваемых алгоритмом $\mathrm{Alg}_{k-1}(n-1)$. В этом случае алгоритм DADA завершается.

В противном случае в конце этой процедуры получится какое-то количество облаков и какое-то количество неполных облаков, полностью покрывающих пространство.

В дальнейшем будем брать одно неполное облако, последовательности в котором начинаются на 1, и одно неполное облако, последовательности в котором начинаются на 0, и уничтожать их, превращая все их элементы в свободные точки. Такая

операция дает $2n$ свободных точек. Далее, свободные точки используются на то, чтобы из неполных облаков сделать облака. Операция повторяется до тех пор, пока неполные облака не закончатся.

В конце процедуры останется четное количество облаков и не более $2n$ свободных точек. Если количество свободных точек равно $2n$, то это значит, что только что два неполных облака были преобразованы в эти $2n$ свободных точек. Восстановим одно из этих неполных облаков обратно и превратим в облако, дополнив одной свободной точкой. В результате получится дополнительное облако.

Таким образом, доказана следующая

Теорема 2. *Предположим, что на длине $n-1$ построено $M(n-1)$ облаков для передачи сообщений с одной ошибкой и $k-1$ обратными связями, $k = 1, \dots, n-1$. Пусть*

$$U(n) = 2\left\lfloor \frac{2^n}{2(n+1)} \right\rfloor, \quad r(n) = 2^n - (n+1)U(n).$$

Тогда алгоритм DADA строит стратегию $\mathrm{Alg}_k(n)$, передающую $M(n)$ сообщений, где

$$M(n) = \begin{cases} 2M(n-1), & \text{если } 2M(n-1) \leqslant \dfrac{2^n}{n+1}, \\ U(n), & \text{если } 2M(n-1) > \dfrac{2^n}{n+1} \text{ и } r(n) < 2n, \\ U(n)+1, & \text{если } 2M(n-1) > \dfrac{2^n}{n+1} \text{ и } r(n) \geqslant 2n. \end{cases}$$

В случае полной обратной связи оптимальное количество сообщений, которое можно передать с одной ошибкой, было вычислено в работе [5]. В теореме 3 мы приводим новое более простое доказательство этого результата.

Теорема 3. *Пусть*

$$U(n) = 2\left\lfloor \frac{2^n}{2(n+1)} \right\rfloor, \quad r(n) = 2^n - (n+1)U(n).$$

Тогда по каналу с одной ошибкой возможно передать $M_{\mathrm{ad}}(n)$ сообщений, где

$$M_{\mathrm{ad}}(n) = \begin{cases} U(n), & \text{если } r(n) < 2n, \\ U(n)+1, & \text{если } r(n) \geqslant 2n. \end{cases} \tag{3}$$

Более того, это количество сообщений является оптимальным.

Замечание 1. На самом деле, r всегда четно и меньше $2n+2$, поэтому в последней строке условие $r \geqslant 2n$ можно заменить на $r = 2n$. Отметим, что второй случай реализуется очень редко. А именно, мощность кода равна $U(n)+1$ при $n = 1, 2$, а следующая длина кода, при которой это происходит, равна 49736. Таким образом, оптимальным количеством сообщений чаще всего является максимальное четное число, не превосходящее границы Хэмминга.

Доказательство. Будем строить стратегию передачи сообщений индуктивно. Для $n \leqslant 8$ формула проверяется вручную.

Теперь предположим, что для длины $n-1$, $n \geqslant 9$, у нас построено $M_{\mathrm{ad}}(n-1)$ облаков. Заметим, что количество неполных облаков не меньше

$$2M_{\mathrm{ad}}(n-1) \geqslant \frac{2^n}{n} - 4 > \frac{2^n}{n+1}$$

Таблица 1

Максимальные количества передаваемых сообщений в двоичном симметричном канале с одной ошибкой с однократной обратной связью и с полной обратной связью

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
M_1	2	2	4	8	16	28	50	90	168	312	580	1088	2048	3854
M_{ad}	2	2	4	8	16	28	50	92	170	314	584	1092	2048	3854

при $n \geqslant 9$. Используем алгоритм DADA для построения адаптивной стратегии на длине n из стратегии на длине $n-1$. Так как $2M_{\text{ad}}(n-1) > \dfrac{2^n}{n+1}$, то $M_{\text{ad}}(n)$ равно $U(n)$ или $U(n)+1$ в зависимости от $r(n)$, что и требовалось доказать. ▲

Теорема 4. *В двоичном канале с двумя обратными связями и одной ошибкой можно передать $M_{\text{ad}}(n)$ сообщений, т.е. столько же, сколько и при полной обратной связи.*

Отметим, что однократной обратной связи для этого недостаточно, что можно увидеть из табл. 1.

Доказательство. Воспользуемся алгоритмом DADA для построения $\text{Alg}_2(n)$ из $\text{Alg}_1(n-1)$. В качестве $\text{Alg}_1(n-1)$ возьмем стратегию, построенную в следствии 1 с $M_1(n-1) = \left\lfloor \dfrac{2^{n_2}}{n_1+n_2+1} \right\rfloor 2^{n_1}$, где $n_2 = 2^k - 1$, $n_1 = n-1-n_2$.

Заметим (см. табл. 1), что для $n \leqslant 9$ даже однократной обратной связи достаточно для передачи такого же количества сообщений, как и при кодировании с полной обратной связью. Поэтому достаточно доказать утверждение для $n \geqslant 10$. Покажем, что $2M_1(n-1) > \dfrac{2^n}{n+1}$ при $n \geqslant 10$.

Это эквивалентно неравенству

$$2^{n_1+1} \left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_1+n_2+1}}{n_1+n_2+2}.$$

Сократив на 2^{n_1+1} и применив неравенство $\lfloor x \rfloor > x-1$, получаем

$$\left\lfloor \frac{2^{n_2}}{n_1+n_2+1} \right\rfloor > \frac{2^{n_2}}{n_1+n_2+1} - 1 \geqslant \frac{2^{n_2}}{n_1+n_2+2}.$$

Последнее неравенство эквивалентно

$$2^{n_2} \geqslant (n_1+n_2+1)(n_1+n_2+2).$$

Вспоминая, что $n_2 \geqslant n_1$ и $n_2 = 2^k - 1$, получаем, что неравенство выполнено при $n_2 \geqslant 15$.

Таким образом, мы доказали неравенство $2M_1(n-1) > \dfrac{2^n}{n+1}$ для $n \geqslant 16$. Для $n \in [10, 15]$ неравенство можно проверить вручную по табл. 1. Воспользовавшись теоремами 2 и 3, получаем требуемое утверждение. ▲

§ 5. Двоичный асимметричный канал

В данном параграфе мы применяем полученные ранее теоремы к двоичному асимметричному каналу. Для этого нам нужно составить таблицы кодов с большим числом свободных точек. Для нахождения таких кодов будет использован метод линейного программирования.

В работах [16–18] линейное программирование использовалось для доказательства верхних оценок мощности неадаптивных кодов, исправляющих асимметричные

ошибки. Мы модифицируем методы этих работ для получения верхних оценок количества свободных точек в коде фиксированной длины и мощности.

Обозначим через $M_Z(n,t)$ максимальную мощность асимметричного кода длины n, исправляющего t ошибок. Кроме того, обозначим через $L(n,d,w)$ и $U(n,d,w)$ нижнюю и верхнюю границы мощности равновесного кода веса w и длины n с расстоянием d.

Теорема 5. *Пусть $n \geqslant 2t \geqslant 2$, $1 \leqslant M \leqslant M_Z(n,t)$. Определим*

$$\overline{F}(n,M,t) = \max\left(2^n - \sum_{i=0}^{n}\left(z_i \sum_{j=0}^{t}\binom{i}{i-j}\right)\right),$$

где максимум берется по всем z_i, удовлетворяющим следующим условиям:

1) z_i – *неотрицательные целые*;

2) $z_0 = 1$, $z_1 = z_2 = \ldots = z_t = 0$;

3) $\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$;

4) $\displaystyle\sum_{j=s}^{r} z_j L(r-s, 2t+2, r-j) \leqslant U(n+r-s, 2t+2, r)$ *для* $0 \leqslant s \leqslant r$;

5) $\displaystyle\sum_{j=s}^{r} z_{n-j} L(r-s, 2t+2, r-j) \leqslant U(n+r-s, 2t+2, r)$ *для* $0 \leqslant s \leqslant r$;

6) $\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} + \left(\binom{w+t-s+1}{w} - \binom{t+1}{t-s+1} \times \right.$
$\displaystyle\left. \times \left\lfloor \frac{w+t-s+1}{t+1} \right\rfloor\right) z_{w+t-s+1} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$,

$\displaystyle\sum_{i=1}^{s}\binom{n-w+i}{i} z_{w-i} + \sum_{j=0}^{t-s}\binom{w+j}{j} z_{w+j} + \left(\binom{n-w+s+1}{s+1} - \binom{t+1}{t-s} \times \right.$
$\displaystyle\left. \times \left\lfloor \frac{n-w+s+1}{t+1} \right\rfloor\right) z_{w-s-1} \leqslant \binom{n}{w}$ *для* $0 \leqslant s \leqslant t < w < n-t$;

7) $\displaystyle\sum_{i=0}^{n} z_i = M$.

Тогда количество свободных точек F в коде длины n и мощности M, исправляющем t асимметричных ошибок, не превосходит $\overline{F}(n,M,t)$.

Доказательство. Обозначим через z_i, $0 \leqslant i \leqslant n$, количество кодовых слов веса i в коде длины n, исправляющем t асимметричных ошибок. В работах [16–18] было доказано, что числа z_i должны удовлетворять ограничениям 1), 3)–6). Легко видеть, что код с максимальным количеством свободных точек должен удовлетворять условию 2). Последнее условие фиксирует мощность рассматриваемого кода. Оптимизируемое выражение $\overline{F}(n,M,t)$ соответствует количеству свободных точек в коде с весовым распределением $\{z_i\}$. ▲

Используем также метод линейного программирования для поиска кодов с максимальным количеством свободных точек. Зафиксируем длину кода n, мощность кода M и количество исправляемых асимметричных ошибок t. Введем 2^n двоичных переменных x_i, соответствующих всем возможным кодовым словам. Для каждой точки p определим множество $D_t(p)$ кодовых слов, из которых в эту точку мож-

Таблица 2

Оптимальное количество свободных точек $(n, M, 1)$-кодов

$n = 6$	Мощность M	12	11	10	9	8
	Свободные точки F	16	23	28	33	38
$n = 7$	Мощность M	18	17	16	15	14
	Свободные точки F	48	56	62	68	73
$n = 8$	Мощность M	36	35	34	33	32
	Свободные точки F	76	85	92	99	106
$n = 9$	Мощность M	62	61	60	59	58
	Свободные точки F	177	186	193	200	207

но попасть, совершив t асимметричных ошибок. Введем ограничение $\sum\limits_{i \in D_t(p)} x_i \leqslant 1$. Максимизируем количество свободных точек $2^n - \sum\limits_{i=0}^{n} z_i(i+1)$, где z_i – количество кодовых слов веса i. Отметим, что количество свободных точек выражается через переменные x_i. Добавим ограничение $\sum x_i = M$, чтобы зафиксировать мощность кода. Отметим, что любое решение данной задачи линейного программирования (если оно существует) выдает оптимальное количество свободных точек для фиксированных длины и мощности кода. Для ускорения вычислений мы добавили ограничения из теоремы 5.

Несмотря на эти оптимизации, программа работает с 2^n переменными, а значит, решение может быть найдено только для достаточно малых значений n. В табл. 2 приводятся параметры некоторых F-оптимальных кодов для $t = 1$ и $n = 6, 7, 8$ и 9. Оптимальные весовые распределения приведены в табл. 3.

Параметры кодов длины $n = 6, 8$ и 9 совпадают с верхними границами, которые дает теорема 5. Для $n = 7$ и $M = 18$ мы получили 48 свободных точек вместо 49, которые дает верхняя граница из теоремы 5, т.е. верхняя граница из теоремы 5 не достигается. Все остальные значения совпадают с верхними границами.

Коды с оптимальным весовым распределением для длины $n = 7, 8$ были построены в [16]. Код для длины $n = 6$ тоже был известен ранее. Для длин $n = 6, 8$ и всех мощностей $M \leqslant M_Z(n, 1)$ оптимальные коды могут быть получены из кода максимальной мощности с весовым распределением, указанным в табл. 3, путем удаления $M_Z(n, d) - M$ кодовых слов максимального веса. Для длины $n = 7$ и мощности $M = 17$ нам известны два кода с разными весовыми распределениями с оптимальным количеством свободных точек: 1+0+3+5+5+3+0+0 и 1+0+3+5+6+1+1+0. Удаляя кодовые слова максимального веса из кода со вторым весовым распределением, получаем F-оптимальные коды для всех $M < 17$. Однако только код с первым весовым распределением можно дополнить до кода мощности 18.

Программа работает для всех длин $n < 9$. Для больших длин сложность слишком велика. Так как F-оптимальные конструкции для длин $n = 6, 8$ являются вложенными кодами, то мы ограничиваемся поиском среди таких семейств и для длины $n = 9$. Этот подход позволил найти такое семейство вложенных кодов, что максимальный код мощности 62 имеет весовое распределение, приведенное в табл. 3. Количество свободных точек в кодах семейства совпадает с верхними границами из теоремы 5 для всех мощностей M. Это означает, что коды из построенного семейства являются F-оптимальными. Отметим, что код максимальной мощности длины $n = 9$, построенный в [16], имеет 171 свободную точку, в то время как в нашем коде 177 свободных точек.

Имея в своем распоряжении таблицы кодов со свободными точками, мы можем воспользоваться теоремой 1 для построения стратегий передачи данных по асиммет-

Таблица 3

Оптимальные весовые распределения

Длина и мощность	Весовое распределение
$n = 6,\ M = 12$	$1+0+3+4+3+0+1$
$n = 7,\ M = 18$	$1+0+3+5+5+3+1+0$
$n = 7,\ M = 17$	$1+0+3+5+6+1+1+0$
$n = 8,\ M = 36$	$1+0+4+8+10+8+4+0+1$
$n = 9,\ M = 62$	$1+0+4+9+17+17+11+2+1+0$

Таблица 4

Количество передаваемых сообщений по асимметричному каналу с однократной обратной связью и одной ошибкой

n	5	6	7	8	9	10	11	12	13
M (следствие 2)	9	16	29	52	96	177	327	607	1120
M (теорема 1)	9	16	29	53	97	$\geqslant 177$	$\geqslant 329$	$\geqslant 607$	$\geqslant 1120$

ричному каналу с обратной связью. В случае, когда параметры $M(v)$ и $F(v)$ зависят только от веса слова, получаем следующее утверждение.

Следствие 2. *Пусть $M(v) = M_w$ и $F(v) = F_w$ для всех $v \in V$, таких что количество единиц в v равно w, т.е. $M(v)$ и $F(v)$ зависят только от веса слова v. Если условия*

$$(n_1 - w)M_{w+1} \leqslant F_w \tag{4}$$

выполняются для всех $w \in [0, n_1 - 1]$, то количество передаваемых сообщений равно

$$M = \sum_{w=0}^{n_1} \binom{n_1}{w} M_w. \tag{5}$$

Количества сообщений, передаваемых алгоритмами, построенными с помощью следствия 2 и теоремы 1, приведены в табл. 4. Для вычисления значений M_w и F_w, дающих оптимальный ответ, была использована техника динамического программирования. В приведенных ниже примерах мы даем подробное описание кодов, полученных с помощью следствия 2 и теоремы 1 для длин $n = 9$ и $n = 8$ соответственно.

Будем обозначать через $(n, M, F, t)_Z$ неадаптивный код длины n, исправляющий t асимметричных ошибок, имеющий M кодовых слов и F свободных точек. В первом примере продемонстрируем применение следствия 2, где используемый после обратной связи код зависит только от веса слова, передаваемого до обратной связи. На длине $n = 8$ применение следствия 2 позволяет передать только 52 сообщения. Во втором примере мы показываем, как с помощью теоремы 1 можно передать 53 сообщения. Это означает, что следствие 2 не всегда дает оптимальный ответ.

Пример 1. $n = 9,\ M = 96$.

Пусть $n_1 = 5$, $n_2 = 4$. Вершинам, соответствующим двоичным словам веса 0 и 1, мы сопоставляем $(4, 2, 12, 1)_Z$-код из двух слов $\{0000, 0011\}$. Вершинам веса 2 и 3 сопоставляем $(4, 3, 9, 1)_Z$-код из трех слов $\{0000, 0011, 1100\}$. Весам 4 и 5 сопоставляем $(4, 4, 4, 1)_Z$-код из четырех слов $\{0000, 0011, 1100, 1111\}$.

Проверим ограничения $(n_1 - w)M_{w+1} \leqslant F_w$ для $w \in [0, 4]$:

$w = 0:\ 5 \cdot 2 \leqslant 12,$

$w = 1:\ 4 \cdot 3 \leqslant 12,$

$w = 2:\ 3 \cdot 3 \leqslant 9,$

Таблица 5

Мощности кодов для асимметричного канала с полной обратной связью и одной ошибкой

n	5	6	7	8	9	10	11	12	13
M [11]	8	16	32	32	64	128	256	512	1024
M_{ad}	11	20	36	66	121	223	415	774	1452

$w = 3: \ 2 \cdot 4 \leqslant 9,$

$w = 4: \ 1 \cdot 4 \leqslant 4.$

С помощью формулы (5) вычисляем количество передаваемых сообщений:

$$1 \cdot 2 + 5 \cdot 2 + 10 \cdot 3 + 10 \cdot 3 + 5 \cdot 4 + 1 \cdot 4 = 96.$$

Пример 2. $n = 8$, $M = 53$.

Пусть $n_1 = 6$, $n_2 = 2$. Вершине 111111 сопоставим $(2, 2, 0, 1)_Z$-код $\{00, 11\}$. Вершинам 111000, 001110, 010101, 100011, 100100, 010010, 001001, 110000, 010100, 001000, 000010, 000001 сопоставим $(2, 0, 4, 1)_Z$-код из 0 слов. Остальным вершинам сопоставим $(2, 1, 3, 1)_Z$-код из одного слова $\{00\}$. Легко проверить, что условия (2) из теоремы 1 выполняются. Например, проверим условия для вершины $v = 101000$: есть всего 4 вершины $\{111000, 101100, 101010, 101001\}$, из которых можно попасть в v. Мощности соответствующих кодов

$$M(111000) = 0, \quad M(101100) = 1,$$
$$M(101010) = 1, \quad M(101001) = 1.$$

Сумма этих мощностей не превосходит $F(101000) = 3$, т.е. ограничение для вершины $v = 101000$ выполнено. Таким же образом можно проверить и ограничения для остальных вершин.

Суммарное количество передаваемых сообщений равно $2 + 0 + 51 = 53$.

Приведем таблицу с количеством сообщений, которое можно передать по каналу с одной асимметричной ошибкой и полной обратной связью. Наилучшие результаты получены в работе [11], где для передачи $M = 2^m$ сообщений требуется длина $n = m - 1 + \lceil \log_2(m + 3) \rceil$. Несмотря на то, что мы используем только однократную обратную связь, нам удается передать больше сообщений, чем в [11], при $n \leqslant 13$, кроме случая $n = 7$. Для асимметричного канала с полной обратной связью и одной ошибкой можно использовать алгоритм, аналогичный DADA, позволяющий строить коды с оптимальным количеством передаваемых сообщений M_{ad}. Мощности этих кодов приведены в табл. 5. Подробное описание построения таких кодов будет приведено в одной из последующих работ.

СПИСОК ЛИТЕРАТУРЫ

1. *Rényi A.* On a Problem of Information Theory // Magyar Tud. Akad. Mat. Kutató Int. Közl. 1961. V. 6. P. 505–516.
2. *Berlekamp E.R.* Block Coding for the Binary Symmetric Channel with Noiseless, Delayless Feedback // Error-Correcting Codes (Proc. Conf. Conducted by the Mathematics Research Center, United States Army, at the University of Wisconsin, Madison, May 6–8, 1968). New York: Wiley, 1969. P. 61–85.
3. *Зигангиров К.Ш.* О числе исправляемых ошибок при передаче по ДСК с обратной связью // Пробл. передачи информ. 1976. Т. 12. № 2. С. 3–19. `http://mi.mathnet.ru/ppi1683`
4. *Ulam S.M.* Adventures of a Mathematician. New York: Scribner, 1976.

5. *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
6. *Guzicki W.* Ulam's Searching Game with Two Lies // J. Combin. Theory Ser. A. 1990. V. 54. № 1. P. 1–19. https://doi.org/10.1016/0097-3165(90)90002-E
7. *Deppe C.* Solution of Ulam's Searching Game with Three Lies or an Optimal Adaptive Strategy for Binary Three-Error-Correcting Codes // Discrete Math. 2000. V. 224. № 1–3. P. 79–98. https://doi.org/10.1016/S0012-365X(00)00109-6
8. *desJardins D.L.* Precise Coding with Noiseless Feedback. Ph.D. Thesis. Dept. of Mathematics, Univ. of California, Berkeley, 2002. Available at http://www.desjardins.org/david/thesis/thesis.pdf
9. *Rivest R.L., Meyer A.R., Kleitman D.J., Winklmann K., Spencer J.* Coping with Errors in Binary Search Procedures // J. Comput. System Sci. 1980. V. 20. № 3. P. 396–404. https://doi.org/10.1016/0022-0000(80)90014-8
10. *Cicalese F.* Fault-Tolerant Search Algorithms: Reliable Computation with Unreliable Information. Berlin: Springer, 2013.
11. *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
12. *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
13. *Spencer J., Yan C.H.* The Halflie Problem // J. Combin. Theory Ser. A. 2003. V. 103. № 1. P. 69–89. https://doi.org/10.1016/S0097-3165(03)00068-2
14. *Бассалыго Л.А.* Недвоичные коды, исправляющие ошибки при наличии одноразовой безошибочной обратной связи // Пробл. передачи информ. 2005. Т. 41. № 2. С. 63–67. http://mi.mathnet.ru/ppi96
15. *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
16. *Delsarte P., Piret P.* Bounds and Constructions for Binary Asymmetric Error-Correcting Codes // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 125–128. https://doi.org/10.1109/TIT.1981.1056290
17. *Kløve T.* Upper Bounds on Codes Correcting Asymmetric Errors // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 128–131. https://doi.org/10.1109/TIT.1981.1056291
18. *Weber J., de Vroedt C., Boekee D.* New Upper Bounds on the Size of Codes Correcting Asymmetric Errors // IEEE Trans. Inform. Theory. 1987. V. 33. № 3. P. 434–437. https://doi.org/10.1109/TIT.1987.1057301

Воробьев Илья Викторович
Деппе Кристиан (Deppe, Christian)
Технический университет Мюнхена, Германия
vorobyev.i.v@yandex.ru
christian.deppe@tum.de
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
20.09.2022
После доработки
28.11.2022
Принята к публикации
28.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.72

© 2022 г. **А. Джанабекова, Г.А. Кабатянский**[1], **И. Камель, Т.Ф. Рабие**

НЕПЕРЕКРЫВАЮЩИЕСЯ ВЫПУКЛЫЕ МНОГОГРАННИКИ С ВЕРШИНАМИ ИЗ БУЛЕВА КУБА И ДРУГИЕ ЗАДАЧИ ТЕОРИИ КОДИРОВАНИЯ

Устанавливается связь между несколькими задачами, которые, на первый взгляд, довольно далеки друг от друга, и формулируется ряд открытых проблем.

Ключевые слова: выпуклые многогранники, булев куб, групповое тестирование, поиск фальшивых монет, сигнатурные коды для каналов с множественным доступом и шумом, мультимедийные коды цифровых отпечатков пальцев, определение носителя вектора по линейным измерениям с шумом.

DOI: 10.31857/S0555292322040052, **EDN:** ECJVMW

§ 1. Неперекрывающиеся выпуклые многогранники с вершинами из булева куба, поиск фальшивых монет на точных весах и другие задачи

Начнем с выпуклых многогранников, вершины которых берутся из булева куба $B^n = \{0,1\}^n \subset \mathbb{R}^n$. Мы будем рассматривать множества $A \subset B^n$ мощности не более t и их выпуклые оболочки (выпуклые многогранники)

$$\langle A\rangle = \left\{ \sum_{\boldsymbol{a}\in A} \lambda_{\boldsymbol{a}} \boldsymbol{a} : \sum_{\boldsymbol{a}\in A} \lambda_{\boldsymbol{a}} = 1,\ \lambda_{\boldsymbol{a}} \geqslant 0 \right\}.$$

Точка

$$\boldsymbol{x} = \sum_{\boldsymbol{a}\in A} \lambda_{\boldsymbol{a}} \boldsymbol{a}$$

с неотрицательными коэффициентами $\lambda_{\boldsymbol{a}}$, такими что $\sum\limits_{\boldsymbol{a}\in A} \lambda_{\boldsymbol{a}} = 1$, называется *выпуклой комбинацией* точек множества A, а если коэффициенты $\lambda_{\boldsymbol{a}} > 0$ для всех точек из A, то про точку $\boldsymbol{x}$ будем говорить, что она представима в виде *строго выпуклой комбинации* точек из A и называть ее *строго внутренней точкой* выпуклой оболочки $\langle A\rangle$.

Определение 1. Множество $\mathcal{C}$ вершин n-мерного булева куба B^n называется *t-независимым*, если для любых его двух непересекающихся подмножеств $A, B \subset \mathcal{C}$, таких что $|A|, |B| \leqslant t$, их выпуклые оболочки не пересекаются.

Это определение, как мы сейчас покажем, эквивалентно следующему.

[1] Исследование выполнено при финансовой поддержке Российского научного фонда в рамках гранта РНФ 22-41-02028.

Определение 2. Множество $\mathcal{C}$ вершин n-мерного булева куба B^n называется *t-независимым*, если для любых двух различных подмножеств $A, B \subset \mathcal{C}$, таких что $|A|, |B| \leqslant t$, их выпуклые оболочки не пересекаются по строго внутренней точке.

Предложение 1. *Определения* 1 *и* 2 *эквивалентны.*

Доказательство. $1 \to 2$. Пусть это не так, т.е. условия определения 1 выполнены, но имеются два различных подмножества $A, B \subset \mathcal{C}$, таких что $|A|, |B| \leqslant t$ и их выпуклые оболочки пересекаются по *строго* внутренней точке $\boldsymbol{x}$. Тем самым,

$$\boldsymbol{x} = \sum_{\boldsymbol{a} \in A} \lambda_{\boldsymbol{a}} \boldsymbol{a} = \sum_{\boldsymbol{b} \in B} \lambda'_{\boldsymbol{b}} \boldsymbol{b}, \tag{1}$$

где все коэффициенты λ положительны и

$$\sum_{\boldsymbol{a} \in A} \lambda_{\boldsymbol{a}} = \sum_{\boldsymbol{b} \in B} \lambda'_{\boldsymbol{b}} = 1.$$

Рассмотрим множества

$$\Delta := A \cap B, \quad \Delta_A := \{i \in \Delta : \ \lambda_i > \lambda'_i\}, \quad \Delta_B := \{i \in \Delta : \ \lambda_i < \lambda'_i\}.$$

Из уравнения (1) следует, что

$$\sum_{\boldsymbol{a} \in A - \Delta} \lambda_{\boldsymbol{a}} \boldsymbol{a} + \sum_{\boldsymbol{a} \in \Delta_A} (\lambda_{\boldsymbol{a}} - \lambda'_{\boldsymbol{a}}) \boldsymbol{a} = \sum_{\boldsymbol{b} \in B - \Delta} \lambda'_{\boldsymbol{b}} \boldsymbol{b} + \sum_{\boldsymbol{b} \in \Delta_B} (\lambda'_{\boldsymbol{b}} - \lambda_{\boldsymbol{b}}) \boldsymbol{b}. \tag{2}$$

Легко видеть, что сумма коэффициентов в левой части и правой части уравнения (2) одна и та же, поэтому пронормировав на это число (сумму) левую и правую часть (2), получим, что выпуклые оболочки непересекающихся множеств $(A - \Delta) \cup \cup \Delta_A$ и $(B - \Delta) \cup \Delta_B$ пересекаются. Противоречие.

$2 \to 1$. Пусть это не так, т.е. условия определения 2 выполнены, но имеются два непересекающихся подмножества $A, B \subset \mathcal{C}$, таких что $|A|, |B| \leqslant t$ и их выпуклые оболочки пересекаются в некоторой точке $\boldsymbol{x}$. Тем самым,

$$\boldsymbol{x} = \sum_{\boldsymbol{a} \in A} \lambda_{\boldsymbol{a}} \boldsymbol{a} = \sum_{\boldsymbol{b} \in B} \lambda'_{\boldsymbol{b}} \boldsymbol{b}, \tag{3}$$

где все коэффициенты λ неотрицательны и $\sum\limits_{\boldsymbol{a} \in A} \lambda_{\boldsymbol{a}} = \sum\limits_{\boldsymbol{b} \in B} \lambda'_{\boldsymbol{b}} = 1$. Введем множества

$$\widehat{A} := \{a \in A : \ \lambda_{\boldsymbol{a}} > 0\}, \quad \widehat{B} := \{b \in B : \ \lambda_{\boldsymbol{b}} > 0\}.$$

Тогда $\boldsymbol{x}$ является общей строго внутренней точкой для двух различных (и даже непересекающихся) множеств $\widehat{A}$ и $\widehat{B}$. Противоречие. ▲

Определение 1 представляется нам более естественным, а определение 2 – это новая математическая формулировка задачи о мультимедийных кодах, устойчивых к произвольным линейным атакам коалиций из не более чем t легальных пользователей (см. [1] и обзор [2]). Действительно, линейная атака коалиции $A \subset \mathcal{C}$ означает, что эта коалиция может подставить ложный вектор $\widehat{\boldsymbol{a}}$, сформированный как взвешенная сумма векторов, соответствующих членам коалиции, т.е.

$$\widehat{\boldsymbol{a}} = \sum_{\boldsymbol{a} \in A} p_{\boldsymbol{a}} \boldsymbol{a},$$

где все $p_{\boldsymbol{a}} \geqslant 0$ и $\sum\limits_{\boldsymbol{a} \in A} p_{\boldsymbol{a}} = 1$. Тогда использование t-независимого кода гарантирует, согласно определению 2, что данный ложный вектор $\widehat{\boldsymbol{a}}$ является строго внутренним

для единственной коалиции, и тем самым, все пользователи, внесшие *ненулевой* вклад в создание ложного вектора, могут быть однозначно определены. Отметим, что для обычных кодов цифровых отпечатков пальцев [3,4] это свойство – однозначное нахождение коалиции активных пользователей – принципиально недостижимо.

Обозначим через $M_1(t\,|\,n)$ максимальную мощность t-независимых множеств n-мерного булева куба и рассмотрим частный случай $t = 2$. Определение 1 говорит, что множество $\mathcal{C}$ вершин булева куба является 2-независимым, если для любых четырех различных точек $a, b, c, d \in \mathcal{C}$ отрезки $[a, b]$ и $[c, d]$ не пересекаются. Заметим, что если отрезки $[a, b]$ и $[c, d]$ пересекаются, то точка пересечения – это середина каждого из отрезков. Действительно, любая точка отрезка, концы которого являются вершинами булева куба, имеет все координаты из множества $\{0, \gamma, 1-\gamma, 1\}$ для некоторого $\gamma \leqslant 1/2$. Если $\gamma < 1/2$ (т.е. это не середина отрезка), то по координатам этой точки концы отрезка восстанавливаются однозначно.

Следовательно, условие 2-независимости равносильно тому, что для любых четырех различных точек $a, b, c, d \in \mathcal{C}$ справедливо $a+b \neq c+d$ (то свойство, что никакая точка-вершина куба не может быть выпуклой комбинацией других точек-вершин, очевидно). В свою очередь, это аналог хорошо известного определения последовательности Сидона [5, 6] или B_2-последовательности [7], примененного к булевому кубу как подмножеству $\mathbb{R}^n$, или, что то же самое, сигнатурный код для двоичного суммирующего канала с двумя активными пользователями [8, 9].

Пример. Легко проверить, что для кода

$$\mathcal{C} = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1), (1,1,1)\}$$

все попарные суммы векторов различны, т.е. код является 2-независимым.

С другой стороны, несложно показать, что не существует 2-независимого кода мощности 6, и следовательно, $M_1(2\,|\,3) = 5$.

Ниже мы увидим, что при любом фиксированном t величина $M_1(t\,|\,n)$ растет экспоненциально от n и поэтому естественно рассматривать "скорость" $R_t^{(1)}$ ее роста, определяемую как

$$R_t^{(1)} := \lim_{n\to\infty} n^{-1} \log_2 M_1(t\,|\,n), \tag{4}$$

где предел не обязан существовать, и строго говоря, нужно рассматривать соответствующие верхний и/или нижний пределы.

Вернемся к случаю $t = 2$. Так как столбцы проверочной матрицы кода, исправляющего две ошибки, являются B_2-последовательностью в группе $\mathbb{Z}_2^n$, т.е. их попарные суммы различны по модулю 2, то следовательно, эти суммы различны и как целые числа. Взяв примитивный код БЧХ (или неприводимый код Гоппы), получим, что $R_2^{(1)} \geqslant 1/2$.

С другой стороны, из очевидного аналога границы Хэмминга

$$M_1(t\,|\,n)(M_1(t\,|\,n) - 1) \leqslant 3^n$$

(см. общий случай (7) ниже) следует, что

$$R_2^{(1)} \leqslant 0{,}5 \log_2 3.$$

Лучшая известная верхняя граница

$$R_2^{(1)} \leqslant 0{,}5753$$

была получена в [7].

Теперь перейдем к тематике комбинаторного поиска, а именно к задаче поиска фальшивых монет на точных весах. Рассмотрим два крайних варианта постановки задачи, различающиеся тем, какая информация известна априори. Пусть имеется m монет, из которых не более t фальшивых. В первой, традиционной постановке задачи предполагается, что все правильные монеты имеют вес α, все фальшивые – вес β, причем величины α, β известны заранее. Будем называть это задачей поиска (фальшивых монет) с полной информацией.

Во второй постановке задачи известно лишь, что все правильные монеты имеют один и тот же вес, а вот веса фальшивых монет могут различаться. Будем называть это задачей поиска с минимальной априорной информацией.

Обозначим через $M_2(t\,|\,n)$ максимальное число монет, среди которых можно найти t фальшивых не более чем за n взвешиваний для задачи поиска с полной информацией, и через $M_3(t\,|\,n)$ – для задачи поиска с минимальной априорной информацией. Также рассмотрим функцию $n(t\,|\,m)$, обратную к $M_2(t\,|\,n)$ и определяемую для задачи поиска с полной информацией как минимальное число взвешиваний, необходимое, чтобы найти среди m монет все фальшивые, если известно, что таковых не более t.

Мы рассматриваем только так называемый *неадаптивный поиск*, т.е. когда взвешивания производятся одновременно.

Обозначим вес j-й монеты через x_j и рассмотрим вектор $\boldsymbol{x} = (x_1, \ldots, x_m)$, который мы хотим найти с помощью взвешивания групп монет на точных весах. Взвешивание (тест) множества монет $J \subset \{0, 1, \ldots, m\}$ выдает в качестве результата суммарный вес $s(J)$ взвешиваемых монет

$$s(J) = \sum_{j \in J} x_j = (\boldsymbol{x}, \boldsymbol{h}),$$

где $\boldsymbol{h}$ – характеристический вектор множества J. Пусть $J_1, \ldots, J_n$ обозначают множества взвешиваемых монет, $\boldsymbol{h}^{(1)}, \ldots, \boldsymbol{h}^{(n)}$ – их характеристические векторы, и пусть $s_k := (\boldsymbol{x}, \boldsymbol{h}^{(k)})$ – результат взвешивания множества J_k. Двоичную $(n \times m)$-матрицу H, строками которой являются векторы $\boldsymbol{h}^{(1)}, \ldots, \boldsymbol{h}^{(n)}$, будем называть матрицей измерений. Тогда результаты взвешиваний можно записать в виде уравнения

$$H\boldsymbol{x}^T = \sum_{j=1}^{m} x_j \boldsymbol{h}_j = \boldsymbol{s}, \tag{5}$$

где вектор-синдром $\boldsymbol{s} = (s_1, \ldots, s_n)$ состоит из результатов взвешиваний, а $\boldsymbol{h}_j$ – j-й столбец матрицы H.

В задаче с полной информацией величина $s(J)$ дает нам точное число фальшивых монет среди взвешенных. Действительно,

$$s(J) = \beta|J \cap E| + \alpha(|J| - |J \cap E|) = \alpha|J| + (\beta - \alpha)|J \cap E|,$$

где E – множество номеров фальшивых монет.

Введем модифицированные результаты взвешиваний

$$\widehat{s_k} := \frac{s_k - \alpha \operatorname{wt}(\boldsymbol{h}^{(k)})}{\beta - \alpha}$$

и, соответственно, модифицированный вектор-синдром $\widehat{\boldsymbol{s}} = (\widehat{s}_1, \ldots, \widehat{s}_n)$, где $\operatorname{wt}(\boldsymbol{h}) = |\{i : h_i \neq 0\}|$ – вес Хэмминга вектора $\boldsymbol{h}$. Тем самым, задача свелась к поиску двоичной $(n \times m)$-матрицы H с максимальным m при заданном n, для которой

уравнение

$$\widehat{\boldsymbol{s}} = H\boldsymbol{y}^T, \tag{6}$$

называемое далее синдромным, имеет не более одного *двоичного* решения $\boldsymbol{y}$ с весом Хэмминга $\mathrm{wt}(\boldsymbol{y}) \leqslant t$, где $\boldsymbol{y}$ – характеристический вектор множества E номеров фальшивых монет. Это уравнение играет роль, аналогичную роли синдромного уравнения для кодов, исправляющих ошибки. Условие, что все суммы по t или меньше стобцов матрицы H, рассматриваемых как вещественные векторы, различны, очевидно равносильно тому, что уравнение (6) имеет не более одного решения веса Хэмминга не более t. Напомним, что код $\mathcal{C} \subset B^n$ называется t-сигнатурным кодом для двоичного суммирующего канала множественного доступа, если все суммы его слов по t или меньше различны и отличны от нуля (см. [8]). Тем самым, матрица H является искомой тогда и только тогда, когда ее столбцы образуют t-сигнатурный код, и величина $M_2(t\,|\,n)$ – это максимально возможная мощность t-сигнатурного кода. Взаимосвязи кодов для каналов множественного доступа и комбинаторной теории поиска посвящено множество работ, начиная с [10, 11].

Задача поиска с полной информацией – классическая, она восходит к работе Эрдеша и Реньи [12], где были получены верхние и нижние границы величины $n(t\,|\,m)$ для случая, когда $t = m$. Затем в [13, 14] была найдена лучшая верхняя граница, асимптотически совпавшая с нижней границей из [12], и тем самым, было доказано, что

$$n(m\,|\,m) = \frac{m}{2\log_2 m}(1 + o(1)).$$

Этот результат был обобщен на недвоичный случай в [15].

Так как суммы по t или менее векторов кода $\mathcal{C}$ мощности m принадлежат множеству $\{0, 1, \ldots, t\}^n$ из $(t+1)^n$ элементов и при этом различны, то

$$\sum_{i=0}^{t} \binom{m}{i} \leqslant (t+1)^n. \tag{7}$$

Определим, аналогично (4), "скорость" роста величины $M_2(t\,|\,n)$ как

$$R_t^{(2)} := \lim_{n\to\infty} n^{-1} \log_2 M_2(t\,|\,n).$$

Из (7) следует, что

$$R_t^{(2)} \leqslant \frac{\log_2 t}{t}(1 + o(1)). \tag{8}$$

Отметим, что эту асимптотическую границу можно в два раза улучшить [10].

Теперь перейдем к задаче поиска в условиях минимальной информации. Эта задача была поставлена и во многом решена в работе [16]. Начнем с замечания из [16] о том, что неизвестный вес α правильной монеты можно найти взвешиванием поодиночке произвольных $2t+1$ монет, поскольку вес α появится среди $2t+1$ результатов взвешивания как минимум $t+1$ раз.

Зная вес α, перепишем синдромное уравнение (5) в виде

$$\boldsymbol{s} = \sum_{j=1}^{m} x_j \boldsymbol{h}_j = \alpha \sum_{j=1}^{m} \boldsymbol{h}_j + \sum_{j\in E} (x_j - \alpha)\boldsymbol{h}_j = \alpha \sum_{j=1}^{m} \boldsymbol{h}_j + H\boldsymbol{y}^T, \tag{9}$$

где вектор $\boldsymbol{y} = (y_1, \ldots, y_m)$ состоит из новых, искусственно введенных весов $y_j := x_j - \alpha$, а $E \subset \{0, 1, \ldots, m\}$, как и выше, – множество позиций фальшивых монет.

Приведем синдромное уравнение к виду

$$\widehat{\boldsymbol{s}} = H\boldsymbol{y}^T, \tag{10}$$

где вектор

$$\widehat{\boldsymbol{s}} = \boldsymbol{s} - \alpha \sum_{j=1}^{m} \boldsymbol{h}_j$$

будем называть модифицированным синдромом. Напомним, что *вектор* $\boldsymbol{y}$ *называется* t*-разреженным, если мощность его носителя* $\operatorname{supp}(\boldsymbol{y}) := \{i : y_i \neq 0\}$ *не превышает* t. Следовательно, задача поиска фальшивых монет в предположении, что вес α правильной монеты известен, равносильна задаче о максимально возможном числе столбцов m в *двоичной* матрице с заданным числом строк n, такой что уравнение (10) при любом $\widehat{\boldsymbol{s}}$ имеет не более одного t-разреженного решения $\boldsymbol{y} \in \mathbb{R}^m$. Это условие, в свою очередь, равносильно тому, что любые $2t$ столбцов матрицы линейно независимы.

Легко видеть, что все три задачи могут быть переформулированы как условие, что синдромное уравнение (10) имеет не более одного t-разреженного решения $\boldsymbol{y}$, где сами задачи различаются соответствующими дополнительными ограничениями на координаты вектора $\boldsymbol{y}$.

А именно, определения 1 или 2 приводят к ограничению, что рассматриваются только стохастические векторы-решения $\boldsymbol{y}$, т.е. такие, что все $y_i \geqslant 0$ и $\sum\limits_{i=1}^{m} y_i = 1$.

Вторая задача – поиск фальшивых монет с полной информацией – описывается тем ограничением, что вектор $\boldsymbol{y}$ двоичный.

Наконец, третья задача – при дополнительном предположении, что известен вес правильной монеты – не накладывает никаких ограничений на вектор $\boldsymbol{y}$, кроме того, что он t-разрежен. Эта задача, как мы только что отмечали, равносильна задаче о максимальном *двоичном* коде, в котором любые $2t$ векторов линейно независимы над полем $\mathbb{R}$.

Тем самым,

$$m^*(t\,|\,n) \leqslant M_1(t\,|\,d), \quad m^*(t\,|\,d) \leqslant M_2(t\,|\,d)$$

и

$$m^*(t\,|\,d) + 2t + 1 \leqslant M_3(t\,|\,d),$$

где $m^*(t\,|\,n)$ обозначает максимальную мощность n-мерного двоичного кода, в котором любые $2t$ векторов линейно независимы над $\mathbb{R}$.

Отметим, что в [16] была доказана асимптотическая нижняя граница

$$R^*(t) := \limsup_{n\to\infty} n^{-1} \log_2 m^*(t\,|\,n) = \Omega(t^{-1}\log t),$$

которая тем самым справедлива для скоростей оптимальных кодов во всех рассматриваемых задачах.

С другой стороны, если во второй задаче предположить, что число фальшивых монет заранее известно и равно t, то это требование оказывается самым слабым из всех перечисленных выше задач. Поэтому для всех трех задач справедливо неравенство

$$\binom{m}{t} \leqslant (t+1)^n$$

(ср. неравенство (7)), и следовательно, для них справедлива асимптотическая верхняя оценка (8) на скорость соответствующих кодов.

Таким образом, мы установили следующее:

Для всех трех задач порядок скорости наилучшего кода равен $t^{-1}\log t$.

§ 2. Ошибки в измерениях и каналах

Перейдем теперь к рассмотрению случая, когда имеются ошибки, например, когда в задаче поиска появляются ошибки во взвешиваниях, или когда ошибки возникают на выходе двоичного суммирующего канала. Как мы увидим ниже, наличие ошибок вносит существенные различия в описанные выше три задачи. Так, например, определения 1 и 2 перестают быть эквивалентными.

Расширим определение 1 на случай ошибок. Очевидно, что для двоичных векторов евклидово расстояние и расстояние Хэмминга связаны соотношением $D^2(\boldsymbol{a},\boldsymbol{b}) = d(\boldsymbol{a},\boldsymbol{b})$ для любых $\boldsymbol{a},\boldsymbol{b}\in B^n$.

Определение 3. Множество $\mathcal{C}$ вершин n-мерного булева куба B^n называется (t,δ)-независимым кодом, если для любых его двух непересекающихся подмножеств $A,B\subset\mathcal{C}$, таких что $|A|,|B|\leqslant t$, их выпуклые оболочки находятся на евклидовом расстоянии не меньше чем δ друг от друга, т.е.

$$D(\langle A\rangle,\langle B\rangle) := \min_{\substack{\boldsymbol{a}\in\langle A\rangle\\ \boldsymbol{b}\in\langle B\rangle}} D(\boldsymbol{a},\boldsymbol{b}) \geqslant \delta. \tag{11}$$

Мы отмечали в § 1, что определение 2 является математической формулировкой задачи о мультимедийных кодах отпечатков пальцев, устойчивых к линейным атакам коалиций, где под линейной атакой коалиции $A\subset\mathcal{C}$ понимается создание ложного вектора $\widehat{\boldsymbol{a}} = \sum\limits_{\boldsymbol{a}\in A} p_{\boldsymbol{a}}\boldsymbol{a}$, где все $p_{\boldsymbol{a}}\geqslant 0$ и $\sum\limits_{\boldsymbol{a}\in A} p_{\boldsymbol{a}} = 1$, и нужно уметь находить A по $\widehat{\boldsymbol{a}}$. Следовательно, использование (t,δ)-независимого кода гарантирует, что если происходящие ошибки имеют евклидову длину не более $\delta/2$, то любые две коалиции, способные породить данный ложный вектор, имеют непустое попарное пересечение. Это свойство аналогично так называемому свойству secure frameproof, введенному ранее для обычных кодов цифровых отпечатков пальцев. Однако оно не только не позволяет найти всю коалицию, но даже не гарантирует нахождение хотя бы одного участника коалиции, так как пересечение всех коалиций, способных породить данный вектор, может быть пусто (см. [3]).

Отметим, что произвольное t-независимое множество $\mathcal{C}$ является одновременно и (t,δ)-независимым кодом. Действительно, достаточно положить

$$\delta = d_t(\mathcal{C}) := \min_{\substack{A,B\subset\mathcal{C}\\ A\cap B=\varnothing\\ |A|=|B|=t}} D(\langle A\rangle,\langle B\rangle). \tag{12}$$

Естественно рассмотреть величину $M_1(t,\delta\,|\,n)$, равную максимальной мощности (t,δ)-независимого кода в n-мерном булевом кубе. Нам неизвестно, как ведет себя величина $\delta(t)$, такая что $M_1(t,\delta\,|\,n)$ растет экспоненциально от n при $\delta<\delta(t)$ и фиксированном t. Более того, нам это неизвестно даже для случая $t=2$.

Заметим, что если взять в качестве кода $\mathcal{C}$ двоичный код длины n с минимальным расстоянием Хэмминга $d=\tau n$, где $0<\tau<1/2$, и мощности $M = 2^{(R(\tau)+o(1))n}$ с $R(\tau)>0$, то все вершины будут на попарном евклидовом расстоянии не менее чем $\sqrt{\tau n}$, однако это не гарантирует даже свойство t-независимости (т.е. выпуклые оболочки могут пересекаться).

Согласно определению 2 множество $\mathcal{C} \subset B^n$ называется t-независимым, если для любых двух различных подмножеств $A, B \subset \mathcal{C}$ мощности не более t каждое их выпуклые оболочки не пересекаются по строго внутренней точке. Очевидно, что сколь угодно малая ошибка может нарушить это свойство.

Рассмотрим для примера $t = 2$, $A = \{\boldsymbol{a}, \boldsymbol{c}\}$, $B = \{\boldsymbol{b}, \boldsymbol{c}\}$ и две внутренние точки:

$$\boldsymbol{x_a} = \varepsilon\boldsymbol{a} + (1-\varepsilon)\boldsymbol{c} \in A \quad \text{и} \quad \boldsymbol{x_b} = \varepsilon\boldsymbol{b} + (1-\varepsilon)\boldsymbol{c} \in B,$$

находящиеся на расстоянии $\varepsilon\|\boldsymbol{a} - \boldsymbol{b}\|_2$ друг от друга. Иначе говоря, малые ошибки $-\varepsilon\boldsymbol{a}$ и $-\varepsilon\boldsymbol{b}$, соответственно, переведут эти точки в точку $(1-\varepsilon)\boldsymbol{c}$.

Это замечание может быть интерпретировано как то, что мультимедийные коды отпечатков пальцев не способны полностью найти коалицию недобросовестных пользователей в условиях общей линейной атаки и сколь угодно малого целенаправленного шума (см. [17]). Тем не менее, как было показано в [18], такие коды существуют, если ограничиться атакой усреднения, т.е. когда ложный вектор $\widehat{\boldsymbol{a}} = |A|^{-1} \sum\limits_{\boldsymbol{a}\in A} \boldsymbol{a}$. Иначе говоря, мы ослабляем условие на расстояние между выпуклыми оболочками различных t-подмножеств, а именно требуем только, чтобы центры масс выпуклых оболочек были друг от друга на расстоянии не меньше заданного порога, равного удвоенной длине ошибки. Если мощность коалиции известна априори, то возникающая задача превращается в задачу 2 поиска фальшивых монет при полной информации и ошибках измерений, или, что равносильно, задачу о сигнатурных кодах для двоичного суммирующего канала, исправляющих ошибки на выходе канала.

Код $\mathcal{C} \subset B^n$ будем называть (t, δ)-сигнатурным кодом для двоичного суммирующего канала, если любые две суммы его слов по t или меньше не просто различны, а находятся на евклидовом расстоянии не менее δ друг от друга. Таким образом, (t, δ)-сигнатурный код способен правильно находить группу из не более чем t активных пользователей в условиях, когда выход двоичного суммирующего канала может быть искажен ошибкой длины (евклидовой) меньше $\delta/2$.

Напомним конструкцию (t, δ)-сигнатурных кодов из [18]. Рассмотрим двоичный n-мерный код $\mathcal{H}$ мощности m, который состоит из столбцов проверочной $(n \times m)$-матрицы двоичного примитивного кода БЧХ длины $m = 2^{n/t} - 1$ или неприводимого кода Гоппы длины $m = 2^{n/t}$, исправляющих t ошибок, где n – число проверочных символов данных кодов. Кроме того, пусть V – линейный двоичный код длины N с n информационными символами и минимальным кодовым расстоянием $d(V)$, а $\varphi\colon B^n \to V \subset B^N$ – произвольное систематическое кодирование этого кода.

В [18] было показано, что двоичный код

$$\mathcal{H}' = \varphi(\mathcal{H}) = \{\varphi(h) :\ h \in \mathcal{H}\} \subset V$$

длины N является (t, δ)-сигнатурным кодом с $\delta = \sqrt{d(V)}$. Если взять в качестве V коды мощности 2^{RN} с линейно растущим по N расстоянием $d(V) = \tau N$, то получатся (t, δ)-сигнатурные коды с расстоянием $\delta(V)$, растущим как $c\sqrt{N}$. Так как рассматриваемые коды двоичные, то евклидова длина кодовых векторов имеет порядок $\Omega(\sqrt{N})$, и следовательно, минимальное расстояние этих кодов имеет оптимальный порядок $\Omega(\sqrt{N})$. Важно отметить, что данные коды можно строить со сложностью, полиномиальной от N, т.е., с *полилогарифмической сложностью по* m. Отметим, что случайное кодирование позволяет увеличить скорость в $\log t$ раз и, тем самым, получить коды с оптимальной по порядку скоростью (см. [19]).

Также отметим, что схожая постановка задачи была исследована в [20], где рассматривалась вероятностная модель ошибок (с нормальным распределением).

Перейдем теперь к задаче 3 и рассмотрим наиболее общий вариант постановки задачи, когда, несмотря на ошибки в измерениях, требуется найти не только фальшивые монеты, но и веса всех монет. Заметим, что нахождение веса правильной монеты уже не так очевидно, как в случае, когда ошибок нет, поэтому мы будем рассматривать упрощенный вариант, когда вес правильной монеты известен и равен 0. Для $(n \times m)$-матрицы H измерений и неизвестного t-разреженного вектора $\boldsymbol{y} \in \mathbb{R}^m$ соответствующее синдромное уравнение примет вид

$$\widehat{\boldsymbol{s}} = H\boldsymbol{y}^T + \boldsymbol{e}, \tag{13}$$

где $\boldsymbol{e} \in \mathbb{R}^n$ – вектор ошибки длины $\|\boldsymbol{e}\|_2 \leqslant \varepsilon$.

Задача нахождения разреженного решения уравнения (13) стала популярной после основополагающих работ [21, 22], в которых было предложено искать аппроксимацию такого решения уравнения (13) заменой минимизации веса Хэмминга решения на минимизацию его ℓ_1-нормы. А именно было предложено рассмотреть задачу минимизации $\|\boldsymbol{y}\|_1$ при ограничении $\|\widehat{\boldsymbol{s}} - H\boldsymbol{y}^T\|_2 \leqslant \varepsilon$. Предложенный подход получил название сжатого измерения (compressed sensing). В качестве матриц измерений было предложено использовать матрицы со свойством ограниченной изометрии (restricted isometry property), или, сокращенно, RIP-матрицы.

Матрица H называется γ_t-RIP-матрицей, если для любого t-разреженного вектора $\boldsymbol{y} \in \mathbb{R}^n$ справедливо

$$(1 - \gamma_t)\|\boldsymbol{y}\|_2^2 \leqslant \|H\boldsymbol{y}^T\|_2^2 \leqslant (1 + \gamma_t)\|\boldsymbol{y}\|_2^2. \tag{14}$$

Обозначим через $\boldsymbol{y}^*$ вектор минимальной ℓ_1-нормы в множестве

$$\big\{\boldsymbol{z} \in \mathbb{R}^n : \ \|\widehat{\boldsymbol{s}} - H\boldsymbol{z}^T\|_2 \leqslant \varepsilon\big\}.$$

Основной результат теории сжатых измерений можно неформально сформулировать следующим образом: если параметр γ_T, где T в несколько раз больше t, достаточно мал, то $\|\boldsymbol{y}^* - \boldsymbol{y}\|_2 \leqslant C\varepsilon$. Приведем в качестве примера точной формулировки теорему 1 из [23]:

"Пусть для матрицы H выполнено $\gamma_{3t} + 3\gamma_{4t} < 2$. Тогда $\|\boldsymbol{y}^* - \boldsymbol{y}\|_2 \leqslant C_t\varepsilon$, где константа C_t зависит только от γ_{4t}. Например, $C_t \approx 8{,}82$ для $\gamma_{4t} = 1/5$."

В литературе, посвященной теории сжатых измерений, неоднократно указывалось, что для нахождения хорошей аппроксимации решения уравнения (13) достаточно найти носитель неизвестного вектора $\boldsymbol{y}$, а затем применить, например, метод наименьших квадратов. С другой стороны, нахождение хорошего приближения $\boldsymbol{y}^*$ еще не гарантирует, что носители векторов $\boldsymbol{y}^*$ и $\boldsymbol{y}$ совпадают, если не наложить то ограничение, что

$$y_{\min} = \min_{i \in \operatorname{supp}(y)} |y_i| \geqslant \Omega(\varepsilon).$$

В противном случае, как мы уже указывали, точное нахождение носителя невозможно. Тем не менее, если найдено хорошее приближение $\boldsymbol{y}^*$ к искомому вектору $\boldsymbol{y}$, а именно если $\|\boldsymbol{y}^* - \boldsymbol{y}\|_2 \leqslant \widehat{\varepsilon}$ и одновременно $y_{\min} > 2\widehat{\varepsilon}$, то $\operatorname{supp}(\boldsymbol{y}) = \{i : \ |y_i^*| > \widehat{\varepsilon}\}$.

В ряде работ (см. [24,25] и библиографию в них) был рассмотрен прямой подход к восстановлению носителя вектора с помощью RIP-матриц, что накладывало условия на величину γ_T для сравнительно малых T. Так, в [24] был предложен алгоритм, однозначно находящий носитель вектора $\boldsymbol{y}$, если выполнены условия

$$\gamma_{t+1}\sqrt{t+1} < 1 \quad \text{и} \quad y_{\min} > 2\varepsilon(1 - \gamma_{t+1}\sqrt{t+1})^{-1}.$$

Хорошо известно, что для RIP-матриц минимальное n имеет вид

$$n = \Omega\Big(t \log \frac{m}{t}\Big),$$

что при фиксированном t и растущем m дает $n = O(t \log m)$. Однако явные конструкции таких матриц неизвестны, тогда как (t, δ)-сигнатурные коды из [18] строятся явно и со сложностью $\mathrm{polylog}(m)$ (см. выше), и при этом имеют ту же асимптотику n, что и случайные RIP-матрицы. Недостаток кодов из [18] состоит в том, что они позволяют находить носитель только у таких t-разреженных векторов, что все их ненулевые координаты равны 1. Сейчас мы частично устраним этот недостаток.

Вектор $\boldsymbol{y}$ будем называть θ-равномерным в норме ℓ_1, если

$$\|\boldsymbol{y} - \mathbf{1}_E\|_1 = \sum_{i \in E} |y_i - 1| \leqslant \theta,$$

где E – носитель вектора $\boldsymbol{y}$, а $\mathbf{1}_E$ – характеристический вектор множества E.

Предложение 2. *Любой (t, δ)-сигнатурный код $\mathcal{H}$ позволяет находить носитель произвольного θ-равномерного вектора, если $\delta > 2(\theta h + \varepsilon)$, где h – максимальная евклидова длина векторов из $\mathcal{H}$.*

Доказательство. Пусть код $\mathcal{H} \subset B^n$ является (t, δ)-сигнатурным кодом, т.е. для любых двух различных подмножеств $A, B \subset \mathcal{H}$, таких что $|A| \leqslant t$, $|B| \leqslant t$, справедливо

$$\left\| \sum_{\boldsymbol{a} \in A} \boldsymbol{a} - \sum_{\boldsymbol{b} \in B} \boldsymbol{b} \right\|_2 \geqslant \delta.$$

Пусть $\boldsymbol{y}, \boldsymbol{y}'$ – два θ-равномерных t-разреженных вектора с различными носителями A и B соответственно, для которых $\|\widehat{\boldsymbol{s}} - H\boldsymbol{y}^T\|_2 \leqslant \varepsilon$ и $\|\widehat{\boldsymbol{s}} - H\boldsymbol{y}'^T\|_2 \leqslant \varepsilon$. Тогда

$$\Delta := \|H\boldsymbol{y}^T - H\boldsymbol{y}'^T\|_2 \leqslant 2\varepsilon.$$

Обозначим $\mu_{\boldsymbol{a}} = 1 - y_{\boldsymbol{a}}$, $\mu_{\boldsymbol{b}} = 1 - y_{\boldsymbol{b}}$ для $\boldsymbol{a} \in A$, $\boldsymbol{b} \in B$ соответственно. Тогда, с другой стороны,

$$\Delta = \left\| \left(\sum_{\boldsymbol{a} \in A} \boldsymbol{a} - \sum_{\boldsymbol{b} \in B} \boldsymbol{b} \right) - \sum_{\boldsymbol{a} \in A} \mu_{\boldsymbol{a}} \boldsymbol{h}_{\boldsymbol{a}} + \sum_{\boldsymbol{b} \in B} \mu_{\boldsymbol{b}} \boldsymbol{h}_{\boldsymbol{b}} \right\|_2 \geqslant \delta - 2\theta h > 2\varepsilon.$$

Полученное противоречие и доказывает утверждение. ▲

Мы *предполагаем*, что это утверждение можно распространить на произвольные t-разреженные векторы, или, по крайней мере, на стохастические разреженные векторы. Если эта гипотеза справедлива, то из [19, теорема 1] будет следовать существование матриц измерений с $n = \Omega\Big(t \dfrac{\log m}{\log t}\Big)$, позволяющих находить носитель t-разреженных векторов, что и будет асимптотическим ответом для задачи поиска носителя t-разреженного вектора для случая, когда t фиксировано, а размерность m вектора стремится к бесконечности.

СПИСОК ЛИТЕРАТУРЫ

1. *Cheng M., Miao Y.* On Anti-Collusion Codes and Detection Algorithms for Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2011. V. 57. № 7. P. 4843–4851. `https://doi.org/10.1109/TIT.2011.2146130`

2. *Егорова Е.Е., Кабатянский Г.А.* Разделимые коды для защиты мультимедиа от нелегального копирования коалициями // Пробл. передачи информ. 2021. Т. 57. № 2. С. 90–111. https://doi.org/10.31857/S0555292321020066
3. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Trans. Inform. Theory. 1998. V. 44. № 5. P. 1897–1905. https://doi.org/10.1109/18.705568
4. *Barg A., Blakley G.R., Kabatiansky G.A.* Digital Fingerprinting Codes: Problem Statements, Constructions, Identification of Traitors // IEEE Trans. Inform. Theory. 2003. V. 49. № 4. P. 852–865. https://doi.org/10.1109/TIT.2003.809570
5. *Erdős P., Turán P.* On a Problem of Sidon in Additive Number Theory, and on Some Related Problems // J. London Math. Soc. 1941. V. 16. № 4. P. 212–215. https://doi.org/10.1112/jlms/s1-16.4.212
6. *Babai L., Sós V.T.* Sidon Sets in Groups and Induced Subgraphs of Cayley Graphs // European J. Combin. 1985. V. 6. № 2. P. 101–114. https://doi.org/10.1016/S0195-6698(85)80001-9
7. *Cohen G., Litsyn S., Zémor G.* Binary B_2-Sequences: A New Upper Bound // J. Combin. Theory Ser. A. 2001. V. 94. № 1. P. 152–155. https://doi.org/10.1006/jcta.2000.3127
8. *Györfi L., Győri S., Laczay B., Ruszinkó M.* Lectures on Multiple Access Channels. Book draft, 2005. Available at http://www.szit.bme.hu/~gyori/AFOSR_05/book.pdf.
9. *Кабатянский Г.А. Лебедев В.С.* О метрической размерности недвоичных пространств Хэмминга // Пробл. передачи информ. 2018. Т. 54. № 1. С. 54–62. http://mi.mathnet.ru/ppi2259
10. *Дьячков А.Г., Рыков В.В.* Об одной модели кодирования для суммирующего канала с множественным доступом // Пробл. передачи информ. 1981. Т. 17. № 2. С. 26–38. http://mi.mathnet.ru/ppi1390
11. *Wolf J.K.* Born Again Group Testing: Multiaccess Communications // IEEE Trans. Inform. Theory. 1985. V. 31. № 2. P. 185–191. https://doi.org/10.1109/TIT.1985.1057026
12. *Erdős P., Rényi A.* On Two Problems of Information Theory // Magyar Tud. Akad. Mat. Kutató Int. Közl. 1963. V. 8. № 1–2. P. 229–243. Available at http://static.renyi.hu/renyi_cikkek/1963_on_two_problems_of_information_theory.pdf
13. *Lindström B.* On a Combinatory Detection Problem. I // Magyar Tud. Akad. Mat. Kutató Int. Közl. 1964. V. 9. № 1–2. P. 195–207.
14. *Cantor D.G., Mills W.H.* Determination of a Subset from Certain Combinatorial Properties // Canad. J. Math. 1966. V. 18. P. 42–48. https://doi.org/10.4153/CJM-1966-007-2
15. *Jiang Z., Polyanskii N.* On the Metric Dimension of Cartesian Powers of a Graph // J. Combin. Theory Ser. A. 2019. V. 165. P. 1–14. https://doi.org/10.1016/j.jcta.2019.01.002
16. *Bshouty N.H., Mazzawi H.* On Parity Check $(0,1)$-Matrix over $\mathbb{Z}_p$ // Proc. 22nd Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'11). San Francisco, CA. Jan. 23–25, 2011. P. 1383–1394. https://dl.acm.org/doi/10.5555/2133036.2133142
17. *Fan J., Gu Y., Hachimori M., Miao Y.* Signature Codes for Weighted Binary Adder Channel and Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2021. V. 67. № 1. P. 200–216. https://doi.org/10.1109/TIT.2020.3033445
18. *Егорова Е.Е., Фернандес М., Кабатянский Г.А., Мяо И.* Существование и конструкции мультимедийных кодов, способных находить полную коалицию при атаке усреднения и шуме // Пробл. передачи информ. 2020. Т. 56. № 4. С. 97–108. https://doi.org/10.31857/S0555292320040087
19. *Vorobyev I.* Complete Traceability Multimedia Fingerprinting Codes Resistant to Averaging Attack and Adversarial Noise with Optimal Rate // Des. Codes Cryptogr. 2022. Open Access Article. https://doi.org/10.1007/s10623-022-01144-x
20. *Gkagkos M., Pradhan A.K., Amalladinne V., Narayanan K., Chamberland J-F., Georghiades C.N.* Approximate Support Recovery Using Codes for Unsourced Multiple Access // Proc. 2021 IEEE Int. Symp. on Information Theory (ISIT'2021). Melbourne, Australia. July 12–20, 2021. P. 2948–2953. https://doi.org/10.1109/ISIT45174.2021.9517995
21. *Donoho D.L.* Compressed Sensing // IEEE Trans. Inform. Theory. 2006. V. 52. № 4. P. 1289–1306. https://doi.org/10.1109/TIT.2006.871582

22. *Candès E.J., Tao T.* Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? // IEEE Trans. Inform. Theory. 2006. V. 52. № 12. P. 5406–5425. https://doi.org/10.1109/TIT.2006.885507
23. *Candès E.J., Romberg J.K., Tao T.* Stable Signal Recovery from Incomplete and Inaccurate Measurements // Comm. Pure Appl. Math. 2006. V. 59. № 8. P. 1207–1223. https://doi.org/10.1002/cpa.20124
24. *Wen J., Zhou Z., Wang J., Tang X., Mo Q.* A Sharp Condition for Exact Support Recovery with Orthogonal Matching Pursuit // IEEE Trans. Signal Process. 2017. V. 65. № 6. P. 1370–1382. https://doi.org/10.1109/TSP.2016.2634550
25. *Mehrabi M., Tchamkerten A.* Error-Correction for Sparse Support Recovery Algorithms // Proc. 2021 IEEE Int. Symp. on Information Theory (ISIT'2021). Melbourne, Australia. July 12–20, 2021. P. 1754–1759. https://doi.org/10.1109/ISIT45174.2021.9518027

Джанабекова Алия
Московский физико-технический институт
(государственный университет),
факультет управления и прикладной математики,
кафедра проблем передачи информации и анализа данных
dzhanabekova@phystech.edu
Кабатянский Григорий Анатольевич
Сколковский институт науки и технологий (Сколтех)
g.kabatyansky@skoltech.ru
Камель Ибрахим (Kamel, Ibrahim)
Рабие Тамер Фарук (Rabie, Tamer Farouk)
Университет Шарджи, Шарджа, ОАЭ
Kamel@sharjah.ac.ae
trabie@sharjah.ac.ae

Поступила в редакцию
01.11.2022
После доработки
22.11.2022
Принята к публикации
23.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.725

© 2022 г. **П. Бойваленков[1], К. Делчев[2], В.А. Зиновьев[3], Д.В. Зиновьев[3]**

О КОДАХ С РАССТОЯНИЯМИ d И n

Перечислены все q-ичные аддитивные (и в частности, линейные) блоковые коды длины n и мощности $N \geqslant q^2$, имеющие ровно два расстояния: d и n. Для произвольных кодов длины n с расстояниями d и n получены верхние оценки на мощность с помощью линейного программирования и через связь с множествами точек на евклидовой сфере с двумя расстояниями.

Ключевые слова: код с двумя расстояниями, двухвесовой код, линейный двухвесовой код, разностная матрица, максимальная дуга, латинский квадрат, ортогональная таблица, оценка на коды, граница линейного программирования, сферический код.

DOI: 10.31857/S0555292322040064, **EDN:** NAWXWG

§ 1. Введение

В статье рассматриваются q-ичные блоковые коды длины n, имеющие ровно два расстояния – d и n. Коды с двумя расстояниями – это классический объект исследования в алгебраической теории кодирования в течение более 55 лет. Исчерпывающий обзор таких кодов можно найти в работе [1]. Построение новых семейств таких кодов, так же как и описание некоторых существующих классов таких кодов, остаются важнейшими открытыми проблемами алгебраической теории кодирования (см., например, работу [2] и библиографию в ней). Несмотря на многие известные бесконечные классы двухвесовых кодов, полная классификация таких линейных кодов весьма далека от завершения. Даже в случае кодов с расстояниями d и n до этой статьи мы не могли сказать, что все такие коды известны.

В двух предыдущих работах [3, 4] мы описали такие коды для специального случая, когда два расстояния – это d и $d+1$, и показали, что все такие коды получаются из эквидистантных кодов двумя способами: либо добавлением одной произвольной позиции (так чтобы сохранить линейность кода) ко всем словам, либо выбрасыванием одной произвольной позиции из всех кодовых слов. Затем в работах [5, 6] мы рассмотрели произвольные линейные и нелинейные коды с двумя весами d и $d+\delta$ и усилили известные результаты Дельсарта [7, 8], касающиеся необходимых условий существования таких проективных кодов. Следует также упомянуть работу [9], где с помощью описания всех дуг в проективной геометрии $PG(r, q)$ с кратностями

[1] Работа выполнена при частичной поддержке Национального научного фонда Болгарии (NSF) (проект КР-06-Russia/33-2020).

[2] Работа выполнена при частичной поддержке Национального научного фонда Болгарии (NSF) (проект КР-06-N32/2-2019).

[3] Исследования были выполнены в ИППИ им. А.А. Харкевича РАН в рамках проводимых фундаментальных исследований по теме “Математические теории корректирующих кодов”, а также поддержаны грантом Национального научного фонда Болгарии (номер проекта 20-51-18002).

пересекающих их гиперплоскостей w, $w+1$ и $w+2$ были классифицированы все q-ичные линейные коды с расстояниями d, $d+1$ и $d+2$.

Главная цель данной статьи – это перечисление аддитивных и неаддитивных (включая дистанционно инвариантные) блоковых кодов длины n, имеющих ровно два расстояния для очень специального случая, когда эти расстояния равны d и n. Интересно, что линейные коды такого вида имеют порождающие матрицы, связанные с порождающими матрицами эквидистантных линейных кодов (они получаются из последних добавлением нулевого столбца и строки из всех единиц). Этот эффект был замечен в [10] в терминах полностью регулярных кодов с радиусом покрытия $\rho = 2$. Мы приводим необходимые и достаточные условия для существования таких кодов и даем их простое описание. Мы также приводим некоторые новые верхние оценки на мощность таких произвольных кодов ровно с двумя расстояниями d и n. Одна из таких оценок это граница линейного программирования, а другая оценка связана со сферическими кодами, имеющими между кодовыми точками ровно два расстояния в евклидовой метрике.

§ 2. Предварительные результаты

Пусть $q \geqslant 2$ – целое положительное число, и пусть всюду далее $Q = \{0, 1, \ldots, q-1\}$ – абелева группа, представленная в аддитивной форме, с нейтральным элементом 0. Любое подмножество $C \subseteq Q^n$ представляет собой код длины n, мощности $N = |C|$ с минимальным расстоянием d (т.е. $d = \min\{d(x,y) : x, y \in C,\ x \neq y\}$), где

$$d(x,y) = |\{i\} : x_i \neq y_i,\ i = 1, \ldots, n\}| \quad \text{для } x = (x_1, \ldots, x_n) \text{ и } y = (y_1, \ldots, y_n),$$

который обозначается через $(n, N, d)_q$. Если q – степень простого числа, то Q – это множество элементов поля Галуа $\mathbb{F}_q$, которые мы также будем обозначать через $0, 1, \ldots, q-1$, но операции над этими элементами будут осуществляться в поле $\mathbb{F}_q$. Если $(n, N, d)_q$-код C представляет собой k-мерное подпространство линейного пространства Q^n, то мы используем для такого кода стандартное обозначение $[n, k, d]_q$, где $N = q^k$. Для двоичного случая, т.е. когда $q = 2$, символ q опускается и используются обозначения (n, N, d) и $[n, k, d]$ соответственно. В настоящей статье под понятием *аддитивный* мы имеем ввиду абелеву подгруппу в абелевой группе Q^n с аддитивной покоординатной операцией в Q (так что, конечно, эти коды включают в себя и линейные коды).

Пусть $(n, N, \{d, n\})_q$ обозначает $(n, N, d)_q$-код $C \subset Q^n$, обладающий следующим свойством: для любых двух различных кодовых слов x и y кода C расстояние Хэмминга $d(x, y)$ между этими словами равно либо d, либо n. Если не оговорено противное, то мы всегда полагаем, что в таком коде оба расстояния d и n реализуются.

Нас будут интересовать вопросы существования, построения и перечисления таких $(n, N, \{d, n\})_q$-кодов, а также верхние оценки максимально возможной мощности произвольных кодов такого вида.

Мы не рассматриваем тривиальные случаи таких кодов, как, например, повторение двух (или более) $(n_1, N, \{d_1, n_1\})_q$- и $(n_2, N, \{d_2, n_2\})_q$-кодов с одинаковыми или разными параметрами, эквидистантные коды, коды с тривиальными (т.е. постоянными) координатными позициями и так далее.

Определение 1. Пусть G – абелева группа порядка q, представленная в аддитивном виде. Квадратная матрица D порядка $q\mu$ с элементами из G называется *разностной матрицей* и обозначается через $D = D(q, \mu)$, если покоординатная разность любых двух ее различных строк содержит каждый элемент G ровно μ раз.

Ясно, что матрица D инвариантна относительно сложения любой ее строки или столбца с постоянным вектором $(a, a, \ldots, a)$, где $a \in G$. Осуществляя такие операции, мы всегда можем привести разностную матрицу D к *нормализованной* разностной

матрице, которая имеет нулевую первую строку и нулевой первый столбец. В дальнейшем, если не оговорено противное, без ограничения общности мы всегда будем полагать, что разностная матрица представлена в нормализованной форме.

Из [11] (см. также [12]) известен следующий результат.

Лемма 1. *Для любого простого числа p и любых натуральных чисел ℓ и h существует разностная матрица $D(p^\ell, p^h)$.*

Опишем кратко построение всех таких разностных матриц $D(p^\ell, p^h)$ из работы [12]. Для любого целого $m \geqslant 1$ зафиксируем взаимно-однозначное соответствие между элементами поля $\mathbb{F}_{p^m}$ и элементами векторного пространства $\mathbb{F}_p^m$. Для любых натуральных чисел ℓ и h положим $u = \ell + h$. Для поля Галуа $\mathbb{F}_{p^u}$ с элементами $\{f_0 = 0,\ f_1 = 1,\ f_2,\ \ldots,\ f_{p^u-1}\}$ обозначим через $F = [f_{i,j}]$ матрицу размера $p^u \times p^u$, строки и столбцы которой индексированы элементами поля $\mathbb{F}_{p^u}$, где $f_{i,j} = f_i f_j$, т.е. F – таблица умножения элементов $\mathbb{F}_{p^u}$. Определим оператор $\Phi = \Phi_{u\to\ell}$, отображающий элементы $x = (x_1, \ldots, x_u)$ поля $\mathbb{F}_p^u$ в элементы $x^{(\ell)} = (x_1, \ldots, x_\ell)$ поля $\mathbb{F}_p^\ell$ путем удаления правых $u - \ell$ координатных позиций векторов из $\mathbb{F}_p^u$:

$$\Phi_{u\to\ell}(x_1, \ldots, x_\ell, \ldots, x_u) = (x_1, \ldots, x_\ell).$$

Обозначим через $F^{[\ell]}$ матрицу, полученную из матрицы F действием оператора Φ на все элементы матрицы F:

$$F^{[\ell]} = \left[f_{i,j}^{[\ell]}\right]: \quad f_{i,j}^{[\ell]} = \Phi_{u\to\ell}(f_{i,j}).$$

Получаем теперь (см. [11], а также [12]), что имеет место следующая

Лемма 2. *Для любого простого числа p и любых натуральных чисел ℓ и h матрица $F^{[\ell]}$ представляет собой аддитивную разностную матрицу $D = D(p^\ell, p^h)$. Если ℓ делит h, т.е. $N = p^{h+\ell} = p^{\ell(h/\ell+1)}$, то $F^{[\ell]}$ является векторным пространством, откуда вытекает, что разностная матрица D линейна.*

Опишем построение $(n, N, \{d, n\})_q$-кода на основе разностной матрицы $D(q, \mu)$ над G. В рассматриваемом случае $G = \mathbb{F}_q$. Предположим, что первая строка D состоит из нулей. Обозначим через $D^{(g)}$ матрицу, полученную из D прибавлением элемента $g \in G$ ко всем элементам D, т.е. если $D = [d_{i,j}]$, то $D^{(g)} = [d_{i,j} + g]$ для всех i и j (напомним, что сложение осуществляется в G). По определению D матрица $D^{(g)}$ является разностной матрицей $D(q, \mu)$. Из определения следует также, что для любых двух строк $\boldsymbol{r}$ из D и $\boldsymbol{r}^{(g)}$ из $D^{(g)}$ выполняется следующее свойство [12]:

$$d(\boldsymbol{r}, \boldsymbol{r}^{(g)}) = \begin{cases} q\mu, & \text{если } \boldsymbol{r}^{(g)} = \boldsymbol{r} + (g, g, \ldots, g), \\ (q-1)\mu, & \text{если } \boldsymbol{r}^{(g)} \neq \boldsymbol{r} + (g, g, \ldots, g). \end{cases} \tag{1}$$

Ясно, что матрица $D(q, \mu)$ индуцирует эквидистантный $(q\mu - 1, q\mu, \mu(q-1))_q$-код, оптимальный относительно верхней границы Плоткина

$$N \leqslant \frac{qd}{qd - (q-1)n}, \tag{2}$$

если знаменатель положителен. Чтобы убедится в этом, следует вначале представить D в нормализованной форме, при которой первый столбец состоит из нулей, а затем выкинуть этот тривиальный столбец. Из (1) вытекает следующий результат.

Лемма 3 [12]. *Строки $(N \times n)$-матрицы $\left[D^{(0)} \mid \ldots \mid D^{(q-1)}\right]^t$ образуют двухвесовой $(n, N, \{d, n\})_q$-код с параметрами*

$$n = q\mu, \quad N = q^2\mu, \quad d = \mu(q-1). \tag{3}$$

Назовем код C, основанный на разностной матрице D (как описано выше), *разностным матричным кодом*, или кратко *РМ-кодом*. Любой $(n, N, \{d, n\})_q$-код, параметры которого удовлетворяют (3), будем называть *псевдоразностным матричным кодом*, или кратко *ПРМ-кодом*. Ниже мы убедимся, что аддитивные ПРМ-коды представляют собой РМ-коды. Все эти коды оптимальны относительно q-ичного аналога верхней границы Грея – Рэнкина [13], которого они достигают с точным равенством. Любой q-ичный $(n, N, \{d, n\})_q$-код, который можно разбить на тривиальные $(n, q, n)_q$-подкоды (называемые *симплексами*), удовлетворяет этой границе [13]

$$\frac{N}{q} \leqslant \frac{q(qd - (q-2)n)(n-d)}{n - ((q-1)n - qd)^2} \tag{4}$$

при условии, что $n - ((q-1)n - qd)^2 > 0$.

Напомним также границу линейного программирования на мощность N кода C, в котором максимальное расстояние между кодовыми словами ограничено, скажем, величиной D (см. работы [14] для первого случая границы $D = n$ и [15] для общего случая). Для $D = n$ эта оценка выглядит следующим образом:

$$N \leqslant \frac{q^2 d}{dq - (q-1)(n-1)}, \tag{5}$$

если знаменатель положителен. Заметим, что $(n, N, \{d, n\})_q$-ПРМ-код достигает этой границы с точным равенством.

Как мы уже упоминали, мы рассматриваем не только аддитивные коды, но также и те, которые не являются аддитивными. В частности, рассматриваются *дистанционно инвариантные* коды, т.е. такие, весовой спектр которых не зависит от выбора нулевого слова.

Напомним, что q-ичная $(N \times n)$-матрица M называется *ортогональной таблицей* силы t индекса $\lambda = N/q^t$ с n ограничениями и обозначается через $\mathrm{OA}(N, n, q, t)$, если каждая $(N \times t)$-подматрица содержит в качестве строк каждый q-ичный вектор длины t ровно λ раз [16].

Будем говорить, что $(n+1, N, d^*)_q$-код C^*, где $d^* \in \{d, d+1\}$, получен расширением $(n, N, d)_q$-кода C, если ко всем кодовым словам кода C добавлена координатная позиция общей проверки на четность, т.е.

$$C^* = \{(c_1, \ldots, c_n, c_{n+1}) : (c_1, \ldots, c_n) \in C\}, \quad \text{где} \quad c_{n+1} = \sum_{i=1}^{n+1} c_i.$$

Следующий результат хорошо известен; его можно найти, например, в [17]. Для заданного q и натурального m введем величину $n_m = (q^m - 1)/(q-1)$.

Лемма 4. *Пусть $\mathcal{H}_m$ – $[n_m, k, 3]_q$-код Хэмминга. Тогда расширенный код $\mathcal{H}_m^*$ имеет минимальное расстояние 4, если и только если*

(i) $q = 2$ *и* $m \geqslant 2$, *или*

(ii) $q = 2^r \geqslant 4$ *и* $m = 2$, *т.е.* $n_m + 1 = q + 2$ *и* $k = q - 1$.

Для произвольного $(n, N, d)_q$-кода C определим его *радиус покрытия* $\rho = \rho_C$ как наименьшее целое число, такое что все шары радиуса ρ, проведенные вокруг всех кодовых слов C (с центрами в этих словах), покрывают все пространство Q^n.

§ 3. Необходимые условия

Естественный вопрос о существовании q-ичного двухвесового $(n, N, \{d, d+\delta\})_q$-кода – это при каких условиях существует такой код? Здесь мы отвечаем на этот

вопрос для случая, когда $d+\delta=n$ и код удовлетворяет некоторым условиям регулярности. Нам потребуются некоторые известные факты о проективных двухвесовых кодах (см. работы [1, 7, 8] и библиографию в них). Пусть $\mathrm{PG}(n,q)$ обозначает n-мерное проективное пространство над полем $\mathbb{F}_q$. Тогда *m-дуга* точек в $\mathrm{PG}(n,q)$, где $m \geqslant n+1$ и $n \geqslant 2$, – это множество M, содержащее m точек, такое что никакие $n+1$ точек множества M не лежат в гиперплоскости пространства $\mathrm{PG}(n,q)$. Дуга, содержащая $(q+1)$ точек $\mathrm{PG}(2,q)$, называется *овалом*, а дуга из $(q+2)$ точек пространства $\mathrm{PG}(2,q)$ для четного q называется *полным овалом*, или *гиперовалом* (см., например, [18–20]).

Линейный код C называется *проективным*, если дуальный к нему код $C^\perp$ имеет минимальное расстояние $d^\perp \geqslant 3$ (т.е. любая порождающая матрица C не содержит двух столбцов, являющихся скалярными кратными друг друга). Для проективных $[n,k,d]_q$-кодов C можно ввести понятие *дополнительного* к нему кода C_c (см., например, [1, 7]). Пусть $[C]$ обозначает матрицу, образованную всеми кодовыми словами кода C (т.е. строками $[C]$ являются кодовые слова C). Код C_c называется дополнительным к коду C, если матрица $\big[[C]\,|\,[C_c]\big]$ является линейным эквидистантным кодом и C_c имеет минимально возможную длину, обеспечивающую это свойство. Для данного $[n,k,d]_q$-кода C с проверочной матрицей H дополнительный к нему $[n_{n-k}-n,k,d_c]$-код C_c имеет проверочную матрицу H_c, полученную из матрицы H_{n-k} удалением всех столбцов матрицы H и столбцов, кратных столбцам H. Напомним важное свойство дополнительного кода: *любому кодовому слову веса w в $[n,k,d]_q$-коде C соответствует кодовое слово веса $w_c=q^{k-1}-w$ в дополнительном к нему коде C_c.* Следствием этого простого факта является

Лемма 5 [7]. *Линейный $[n,k,d]_q$-код C с радиусом покрытия $\rho=2$, не дуальный РМ-коду, существует одновременно с дуальным к нему проективным кодом C_c с тем же самым радиусом покрытия $\rho_c=2$.*

Обобщение этих хорошо известных фактов на произвольные линейные двухвесовые $[n,k,\{d,d+\delta\}]_q$-коды было получено в [5, 6]. Здесь мы приводим вариант этого результата на случай $[n,k,\{d,n\}]_q$-кодов. Для любого кода C с проверочной матрицей H обозначим через s максимальное число появлений любого столбца H с учетом кратных к нему столбцов, т.е. полученных из него умножением на ненулевой элемент поля $\mathbb{F}_q$.

Лемма 6 [5, 6]. *Пусть C – q-ичный линейный нетривиальный двухвесовой $[n,k,\{d,n\}]_q$-код, не дуальный s раз повторенному РМ-коду, и пусть μ_1 и μ_2 обозначают число кодовых слов веса d и n соответственно. Тогда существует дополнительный к нему линейный двухвесовой $[n_c,k,\{d_c,d_c+\delta\}]_q$-код C_c, такой что*

$$n+n_c=s\frac{q^k-1}{q-1},\quad d+d_c+\delta=sq^{k-1},\quad n=d+\delta,\quad s=1,2,\ldots,$$

причем C_c содержит μ_1 кодовых слов веса $d_c+\delta$ и μ_2 кодовых слов веса d_c, и C_c имеет минимально возможную длину n_c, такую что матрица $\big[[C]\,|\,[C_c]\big]$ представляет собой эквидистантный $[s(q^k-1)/(q-1),k,sq^{k-1}]_q$-код.

Заметим, что целое число s в лемме 6 является максимальным числом столбцов в порождающей матрице C, которые являются скалярными кратными одного столбца. Для проективных двухвесовых $[n,k,\{d,n\}]_q$-кодов (т.е. для случая $s=1$) известны следующие результаты.

Лемма 7 [8]. *Пусть C – проективный двухвесовой $[n,k,\{w,n\}]_q$-код над $\mathbb{F}_q$, где $q=p^m$ и p простое. Тогда существуют два целых числа $u\geqslant 0$ и $h\geqslant 1$, такие что*

$$w=hp^u,\quad n=(h+1)p^u.$$

Напомним для проективного случая следующий результат (который прямо вытекает из тождеств Мак-Вильямс, если принять во внимание, что дуальный код $C^\perp$ имеет минимальное расстояние $d^\perp \geqslant 3$) (см. [8]).

Лемма 8. *Пусть C – двухвесовой проективный $[n, k, \{w, n\}]_q$-код над $\mathbb{F}_q$, где $q = p^m$ и p – простое число. Обозначим через μ_1 и μ_2 число кодовых слов кода C веса w и n соответственно. Тогда*

$$\begin{cases} w\mu_1 + n\mu_2 = n(q-1)q^{k-1}, \\ w^2\mu_1 + n^2\mu_2 = n(q-1)(n(q-1)+1)q^{k-2}. \end{cases} \tag{6}$$

В [5, 6] (см. также [4] для специального случая $n - d = 1$) нами были получены условия целочисленности, аналогичные условиям, полученным Дельсартом в [8] (см. также [1]), для проективных двухвесовых кодов на основе простых комбинаторных аргументов, не связанных с собственными значениями сильно регулярных графов. Для случая произвольных двухвесовых $(n, N, \{d, n\})_q$-кодов с расстояниями d и n эти условия сводятся к следующему. Как и в работах [8] и [1], мы рассматриваем здесь только двухвесовые $(n, N, \{d, n\})_q$-коды мощности $N \geqslant q^2$. Имеются тривиальные и нетривиальные примеры таких кодов с $N \leqslant q^2$, которые мы упомянем ниже. Мы считаем такие коды неинтересными, так как их мощность не всегда оптимальна, т.е. не достигает верхних границ. Напомним, что под тривиальными кодами мы понимаем также такие двухвесовые коды, которые можно представить в виде прямой суммы (или повторения) двух или более $(n_i, N, \{d_i, n_i\})_q$-кодов.

Теорема 1. *Пусть Q – алфавит любого размера q, и пусть C – произвольный нетривиальный q-ичный двухвесовой $(n, N, \{d, n\})_q$-код, где $N \geqslant q^2$. Тогда*

(i) *Мощность N кода C лежит в следующих пределах*:

$$(q-1)n + 1 \leqslant N \leqslant \frac{q^2 d}{qd - (q-1)(n-1)} \tag{7}$$

при условии, что $qd - (q-1)(n-1) > 0$;

(ii) *Правое неравенство в (7) становится равенством, если и только если матрица $[C]$, образованная всеми кодовыми словами кода C, является ортогональной таблицей силы $t \geqslant 2$;*

(iii) *Если правое неравенство в (7) является равенством, то длина n и расстояние d кода C имеют следующий вид*:

$$n = \frac{N(q(d+1)-1) - q^2 d}{N(q-1)} \tag{8}$$

и

$$d = (n-1)\frac{(q-1)N}{q(N-q)}; \tag{9}$$

(iv) *Левое неравенство в (7) становится равенством, если и только если C – эквидистантный $(n, N, d)_q$-код;*

(v) *Если правое неравенство в (7) является равенством, то число N делит $q^2 d$, а число $q - 1$ делит $(N - 1)d$.*

Доказательство. (i) Для случая, когда C – произвольный q-ичный двухвесовой $(n, N, \{d, n\})_q$-код, это утверждение следует непосредственно из границы линейного программирования для этих кодов, которую мы приводим в п. 5.1. Для случая, когда C – ортогональная таблица силы $t \geqslant 2$, этот результат получается из аргументов, аналогичных тем, которые мы использовали в [6]. Здесь мы приведем простое доказательство для общего случая, когда C – произвольный дистанционно

инвариантный $(n, N, \{d, n\})_q$-код мощности $N \geqslant q^2$; приводимые здесь аргументы понадобятся нам в дальнейшем.

Предположим, что C содержит нулевое кодовое слово и μ кодовых слов веса d. Пусть код C^* состоит только из кодовых слов веса d, и пусть $[C^*]$ – матрица размера $\mu \times n$, строками которой являются слова кода C^*.

Сначала подсчитаем полное число нулей (которое мы обозначим Σ_0) в матрице $[C^*]$ двумя разными (очевидными) способами. Действительно, по определению

$$\Sigma_0 = \mu(n-d) = (N/q-1)n.$$

Далее, так как C дистанционно инвариантен, и следовательно, каждый столбец содержит одно и то же число нулей, а именно $N/q = \mu(n-d)/n + 1$, то получаем, что

$$\mu = \frac{n(N-q)}{q(n-d)}. \tag{10}$$

Затем найдем полное число $\Sigma_{(0,0)}$ пар координатных позиций, содержащих нулевые элементы $(0,0)$, которые встречаются во всех $n(n-1)/2$ позициях всех строк матрицы $[C^*]$. Обозначим через $s(i,j)$ число таких нулевых пар $(0,0)$, встречающихся в столбцах с номерами i и j матрицы $[C^*]$. Получаем очевидным образом

$$\left(\frac{N}{q^2} - 1\right) n(n-1) \leqslant \Sigma_{(0,0)} = \sum_{1 \leqslant i < j = n} s(i,j) = \mu(n-d)(n-d-1). \tag{11}$$

Подставляя выражение для μ из (10) в формулу (11), получаем следующее неравенство:

$$N\,(qd - (q-1)(n-1)) \leqslant q^2 d. \tag{12}$$

Отсюда получаем правое неравенство в (7), так как выполняется условие

$$qd - (q-1)(n-1) > 0.$$

Рассмотрим теперь левое неравенство в (7). Правое неравенство в (7) (которое имеет место для произвольного двухвесового $(n, N, \{d, n\})_q$-кода) влечет следующую верхнюю оценку на величину d:

$$d \leqslant (n-1)\frac{N(q-1)}{q(N-q)}.$$

Но величина d для $(n, N, \{d, n\})_q$-кода не может быть больше величины (обозначим ее через $d^{(p)}$), гарантируемой верхней границей Плоткина (2), которая точна для эквидистантного кода (действительно, средняя оценка по всем расстояниям всегда больше минимального расстояния кода с несколькими расстояниями). Поэтому из неравенства

$$d \leqslant (n-1)\frac{N(q-1)}{q(N-q)} \leqslant d^{(p)} = n\frac{(q-1)N}{q(N-1)}$$

получаем, что

$$(n-1)(N-1) \leqslant n(N-q),$$

откуда вытекает левое неравенство для N в формуле (7).

(ii) Правое неравенство в (7) становится равенством, если и только если выражение (11) является равенством. Это имеет место, когда код C удовлетворяет

следующему условию: *величина* $s_0(i,j) = s(i,j)$ *постоянна для любых выбранных позиций кода с номерами* i *и* j. Мы утверждаем, что это возможно только тогда, когда матрица $[C]$ является ортогональной таблицей силы $t \geqslant 2$. Предположим противное – пусть для некоторого элемента $a \in Q$ величина $s_a(i,j)$ не одна и та же для всех i и j. Тогда определим новый код $C^{(a)}$, полученный из C перестановкой элементов алфавита 0 и a во всех кодовых словах C. Производя для него такие же вычисления, мы придем к противоречию. Так как величина $s_a(i,j)$ не постоянна в выражении (7), мы получим строгое неравенство, противоречащее условию утверждения. Итак, заключаем, что матрица $[C]$ должна быть ортогональной таблицей. Но если $[C]$ – ортогональная таблица, то тогда $s_0(i,j) = s(i,j)$ является постоянной величиной для всех i j, выражение (11) представляет собой равенство, и следовательно, правое неравенство в (7) является равенством.

(iii) Если правая часть (7) является равенством, то это означает, что неравенство (11) также является равенством, что можно переписать в следующем виде:

$$(N - q^2)n(n-1) = qn(N-q)(n-d-1). \tag{13}$$

Поэтому можно выписать выражение для n как функции от q, d и N, получая таким образом (8), и выражение для d как функции от q, n и N, получая (9).

(iv) Условие $N = (q-1)n+1$ относится к случаю эквидистантных кодов, подробно рассмотренному в [21] (в этом случае матрица $[C]$ также является ортогональной таблицей силы $t = 2$).

(v) Так как n – натуральное число, мы заключаем из (13), что число d должно быть кратным N/q^2. Из этого же равенства, учитывая, что

$$N(q(d+1)-1) - q^2 d = (q-1)\left(N(d+1) - d(q+1)\right) + d(N-1),$$

мы заключаем, что $d(N-1)$ кратно $q-1$. ▲

Следующий результат показывает, что существование аддитивного двухвесового $(n, N, \{d, n\})_q$-кода C над алфавитом Q, представляющим собой абелеву группу, накладывает очень сильное условие на эту группу. Порядок группы q, а также структура группы Q совсем не произвольны. Напомним, что для заданной аддитивно абелевой группы Q порядком элемента x, обозначаемым через $\mathrm{ord}(x)$, называется минимальное число t, такое что $tx = \underbrace{x + x + \ldots + x}_{t \text{ раз}} = 0$.

Имеет место следующая

Теорема 2. *Пусть* Q *– абелева группа порядка* q*, и пусть* C *– аддитивный нетривиальный* q*-ичный двухвесовой* $(n, N, \{d, n\})_q$*-код* C *над алфавитом* Q*, содержащий нулевое кодовое слово. Тогда*

(i) *Все элементы* Q *имеют один и тот же порядок, т.е.* $\mathrm{ord}(x) = \mathrm{ord}(y)$*, для любой пары ненулевых элементов* $x, y \in Q^*$;

(ii) *Группа* Q *является прямой суммой* m *циклических групп* $\mathbb{Z}_p$*, так что*

$$Q = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p;$$

(iii) *Число* q *имеет вид* $q = p^m$*, где* p *– простое число, а* m *– натуральное*;

(iv) *Код* C *содержит не менее чем* $q-1$ *слов веса* n.

Доказательство. Очевидно, что любая перестановка π элементов Q, такая что $\pi(0) = 0$, примененная к любой позиции кода C, сохраняет свойство кода оставаться двухвесовым $(n, N, \{d, n\})_q$-кодом с нулевым кодовым словом. Обозначим через π перестановку, которая не меняет свойство кода C быть аддитивным, так что

$$x - y = \pi(x) - \pi(y) = \pi(x - y).$$

(i) Для заданной пары элементов алфавита $x, y \in Q^* = Q \setminus \{0\}$ и кодового слова $c = (x_1, x_2, \ldots, x_n) \in C$ веса n выберем некоторые перестановки $\pi_1, \ldots, \pi_n$ элементов Q с условием $\pi_i(0) = 0$ и такие, что при их применении ко всем координатным позициям кодового слова c мы получим слово $c' = (x, y, \ldots, y)$ аддитивного кода (действительно, применение таких перестановок π_i ко всем координатам не меняет свойство кода быть аддитивным). Предположим, что $t = \mathrm{ord}(x) \neq \mathrm{ord}(y)$. Тогда t-кратная сумма c' с самим собой $c'+\ldots+c'$ будет равна кодовому слову $(0, ty, \ldots, ty)$, вес которого равен $n-1$, так как по предположению $ty \neq 0$. Тем самым, приходим к противоречию, и поэтому все ненулевые элементы алфавита имеют один и тот же порядок.

(ii) Этот факт прямо следует из (i). Действительно, хорошо известно, что любая абелева группа представляет собой прямую сумму (прямое произведение) циклических групп. С другой стороны, любая циклическая группа $\mathbb{Z}_{p_1 p_2}$ имеет элементы порядка p_1, p_2 и $p_1 p_2$, что противоречит (i) и доказывает утверждение.

(iii) Из (ii) следует, что все p_i равны, откуда получаем утверждение.

(iv) Так как код аддитивен, мы заключаем, что $N \geqslant qn$. Зафиксируем координатную позицию, скажем, первую. Разобьем все кодовые слова на смежные классы согласно элементам, стоящим на первой позиции. Каждый смежный класс является эквидистантным кодом, мощность которого не менее n [21] (откуда следует вышеприведенное неравенство). Так как код является группой, то ясно, что мы можем сдвинуть смежный класс с нулем на первой позиции в любой другой смежный класс. Отсюда следует также, что каждый элемент алфавита встречается в столбце одно и то же число раз.

Пусть μ_1 обозначает число слов кода C веса d, а μ_2 – число слов веса n. Рассмотрим сначала случай $N = qn$. Положим $\mu = n - d$. Тогда можно подсчитать общее число ненулевых позиций в коде C. Имеем следующие два выражения:

$$\begin{cases} \mu_1 + \mu_2 = N - 1, \\ d\mu_1 + n\mu_2 = nN\Big(1 - \dfrac{1}{q}\Big). \end{cases} \tag{14}$$

Выражение для μ_1 из первого уравнения подставим во второе, и учитывая, что $N = nq$, приведем его к виду

$$d(N - 1 - \mu_2) + n\mu_2 = nN\left(1 - \frac{1}{q}\right) = n^2(q-1).$$

Учитывая, что $\mu = n - d$, получаем

$$d(qn - 1 - \mu_2) + n\mu_2 = d(qn-1) + (n-d)\mu_2 = (n-\mu)(qn-1) + \mu\mu_2 = n^2(q-1).$$

Таким образом, приходим к уравнению

$$\mu\mu_2 = n(q\mu - n) + n - \mu. \tag{15}$$

Так как обе его части – положительные целые числа, заключаем, что $q\mu - n \geqslant 0$. Поэтому можно положить

$$q\mu = n + \lambda,$$

где $\lambda \geqslant 0$ – целое число. Уравнение (15) можно переписать в следующем виде (где μ перенесено в левую сторону):

$$\begin{cases} q\mu = n + \lambda, \\ \mu(\mu_2 + 1) = (\lambda + 1)n. \end{cases} \tag{16}$$

Так как $(\lambda+1)n \geqslant n+\lambda$, то отсюда вытекает, что

$$\mu(\mu_2+1) \geqslant q\mu,$$

или, эквивалентным образом, $\mu_2+1 \geqslant q$. Следовательно, мы получаем, что $\mu_2 \geqslant q-1$. Для случая $N > qn$ доказательство не изменяется. ▲

В следующем утверждении мы сформулируем вариант теоремы 2 из [6] для случая нетривиальных $[n,k,\{d,n\}]_q$-кодов, и поэтому это утверждение не нуждается в доказательстве. Здесь мы предположим, что $q=p^m$, где $m \geqslant 1$ и p – простое. Для заданного $q=p^m$ и произвольного натурального числа a обозначим через $\gamma_a \geqslant 0$ максимальное целое число, такое что p^{γ_a} делит a, т.е. $a=p^{\gamma_a}h$, где h и p взаимно просты. Пусть числа γ_d, γ_δ и γ_c определены аналогичным образом для d, δ и d_c соответственно. Напомним, что через (a,b) обозначается наибольший общий делитель целых чисел a и b.

Теорема 3. *Пусть $q=p^m$, где $m \geqslant 1$ и p – простое число. Пусть C – q-ичный линейный (двухвесовой) $[n,k,\{d,n\}]_q$-код размерности $k \geqslant 2$, и пусть C_c – дополнительный к нему двухвесовой $[n_c,k,\{d_c,d_c+\delta\}]_q$-код C_c, где*

$$d+\delta=n \quad и \quad d+d_c+\delta=sq^{k-1}, \quad s \geqslant 1.$$

(i) *Если $s=1$ и $k \geqslant 4$, т.е. C и, следовательно, C_c – проективные коды, то справедливы следующие два равенства*:

$$(q,d)=(q,\delta) \quad и \quad (q,d_c)=(q,\delta); \tag{17}$$

(ii) *Если $s=1$ и $k=3$, то оба равенства в (17) имеют место, если справедливо одно из следующих двух условий*:

$$(d,q)^2 \leqslant q(n(n-1),q) \quad или \quad (d+\delta,q)^2 > q(n_c(n_c-1),q);$$

(iii) *Если $s=1$ и $k \geqslant 2$, то выполняется по крайней мере одно из следующих двух равенств*:

$$\gamma_d=\gamma_\delta \quad или \quad \gamma_c=\gamma_\delta; \tag{18}$$

(iv) *Если $s \geqslant 1$ и $k \geqslant 3$, то выполняется по крайней мере одно из двух равенств в (18) (соответственно, в (17)).*

§ 4. Известные $(n, N, \{d, n\})_q$-коды

Здесь мы перечислим все известные нетривиальные аддитивные $(n,N,\{d,n\})_q$-коды. Большинство этих двухвесовых кодов можно найти в подробном обзоре таких кодов в [1].

Мы начнем с формулировки утверждения, которое является перефразировкой соответствующего результата из [10], где были приведены все известные полностью регулярные линейные коды с радиусом покрытия 2, для которых дуальные коды антиподальны (т.е. содержат слова веса n). В работе [10] эта теорема была приведена и доказана для случая линейных кодов. Здесь мы сформулируем аналогичный результат для произвольных аддитивных кодов.

Теорема 4. *Пусть C – нетривиальный аддитивный $(n,N,\{d,n\})_q$-код мощности $N \geqslant q^2$ над Q. Код C можно привести эквивалентными преобразованиями к коду C^* так, чтобы имели место следующие условия*:

(i) *Для каждого ненулевого кодового слова $\boldsymbol{v} \in C^*$ веса d каждый элемент $a \in Q$, который встречается в координатной позиции этого слова $\boldsymbol{v}$, встречается в этом слове ровно $n-d$ раз*;

(ii) *Каждое ненулевое кодовое слово* $\boldsymbol{v} \in C^*$ *веса* n *либо удовлетворяет свойству* (i), *либо имеет вид* $\boldsymbol{v} = (a, a, \ldots, a)$, *где* $a \in Q$;

(iii) *Длина* n *кода* C^* (*а значит, и кода* C) *кратна* $n - d$.

Напомним, что в § 2, следуя [13], мы назвали тривиальный $(n, q, n)_q$-код *симплексом*. Напомним также, что q-ичный дистанционно инвариантный код длины n является *симплексным кодом*, если он содержит в качестве подкода симплекс, т.е. $(n, q, n)_q$-код. Ясно, что аддитивный $(n, N, \{d, n\})_q$-код, содержащий симплекс, представляет собой дистанционно инвариантный симплексный код. Следующий результат можно найти в [13].

Предложение 1. *Пусть* q*-ичный код* C *длины* n *с минимальным расстоянием* $d = \dfrac{(q-1)n}{q}$ *имеет мощность* $N = qn$. *Тогда этот код* C *можно представить в виде объединения непересекающихся симплексов.*

Возникает естественный вопрос: *при каких условиях симплексный код, указанный в предложении* 1, *является ПРМ- или РМ-кодом*? Следующее утверждение дает частичный ответ на этот вопрос.

Теорема 5. *Пусть* C – *дистанционно инвариантный симплексный код с параметрами* $(n, N, \{d, n\})_q$. *Тогда*

(i) *Код* C *можно разбить на непересекающиеся подкоды следующим образом*:

$$C = \bigcup_{i=1}^{N/q} C_i,$$

где C_i *для каждого* i *является симплексом, а мощность* N *кратна* q;

(ii) *Для любого кодового слова* $\boldsymbol{c} \in C$, *отличного от слов вида* $(a, a, \ldots, a)$, $a \in Q$, *каждый символ* $\alpha \in Q$, *который встречается на координатной позиции слова* $\boldsymbol{c}$, *встречается на этой позиции ровно* μ *раз, где* $\mu = n - d$, a n *кратно числу* μ;

(iii) *Расстояние* d *кода* C *удовлетворяет неравенству*

$$d \leqslant n\frac{q-1}{q}; \tag{19}$$

(iv) *Если* (19) *обращается в равенство и* $N = qn$, *то код* C *представляет собой ПРМ-код с параметрами*

$$n = \mu q, \quad N = \mu q^2, \quad d = \mu(q-1), \quad \mu = n - d;$$

(v) *Если в* (iv) *код* C *аддитивен, то он является РМ-кодом.*

Доказательство. (i) Так как C содержит в качестве подкода симплекс, содержащий нулевое кодовое слово $\mathbf{0}$, то можно выбрать $q-1$ кодовых слов веса n вида $\boldsymbol{a} = (a, a, \ldots, a)$, где $a \in \{1, \ldots, q-1\}$, которые имеются в C. В противном случае можно получить такие слова из кодовых слов веса n с помощью перестановок элементов алфавита. Так как C дистанционно инвариантен, это справедливо для любого выбора нулевого кодового слова. Для любого такого выбора мы получаем в качестве подкода некоторый симплекс, содержащий $q-1$ кодовых слов веса n. Таким способом мы получаем разбиение кода C на подкоды, каждый из которых представляет собой симплекс. Ясно, что каждое кодовое слово кода C будет принадлежать некоторому симплексу. Осталось показать, что никакие два разных симплекса не могут иметь одно и то же кодовое слово. В самом деле, один из таких симплексов мы можем сдвинуть в симплекс, содержащий кодовые слова вида $\boldsymbol{a} = (a, a, \ldots, a)$. Ни одно из его слов не может принадлежать другому симплексу, так как все кодовые слова из других симплексов находятся на расстоянии d от этого симплекса.

Мы заключаем, что C можно разбить на непересекающиеся подкоды мощности q, и следовательно, мощность N должна быть кратна q.

(ii) Обозначим через C_0 симплекс, который содержит нулевое кодовое слово и остальные $q-1$ кодовых слов вида $\boldsymbol{a} = (a, a, \ldots, a)$. Рассмотрим любое кодовое слово $\boldsymbol{c}$, не принадлежащее симплексу C_0. Ясно, что каждый элемент a, встречающийся на координатной позиции слова $\boldsymbol{c}$, должен встречаться (для того чтобы расстояние было в точности d от q слов симплекса C_0) ровно $n-d$ раз. Отсюда следует, во-первых, что каждый элемент, который встречается на позициях $\boldsymbol{c}$, должен встречаться ровно $\mu = n-d$ раз, а во-вторых, что число n должно быть кратным $n-d$.

(iii) Так как на позициях любого кодового слова $\boldsymbol{c}$, не принадлежащего C_0, имеются q различных элементов, то должно выполняться следующее очевидное неравенство: $n \leqslant q(n-d)$. Отсюда вытекает неравенство (19).

(iv) Равенство в (19) означает, что n можно представить в виде $n = q\mu$, где $\mu = n-d$, и следовательно, $d = \mu(q-1)$. Для этих значений n и d мы заключаем из оценки (4), что $N \leqslant q^2\mu$. Если $N = qn$, то $N = q^2\mu$, и согласно [13] код C представляет собой ПРМ-код, что дает (iv).

(v) Из (iv) мы получили, что C является ПРМ-кодом. Покажем теперь, что аддитивный ПРМ-код является РМ-кодом. Так как C аддитивен, то сумма любых двух строк, скажем, $\boldsymbol{r}_1$ и $\boldsymbol{r}_2$, принадлежит C и содержит на координатных позициях каждый элемент алфавита μ раз (теорема 4). Из кода C строим матрицу D размера $q\mu \times q\mu$, содержащую все кодовые слова с нулем на первой позиции, где $\mu = n-d$. Ясно, что это справедливо, так как C – аддитивный код.

Итак каждая строка D содержит любой элемент Q ровно μ раз (теорема 4), и для любых двух строк $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ кода D покомпонентная разность этих строк $\boldsymbol{c}_1 - \boldsymbol{c}_2$ также принадлежит (по определению слова D имеют 0 в первой позиции) коду D. Любое кодовое слово $\boldsymbol{c} \in C$ с первой ненулевой позицией $a \in Q$ получено из D сложением с вектором $(a, a, \ldots, a)$, который принадлежит C, так как C – симплексный код по условию. Мы заключаем, что D – разностная матрица $D(q, n-d)$, а C – $(n, qn, \{d, n\})_q$-РМ-код. ▲

Замечание 1. Условия $n = q(n-d)$ и $N = qn$ в (iv) и (v) опустить нельзя, как показывает следующий пример. Рассмотрим матрицу $[C] = [D^{(0)} \mid \ldots \mid D^{(q-1)}]^t$, образованную сдвигами $D^{(i)}$ разностной матрицы $D = D(q, \mu)$, где C – $(n, N, \{d, n\})_q$-РМ-код. Если мы удалим одну или несколько таких матриц $D^{(i)}$ из матрицы $[C]$, то получим дистанционно инвариантный симплексный код некоторой мощности $N^* < qn$, т.е. нелинейный двухвесовой $(n, N^*, \{d, n\})_q$-код, удовлетворяющий условию теоремы. Аналогично нельзя опустить условие $N = qn$ в (iv) и (v). Например, линейный код Боуза – Буша имеет длину (см. ниже) $n < q(n-d)$. Аналогично, аддитивный $(n, N, \{d, n\})_q$-код не обязательно должен иметь мощность q^k. Так, например, разностная матрица $D(4, 2)$ индуцирует оптимальный аддитивный $(8, 32, \{6, 8\})_4$-код мощности $N \neq 4^k$.

Замечание 2. Случай кодов мощности $N = q^2$ также очень специален. Хорошо известный результат гарантирует, что $r-2$ взаимно ортогональных латинских квадратов порядка q индуцирует $(r, q^2, \{r-1, r\})_q$-код. Для случая, когда q – степень простого числа, существуют $q-1$ взаимно ортогональных латинских квадратов, индуцирующих линейный эквидистантный $[q+1, 2, q]_q$-код (обратное утверждение также имеет место для любой длины $r \geqslant 2$ и также хорошо известно). Используя эти коды с соответствующими значениями r_i, можно построить с помощью прямой суммы (используя разбиения на симплексы) $(n, q^2, \{d, n\})_q$-код для любых натуральных $d = n-s$ и $n = r_1 + \ldots + r_s$, рассматривая прямую сумму s исходных $(r_i, q^2, \{r_i - 1, r_i\})_q$-кодов латинских квадратов. Поэтому мы исключили (как и в [1,8]) все эти тривиальные коды, за исключением $(r, q^2, \{r-1, r\})_q$-кодов длины $r \leqslant q$, которые индуцируются $r-2$ взаимно ортогональными латинскими квадратами по-

рядка q. Кроме того, имеются еще, конечно, $[q+2, 2, \{q+1, q+2\}]_q$-коды, полученные из эквидистантных $[q+1, 2, q]_q$-кодов добавлением одной позиции (см [4]).

Теперь мы можем привести все известные семейства нетривиальных аддитивных $(n, N, \{d, n\})_q$-кодов, которые были приведены в обзоре [1] (а также были указаны в [10] для линейного случая). Если исключить коды, образованные латинскими квадратами, то все известные $(n, N, \{d, n\})_q$-коды делятся на два больших класса кодов: разностно-матричные $(n = q\mu, N = qn, \{(q-1)\mu, q\mu\})_q$-коды, длина n которых кратна q, и $[n, k, \{d, n\}]_q$-коды Деннистона длины n, такой что $n-1$ кратно $(q^{k-1}-1)/(q-1)$.

Разностно-матричные коды (РМ-коды). Это $(q\mu, q^2\mu, \{(q-1)\mu, q\mu\})_q$-коды [12], индуцированные разностными матрицами. Лемма 1 описывает построение таких кодов для значений $q = p^h$ и $\mu = p^\ell$, где p – простое, а h и ℓ – произвольные натуральные числа.

Следует заметить, что эти коды включают в себя (двоичные) $(4m, 8m, \{2m, 4m\})$-*коды Адамара.* Действительно, двоичная (т.е. состоящая из элементов 0 и 1) матрица Адамара является разностной матрицей $D(2, 2m)$.

Коды Деннистона. Это $[n = 1+(q+1)(h-1), 3, \{q(h-1), n\}]_q$-коды, где $1 < h < q$ и h делит q, для $q = 2^r \geqslant 4$ (см. семейство TF2 в [1]). В теореме 1 этот случай соответствует расстоянию $d = n - h + 1 = (n-1)q/(q+1)$, из которого следует, что $N = q^3$. Для случая $h = 2$ мы получаем $[n = q+2, 3, \{q, n\}]_q$-коды Боуза – Буша (см. семейство TF1 в [1]), построенные в 1952 г. [11], которые индуцируются гиперовалами в $PG(3, q)$. Значению $h = q/2$ соответствуют $[n = q(q-1)/2, 3, \{q(q-2)/2, n\}]_q$-коды Дельсарта [7] (см. семейство $\mathrm{TF1}^d$ в [1]), построенные независимо в 1971 г., которые проективно дуальны кодам Боуза – Буша [1].

Коды Деннистона образованы максимальными дугами в проективных плоскостях [18] (см. также [19, 20]). Коротко объясним, как построить такие коды для произвольного $q = 2^m \geqslant 4$ и натурального $h \geqslant 2$, делящего q, т.е. $h = 2^u \leqslant q/2$. Для заданного $\mathbb{F}_q$ пусть H обозначает подгруппу порядка h аддитивной группы поля $\mathbb{F}_q$. Пусть $\varphi(x, y) = ax^2 + bxy + cy^2$ – неприводимая квадратичная форма над $\mathbb{F}_q$. Тогда $[n, 3, \{d, n\}]_q$-код Деннистона порождается следующей $(3 \times n)$-матрицей:

$$G_d = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{bmatrix}, \tag{20}$$

где $n = (q+1)(h-1)+1$, $d = n-h$, а (x_i, y_i) – все упорядоченные пары элементов поля $\mathbb{F}_q$, которые отображаются в H, т.е. $\varphi(x_i, y_i) \in H$.

Приведем также порождающие матрицы для кодов Боуза – Буша, а также кодов Дельсарта, так как они приводятся в явном виде. Пусть матрица G имеет вид

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 0 & x_0 & x_1 & \dots & x_i & \dots & x_{q-2} \\ 0 & 0 & 1 & y_0 & y_1 & \dots & y_i & \dots & y_{q-2} \end{bmatrix}, \tag{21}$$

где x_i и y_i пробегают все ненулевые элементы поля $\mathbb{F}_q$. Тогда, если $y_i = x_i^2$, то матрица G порождает код Боуза – Буша. Если же x_i и y_i пробегают все упорядоченные пары ненулевых элементов (x_i, y_i) (число таких различных пар равно, очевидно, $(q-1) \times q/2$, т.е. длине кодов Дельсарта), такие что $\mathrm{Tr}(x_i y_i) = 1$, где $\mathrm{Tr}(x)$ – функция следа из $\mathbb{F}_q$ в поле $\mathbb{F}_2$, т.е.

$$\mathrm{Tr}(x) = x + x^2 + x^4 + \ldots + x^{q/2},$$

то матрица G порождает код Дельсарта.

Теорема 6. *Пусть C – аддитивный нетривиальный $(n, N, \{d, n\})_q$-код, где $q = p^m$, p – произвольное простое число и $m = 1, 2, \ldots$ Предположим, что $N \geqslant q^2$ и $n > 2$. Тогда параметры этого кода совпадают с параметрами кода, принадлежащего одному из семейств указанных выше кодов.*

Доказательство. Так как C – нетривиальный аддитивный код, то он имеет мощность $N = q^2\mu \geqslant q^2$.

Начнем со случая $N = q^2$. Для любого натурального q существование r попарно ортогональных латинских квадратов влечет существование $(r+2, q^2, \{r+1, r+2\})_q$-МДР-кода (см. также замечание 2). Эти коды включают в себя самые короткие нетривиальные $(q, q^2, \{q-1, q\})_q$-РМ-коды, которые существуют для любой степени простого числа q и совпадают с кодами по латинским квадратам. Еще раз подчеркнем, что существует большое количество тривиальных аддитивных двухвесовых $(n, q^2, \{d, n\})_q$-кодов, указанных в замечаниях выше, которые мы не рассматриваем. Напомним также, что так как C аддитивен, то все ПРМ-коды согласно теореме 5 являются РМ-кодами.

Теперь докажем, что для случая $N = q^2\mu$, где $2 \leqslant \mu < q$, нетривиальный аддитивный $(n, N, \{d, n\})_q$-код C есть не что иное, как $(q\mu, q^2\mu, \{(q-1)\mu, n\})_q$-код ПРМ или РМ. Следующий аргумент использовался в [13] (см. также [21]), где были введены q новых кодов C_j, $j = \{0, 1, \ldots, q-1\}$, полученных из C выбором всех кодовых слов кода C, имеющих элемент j на первой позиции, и затем удалением этой первой позиции. Легко видеть [13], что каждый код C_j имеет только одно расстояние, а именно d. Следовательно, C_j – эквидистантный $(n_0, N_0, d_0)_q = (n-1, q\mu, d)_q$-код мощности $N_0 = q\mu$. Более того, параметры этого кода достигают верхней границы Плоткина (2) с точным целочисленным равенством, и следовательно, каждый символ i алфавита $\{0, 1, \ldots, q-1\}$ встречается одно и то же число раз (а именно μ) в каждой позиции всех кодовых слов кода C_j (см. [21]). Теперь применим теорему 4, которая утверждает, что каждое кодовое слово $\boldsymbol{c}$ кода C_j содержит все элементы $i \neq j$ алфавита как координатные элементы ровно μ раз, а элемент j – ровно $\mu - 1$ раз.

Так как C – аддитивный код, то его подкод C_0 также является аддитивным кодом, удовлетворяющим следующему свойству: каждое ненулевое слово кода C_0 содержит каждый ненулевой элемент алфавита ровно μ раз. Мы заключаем, следовательно, что по теореме 5 код C_0 станет разностной матрицей, если мы добавим ко всем словам кода C_0 нулевые позиции. Из свойства аддитивности вытекает, что любой подкод C_j представляет собой сдвиг кода C_0. Таким образом, C является РМ-кодом.

Рассмотрим теперь случай $N = q^3$. Сначала покажем, что в кодах Деннистона число h должно делить q. Из теоремы 5 заключаем, что n кратно $n-d$. Следовательно, n можно представить в виде $n = (n-d)\ell$ для некоторого натурального числа ℓ. Поэтому $d = n(\ell-1)/\ell$, и мы получаем из (19), что

$$d = n\frac{\ell-1}{\ell} \leqslant n\frac{q-1}{q},$$

откуда следует, что $\ell \leqslant q$. Но случай $\ell = q$ дает РМ-код. Мы заключаем, следовательно, что $\ell < q$. Предположим теперь, что

$$n = 1 + (q+1)(h-1) \quad \text{и} \quad d = q(h-1)$$

для некоторого натурального числа $h \geqslant 2$. Это означает, что

$$n = q(h-1) + h = d + h.$$

Таким образом, объединяя равенства

$$n = 1 + (q+1)(h-1) \quad \text{и} \quad d = q(h-1) = n\frac{\ell-1}{\ell},$$

получаем

$$q(h-1) = (q(h-1)+h)\frac{\ell-1}{\ell},$$

откуда вытекает, что $h(\ell-1) = q(h-1)$. Так как $h \geqslant 2$, и следовательно, h и $h-1$ взаимно просты, мы заключаем, что h делит q, откуда следует, что получается код с параметрами кода Деннистона.

Случай $N > q^3$ исключается из аналогичных аргументов. Сначала рассматривается случай $N = q^3\mu$, где $2 \leqslant \mu < q$. Напомним, что $q = p^m$. Мы утверждаем, что в этом случае могут получиться только РМ-коды. Действительно, для всех значений $\mu = p^r$, где $0 < r < m$, существует $(q^2\mu, q^3\mu, \{q(q-1)\mu, n\})_q$-РМ-код. В § 2 мы описали построение всех таких кодов (см. текст после леммы 1), которое можно найти в [12]. Убедимся, почему это единственно возможные случаи. Деля обе стороны выражения (8) на $q^3\mu$, мы получим, что $d = n(q-1)/q$, поэтому это должна быть разностная матрица. Следовательно, для случая, когда $d \neq n(q-1)/q$, который (для случая $q^3\mu$) эквивалентен условию $d = q(q-1)\mu$, мы не получим целочисленное равенство в (8). Так как повторение s копий РМ-кода не меняет равенства $d = n(q-1)/q$, заключаем, что вышеуказанный нетривиальный РМ-код является единственным нетривиальным кодом для этих значений N.

Рассмотрим теперь случай $N = q^4$, который дает линейные разностно-матричные коды [12]. В самом деле, имея такой $[n, 4, \{d, n\}]_q$-код C, можно построить (как мы делали это раньше, например, в теореме 5) код C_0, представляющий собой линейный эквидистантный $[n-1, 3, d]_q$-код длины $n-1 = (q^4-1)/(q-1)$ с расстоянием $d = q^3$, дуальным к которому является q-ичный совершенный код Хэмминга.

Покажем теперь, что для случая $N = q^4$ не существует кодов типа Деннистона. По теореме 4 длина кода типа Деннистона должна иметь вид $n = s(q^3-1)/(q-1)+1$. Так как n кратно $n-d$ (см. снова теорему 4), то это выражение принимает вид $n = d\ell/(\ell-1)$ для некоторого натурального $\ell \leqslant q$. Учитывая, что $d = sq^2$, получаем

$$n = s\frac{q^3-1}{q-1} + 1 = d\frac{\ell}{\ell-1} = sq^2\frac{\ell}{\ell-1}. \tag{22}$$

Теперь следует рассмотреть отдельно случаи $(s, q-1) = 1$ и $(s, q-1) \geqslant 2$.

Пусть вначале $(s, q-1) = 1$. Тогда мы видим, что выражение для n в левой части (22) не делится на s и на q, а в правой части оно делится на оба эти числа. Мы заключаем, следовательно, что коды такого типа не существуют.

Рассмотрим теперь случай $(s, q-1) \geqslant 2$. Для случая $s = q-1$ получаем, что $n = q^3$, и так как $N = q^4$, т.е. $N = qn$, то заключаем, что C является РМ-кодом.

Предположим теперь, что $s = u(q-1)$, где $u \geqslant 2$. Используя это s в (22), приходим к равенству

$$u(q-1)\frac{q^3-1}{q-1} + 1 = u(q-1)q^2\frac{\ell}{\ell-1},$$

которое после упрощения и умножения обеих сторон на $(\ell-1)$ принимает следующий вид:

$$(\ell-1)(u(q^3-1)+1) = \ell u(q^3-q^2).$$

Упрощая, приходим к неравенству

$$0 \leqslant uq^2(q-\ell) = -u\ell + (u+\ell) - 1 \leqslant -1,$$

что невозможно, так как $2 \leqslant \ell \leqslant q$ и $u \geqslant 2$, что завершает рассмотрение случая $N = q^4$.

Случай $q^4 < N < q^5$ рассматривается аналогично. Здесь мы имеем только аддитивные РМ-коды для значений $n = q^4\mu$, где μ пробегает все степени p и $q = p^m$.

Случай $N = q^k$ для $k \geqslant 5$ можно рассмотреть аналогичным образом, и мы его опускаем, чтобы не повторять одни и те же рассуждения.

Теперь следует сделать несколько замечаний для случая, когда q – степень простого нечетного числа. Буш в 1952 г. доказал в [22] несуществование $[q+2, 3, q]_q$-кодов для нечетного q, что влечет несуществование $[q(q-1)/2, 3, \{q(q-2)/2, q(q-1)/2\}]_q$-кодов Дельсарта, так как они проективно дуальны друг другу (см. семейства TF1 и $\mathrm{TF1}^d$ в [1]). Затем в 1997 г. в [23] было доказано несуществование максимальных дуг (на которых основаны коды Деннистона) в дезарговых плоскостях $PG(2, q)$ нечетного порядка, что автоматически влечет несуществование всех кодов Деннистона для нечетных q. ▲

§ 5. Верхние границы

Здесь мы рассмотрим верхние границы для величины

$$A_q(n; \{d, n\}) = \max\{N : \exists\, (n, N, \{d, n\})\text{-код}\},$$

т.е. границы на максимально возможную мощность кода в Q_q^n с двумя расстояниями d и n.

5.1. Границы линейного программирования. Мы провели всестороннее исследование границы линейного программирования (ЛП) Дельсарта на $A_q(n; \{d, n\})$, используя эту границу в следующем виде. Определим многочлены Кравчука

$$Q_i^{(n,q)}(t) = \frac{1}{r_i} K_i^{(n,q)}(z), \quad z = \frac{n(1-t)}{2}, \quad r_i = (q-1)^i \binom{n}{i},$$

где

$$K_i^{(n,q)}(z) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{z}{j} \binom{n-z}{i-j}$$

представляют собой (обычные) многочлены Кравчука. Для вещественного многочлена $f(t)$ степени не выше n рассмотрим его разложение

$$f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t) \tag{23}$$

по многочленам Кравчука.

Теорема 7. *Пусть $n \geqslant q \geqslant 2$, и пусть $f(t) \in \mathbb{R}[t]$ – многочлен степени не выше n, такой что*:

(A1) $f(-1) \leqslant 0$ *и* $f(1 - 2d/n) \leqslant 0$;

(A2) *Коэффициенты в разложении* (23) *удовлетворяют условиям* $f_0 > 0$ *и* $f_i \geqslant 0$ *для каждого* $i \geqslant 1$.

Тогда $A_q(n;\{d,n\}) \leqslant f(1)/f_0$. *Если* $(n, N, \{d,n\})_q$*-код* C *достигает этой границы для некоторого* $f(t)$, *то* $f(1-2d/n) = f(-1) = 0$ *и* $f_i M_i(C) = 0$ *для каждого* $i \geqslant 1$, *где*

$$M_i(C) = \sum_{x,y\in C} Q_i^{(n,q)}(1-2d(x,y)/n). \tag{24}$$

Граница линейного программирования из нашей работы [6] (формула (40)), которая была выведена для $\delta = n-d$, дает для нашего случая оценку (5) (которая в точности представляет собой верхнюю границу в (7)). Это дает нам простое доказательство необходимого условия в утверждении (ii) теоремы 4.

Второе доказательство утверждения (ii) теоремы 1. Верхняя граница в (5) получена с помощью теоремы 1 с использованием многочлена $f(t) = (t-1+2d/n)(t+1)$ второй степени. Если эта оценка достигается $(n, N, \{d,n\})_q$-кодом C, то из условий теоремы 7 следует, что $M_1(C) = M_2(C) = 0$, так как $f_1 > 0$ и $f_2 > 0$. Это означает, что код C является ортогональной таблицей силы 2. Мы заключаем очевидным образом, что мощность N кода C, т.е. величина

$$N = \frac{dq^2}{qd-(q-1)(n-1)},$$

делится на q^2 и что d делится на $qd-(q-1)(n-1)$. ▲

Численные результаты дают несколько общих ЛП-границ для специальных случаев семейств параметров q, n, d. Одну из них (другие оценки кажутся слабее) мы приведем здесь. Эта оценка представляет собой специальной случай границы, недавно полученной в работе [24], для диапазона чуть вне диапазона границы Плоткина.

Т е о р е м а 8. *Для каждого натурального числа* $m \geqslant 2$ *имеет место неравенство*

$$A_2(4m+1, \{2m, 4m+1\}) \leqslant 4m+2. \tag{25}$$

Д о к а з а т е л ь с т в о. Используем теорему 7 для длины $n = 4m+1$ и расстояния $d = 2m$ с многочленом

$$f(t) = 1 + 2mQ_2^{(4m+1,2)}(t) + (2m+1)Q_{4m-1}^{(4m+1,2)}(t). \tag{26}$$

Условие (A2) очевидным образом выполняется. Докажем, что условие (A1) выполняется с равенствами.

Из условия $Q_i^{(n,2)}(-1) = (-1)$ получаем $f(-1) = 0$. Так как $1-2d/n = 1/(4m+1)$, рассмотрим выражение

$$f\left(\frac{1}{4m+1}\right) = 1 + \frac{2m}{\binom{4m+1}{2}} \sum_{j=0}^{2} (-1)^j \binom{2m}{j}\binom{2m+1}{2-j} +$$
$$+ \frac{2m+1}{\binom{4m+1}{4m-1}} \sum_{j=0}^{4m-1} (-1)^j \binom{2m}{j}\binom{2m+1}{4m-1-j}.$$

Первую сумму можно подсчитать непосредственно, и она равна $-2m/(4m+1)$. Для подсчета второй суммы заметим, что единственные значения j, для которых оба биномиальных коэффициента ненулевые, – это $2m-2 \leqslant j \leqslant 2m$. Отсюда приходим к равенству $f(1/(4m+1)) = 0$.

Таблица 1

Оптимальные многочлены с одним ненулевым коэффициентом, $q = 3$

n	d	f_3	$\mathrm{sb}_3(n,d)$	n	d	f_3	$\mathrm{sb}_3(n,d)$
4	1	8	9	4	2	8	9
5	2	8	9	9	4	28	29
10	5	32	33	12	6	44	45
16	8	80	81	20	10	152	153
22	11	224	225				

Вычисление соответствующих моментов $M_i(C)$, заданных выражением (24), дает равенство $M_2(C) = M_{4m-1}(C) = 0$ (так как $f_2 > 0$ и $f_{2m+1} > 0$) для любого $(4m+1, 4m+2, \{2m, 4m+1\})$-кода, достигающего этой оценки. ▲

5.2. Численные вычисления верхних оценок линейного программирования. Здесь мы представим ЛП-границы для величины $A_q(n, \{d, n\})$, полученные прямым вычислением ЛП-границы с помощью симплекс-метода с использованием программного пакета Maple 19. Используемый алгоритм был применен нами для каждого $q \leqslant 5$ и $n \leqslant 50$. Имеется много случаев, для которых наилучшие оценки получались с помощью многочленов степени 1 и 2, приводящих к уже существующим оценкам. Поэтому мы исключили все такие случаи, предпочитая исследовать границы, полученные с помощью многочленов степени 3 или выше. Более того, мы исключили границы на все тривиальные коды мощности 4 или менее, границу, заданную выражением (5), а также все границы, значения которых не являются натуральными числами. Наконец, мы исключили также случаи, для которых граница, полученная с помощью сферических кодов (см. п. 5.3 ниже), лучше, или которые соответствуют случаю, включенному в теорему 8.

Нашу ЛП-границу мы нормализовали, положив $f_0 = 1$, и поэтому оценка, задаваемая допустимым многочленом f, выглядит следующим образом:

$$A_q(n, \{d, n\}) \leqslant 1 + f_1 + f_2 + \ldots + f_n,$$

в точности как и в классической формулировке Дельсарта границы линейного программирования. Во всех интересных случаях только один или два коэффициента f_i не равны нулю. Отметим, что благодаря специфике ЛП-границы мы не ожидаем большого числа ненулевых коэффициентов, и на самом деле, мы не увидели ни одного случая с тремя или более ненулевыми коэффициентами.

Обозначим через $\mathrm{sb}_q(n, d)$ наилучший численный результат, полученный указанным выше путем, для величины $A_q(n, \{d, n\})$. Так как все случаи для $q = 2$ уже покрыты указанными выше исключениями и результатами из работы [24], мы начнем наш обзор результатов по интересующей нас ЛП-границе с $q = 3$.

Результаты для $q = 3$. Как и для двоичного случая, для случая $q = 3$ среди множеств числовых параметров, содержащих только один ненулевой коэффициент (не считая, конечно, $f_0 = 1$) в разложении по многочленам Кравчука оптимального многочлена, мы наблюдали только коэффициент f_3. Это означает, что ЛП-многочлен имеет вид $f(t) = 1 + f_3 Q_3^{(n,3)}(t)$. Все эти многочлены, кроме одного, имеют d, близкое к $n/2$. Все эти результаты систематизированы в табл. 1.

Остальные случаи, где мы имели два ненулевых коэффициента, кроме обязательного значения $f_0 = 1$, приведены в табл. 2.

Наконец, мы приводим два случая многочленов

$$f(t) = 1 + f_5 Q_5^{(n,3)}(t)$$

Таблица 2

Оптимальные многочлены с двумя ненулевыми коэффициентами, $q = 3$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_3(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_3(n,d)$
7	4	$f_2 = 6,\ f_3 = 20$	27	10	6	$f_2 = 12,\ f_3 = 20$	45
24	12	$f_3 = 113,\ f_4 = 210$	324	28	14	$f_3 = 208,\ f_4 = 400$	609
30	15	$f_3 = 320,\ f_4 = 624$	945	7	2	$f_3 = 4,\ f_5 = 16$	21

Таблица 3

Оптимальные многочлены для $q = 4$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_4(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_4(n,d)$
5	2	$f_1 = 3/4,\ f_3 = 81/4$	22	5	3	$f_3 = 27$	28
6	3	$f_1 = 1/2,\ f_3 = 45/2$	24	9	6	$f_2 = 12,\ f_3 = 63$	76
10	5	$f_3 = 81$	82	18	12	$f_2 = 33,\ f_3 = 126$	160
24	16	$f_2 = 57,\ f_3 = 198$	256	42	28	$f_3 = 615$	616

для $(n,d) = (46,23)$ и $(48,24)$, что дает

$$\mathrm{sb}_3(46,23) = 2753 \quad \text{и} \quad \mathrm{sb}_3(48,24) = 3009$$

соответственно.

Результаты для $q = 4$. Для $q = 4$ мы нашли оптимальные многочлены почти полностью третьей степени, всего восемь таких случаев, как показано в табл. 3.

Единственный случай, отличный от приведенных в табл. 3, был многочлен пятой степени

$$f(t) = 1 + 75Q_4^{(18,4)}(t) + 468Q_5^{(18,4)}(t),$$

который дает

$$\mathrm{sb}_4(18,9) = 544.$$

Результаты для $q = 5$. Найденные нами для случая $q = 5$ оптимальные многочлены приведены в табл. 4.

5.3. Верхние границы с помощью сферических кодов. Взаимосвязь между кодами с двумя расстояниями в множестве Q_q^n и сферическими кодами с двумя расстояниями на евклидовой сфере $\mathbb{S}^{n-1}$ (описанной, например, в [6, раздел 4.3]) влечет, что каждый $(n, N, \{d,n\})_q$-код $C \subset Q_q^n$ соответствует сферическому коду с двумя расстояниями $W \subset \mathbb{S}^{(q-1)n-1}$. Квадраты расстояний между точками W равны $2dq/(q-1)n$ и $2q/(q-1)$. Используя классический результат работы [25], а также результаты из [6], мы заключаем, что либо

$$d = \frac{(k-1)n}{k} \tag{27}$$

для некоторого натурального $k \in \left[2, (\sqrt{2(q-1)n}+1)/2\right]$ (и число n очевидным образом делится на k), либо мощность N ограничена сверху неравенством $N \leqslant 2(q-1)n+1$.

Для произвольного $q \geqslant 3$ выражение (27) при $k > q$ влечет, что $d > (q-1)n/q$, т.е. величина d находится в диапазоне границы Плоткина. Используя оценку Плоткина, получаем, что ее можно записать в виде $N \leqslant (k-1)q/(k-q)$. Эти наблюдения можно суммировать следующим образом.

Таблица 4

Оптимальные многочлены для $q = 5$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_5(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_5(n,d)$
6	3	$f_1 = 4/3,\ f_3 = 128/3$	45	6	4	$f_3 = 64$	65
7	4	$f_1 = 1,\ f_3 = 48$	50	16	12	$f_2 = 40,\ f_3 = 224$	265
21	14	$f_3 = 304$	305	27	18	$f_3 = 624,$	625
32	24	$f_2 = 92,\ f_3 = 432$	525	33	22	$f_3 = 1984$	1985
44	33	$f_2 = 152,\ f_3 = 672$	825	36	24	$f_3 = 32,\ f_4 = 2272$	2405
42	28	$f_3 = 1696,\ f_4 = 6528$	8225				

Теорема 9. *Если C – $(n, N, \{d, n\})_q$-код, то либо*

$$N \leqslant 2(q-1)n + 1,$$

либо

$$d = (k-1)n/k,$$

где $k \in \left[2, (\sqrt{2(q-1)n} + 1)/2\right]$ – натуральное число, и более того, имеет место неравенство

$$N \leqslant \frac{(k-1)q}{k-q}$$

для $q \geqslant 3$ и $q < k \leqslant (\sqrt{2(q-1)n} + 1)/2$.

Дальнейший набор оценок (для применения их к различным режимам для d и n) можно извлечь из результатов по сферическим множествам с двумя расстояниями, которые были рассмотрены и использованы в [26]. Отметим, что работа [26] имеет дело только с двоичными кодами, но при этом лемму 3.3 и теорему 3.5 из этой работы можно также применять и для $q \geqslant 3$. Хотя мы интересуемся здесь случаем, когда расстояния равны d и n, другие случаи также следуют из этих результатов. В дальнейшем предположим, что $q \geqslant 3$.

В этом месте будет удобно переключится на скалярные произведения для точек сферического кодов. Легко видеть, что скалярные произведения α и β, $-1 < \alpha < \beta < 1$, для точек из множества W равны

$$\alpha = -\frac{1}{q-1}, \quad \beta = \frac{n(q-1) - dq}{n(q-1)}.$$

Теперь из [26, лемма 3.3] вытекает, что если $d > n(q-2)/q$ (это эквивалентно условию $\alpha + \beta < 0$), то

$$A_q(n, \{d, n\}) \leqslant \binom{n(q-1)}{2}$$

за исключением (возможно) случаев $n(q-1) = \gamma^2 - 2$ и $n(q-1) = \gamma^2 - 3$, где $\gamma := (n-d)q/n(q-1)$ – целое нечетное число. Аналогично [26, теорема 3.5] (первоначально полученная в [27]) дает оценку

$$A_q(n, \{d, n\}) \leqslant \frac{n(q-1) + 2}{1 - (n(q-1) - 1)(q-1)^2/dq},$$

которая справедлива для $dq > (n(q-1) - 1)(q-1)^2$.

СПИСОК ЛИТЕРАТУРЫ

1. *Calderbank R., Kantor W.M.* The Geometry of Two-Weight Codes // Bull. London Math. Soc. 1986. V. 18. № 2. P. 97–122. https://doi.org/10.1112/blms/18.2.97
2. *Shi M., Guan Y., Solé P.* Two New Families of Two-Weight Codes // IEEE Trans. Inform. Theory. 2017. V. 63. № 10. P. 6240–6246. https://doi.org/10.1109/TIT.2017.2742499
3. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* Codes with Two Distances: d and $d+1$ // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVI). Svetlogorsk, Kaliningrad region, Russia. Sept. 2–8, 2018. P. 40–45. Available at https://www.dropbox.com/s/h7u89lh8vyirww9.
4. *Бойваленков П., Делчев К., Зиновьев Д.В., Зиновьев В.А.* О q-ичных кодах с двумя расстояниями d и $d+1$ // Пробл. передачи информ. 2020. Т. 56. № 1. С. 38–50. https://doi.org/10.31857/S0555292320010040
5. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* Two-Weight (Linear and Non-linear) Codes // Proc. 17th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2020). On-line, Bulgaria. Oct. 11–17, 2020. P. 11–17. https://doi.org/10.1109/ACCT51235.2020.9383353
6. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* On Two-Weight Codes // Discrete Math. 2021. V. 344. № 5. Paper No. 112318 (15 pp.). https://doi.org/10.1016/j.disc.2021.112318
7. *Delsarte P.* Two-Weight Linear Codes and Strongly Regular Graphs // MBLE Research Lab. Report R160. Brussels, Belgium, 1971.
8. *Delsarte P.* Weights of Linear Codes and Strongly Regular Normed Spaces // Discrete Math. 1972. V. 3. № 1–3. P. 47–64. https://doi.org/10.1016/0012-365X(72)90024-6
9. *Landjev I., Rousseva A., Storme L.* On Linear Codes of Almost Constant Weight and the Related Arcs // C. R. Acad. Bulgare Sci. 2019. V. 72. № 12. P. 1626–1633. https://doi.org/10.7546/CRABS.2019.12.04
10. *Borges J., Rifà J., Zinoviev V.A.* On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal Dual // Adv. Math. Commun. 2010. V. 4. № 4. P. 567–578. https://doi.org/10.3934/amc.2010.4.567
11. *Bose R.C., Bush K.A.* Orthogonal Arrays of Strength Two and Three // Ann. Math. Statist. 1952. V. 23. № 4. P. 508–524. https://doi.org/10.1214/aoms/1177729331
12. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87. http://mi.mathnet.ru/ppi1804
13. *Бассалыго Л.А., Додунеков С.М., Зиновьев В.А., Хеллесет Т.* Граница Грея – Рэнкина для недвоичных кодов // Пробл. передачи информ. 2006. Т. 42. № 3. С. 37–44. http://mi.mathnet.ru/ppi51
14. *Helleseth T., Kløve T., Levenshtein V.I.* A Bound for Codes with Given Minimum and Maximum Distances // Proc. 2006 IEEE Int. Symp. on Information Theory (ISIT'2006). Seattle, WA, USA. July 9–14, 2006. P. 292–296. https://doi.org/10.1109/ISIT.2006.261600
15. *Boyvalenkov P.G., Dragnev P.D., Hardin D.P., Saff E.B., Stoyanova M.M.* Universal Bounds for Size and Energy of Codes of Given Minimum and Maximum Distances // IEEE Trans. Inform. Theory. 2021. V. 67. № 6. P. 3569–3584. https://doi.org/10.1109/TIT.2021.3056319
16. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge, UK: Cambridge Univ. Press, 1986.
17. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
18. *Denniston R.H.F.* Some Maximal Arcs in Finite Projective Planes // J. Combin. Theory. 1969. V. 6. № 3. P. 317–319. https://doi.org/10.1016/S0021-9800(69)80095-5

19. *Thas J.A.* Construction of Maximal Arcs and Partial Geometry // Geom. Dedicata. 1974. V. 3. № 1. P. 61–64. https://doi.org/10.1007/BF00181361
20. *Thas J.A.* Projective Geometry over a Finite Field // Handbook of Incidence Geometry: Buildings and Foundations. Amsterdam: Elsevier, 1995. Ch. 7. P. 295–347. https://doi.org/10.1016/B978-044488355-1/50009-8
21. *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://mi.mathnet.ru/ppi1845
22. *Bush K.A.* Orthogonal Arrays of Index Unity // Ann. Math. Statist. 1952. V. 23. № 3. P. 426–434. https://doi.org/10.1214/aoms/1177729387
23. *Ball S., Blokhuis A., Mazzocca F.* Maximal Arcs in Desarguesian Planes of Odd Order Do Not Exist // Combinatorica. 1997. V. 17. № 1. P. 31–41. https://doi.org/10.1007/BF01196129
24. *Landjev I., Rousseva A., Vorobev K.* Constructions of Binary Codes with Two Distances. Preprint, 2022.
25. *Larman D.G., Rogers C.A., Seidel J.J.* On Two-Distance Sets in Euclidean Space // Bull. London Math. Soc. 1977. V. 9. № 3. P. 261–267. https://doi.org/10.1112/blms/9.3.261
26. *Barg A., Glazyrin A., Kao W.-J., Lai C.-Y., Tseng P.-C., Yu W.-H.* On the Size of Maximal Binary Codes with 2, 3, and 4 Distances, https://arXiv.org/abs/2210.07496 [math.CO], 2022.
27. *Glazyrin A., Yu W.-H.* Upper Bounds for s-Distance Sets and Equiangular Lines // Adv. Math. 2018. V. 330. P. 810–833. https://doi.org/10.1016/j.aim.2018.03.024

Бойваленков Петър
Делчев Константин
Институт математики и информатики
Болгарской академии наук, София, Болгария
peter@math.bas.bg
kdelchev@math.bas.bg
Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
14.11.2022
После доработки
25.11.2022
Принята к публикации
28.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.216.3

© 2022 г. **Н.Г. Докучаев**

ПРЕДИКТОРЫ ДЛЯ ВЫСОКОЧАСТОТНЫХ СИГНАЛОВ НА ОСНОВЕ АППРОКСИМАЦИИ ПЕРИОДИЧЕСКИХ ЭКСПОНЕНТ РАЦИОНАЛЬНЫМИ МНОГОЧЛЕНАМИ

Представлены линейные интегральные предикторы для высокочастотных сигналов непрерывного времени с конечным спектральным зазором. Предикторы основаны на аппроксимации комплекснозначной периодической экспоненты (комплексной синусоиды) рациональными многочленами.

Ключевые слова: прогнозирование, линейные предикторы, передаточные функции, периодические экспоненты, высокочастотные сигналы.

DOI: 10.31857/S0555292322040076, **EDN:** NAZTGC

§ 1. Введение

Мы рассматриваем прогнозирование и предикторы для сигналов непрерывного времени. Типичный подход к прогнозированию сигналов основан на удалении высокочастотной составляющей, рассматриваемой как шум, с помощью некоторых фильтров в качестве первого шага и прогнозировании плавной низкочастотной составляющей, что считается более простым. Этот подход предполагает потерю информации, содержащейся в высокочастотной составляющей, которая расценивается как шум. Но есть и работы, направленные на извлечение информации, содержащейся в высокочастотной составляющей. Эти работы основаны на различных статистических методах и моделях обучения (см., например, работы [1–6] и библиографию в них).

Мы изучаем потраекторную предсказуемость и предикторы для сигналов непрерывного времени в рамках детерминисткой модели и частотного анализа. Хорошо известно, что определенные ограничения на спектр могут обеспечить возможности прогнозирования и интерполяции сигналов (см., например, работы [7–12] и библиографию в них). В этих работах рассматривались задачи предсказания сигналов с ограниченной полосой пропускания, и полученные предикторы не были робастными по отношению к небольшому шуму на высоких частотах (см., например, обсуждение в [13, гл. 17]).

В настоящей статье мы изучаем предикторы для высокочастотных сигналов, т.е. для сигналов без каких-либо ограничений на степень затухания спектра на высоких частотах. Мы рассматриваем сигналы, спектр которых имеет конечный спектральный зазор, т.е. конечный интервал, на котором его преобразование Фурье обращается в нуль. Известно, что эти сигналы допускают однозначную экстраполяцию по своим прошлым наблюдениям. Однако из этой однозначности еще не следует существование алгоритма прогнозирования. В целом однозначность экстраполяции не обеспечивает возможности предсказания сигнала; некоторое обсуждение этого можно найти в [14, 15].

Предикторы антикаузальных сверток (т.е. интегралов, включающих будущие значения) высокочастотных сигналов были получены в [16] для сигналов с интервальным спектральным зазором, а также в [14] для сигналов с одноточечным спектральным вырождением. Предикторы в этих работах были независимы от спектральных характеристик входных сигналов из класса с определенным спектральным вырождением для низких частот. Эти предикторы зависели от ядер соответствующих антикаузальных сверток.

В настоящей статье предлагаются принципиально новые предикторы для высокочастотных сигналов. Передаточные функции для этих предикторов представляют собой многочлены от $1/\omega$, аппроксимирующие периодическую экспоненту $e^{i\omega T}$, где $\omega \in \mathbb{R}$ – частота, а $T > 0$ – предварительно выбранный горизонт прогнозирования. Эти предикторы допускают компактное явное представление во временной области и в частотной области. Кроме того, предикторы не зависят от спектральных характеристик входных сигналов с фиксированным и известным интервальным спектральным зазором. Метод основан на подходе из [17] для предсказания сигналов с быстроубывающим спектром, где использовались полиномиальные приближения периодической экспоненты.

Статья организована следующим образом. В § 2 мы формулируем определения и основные факты, связанные с линейной слабой предсказуемостью. В § 3 сформулированы основные теоремы о предсказуемости и предикторах (теоремы 1, 2). В § 4 мы обсуждаем некоторые проблемы реализации, и наконец, § 5 содержит доказательства.

§ 2. Постановка задачи и определения

Пусть $x(t)$ – наблюдаемый в текущие моменты времени $t \in \mathbb{R}$ комплекснозначный процесс с непрерывным временем. Цель состоит в том, чтобы оценить в текущие моменты времени t значения $x(t+T)$, используя исторические значения наблюдаемого процесса $x(s)|_{s\leqslant t}$. Здесь $T > 0$ – заданный горизонт прогнозирования.

Нам понадобятся некоторые обозначения и определения.

Для $p \in [1, +\infty)$ и области $G \subset \mathbb{R}$ обозначим через $L_p(G, \mathbb{R})$ и $L_p(G, \mathbb{C})$ обычные L_p-пространства функций $x\colon G \to \mathbb{R}$ и $x\colon G \to \mathbb{C}$ соответственно. Обозначим через $C(G, \mathbb{R})$ и $C(G, \mathbb{C})$ обычные линейные нормированные пространства ограниченных непрерывных функций $x\colon G \to \mathbb{R}$ и $x\colon G \to \mathbb{C}$, соответственно, с супремум-нормой.

Для $x \in L_p(\mathbb{R}, \mathbb{C})$, $p = 1, 2$, обозначим через $X = \mathcal{F}x$ функцию, определенную на $i\mathbb{R}$ как преобразование Фурье x:

$$X(i\omega) = (\mathcal{F}x)(i\omega) = \int\limits_{-\infty}^{\infty} e^{-i\omega t} x(t)\, dt, \quad \omega \in \mathbb{R}.$$

Известно, что если $x \in L_2(\mathbb{R}, \mathbb{C})$, то $X(i\,\cdot) \in L_2(\mathbb{R}, \mathbb{C})$.

Пусть $\bar{\mathcal{X}}$ – множество сигналов $x\colon \mathbb{R} \to \mathbb{R}$, таких что их преобразования Фурье $X(i\,\cdot) \in L_1(\mathbb{R}, \mathbb{C})$. В частности, в класс $\bar{\mathcal{X}}$ входят сигналы, образованные как $x(t) = \int\limits_{t}^{t+\delta} y(s)\, ds$ для $y \in L_2(\mathbb{R}, \mathbb{R})$, $\delta \in \mathbb{R}$. Ясно, что $\bar{\mathcal{X}} \subset C(\mathbb{R}, \mathbb{C})$, т.е. эти сигналы ограничены и непрерывны.

Мы рассматриваем $\bar{\mathcal{X}}$ как линейное нормированное пространство, снабженное нормой $\|X(i\,\cdot)\|_{L_1(\mathbb{R},\mathbb{C})}$, где $X(i\,\cdot) = \mathcal{F}x$ для $x \in \bar{\mathcal{X}}$. Определим $\mathcal{P}$ как множество всех непрерывных отображений $p\colon \bar{\mathcal{X}} \to C(\mathbb{R}, \mathbb{C})$, таких что для любых $x_1, x_2 \in \bar{\mathcal{X}}$ и $\tau \in \mathbb{R}$ имеем $p(x_1(\cdot))(t) = p(x_2(\cdot))(t)$ для всех $t \leqslant \tau$, если $x_1(t) = x_2(t)$ для всех

$t \leqslant \tau$. Другими словами, это набор "каузальных" отображений; мы будем искать предикторы в этом классе.

Пусть задано $T > 0$.

О п р е д е л е н и е 1. Будем говорить, что класс $\mathcal{X} \subset \bar{\mathcal{X}}$ *линейно предсказуем с горизонтом предсказания* T, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}$, такая что

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

где

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

О п р е д е л е н и е 2. Скажем, что класс $\mathcal{X} \subset \bar{\mathcal{X}}$ *равномерно линейно предсказуем с горизонтом предсказания* T, если существует последовательность $\{\widetilde{p}_d(\cdot)\}_{d=1}^{+\infty} \subset \mathcal{P}$, такая что

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

где $\widetilde{y}_d(\cdot)$ такое же, как в определении 1.

Функции $\widetilde{y}_d(t)$ в приведенном выше определении можно рассматривать как приближенные предсказания процесса $x(t+T)$.

§ 3. Основной результат

Пусть задано $\Omega > 0$. Зададим $\mathcal{X}_\Omega$ как множество всех сигналов $x(\cdot) \in \bar{\mathcal{X}}$, таких что $X(i\omega) = 0$ при $\omega \in (-\Omega, \Omega)$ для $X = \mathcal{F}x$.

Пусть $\mathcal{U}_\Omega$ – некоторое множество сигналов $x \in \mathcal{X}_\Omega$, таких что

$$\|X(i\,\cdot)\|_{L_1(\mathbb{R},\mathbb{C})} \leqslant 1 \quad \text{и} \quad \int\limits_{\omega:\,|\omega|\geqslant M} |X(i\omega)|\,d\omega \to 0 \quad \text{при } M \to +\infty$$

равномерно по $x \in \mathcal{U}_\Omega$ для $X = \mathcal{F}x$.

Т е о р е м а 1. *Для любого* $T > 0$ *справедливы следующие утверждения*:

(i) *Класс* $\mathcal{X}_\Omega$ *линейно предсказуем с горизонтом предсказания* T;

(ii) *Класс* $\mathcal{U}_\Omega$ *равномерно линейно предсказуем с горизонтом предсказания* T.

3.1. Семейство предикторов. В этом пункте мы введем некоторые предикторы.

Для $d = 1, 2, \ldots$ обозначим через Ψ_d множество всех функций $\sum\limits_{k=1}^{d} \dfrac{a_k}{z^k}$, определенных для $z \in \mathbb{C} \setminus \{0\}$, для всех $a_k \in \mathbb{R}$. Обозначим $\Psi := \bigcup\limits_d \Psi_d$.

Для $d = 0, 1, 2, \ldots$ и $s \in \mathbb{R}$ обозначим через $\mathcal{X}^{(d)}(s)$ множество всех сигналов $x \in \bar{\mathcal{X}}$, таких что $\int\limits_{-\infty}^{s} |t^d x(t)|\,dt < +\infty$. Можно отметить, что к этому классу относятся, в частности, сигналы $x \in \bar{\mathcal{X}}$, такие что $\int\limits_{\mathbb{R}} \left|\dfrac{d^k X}{d\omega^k}(i\omega)\right|^2 d\omega < +\infty$ для $k = 0, 1, \ldots, d+1$, $X = \mathcal{F}x$.

Пусть $r\colon \mathbb{R} \to (0, 1]$ – непрерывная функция, такая что $r(0) = 1$, $r(\omega) \equiv r(-\omega)$, функция $r(\omega)$ монотонно не возрастает на $(0, +\infty)$, и $r(\omega) \to 0$ при $|\omega| \to +\infty$. Пусть $r_\nu(\omega) := r(\nu\omega)$, $\nu \in (0, 1]$.

Т е о р е м а 2. *Справедливы следующие утверждения*:

(i) *Для любого* $\varepsilon_1 > 0$ *и любого* $x \in \mathcal{X}_\Omega$, *такого что* $\|X(i\,\cdot)\|_{L_1(\mathbb{R},\mathbb{C})} \leqslant 1$, *существует* $\nu_0 = \nu_0(\varepsilon_1, x) > 0$, *такое что для* $X = \mathcal{F}x$ *и любого* $\nu \in (0, \nu_0]$

$$\int\limits_{\omega:\,|\omega|\geqslant\Omega} (1 - r_\nu(\omega))|X(i\omega)|\,d\omega \leqslant \varepsilon_1. \tag{1}$$

Более того, можно выбрать одно и то же $\nu_0 = \nu_0(\varepsilon_1)$ *для всех* $x \in \mathcal{U}_\Omega$;

(ii) *Для любых* $\varepsilon_2 > 0$ *и* $\nu > 0$ *существуют целое число* $d = d(\nu, \varepsilon_2, T) > 0$ *и функция* $\psi_d \in \Psi_d$, *такие что*

$$\sup_{\omega:\,|\omega|\geqslant\Omega} |e^{i\omega T} r_\nu(\omega) - \psi_d(i\omega)| \leqslant \varepsilon_2; \tag{2}$$

(iii) *Предсказуемость, указанную в утверждении* (i) *теоремы* 1 *для* $x \in \mathcal{X}_\Omega$, *а также предсказуемость, указанную в утверждении* (ii) *теоремы* 1 *для* $x \in \mathcal{U}_\Omega$, *можно обеспечить с помощью последовательности предикторов*

$$p_d\colon \mathcal{X}_\Omega \to C(\mathbb{R}, \mathbb{C}), \quad d = 1, 2, \ldots,$$

определяемых их передаточными функциями $\psi_d(i\omega)$. *Точнее, для любых* $\varepsilon > 0$ *и* $\widehat{y}_d(t) = p_d(x(\cdot))(t)$ *оценка*

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

выполняется, если ν, d *и* ψ_d *таковы, что* (1), (2) *выполняются для достаточно малых* ε_1 *и* ε_2, *таких что*

$$\varepsilon_1 + \varepsilon_2 \leqslant 2\pi\varepsilon.$$

Можно отметить, что для входных сигналов $x \in \mathcal{X}_\Omega$ *передаточные функции* $\psi_d(i\omega)$ *можно заменить функциями* $\psi_d(i\omega)\mathbb{I}_{\omega:\,|\omega|\geqslant\Omega}$, *где* $\mathbb{I}$ *обозначает индикаторную функцию*;

(iv) *Для* $x \in \mathcal{X}^{(d-1)}(t) \cap \mathcal{X}_\Omega$ *описанные выше предикторы можно представить в виде*

$$p_d(x(\cdot))(t) = \int\limits_{-\infty}^{t} K(t-\tau)x(\tau)\,d\tau, \tag{3}$$

где

$$K(t) = \sum_{k=1}^{d} a_k \frac{t^{k-1}}{(k-1)!}.$$

Здесь $a_k \in \mathbb{C}$ – *коэффициенты при* $\psi_d(z) = \sum\limits_{k=1}^{d} a_k z^{-k}$ *из п.* (ii).

3.2. Интегральное представление предикторов для общего типа $x \in \mathcal{X}_\Omega$. Представление (3) для приведенных выше предикторов требует, чтобы $x \in \mathcal{X}^{(d-1)}(t)$. Обсудим возможности представления во временной области для общего типа $x \in \mathcal{X}_\Omega$.

Рассмотрим операторы h_k, определенные на $\mathcal{X}_\Omega$ своими передаточными функциями $(i\omega)^{-k}$, $k = 1, 2, \ldots$ Другими словами, если $y = h_k(x)$ для $x \in \mathcal{X}_\Omega$, то $Y(i\omega) = (i\omega)^{-k}X(i\omega)$ для $Y = \mathcal{F}y$ и $X = \mathcal{F}x$. Очевидно, что $h_k(x(\cdot)) \in \mathcal{X}_\Omega$, преобразования Фурье процессов $h_k(x(\cdot))$ равны нулю на $[-\Omega, \Omega]$, а операторы $h_k\colon \mathcal{X}_\Omega \to C(\mathbb{R}, \mathbb{C})$

непрерывны. Из определений следует, что

$$p_d(x(\cdot))(t) = \sum_{k=1}^{d} a_k h_k(x(\cdot))(t).$$

Можно заметить, что $p_d(\cdot)$ зависит от T через коэффициенты a_k, определенные для функций $\psi_d(\omega)$, аппроксимирующих $e^{i\omega T}$.

Формально оператор $h_k(x(\cdot)$ можно представить в виде

$$h_k(x(\cdot))(s_k) = \int\limits_{-\infty}^{s_k} ds_{k-1} \int\limits_{-\infty}^{s_{k-1}} ds_{k-2} \ \dots \int\limits_{-\infty}^{s_2} ds_1 \int\limits_{-\infty}^{s_1} x(s)\, ds, \tag{4}$$

т.е.

$$h_1(x(\cdot))(t) = \int\limits_{-\infty}^{t} x(s)\, ds, \quad h_k(x(\cdot))(t) = \int\limits_{-\infty}^{t} h_{k-1}(x(\cdot))(s)\, ds, \quad k = 2, 3, \dots$$

Для $x \in \mathcal{X}_\Omega$ общего типа нет гарантии, что $x \in L_1(\mathbb{R}, \mathbb{R})$ или $h_k(x(\cdot)) \in L_1(\mathbb{R}, \mathbb{R})$. Однако приведенные выше интегралы определены корректно, поскольку их можно заменить интегралами по конечным интервалам времени

$$h_1(x(\cdot))(t) = \int\limits_{R_1}^{t} x(s)\, ds, \quad h_k(x(\cdot))(t) = \int\limits_{R_k}^{t} h_{k-1}(x(\cdot))(s)\, ds, \quad k > 1, \tag{5}$$

где R_k – корни сигналов $h_k(x(\cdot))(t)$. Это возможно из-за особых свойств сигналов со спектральным зазором, т.е. с преобразованием Фурье, обращающимся в нуль на отрезке: при любом $\tau < 0$ эти сигналы имеют бесконечно много корней на отрезке $(-\infty, \tau)$ (см., например, [18]). Следовательно, предикторы, определенные в теореме 2 для $x \in \mathcal{X}_\Omega$, допускают альтернативное интегральное представление через (4) или (5).

§ 4. О численной реализации предикторов

Непосредственная реализация предиктора, введенного в теореме 2, требует вычислений интегралов по полубесконечным интервалам, которые могут быть численно сложными. Однако эта теорема может привести к методам прогнозирования, обходящим такие расчеты. Обсудим эти возможности.

Пусть $t_1 \in \mathbb{R}$ задано. Пусть $x_k := h_k(x)$ для $x \in \mathcal{X}_\Omega$, $k = 1, 2, \dots$, и пусть $\eta_k := x_k(t_1)$.

Лемма 1. *В обозначениях теоремы* 2 *для любого* $t \geqslant t_1$ *предсказания* $\widehat{y}_d = p_d(x(\cdot))$ *можно представить в виде*

$$\widehat{y}_d(t) = \sum_{k=1}^{d} a_k \left(\sum_{\ell=1}^{k} c_\ell(t)\eta_\ell + f_k(t) \right), \tag{6}$$

где $c_\ell(t) := (t - t_1)^{(\ell-1)}/(\ell - 1)!$ *и*

$$f_k(t) := \int\limits_{t_1}^{t} d\tau_1 \int\limits_{t_1}^{\tau_1} d\tau_2 \dots \int\limits_{t_1}^{\tau_k} x(s)\, ds. \tag{7}$$

Эта лемма показывает, что предсказание $\widehat{y}_d(t)$ для $x(t+T)$ легко вычислить для $t > t_1$, если мы знаем все η_k и наблюдаем $x|_{[t_1,t]}$.

Обсудим возможные способы вычисления η_k в обход прямого интегрирования по бесконечным интервалам.

Во-первых, заметим, что (6) подразумевает следующее полезное свойство.

Следствие 1. *Для любого $\varepsilon > 0$ существуют целое число $d = d(\varepsilon) > 0$ и числа $a_1, \ldots, a_d \in \mathbb{R}$, такие что для любых $x \in \mathcal{X}_\Omega$ и $t_1 \in \mathbb{R}$ существуют $\bar{\eta}_1, \ldots, \bar{\eta}_d \in \mathbb{R}$, такие что $|x(t+T) - y_d(t)| \leqslant \varepsilon$ для всех $t \geqslant t_1$, где*

$$y_d(t) = y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d) := \sum_{k=1}^{d} a_k \left(\sum_{\ell=1}^{k} c_\ell(t)\bar{\eta}_\ell + f_k(t) \right). \tag{8}$$

В этом следствии $d = d(\varepsilon)$ можно выбрать, как указано в утверждениях (i), (ii) теоремы 2, где ε_1 и ε_2 таковы, что $\varepsilon_1 + \varepsilon_2 \leqslant 2\pi\varepsilon$.

Далее обсуждается использование соотношения (6) для оценки η_k и прогнозирования. Пусть $\theta > t_1$. Предположим, что цель состоит в том, чтобы спрогнозировать значение $x(\theta + T)$ для наблюдений в моменты времени $t \leqslant \theta$. Если $\theta > t_1 + T$, то следствие 1 дает возможность построить предикторы через подгоночные параметры $\eta_1, \ldots, \eta_d$, используя прошлые наблюдения, доступные для $t \in [t_1, \theta - T]$: можно сопоставить значения $y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d)$ с прошлыми наблюдениями $x(t+T)$. Начиная с этого момента, мы предполагаем, что $\theta > t_1 + T$.

Пусть d достаточно велико, чтобы $x(t+T)$ аппроксимировалось величиной $\widehat{y}_d(t)$, как описано в теореме 2, т.е. $\sup\limits_{t\in\mathbb{R}} |x(t+T) - \widehat{y}_d(t)| \leqslant \varepsilon$ для некоторого достаточно малого $\varepsilon > 0$ при некотором выборе a_k.

В качестве приближения истинного набора $\eta_1, \ldots, \eta_d$ мы можем принять набор $\bar{\eta}_1, \ldots, \bar{\eta}_d$, такой что

$$|x(t+T) - y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d)| \leqslant \varepsilon \quad \forall t \in [t_1, \theta - T]. \tag{9}$$

(Напомним, что в момент времени θ значения $x(t+T)$ и $y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d)$ наблюдаемы для этих $t \in [t_1, \theta - T]$.) Если выполняется (9), то можно заключить, что $y_d(t, \bar{\eta}_1, \ldots, \bar{\eta}_d)$ дает приемлемое предсказание $x(t+T)$ для этих t. Ясно, что из теоремы 2 следует, что множество $\bar{\eta}_1, \ldots, \bar{\eta}_d$, обеспечивающее (9), существует, так как это неравенство выполняется при $\bar{\eta}_k = \eta_k$.

Соответствующее значение $y_d(\theta, \bar{\eta}_1, \ldots, \bar{\eta}_d)$ мы можем рассматривать как оценку для $\widehat{y}_d(\theta)$ и, соответственно, для $x(\theta + T)$.

Далее, набор $\bar{\eta}_1, \ldots, \bar{\eta}_d$, обеспечивающий (9), все еще может быть сложно найти. Вместо этого можно рассматривать подходящие предсказания и наблюдения в конечном числе точек $t \in [t_1, T - \theta]$.

Пусть целое число $\bar{d} \geqslant d$ и множество $\{t_m\}_{m=1}^{\bar{d}} \subset \mathbb{R}$ выбраны так, что

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

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

$$\sum_{k=1}^{d} a_k \left(\sum_{\ell=1}^{k} c_\ell(t_m)\bar{\eta}_\ell + f_k(t_m) \right) = \zeta_m, \quad m = 1, \ldots, \bar{d}. \tag{10}$$

Рассмотрим сначала случай, когда $\bar{d} = d$. В этом случае можно выбрать $\zeta_m = x(t_m + T)$; эти значения наблюдаемы непосредственно, без вычисления интегра-

лов на полубесконечных интервалах, необходимых для $\widehat{y}_d(t_m)$. Соответствующий выбор $\bar{\eta}_k$ обеспечивает нулевую ошибку предсказания для $x(t_m+T)$, $m=1,\dots,\bar{d}$.

Включение в рассмотрение большего количества наблюдений, т.е. выбор большего $\bar{d}>d$ и более широкого интервала $[t_1,\theta-T]$ приведет к улучшению оценки η_k. Если мы рассмотрим $\bar{d}>d$, то в общем случае невозможно добиться, чтобы $y_d(t,\bar{\eta}_1,\dots,\bar{\eta}_d)=x(t_m+T)$ для всех m, так как нельзя гарантировать, что система (10) разрешима для $\zeta_m\equiv x(t_m+T)$ – система будет переопределена. Тем не менее оценка, представленная в (9), все еще может быть достигнута для любого сколь угодно большого $\bar{d}$, поскольку (9) выполняется. Решение может быть найдено с помощью методы подгонки линейных моделей.

Далее, вместо вычисления коэффициентов a_k путем решения задачи аппроксимации комплексной экспоненты, описанной в утверждениях (i), (ii) теоремы 2, можно найти эти коэффициенты, рассматривая их как дополнительные неизвестные в системе (10) с $\bar{d}\geqslant 2d$. Из теоремы 2 снова следует, что существуют $\bar{\eta}_k=\eta_k\in\mathbb{R}$ и $a_k\in\mathbb{R}$, такие что (10) выполняется с $\zeta_m=\widehat{y}_d(t_m)$. Это привело бы к нелинейной задаче подбора неизвестных $a_1,\dots,a_d,\bar{\eta}_1,\dots,\bar{\eta}_d$.

Состоятельность этих оценок пока неясна, поскольку выбор меньшего ε приводит к большему d. Мы оставляем анализ этих методов для будущих исследований.

§ 5. Доказательства

Теорема 1 непосредственно вытекает из теоремы 2.

Доказательство теоремы 2. Докажем утверждение (i). Выберем $M>0$ так, чтобы

$$\int\limits_{\omega\colon|\omega|>M}|X(i\omega)|\,d\omega<\varepsilon_1/2\quad\forall x\in\mathcal{U}_\Omega.$$

Тогда $r_\nu(\omega)\to 1$ равномерно на $\omega\in[-M,M]$, так как

$$0<1-r_\nu(\omega)\leqslant 1-r_\nu(M)\quad\text{для}\quad\omega\in[-M,M].$$

Следовательно, можно выбрать $\nu>0$ так, что

$$\int\limits_{-M}^{M}(1-r_\nu(\omega))|X(i\omega)|\,d\omega\leqslant\varepsilon_1/2.$$

Это означает, что

$$\begin{aligned}&\int\limits_{-\infty}^{\infty}(1-r_\nu(\omega))|X(i\omega)|\,d\omega=\\&=\int\limits_{-M}^{M}(1-r_\nu(\omega))|X(i\omega)|\,d\omega+\int\limits_{\omega\colon|\omega|>M}(1-r_\nu(\omega))|X(i\omega)|\,d\omega\leqslant\\&\leqslant\int\limits_{-M}^{M}(1-r_\nu(\omega))|X(i\omega)|\,d\omega+\int\limits_{\omega\colon|\omega|>M}|X(i\omega)|\,d\omega\leqslant\frac{\varepsilon_1}{2}+\frac{\varepsilon_1}{2}\leqslant\varepsilon_1.\end{aligned}$$

Это завершает доказательство утверждения (i).

Докажем утверждение (ii). Из теоремы Стоуна – Вейерштрасса для вещественных непрерывных функций на локально компактных пространствах следует, что существуют $\psi_d^c(\omega) \in \Psi_d$ и $\psi_d^s(\omega) \in \Psi_d$, такие что

$$\sup_{\omega\colon |\omega|\geqslant\Omega} |\cos(T\cdot)r_\nu(\cdot) - \psi_d^c(\cdot)| \leqslant \varepsilon_2/2, \qquad \sup_{\omega\colon |\omega|\geqslant\Omega} |\sin(T\cdot)r_\nu(\cdot) - \psi_d^s(\cdot)| \leqslant \varepsilon_2/2$$

(см., например, [19, теорема 12, с. 240–241]).

Легко видеть, что достаточно выбрать нечетные функции $\psi_d^c(\omega) = \sum\limits_{k=1}^{d} \gamma_k^c \omega^{-k}$ и четные функции $\psi_d^s(\omega) = \sum\limits_{k=1}^{d} \gamma_k^s \omega^{-k}$, т.е. $\gamma_{2m+1}^c = 0$ и $\gamma_{2m}^s = 0$ для целых чисел $m \geqslant 0$. Здесь γ_k^c и γ_k^s вещественные.

Построим искомые функции как

$$\psi_d(i\omega) = \psi_d^c(\omega) + i\psi_d^s(\omega) = \sum_{k=1}^{d} \gamma_k^c \omega^{-k} + i\sum_{k=1}^{d} \gamma_k^s \omega^{-k} = \sum_{k=1}^{d} a_k (i\omega)^{-k},$$

где коэффициенты $a_k \in \mathbb{R}$ определяются следующим образом:

- Если $k = 2m$ для целого числа m, то $a_k = (-1)^m \gamma_k^c$;
- Если $k = 2m+1$ для целого числа m, то $a_k = -(-1)^m \gamma_k^s$.

Такой выбор ψ_d гарантирует выполнение оценки (2). Это завершает доказательство утверждения (ii).

Докажем утверждение (iii). Предположим, что оценки (1), (2) выполнены для данных d, ν, ψ_d. Имеем

$$2\pi(x(t+T) - \widehat{y}_d(t)) = \int\limits_{-\infty}^{\infty} e^{i\omega t}(e^{i\omega T} - \psi_d(i\omega))X(i\omega)\,d\omega = A(t) + B(t),$$

где

$$A(t) = \int\limits_{-\infty}^{\infty} e^{i\omega t}(e^{i\omega T} - e^{i\omega T} r_\nu(\omega))X(i\omega)\,d\omega,$$

$$B(t) = \int\limits_{-\infty}^{\infty} e^{i\omega t}(e^{i\omega T} r_\nu(\omega) - \psi_d(i\omega))X(i\omega)\,d\omega.$$

Очевидно, что

$$|A(t)| \leqslant \int\limits_{-\infty}^{\infty} (1 - r_\nu(\omega))|X(i\omega)|\,d\omega \leqslant \varepsilon_1$$

и

$$|B(t)| \leqslant \int\limits_{-\infty}^{\infty} |e^{i\omega T} r_\nu(\omega) - \psi_d(i\omega)||X(i\omega)|\,d\omega \leqslant$$

$$\leqslant \sup_{\omega\colon |\omega|\geqslant\Omega} |e^{i\omega T} r_\nu(\omega) - \psi_d(i\omega)| \int\limits_{-\infty}^{\infty} |X(i\omega)|\,d\omega \leqslant \varepsilon_2.$$

Следовательно,

$$2\pi|x(t+T)-\widehat{y}_d(t)|\leqslant\varepsilon_1+\varepsilon_2.$$

Это доказывает равномерную предсказуемость, указанную в утверждении (ii) теоремы 1 для сигналов $x\in\mathcal{U}_\Omega$. Предсказуемость, указанная в утверждении (i) теоремы 1, следует из вышеприведенного доказательства, примененного к одноэлементному множеству $\mathcal{U}_\Omega=\{x(\cdot)\}$, возможно, умноженному на константу, чтобы удовлетворить ограничению $\|X(\cdot)\|_{L_1(\mathbb{R},\mathbb{C})\leqslant 1}$. Это доказывает утверждение (iii).

Докажем утверждение (iv). Во-первых, из известных свойств преобразований Фурье производных и первообразных вытекают представления (4), (5) (см. некоторые пояснения в п. 3.2). Утверждение (iv) можно получить последовательным применением теоремы Фубини к интегрируемым в $L_1((-\infty,t],\mathbb{R})$ сигналам $(\tau-s)^\ell x(s)$, представленным в (4) для $\ell=1,2,\ldots$, $\tau\in(\infty,s]$. ▲

Доказательство леммы 1. В обозначениях теоремы 2 для всех $t\geqslant t_1$ имеем $y_d(t)=\sum\limits_{k=1}^{d}a_kx_k(t)$, т.е.

$$y_d(t)=\sum_{k=1}^{d}a_k\left(\eta_k+\int\limits_{t_1}^{t}x_{k-1}(s)\,ds\right)\tag{11}$$

(мы предполагаем здесь что $x_0:=x$). Далее, имеем

$$\int\limits_{t_1}^{t}x_1(t)\,dt=\int\limits_{t_1}^{t}\left(\eta_1+\int\limits_{t_1}^{\tau}x_0(s)\,ds\right)d\tau=\eta_1(t-t_1)+\int\limits_{t_1}^{t}d\tau\int\limits_{t_1}^{\tau}x(s)\,ds$$

и

$$\begin{aligned}\int\limits_{t_1}^{t}x_2(t)\,dt&=\int\limits_{t_1}^{t}\left(\eta_2+\int\limits_{t_1}^{\tau_1}x_1(s)\,ds\right)d\tau_1=\eta_2(t-t_1)+\int\limits_{t_1}^{t}d\tau_1\int\limits_{t_1}^{\tau_1}x_1(s)\,ds=\\&=\eta_2(t-t_1)+\int\limits_{t_1}^{t}d\tau_1\left[\eta_1(\tau_1-t_1)+\int\limits_{t_1}^{\tau_1}d\tau_2\int\limits_{t_1}^{\tau_2}x(s)\,ds\right]=\\&=\eta_2(t-t_1)+\frac{\eta_1^2}{2}(t-t_1)+\int\limits_{t_1}^{t}d\tau_1\int\limits_{t_1}^{\tau_2}x(s)\,ds.\end{aligned}$$

Аналогично получаем, что

$$\begin{aligned}&\int\limits_{t_1}^{t}x_k(t)\,dt=\eta_k(t-t_1)+\frac{\eta_{k-1}}{2}(t-t_1)^2+\ldots+\frac{\eta_1}{k!}(t-t_1)^k+\\&+\int\limits_{t_1}^{t}d\tau_1\int\limits_{t_1}^{\tau_1}d\tau_2\ \ldots\int\limits_{t_1}^{\tau_k}x(s)\,ds.\end{aligned}$$

Из этого следует, что

$$\eta_k + \int_t^t x_{k-1}(s)\,ds = \sum_{\ell=1}^{k} c_\ell(t)\eta_\ell + f_k(t).$$

Вместе с (11) это доказывает (8), что завершает доказательство леммы 1. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Brooks C., Hinich M.J.* Detecting Intraday Periodicities with Application to High Frequency Exchange Rates // J. Roy. Statist. Soc. Ser. C. 2006. V. 55. № 2. P. 241–259. https://doi.org/10.1111/j.1467-9876.2006.00534.x
2. *Christensen H.L., Murphy J., Godsill S.J.* Forecasting High-Frequency Futures Returns Using Online Langevin Dynamics // IEEE J. Sel. Top. Signal Process. 2012. V. 6. № 4. P. 366–380. https://doi.org/10.1109/JSTSP.2012.2191532
3. *Granger C.W.J.* Extracting Information from Mega-panels and High-Frequency Data // Statist. Neerlandica. 1998. V. 52. № 3. P. 258–272. https://doi.org/10.1111/1467-9574.00084
4. *Li Z., Han J., Song Y.* On the Forecasting of High-Frequency Financial Time Series Based on ARIMA Model Improved by Deep Learning // J. Forecast. 2020. V. 39. № 7. P. 1081–1097. https://doi.org/10.1002/for.2677
5. *Luo S., Tian C.* Financial High-Frequency Time Series Forecasting Based on Sub-step Grid Search Long Short-Term Memory Network // IEEE Access. 2020. V. 8. P. 203183–203189. https://doi.org/10.1109/ACCESS.2020.3037102
6. *Engle R.F.* The Econometrics of Ultra-high-Frequency Data // Econometrica. 2000. V. 68. № 1. P. 1–22. https://doi.org/10.1111/1468-0262.00091
7. *Knab J.J.* Interpolation of Band-Limited Functions Using the Approximate Prolate Series // IEEE Trans. Inform. Theory. 1979. V. 25. № 6. P. 717–720. https://doi.org/10.1109/TIT.1979.1056115
8. *Lyman R.J., Edmonson W.W., McCullough S., Rao M.* The Predictability of Continuous-Time, Bandlimited Processes // IEEE Trans. Signal Process. 2000. V. 48. № 2. P. 311–316. https://doi.org/10.1109/78.823959
9. *Lyman R.J., Edmonson W.W.* Linear Prediction of Bandlimited Processes with Flat Spectral Densities // IEEE Trans. Signal Process. 2001. V. 49. № 7. P. 1564–1569. https://doi.org/10.1109/78.928709
10. *Papoulis A.* A Note on the Predictability of Band-limited Processes // Proc. IEEE. 1985. V. 73. № 8. P. 1332–1333. https://doi.org/10.1109/PROC.1985.13284
11. *Marvasti F.* Comments on "A Note on the Predictability of Band-limited Processes" // Proc. IEEE. 1986. V. 74. № 11. P. 1596. https://doi.org/10.1109/PROC.1986.13674
12. *Vaidyanathan P.P.* On Predicting a Band-limited Signal Based on Past Sample Values // Proc. IEEE. 1987. V. 75. № 8. P. 1125–1127. https://doi.org/10.1109/PROC.1987.13856
13. *Higgins J.R.* Sampling Theory in Fourier and Signal Analysis: Foundations. Oxford: Clarendon; New York: Oxford Univ. Press, 1996.
14. *Dokuchaev N.* On Linear Weak Predictability with Single Point Spectrum Degeneracy // Appl. Comput. Harmon. Anal. 2021. V. 53. P. 116–131. https://doi.org/10.1016/j.acha.2021.01.005
15. *Докучаев Н.Г.* К однозначности восстановления данных при ограничениях на множество спектральных значений // Пробл. передачи информ. 2021. Т. 57. № 4. С. 74–78. https://doi.org/10.31857/S0555292321040069
16. *Dokuchaev N.G.* The Predictability of Band-limited, High-Frequency, and Mixed Processes in the Presence of Ideal Low-Pass Filters // J. Phys. A: Math. Theor. 2008. V. 41. № 38. P. 382002 (7 pp.). https://doi.org/10.1088/1751-8113/41/38/382002

17. *Dokuchaev N.* Limited Memory Predictors Based on Polynomial Approximation of Periodic Exponentials // J. Forecast. 2022. V. 41. № 5. P. 1037–1045. https://doi.org/10.1002/for.2843
18. *Blank N., Ulanovskii A.* Paley–Wiener Functions with a Generalized Spectral Gap // J. Fourier Anal. Appl. 2011. V. 17. № 5. P. 899–915. https://doi.org/10.1007/s00041-010-9160-3
19. *Stone M.H.* The Generalized Weierstrass Approximation Theorem // Math. Mag. 1948. V. 21. № 4. P. 167–184; № 5. P. 237–254 (continued). https://doi.org/10.2307/3029750; https://doi.org/10.2307/3029337

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

Поступила в редакцию
01.08.2022
После доработки
12.11.2022
Принята к публикации
14.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.176

© 2022 г. **Я.К. Шубин**

НИЖНЯЯ ОЦЕНКА МИНИМАЛЬНОГО ЧИСЛА РЕБЕР В ПОДГРАФАХ ГРАФА ДЖОНСОНА

Доказана новая нижняя оценка минимального числа ребер в подграфах графа Джонсона в общем случае.

Ключевые слова: графы Джонсона, дистанционные графы.

DOI: 10.31857/S0555292322040088, **EDN:** NBIEMH

§ 1. Введение

В статье рассматривается специальный дистанционный граф $G(n, r, s)$, вершинами которого являются точки в n-мерном булевом кубе, у которых ровно r единиц, а ребро между такими вершинами проводится тогда и только тогда, когда скалярное произведение соответствующих векторов равно s. Данное определение можно также сформулировать в комбинаторных терминах, а именно: вершинами данного графа являются всевозможные r-элементные подмножества множества $\mathcal{R}_n = \{1, 2, \ldots, n\}$, а ребро проводится между подмножествами, имеющими ровно s общих элементов. Именно вторым определением мы будем пользоваться в дальнейшем.

Граф $G(n, r, s)$ имеет большое значение для теории графов, комбинаторной геометрии и исследования кодов с запрещенными расстояниями. Именно с помощью этих графов Франкл и Уилсон установили, что хроматическое число пространства растет экспоненциально с ростом размерности (см. [1]). В 1991 г. Дж. Кан и Г. Калаи использовали результаты Франкла и Уилсона для опровержения классической гипотезы Борсука о том, что всякое ограниченное множество в $\mathbb{R}^n$ мощности больше 1 может быть разбито на $n+1$ частей меньшего диаметра (см. [2–6]). В работах [7–10] исследованы некоторые свойства графа $G(n, r, s)$ и схожих с ним по структуре графов.

Обозначим через $\rho(W)$ количество ребер графа $G = (V, E)$ на множестве $W \subseteq V$. Иными словами,

$$\rho(W) = |\{(x, y) \in E \mid x \in W,\ y \in W\}|.$$

Также положим

$$\rho_G(\ell) = \min_{\substack{|W|=\ell \\ W \subseteq V}} \rho(W).$$

Отметим, что проблема оценивания количества ребер в индуцированных подграфах тесно связана с теорией расширителей и спектральной теорией графов (см. [11–13]).

Будем рассматривать величину $\rho_{G(n,r,s)}(\ell(n))$ при фиксированных r и s в зависимости от асимптотики $\ell(n)$ при $n \to \infty$.

Напомним, что независимым множеством вершин графа G называется такое подмножество его вершин, что никакие две вершины этого подмножества не соединены ребром. Числом независимости $\alpha(G)$ называется наибольшая мощность независимого множества.

Заметим, что если $\ell \leqslant \alpha$, то $\rho_G(\ell) = 0$. Таким образом, мы будем исследовать величину $\rho_{G(n,r,s)}(\ell)$ именно в случае $\alpha < \ell \leqslant |V(G(n,r,s))| = C_n^r$. Число независимости графа $G(n,r,s)$ было исследовано в работе [14].

В работах [15, 16] были доказаны следующие оценки.

Теорема 1. *Для графа $G(n,r,s)$ с фиксированными r, s и любой функции $\ell = \ell(n)$, такой что $\ell > \alpha(G(n,r,s))$, выполнено*

$$\rho_{G(n,r,s)}(\ell) \leqslant (1+o(1))\frac{\ell^2}{n^s}\frac{C_r^s r!}{2(r-s)!}.$$

Теорема 2. *Для графа $G(n,r,s)$ с фиксированными $r, s > 0$ и любой функции $\ell = \ell(n)$, такой что $n^{r-1} = o(\ell)$, выполнено*

$$\rho_{G(n,r,s)}(\ell) \geqslant (1+o(1))\frac{\ell^2}{n^s}\frac{C_r^s r!}{2(r-s)!}.$$

Обратим внимание, что вместе эти две теоремы дают точную оценку в случае "самых больших" функций ℓ для любых фиксированных r и s. При меньших ℓ верхняя оценка из теоремы 1 также верна, однако доказательство нижней оценки аналогично теореме 2 провести пока не удается.

Заметим, что если мы применим для графа $G(n,r,s)$ теорему Турана для дистанционных графов (см. [17]), то получим оценку

$$\rho_{G(n,r,s)}(\ell) \geqslant (1+o(1))\frac{\ell^2}{\alpha(G(n,r,s))}.$$

При $r \leqslant 2s+1$ мы знаем (см. [14]), что

$$n^s c(r,s) \leqslant \alpha(G(n,r,s)) \leqslant n^s d(r,s),$$

где $c(r,s)$ и $d(r,s)$ – константы, зависящие только от r и s.

Таким образом, в случае $r \leqslant 2s+1$ порядок верхней и нижней оценок одинаков, а зазор остается лишь в константу.

Теперь рассмотрим случай $r > 2s+1$. В этом режиме имеем (см. [14])

$$\alpha(G(n,r,s)) \sim \frac{n^{r-s-1}}{(r-s-1)!}.$$

Если подставить это число независимости в турановскую оценку, то в знаменателе будет n^{r-s-1}, а в верхней оценке из теоремы 1 в знаменателе находится n^s. Заметим, что $r-s-1 > s$, а значит, между оценками остается зазор по порядку.

В данной статье будет доказана следующая

Теорема 3. *Для графа $G(n,r,s)$ с фиксированными r и s, где $r > 2s+1$, $s > 1$, и любой функции $\ell = \ell(n)$, такой что $n^{r-2} = o(\ell)$, $\ell = o(n^{r-1})$, выполнено*

$$\rho_{G(n,r,s)}(\ell) \geqslant (1+o(1))\frac{\ell^2}{n^s}c(r,s),$$

где $c(r,s)$ – константа, зависящая от r и s.

Получаем, что в случае $n^{r-2} = o(\ell)$, $\ell = o(n^{r-1})$ и $r > 2s + 1$ по теореме 3 мы также доказали, что нижняя и верхняя оценки отличаются лишь в константу раз.

§ 2. Доказательство теоремы 3

Для каждого n возьмем подмножество вершин W_n графа $G(n, r, s)$, такое что $|W_n| = \ell(n)$, $\ell = o(n^{r-1}), n^{r-2} = o(\ell)$.

Пронумеруем все s-элементные подмножества $\mathcal{R}_n = \{1, 2, \ldots, n\}$ и назовем их $S_1, S_2, \ldots S_m$, где $m = C_n^s$. Для каждого S_i определим подмножество вершин нашего множества W_n, содержащих его:

$$K_i = \{v \mid S_i \subset v,\ v \in W_n\}.$$

Данные множества будут пересекаться по вершинам. Но если две вершины нашего графа соединены ребром, то они будут одновременно входить ровно в одно из K_i, так как они имеют ровно s общих элементов. Тогда

$$\rho(W_n) = \sum_{i=1}^{m} \rho(K_i).$$

Введем обозначение $k_i = |K_i|$. Заметим, что каждая вершина входит ровно в C_r^s различных K_i, поэтому получаем

$$\sum_{i=1}^{m} k_i = \ell C_r^s.$$

Также для каждой пары множества S_i и элемента j (j не входит в S_i) возьмем множество вершин $M_{S_i,j}$ нашего подграфа, содержащее все элементы из S_i и элемент j одновременно:

$$M_{S_i,j} = \{v \mid v \in W_n, (S_i \cup \{j\}) \subset v\}.$$

Обозначим мощности таких подмножеств $m_{S_i,j} = |M_{S_i,j}|$.

Также для каждого множества S_i обозначим через M_i максимальное по мощности $M_{S_i,j}$, а сам элемент j будем обозначать через t_i. Если существует несколько максимальных $M_{S_i,j}$, то выбираем любое из них, поэтому t_i и M_i задаются однозначно. Положим $m_i = |M_i|$.

Назовем индекс i *хорошим*, если для него выполнено

$$m_i \leqslant \frac{2C_r^s - 2}{2C_r^s - 1} k_i,$$

а в противном случае будем называть его *плохим*. Множество хороших индексов назовем A, а плохих – B:

$$A = \left\{ i \;\middle|\; m_i \leqslant \frac{2C_r^s - 2}{2C_r^s - 1} k_i \right\}, \quad B = \left\{ i \;\middle|\; m_i > \frac{2C_r^s - 2}{2C_r^s - 1} k_i \right\}.$$

Лемма 1. *Для любого хорошего индекса i выполнено*

$$\rho(K_i) \geqslant c_1(r, s) k_i^2 - c_2(r, s) n^{r-s-2} k_i.$$

Доказательство. Разделим наше доказательство на два случая:

$$m_i \leqslant \frac{1}{r} k_i$$

и

$$\frac{1}{r}k_i < m_i \leqslant \frac{2C_r^s - 2}{2C_r^s - 1}k_i.$$

Покажем, что

$$\frac{1}{r} < \frac{2C_r^s - 2}{2C_r^s - 1}.$$

Мы рассматриваем $r \geqslant 6$, поэтому $\frac{1}{r} \leqslant \frac{1}{6}$, при этом

$$\frac{2C_r^s - 2}{2C_r^s - 1} = 1 - \frac{1}{2C_r^s - 1} \geqslant 1 - \frac{1}{2r - 1} \geqslant \frac{10}{11}.$$

Получаем, что

$$\frac{2C_r^s - 2}{2C_r^s - 1} > \frac{1}{r},$$

а значит, разделение имеет смысл.

1. Пусть для какого-то i выполнено $m_i \leqslant \frac{1}{r}k_i$. Степень каждой вершины $S_i \cup \cup \{a_1, a_2, \ldots, a_{r-s}\}$ внутри множества вершин K_i не меньше

$$k_i - m_{S_i,a_1} - m_{S_i,a_2} - \ldots - m_{S_i,a_{r-s}} \geqslant k_i - (r-s)m_i \geqslant \frac{s}{r}k_i.$$

Тогда получаем, что

$$\rho(K_i) \geqslant \frac{s}{2r}k_i^2.$$

2. Пусть для i выполнено

$$\frac{1}{r}k_i < m_i \leqslant \frac{2C_r^s - 2}{2C_r^s - 1}k_i.$$

Множество вершин K_i можно поделить на два подмножества: M_i и $Q_i = K_i \setminus M_i$. Также напомним, что все вершины множества M_i имеют еще какой-то общий элемент j по своему определению, а вершины множества Q_i элемент j не содержат. Возьмем любую вершину $v = S_i \cup \{a_1, a_2, \ldots, a_{r-s}\} \in Q_i$. Заметим, что любая вершина множества M_i, не смежная с v, должна содержать элементы S_i, j и еще хотя бы один элемент из множества $\{a_1, \ldots, a_{r-s}\}$. Тогда таких вершин не более

$$(r-s)C_{n-s-2}^{r-s-2} \leqslant (r-s)n^{r-s-2}.$$

Таким образом, количество вершин множества M_i, смежных с v, не меньше, чем $m_i - (r-s)n^{r-s-2}$. Получаем, что

$$\rho(K_i) \geqslant |Q_i|(m_i - (r-s)n^{r-s-2}) = (k_i - m_i)(m_i - (r-s)n^{r-s-2}) =$$
$$= (k_i - m_i)m_i - (r-s)n^{r-s-2}(k_i - m_i).$$

Оценим эту разность по частям: $k_i - m_i \leqslant \frac{r-1}{r}k_i$, поэтому

$$(r-s)n^{r-s-2}(k_i - m_i) \leqslant \frac{(r-s)(r-1)}{r}n^{r-s-2}k_i.$$

Теперь рассмотрим $(k_i - m_i)m_i$ как функцию относительно m_i. Это парабола с ветвями вниз, а значит, ее минимум на интервале достигается на одном из концов: при $m_i = \frac{1}{r}k_i$ получаем $\frac{r-1}{r^2}k_i^2$, а при $m_i = \frac{2C_r^s - 2}{2C_r^s - 1}k_i$ получаем $\frac{2C_r^s - 2}{(2C_r^s - 1)^2}k_i^2$. Обозначим

$$c_1 = \min\left\{\frac{s}{2r}, \frac{2C_r^s - 2}{(2C_r^s - 1)^2}, \frac{r-1}{r^2}\right\}, \quad c_2 = \frac{(r-s)(r-1)}{r}.$$

Таким образом, справедливо неравенство

$$\rho(K_i) \geqslant c_1(r,s)k_i^2 - c_2(r,s)n^{r-s-2}k_i. \quad \blacktriangle$$

Лемма 2. *Справедливо неравенство*

$$\sum_{i=1}^{m} m_i \leqslant (C_r^s - 1)\ell + o(\ell).$$

Доказательство. Каждая вершина множества W_n содержит r элементов, а значит, входит в $x = C_r^s$ соответствующих K_i и не более чем в x соответствующих M_i. Оценим количество вершин, которые входят во все x множеств M_i, т.е. вместе с каждым множеством S_i содержат и элемент t_i, отвечающий ему. Пусть F – множество таких вершин.

Назовем множество A из $s+1$ элементов *самостоятельным*, если при выборе любого его s-элементного подмножества S_i будет выполнено условие $A \setminus S_i = \{t_i\}$. Заметим, что любое s-элементное множество может входить только в одно самостоятельное множество. Получаем, что два самостоятельных множества не могут пересекаться по s элементам. Назовем s-элементное множество *интересным*, если оно является подмножеством какого-то самостоятельного множества. Разобьем все вершины в F на две категории:

1) Вершины, у которых есть не интересное s-элементное подмножество;
2) Вершины, у которых все C_r^s s-элементных подмножеств являются интересными.

Докажем, что вершин первой категории не более n^{r-2}. Пусть вершина первой категории содержит не интересное множество $S_i = \{a_1, \ldots, a_s\}$. По определению F она обязательно содержит и элемент t_i. Множество элементов $a_1, \ldots, a_s, t_i$ не является самостоятельным, поэтому у него есть s-элементное подмножество S_j, такое что t_j не принадлежит ему. Снова заметим, что t_j также принадлежит выбранной вершине. Тогда вершин, содержащих $a_1, \ldots, a_s$, не больше, чем количество способов выбрать остальные $r - s - 2$ вершины, т.е. C_{n-s-2}^{r-s-2}. Учитывая, что всего способов выбрать изначальное не интересное s-элементное множество не более C_n^s, то всего вершин первой категории не более

$$C_n^s C_{n-s-2}^{r-s-2} < n^{r-2} = o(\ell).$$

Теперь оценим количество вершин второй категории. Посчитаем количество вершин второй категории, которые содержат фиксированное $S_i = \{b_1, \ldots, b_s\}$. По определению F такая вершина содержит элемент t_i, причем множество $\{b_1, \ldots, b_s, t_i\}$ – самостоятельное. Пусть вершина, помимо элементов $b_1, \ldots, b_s, t_i$, содержит еще элемент q. Обратим внимание на множество $S_j = \{b_1, \ldots, b_{s-1}, q\}$. Наша вершина обязательно должна содержать элемент t_j. Опять же множество $\{b_1, \ldots, b_{s-1}, q, t_j\}$ – самостоятельное, потому что наша вершина принадлежит второй категории. Заметим, что t_j не совпадает с b_s и t_i, иначе два самостоятельных множества имели бы s общих элементов. Получаем, что рассматриваемая вершина содержит элементы $b_1, \ldots, b_s$, q, t_i, t_j. Заметим, что при условии $r > 2s+1$ и $s > 1$ выполнено $r - s - 3 > s - 2 \geqslant 0$, а значит, наша вершина содержит еще хотя бы один элемент.

Получаем, что таких вершин не больше, чем количество способов выбрать элемент q (их точно меньше n), однозначно зафиксировать t_i и t_j и далее добавить $r-s-3$ из оставшихся $n-s-3$ элементов. Иными словами, вершин второй категории, содержащих S_i, не больше, чем nC_{n-s-3}^{r-s-3}. Учитывая, что всего число способов выбрать изначальное s-элементное множество равно C_n^s, то всего вершин второй категории не более

$$C_n^s n C_{n-s-3}^{r-s-3} < n^{r-2} = o(\ell).$$

Таким образом, мы доказали, что $|F| < 2n^{r-2}$.

Обозначим через $I(v \in M_i)$ индикатор попадания вершины v в множество M_i. Тогда

$$\sum_{i=1}^{m} m_i = \sum_{i=1}^{m} \sum_{v \in W_n} I(v \in M_i) = \sum_{v \in W_n} \sum_{i=1}^{m} I(v \in M_i) =$$
$$= \sum_{v \in F} \sum_{i=1}^{m} I(v \in M_i) + \sum_{v \in (W_n \setminus F)} \sum_{i=1}^{m} I(v \in M_i) \leqslant |F| C_r^s + (\ell - |F|)(C_r^s - 1) =$$
$$= (C_r^s - 1)\ell + |F| \leqslant (C_r^s - 1)\ell + o(\ell),$$

что завершает доказательство леммы 2. ▲

Лемма 3. *Справедливо неравенство*

$$\sum_{i \in A} k_i > \frac{1}{2}\ell - o(\ell).$$

Доказательство. Заметим, что

$$k_i < \frac{2C_r^s - 1}{2C_r^s - 2} m_i$$

для плохого элемента i. Тогда

$$\sum_{i \in B} k_i < \frac{2C_r^s - 1}{2C_r^s - 2} \sum_{i \in B} m_i,$$

а по лемме 2 имеем

$$\sum_{i \in B} m_i \leqslant \sum_{i=1}^{m} m_i < (C_r^s - 1)\,\ell + o(\ell).$$

Получаем

$$\sum_{i \in B} k_i < \frac{2C_r^s - 1}{2C_r^s - 2}\big((C_r^s - 1)\ell + o(\ell)\big) = \Big(C_r^s - \frac{1}{2}\Big)\ell + o(\ell).$$

Тогда для хороших элементов имеем

$$\sum_{i \in A} k_i = \sum_{i=1}^{m} k_i - \sum_{i \in B} k_i = C_r^s \ell - \sum_{i \in B} k_i > C_r^s \ell - \left(\Big(C_r^s - \frac{1}{2}\Big)\ell + o(\ell)\right) = \frac{1}{2}\ell - o(\ell),$$

что завершает доказательство леммы 3. ▲

Наконец, мы сможем оценить общее число ребер. Используя лемму 1, получаем

$$\rho(W_n) = \sum_{i=1}^{m} \rho(K_i) \geqslant \sum_{i \in A} \rho(K_i) \geqslant \sum_{i \in A} \bigl(c_1(r,s) k_i^2 - c_2(r,s) n^{r-s-2} k_i\bigr) \geqslant$$
$$\geqslant c_1(r,s) \sum_{i \in A} k_i^2 - c_2(r,s) n^{r-s-2} C_r^s \ell.$$

По неравенству о средних и лемме 3 получаем

$$\sum_{i \in A} k_i^2 \geqslant \frac{1}{|A|} \biggl(\sum_{i \in A} k_i \biggr)^2 \geqslant \frac{1}{C_n^s} \biggl(\sum_{i \in A} k_i \biggr)^2 \geqslant \frac{\Bigl(\frac{1}{2}\ell - o(\ell)\Bigr)^2}{n^s}.$$

Тогда

$$\rho(W_n) \geqslant c_1(r,s) \frac{\Bigl(\frac{1}{2}\ell - o(\ell)\Bigr)^2}{n^s} - c_2(r,s) n^{r-s-2} C_r^s \ell = \frac{c_1(r,s)}{4} \frac{\ell^2}{n^s} + o\biggl(\frac{\ell^2}{n^s}\biggr).$$

Положим $c(r,s) = \dfrac{c_1(r,s)}{4}$. Утверждение теоремы 3 доказано. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Frankl P., Wilson R.M.* Intersection Theorems with Geometric Consequences // Combinatorica. 1981. V. 1. № 4. P. 357–368. https://doi.org/10.1007/BF02579457
2. *Kahn J., Kalai G.* A Counterexample to Borsuk's Conjecture // Bull. Amer. Math. Soc. (N.S.). 1993. V. 29. № 1. P. 60–62. https://doi.org/10.1090/S0273-0979-1993-00398-7
3. *Raigorodskii A.M.* Cliques and Cycles in Distance Graphs and Graphs of Diameters // Discrete Geometry and Algebraic Combinatorics (AMS Special Session on Discrete Geometry and Algebraic Combinatorics. San Diego, CA, USA. Jan. 11, 2013). Contemp. Math. V. 625. Providence, RI: Amer. Math. Soc., 2014. P. 93–109.
4. *Boltyanski V., Martini H., Soltan P.S.* Excursions into Combinatorial Geometry. New York: Springer, 1997.
5. *Райгородский А.М.* Вокруг гипотезы Борсука // Геометрия и механика. Современная математика. Фундаментальные направления. Т. 23. М: РУДН, 2007. С. 147–164. http://mi.mathnet.ru/cmfd96
6. *Hinrichs A., Richter C.* New Sets with Large Borsuk Numbers // Discrete Math. 2003. V. 270. № 1–3. P. 137–147. https://doi.org/10.1016/S0012-365X(02)00833-6
7. *Balogh J., Cherkashin D., Kiselev S.* Coloring General Kneser Graphs and Hypergraphs via High-Discrepancy Hypergraphs // Europ. J. Combin. 2019. V. 79. P. 228–236. https://doi.org/10.1016/j.ejc.2019.03.004
8. *Бердников А.В., Райгородский А.М.* Оценки чисел Борсука по дистанционным графам специального вида // Пробл. передачи информ. 2021. Т. 57. № 2. С. 44–50. https://doi.org/10.31857/S0555292321020030
9. *Огарок П.А., Райгородский А.М.* Об устойчивости числа независимости некоторого дистанционного графа // Пробл. передачи информ. 2020. Т. 56. № 4. С. 50–63. https://doi.org/10.31857/S0555292320040051
10. *Balogh J., Krueger R.A., Luo H.* Sharp Threshold for the Erdős–Ko–Rado Theorem // Random Structures Algorithms. 2022. Early View Research Article. https://doi.org/10.1002/rsa.21090
11. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10 (97 pp.).

12. *Brouwer A.E., Cioabă S.M., Ihringer F., McGinnis M.* The Smallest Eigenvalues of Hamming Graphs, Johnson Graphs and Other Distance-Regular Graphs with Classical Parameters // J. Combin. Theory Ser. B. 2018. V. 133. P. 88–121. https://doi.org/10.1016/j.jctb.2018.04.005
13. *Lovász L.* On the Shannon Capacity of a Graph // IEEE Trans. Inform. Theory. 1979. V. 25. № 1. P. 1–7. https://doi.org/10.1109/TIT.1979.1055985
14. *Frankl P., Füredi Z.* Forbidding Just One Intersection // J. Combin. Theory Ser. A. 1985. V. 39. № 2. P. 160–176. https://doi.org/10.1016/0097-3165(85)90035-4
15. *Шубин Я.К.* О минимальном числе ребер в индуцированных подграфах специальных дистанционных графов // Матем. заметки. 2022. Т. 111. № 6. С. 929–939. https://doi.org/10.4213/mzm13370
16. *Пушняков Ф.А.* О числе ребер в индуцированных подграфах специальных дистанционных графов: Дисс. ... канд. физ.-мат. наук: 01.01.09. Москва: МФТИ, 2020.
17. *Михайлов К.А., Райгородский А.М.* О числах Рамсея для полных дистанционных графов с вершинами в $\{0,1\}^n$ // Матем. сб. 2009. Т. 200. № 12. С. 63–80. https://doi.org/10.4213/sm6373

Шубин Яков Константинович
Московский государственный университет
им. М.В. Ломоносова,
механико-математический факультет,
кафедра математической статистики
и случайных процессов
shubin.yakoff@gmail.com

Поступила в редакцию
18.10.2022
После доработки
04.11.2022
Принята к публикации
05.11.2022

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.12 : 519.719

© 2022 г. **О.В. Камловский, К.Н. Панков**

КЛАССЫ СБАЛАНСИРОВАННЫХ ФУНКЦИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ, ОБЛАДАЮЩИХ МАЛЫМ ЗНАЧЕНИЕМ ЛИНЕЙНОЙ ХАРАКТЕРИСТИКИ

Приводятся сбалансированные функции над конечными полями, обладающие малым значением линейной характеристики. Ранее линейные характеристики похожих классов функций исследовались лишь для случая поля из двух элементов.

Ключевые слова: сбалансированные функции, линейная характеристика функций, конечные поля, устойчивые функции.

DOI: 10.31857/S055529232204009X, **EDN:** NBPDHY

§ 1. Введение

Одной из важных прикладных математических задач является построение сбалансированных функций над конечными полями, достаточно удаленных от класса всех аффинных функций от заданного числа переменных. Данная проблема значительно проработана для случая булевых функций (см., например, [1–5]). Один из путей ее решения заключается в построении различных классов булевых бент-функций, которые наиболее удалены от всех аффинных функций, и последующем их усложнении с целью получения сбалансированных функций.

Аналогичные вопросы для функций над произвольными конечными полями решаются сложнее. В работе [6] были определены бент-функции над конечными полями. Позже в [7] были рассмотрены бент-функции над произвольными конечными абелевыми группами. В ней для измерения похожести функций использовалась функция “близость”, основанная на том, что две функции f и g наиболее непохожи друг на друга, если последовательность, состоящая из всех значений функции $f - g$ сбалансирована, т.е. в ней каждый элемент поля появляется с одинаковой частотой. В работах [8, 9] похожесть функций над полями характеристики два описывалась функцией “согласие”, отличавшейся от функции “близость” только нормирующим множителем. В работе [10] в качестве меры приближения функции классом всех аффинных функций над конечным полем была определена линейная характеристика функции. Данная характеристика функции тесно связана с понятием корреляции между функциями и последовательностями.

Основными результатами работы являются широкие классы сбалансированных функций над конечными полями, для которых указаны оценки значений линейной характеристики. С целью понимания основных результатов статьи приводятся уже известные результаты в удобных для нас обозначениях.

§ 2. Линейная характеристика функций

Пусть $P = GF(q)$ – произвольное конечное поле из q элементов, $q = p^t$, где p – простое число, а t – натуральное. В данной работе обозначение P всегда будет подразумевать выбор такого поля.

Рассмотрим функцию $f\colon P^n \to P$ от n переменных, заданную на поле P. Будем использовать обозначение $f = f(x_1, \ldots, x_n) = f(\vec{x})$, где $\vec{x} = (x_1, \ldots, x_n)$. Назовем функцию f сбалансированной, если для всех $a \in P$ мощность полного прообраза элемента a при действии отображения f удовлетворяет условию $|f^{-1}(a)| = q^{n-1}$.

Группа всех аддитивных характеров поля P (гомоморфизмов группы $(P, +)$ в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел) состоит из гомоморфизмов (см., например, [11])

$$\chi_a(x) = e^{2\pi i \frac{\mathrm{Tr}_{P_0}^P(ax)}{p}} = \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(ax)}{p}\right\}, \quad x \in P, \tag{1}$$

где $a \in P$, $P_0 = GF(p)$, $\mathrm{Tr}_{P_0}^P$ – функция следа из поля P в простое подполе P_0. Характер χ_0 называют тривиальным характером.

Коэффициентом кросс-корреляции между функциями $f(\vec{x})$ и $g(\vec{x})$, соответствующим характеру χ_a, называют комплексное число

$$C_a(f, g) = \sum_{x_1, \ldots, x_n \in P} \chi_a(f(\vec{x}) - g(\vec{x})). \tag{2}$$

Модуль коэффициента $C_a(f, g)$ характеризует близость между функциями $f(\vec{x})$ и $g(\vec{x})$ (см. [12]).

Обозначим через $A_n(P)$ множество всех аффинных функций $g(\vec{x})$ от n переменных над полем P, т.е. функций вида

$$g(\vec{x}) = a_0 + a_1 x_1 + \ldots + a_n x_n,$$

где $a_0, a_1, \ldots, a_n \in P$. Для линейной функции $g_0(\vec{x})$ от n переменных над полем P будем использовать обозначение

$$g_0(\vec{x}) = a_1 x_1 + \ldots + a_n x_n = \langle \vec{a}, \vec{x} \rangle,$$

где $\vec{a} = (a_1, \ldots, a_n)$, $\vec{x} = (x_1, \ldots, x_n)$.

Мультипликативную группу поля P обозначим через P^*. Линейной характеристикой функции f назовем число

$$C(f) = \max_{a \in P^*} \max_{g \in A_n(P)} |C_a(f, g)|. \tag{3}$$

Предложение 1. *Справедливо равенство*

$$C(f) = \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} \left| \sum_{x_1, \ldots, x_n \in P} \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(af(\vec{x}) - a_1 x_1 - \ldots - a_n x_n)}{p}\right\} \right|.$$

Доказательство. Заметим, что $C_a(f, a_0 + \langle \vec{a}, \vec{x} \rangle) = \chi_a(-a_0) C_a(f, \langle \vec{a}, \vec{x} \rangle)$, и так как $|\chi_a(-a_0)| = 1$, то согласно равенствам (1), (2)

$$C(f) = \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} |C_a(f, \langle \vec{a}, \vec{x} \rangle)| =$$

$$= \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} \left| \sum_{x_1, \ldots, x_n \in P} \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(af(\vec{x}) - aa_1 x_1 - \ldots - aa_n x_n)}{p}\right\} \right|.$$

Отсюда получаем

$$C(f) = \max_{a\in P^*} \max_{a_1,\ldots,a_n\in P} \left| \sum_{x_1,\ldots,x_n\in P} \exp\left\{ 2\pi i \frac{\mathrm{Tr}_{P_0}^{P}(af(\vec{x}) - a_1x_1 - \ldots - a_nx_n)}{p} \right\} \right|. \quad \blacktriangle$$

Рассмотрим, как ведет себя параметр $C(f)$ в частном случае $P = GF(2) = \{0, e\}$. В этой ситуации

$$\exp\left\{ 2\pi i \frac{\mathrm{Tr}_{P_0}^{P}(af(\vec{x}) - a_1x_1 - \ldots - a_nx_n)}{p} \right\} = (-1)^{f(\vec{x})\oplus a_1x_1\oplus\ldots\oplus a_nx_n},$$

коэффициент кросс-корреляции $C_e(f, \langle\vec{a}, \vec{x}\rangle)$ равен коэффициенту Уолша – Адамара

$$W_f(\vec{a}) = \sum_{x_1,\ldots,x_n\in P} (-1)^{f(\vec{x})\oplus a_1x_1\oplus\ldots\oplus a_nx_n}$$

булевой функции f, и справедливо равенство

$$C(f) = \max_{\vec{a}\in P^n} |W_f(\vec{a})|.$$

Отметим, что в двоичном случае наиболее удобной для использования является нелинейность $\mathrm{nl}(f)$ булевой функции f, которая равна расстоянию Хэмминга между столбцом значений функции f и столбцами значений всех аффинных двоичных функций от n переменных. Известно (см., например, [4]), что

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\vec{a}\in P^n} |W_f(\vec{a})| = 2^{n-1} - \frac{1}{2}C(f).$$

В случае произвольного конечного поля P понятие нелинейности функции, основанное на расстоянии Хэмминга, используется в работе [13].

Пусть

$$f\colon P^n \to P, \quad g(\vec{x}) = a_0 + a_1x_1 + \ldots + a_nx_n, \quad b \in P.$$

Обозначим через $N(f, g, b)$ число всех векторов $\vec{x} \in P^n$, таких что $f(\vec{x}) - g(\vec{x}) = b$.

Предложение 2. *Справедлива оценка*

$$\left|N(f, g, b) - q^{n-1}\right| \leqslant \frac{q-1}{q}C(f),$$

где $C(f)$ – линейная характеристика функции f.

Доказательство. Согласно [11]

$$\frac{1}{q}\sum_{a\in P} \chi_a(x) = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0, \end{cases} \tag{4}$$

где χ_a – характер, определенный равенством (1). Используя это соотношение, получаем

$$N(f, g, b) = \frac{1}{q}\sum_{\vec{x}\in P^n}\sum_{a\in P} \chi_a(f(\vec{x}) - g(\vec{x}) - b).$$

Учитывая, что $\chi_0(z) = 1$ для всех $z \in P$, и выделяя отдельно слагаемое, соответствующее случаю $a = 0$, имеем

$$N(f,g,b) - q^{n-1} = \frac{1}{q} \sum_{a \in P^*} \chi_a(-b) \sum_{\vec{x} \in P^n} \chi_a(f(\vec{x}) - g(\vec{x})).$$

Тогда

$$\left|N(f,g,b) - q^{n-1}\right| \leqslant \frac{1}{q} \sum_{a \in P^*} |C_a(f,g)| \leqslant \frac{q-1}{q} C(f). \quad \blacktriangle$$

Функцию $f\colon P^n \to P$ назовем бент-функцией (см. [6, 7]), если $|C_a(f,g)| = q^{n/2}$ для всех $a \in P^*$ и всех $g \in A_n(P)$. Приведем определение бент-функции в терминах линейной характеристики. Непосредственно из результатов работ [6, 7, 9] вытекает следующий результат.

Предложение 3. *Для каждой функции $f\colon P^n \to P$ верна оценка*

$$C(f) \geqslant q^{\frac{n}{2}},$$

которая обращается в равенство тогда и только тогда, когда f является бент-функцией.

§ 3. Некоторые известные результаты

Приведем известные факты, относящиеся к теории функций, заданных на конечных полях. Они понадобятся в дальнейшем для доказательства основных результатов. При этом будем использовать удобные для нас обозначения.

Пусть $n = 2k$, π – подстановка на множестве P^k с координатными функциями $\pi_1, \ldots, \pi_k$, а $h\colon P^k \to P$ – произвольная функция. Для всех $\vec{x}, \vec{y} \in P^k$ определим функцию $f\colon P^n \to P$ равенством

$$f(\vec{x}, \vec{y}) = \langle \pi(\vec{x}), \vec{y} \rangle + h(\vec{x}) = \pi_1(\vec{x}) y_1 + \ldots + \pi_k(\vec{x}) y_k + h(\vec{x}). \tag{5}$$

Такие функции для поля из двух элементов были впервые рассмотрены в статье [14]. Приведем теорему, вытекающую из результатов работы [15].

Теорема 1. *Функция f, определенная равенством* (5), *является бент-функцией, причем для всех $a \in P^*$ и линейных функций $g(\vec{x}, \vec{y}) = \langle (\vec{a}, \vec{b}), (\vec{x}, \vec{y}) \rangle$ верно равенство*

$$C_a(f,g) = q^k \chi_a\big(h(\pi^{-1}(\vec{b})) - \langle \vec{a}, \pi^{-1}(\vec{b}) \rangle\big).$$

Указанное множество бент-функций называется классом Майораны – Макфарланда. Ранее в случае, когда q – простое число, теорема 1 была доказана в работах [16, 17]. Бент-функция $f\colon P^n \to P$ называется регулярной [17], если для всех $a \in P^*$ и $g \in A_n(P)$ выполнено равенство $C_a(f,g) = q^{n/2} e^{2\pi i k(a,g)/p}$, где $0 \leqslant k(a,g) \leqslant p-1$. Функции из класса Майораны – Макфарланда являются регулярными.

Приведем критерий Г. Вейля [18] сбалансированности последовательности элементов поля в удобной для дальнейшего изложения форме. Назовем последовательность $c_0, \ldots, c_{t-1}$ элементов поля P сбалансированной, если в ней каждый элемент поля P появляется одинаковое число раз. В частности, отсюда будет следовать, что t делится на q.

Предложение 4 [18]. *Последовательность $c_0, \ldots, c_{t-1}$ сбалансирована тогда и только тогда, когда для всех $a \in P^*$*

$$\sum_{i=0}^{t-1} \chi_a(c_i) = 0.$$

Укажем критерий сбалансированности функции $f\colon P^n \to P$ в терминах коэффициентов кросс-корреляции. Функция f сбалансирована тогда и только тогда, когда сбалансирована последовательность $f(x_1, \ldots, x_n)$, $x_1, \ldots, x_n \in P$, всех ее значений. Согласно предложению 4 это равносильно условию

$$\sum_{x_1,\ldots,x_n \in P} \chi_a(f(x_1, \ldots, x_n)) = C_a(f, 0) = 0$$

для всех $a \in P^*$. Таким образом, справедлив следующий факт.

Следствие 1. *Функция f является сбалансированной тогда и только тогда, когда $C_a(f, 0) = 0$ для всех $a \in P^*$.*

Пусть $k \in \mathbb{N}$, $f\colon P^n \to P$. Для любых элементов $a_1, \ldots, a_k \in P$ и различных натуральных чисел $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$ обозначим через $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ функцию, полученную из $f(x_1, \ldots, x_n)$ фиксацией переменных $x_{i_1}, \ldots, x_{i_k}$ значениями $a_1, \ldots, a_k$ соответственно. Назовем функцию f корреляционно-иммунной порядка k [19], если для всех $a_1, \ldots, a_k \in P$, $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$, таких что $1 \leqslant i_1 < \ldots < i_k \leqslant n$, и всех $z \in P$ для прообразов элемента z при действии отображений $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ и f верны равенства

$$\left| \left(f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}\right)^{-1}(z) \right| = \frac{|f^{-1}(z)|}{q^k}. \tag{6}$$

Данное определение обобщает на случай произвольного поля P понятие корреляционно-иммунной булевой функции порядка k (см., например, [4]). Корреляционно-иммунную функцию f порядка k, являющуюся сбалансированной, называют еще k-устойчивой, или k-эластичной функцией. Отметим, что наряду с известными применениями в области защиты информации для симметричных криптосистем, k-устойчивые функции как частный случай k-устойчивых отображений (см. [20]) используются в задачах построения протоколов квантового распределения ключей (см., например, [21]).

Несложно заметить, что если функция является корреляционно-иммунной порядка k, то она является корреляционно-иммунной порядка $k-1$. Кроме того, если функция f является 1-устойчивой, то f сбалансирована. Поэтому сбалансированные функции считают 0-устойчивыми. Обозначим через $\|\vec{a}\|$ число ненулевых координат вектора $\vec{a}$. Для корреляционно-иммунных функций f порядка k справедлив аналог теоремы, доказанной ранее для случая $q = 2$ в работе [22].

Теорема 2 [19]. *Функция $f\colon P^n \to P$ является корреляционно-иммунной порядка k тогда и только тогда, когда для каждого $\vec{a} \in P^n$, такого что $1 \leqslant \|\vec{a}\| \leqslant k$, при всех $a \in P^*$ имеет место равенство $C_a(f, (\vec{a}, \vec{x})) = 0$.*

С использованием критерия сбалансированности функции непосредственно из теоремы 2 получим критерий k-устойчивости функции.

Следствие 2 [19]. *Функция $f\colon P^n \to P$ является k-устойчивой тогда и только тогда, когда для каждого $\vec{a} \in P^n$, такого что $0 \leqslant \|\vec{a}\| \leqslant k$, при всех $a \in P^*$ имеет место равенство $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$.*

Пусть $g_1, \ldots, g_{n+1}$ – произвольные подстановки поля P,

$f(x_1, \ldots, x_n) = g_{n+1}(g_1(x_1) + \ldots + g_n(x_n))$.

Для всех $\{i_1, \ldots, i_{n-1}\} \subset \{1, \ldots, n\}$, $a_1, \ldots, a_{n-1} \in P$, $z \in P$ справедливо равенство

$$\left| \left(f_{i_1,\ldots,i_{n-1}}^{a_1,\ldots,a_{n-1}} \right)^{-1} (z) \right| = 1,$$

так как если $\{j\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_{n-1}\}$, то

$f_{i_1,\ldots,i_{n-1}}^{a_1,\ldots,a_{n-1}}(x_j) = g_{n+1}(g_j(x_j) + c)$,

где $c \in P$ – некоторая константа. Таким образом, f является $(n-1)$-устойчивой функцией, и класс k-устойчивых функций непуст при каждом $k < n$.

Остается актуальной задача нахождения числа k-устойчивых функций над конечным полем. В настоящее время получены только асимптотические (см., например, [23]) и рекуррентные (см. [24]) оценки для случаев булевых функций и отображений.

Пусть e – единица поля P. Функция $f\colon P^n \to P$ задается многочленом

$$f(x_1, \ldots, x_n) = \sum_{a_1,\ldots,a_n \in P} f(a_1, \ldots, a_n)\big(e - (x_1 - a_1)^{q-1}\big) \ldots \big(e - (x_n - a_n)^{q-1}\big)$$

(см. [11, 25]), который после раскрытия скобок принимает вид

$$f(x_1, \ldots, x_n) = \sum_{i_1=0}^{q-1} \ldots \sum_{i_n=0}^{q-1} c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

где $c_{i_1 \ldots i_n} \in P$. Среди всех многочленов от n переменных, имеющих степень по каждой переменной не выше $q-1$, многочлен, задающий функцию f, будет единственным. Степень монома $c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ определяется по правилу

$$\deg c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \begin{cases} i_1 + \ldots + i_n, & \text{если } c_{i_1 \ldots i_n} \neq 0, \\ -\infty, & \text{если } c_{i_1 \ldots i_n} = 0. \end{cases}$$

Степень функции f (см., например, [26]) определяется равенством

$$\deg f = \max\big\{\deg c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} : 0 \leqslant i_1 \leqslant q-1, \ldots, 0 \leqslant i_n \leqslant q-1\big\}.$$

Каждое число $j \in \{0, 1, \ldots, q-1\}$ запишем в p-ичном представлении:

$j = j_0 + pj_1 + \ldots + p^{t-1} j_{t-1}$,

где $j_0, j_1, \ldots, j_{t-1} \in \{0, 1, \ldots, p-1\}$. В этом случае число

$\|j\|_p = j_0 + j_1 + \ldots + j_{t-1}$

назовем p-ичным весом числа j. Степенью нелинейности монома $c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ назовем величину

$$\mathrm{dl}\, c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \begin{cases} \|i_1\|_p + \ldots + \|i_n\|_p, & \text{если } c_{i_1 \ldots i_n} \neq 0, \\ -\infty, & \text{если } c_{i_1 \ldots i_n} = 0. \end{cases}$$

Степень нелинейности функции f (см., например, [26]) определяется равенством

$$\mathrm{dl}\, f = \max\big\{\mathrm{dl}\, c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} : 0 \leqslant i_1 \leqslant q-1, \ldots, 0 \leqslant i_n \leqslant q-1\big\}.$$

Согласно результатам работы [19], если f – сбалансированная функция, то

$\deg f \leqslant n(q-1)-1, \quad \mathrm{dl}\, f \leqslant nt(p-1)-1.$

§ 4. Конструкция разветвления функций

Пусть $P = \{r_1, \ldots, r_q\}$, и пусть $f_{r_i} \colon P^{n-1} \to P$, $i = 1, \ldots, q$, – функции от $n-1$ переменных. Зададим функцию $f \colon P^n \to P$ по правилу

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} f_{r_1}(x_2, \ldots, x_n), & \text{если } x_1 = r_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ f_{r_q}(x_2, \ldots, x_n), & \text{если } x_1 = r_q. \end{cases} \tag{7}$$

Функцию f будем называть разветвлением функций $f_{r_1}, \ldots, f_{r_q}$.

Теорема 3. *Пусть функция f построена по правилу* (7). *Тогда*:

1) *Функция f сбалансирована тогда и только тогда, когда для всех $a \in P^*$*

$$C_a(f_{r_1}, 0) + \ldots + C_a(f_{r_q}, 0) = 0;$$

2) *Если функции $f_{r_1}, \ldots, f_{r_q}$ являются корреляционно-иммунными порядка k и для всех $a \in P^*$ выполнено*

$$C_a(f_{r_1}, 0) = \ldots = C_a(f_{r_q}, 0),$$

то функция f является корреляционно-иммунной порядка k;

3) *Если функции $f_{r_1}, \ldots, f_{r_q}$ являются k-устойчивыми, то функция f является k-устойчивой*;

4) *Линейные характеристики функций связаны соотношением*

$$C(f) \leqslant C(f_{r_1}) + \ldots + C(f_{r_q});$$

5) $\deg f \leqslant q - 1 + \max\{\deg f_{r_i} : i = 1, \ldots, q\}$;

6) $\mathrm{dl}\, f \leqslant (p-1)t + \max\{\mathrm{dl}\, f_{r_i} : i = 1, \ldots, q\}$.

Доказательство. Рассмотрим символ Кронекера

$$\delta_{x,a} = \begin{cases} e, & \text{если } x = a, \\ 0, & \text{если } x \neq a, \end{cases}$$

определенный для всех $x, a \in P$, где e – единица поля P. Тогда

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{q} \delta_{x_1, r_i} f_{r_i}(x_2, \ldots, x_n).$$

Для всех $a \in P^*$ рассмотрим

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{x_1, \ldots, x_n \in P} \chi_a\big(f(x_1, \ldots, x_n) - a_1 x_1 - \ldots - a_n x_n\big) =$$

$$= \sum_{i=1}^{q} \sum_{x_2, \ldots, x_n \in P} \chi_a\big(f_{r_i}(x_2, \ldots, x_n) - a_1 r_i - a_2 x_2 - \ldots - a_n x_n\big) =$$

$$= \sum_{i=1}^{q} \chi_a(-a_1 r_i) \sum_{x_2, \ldots, x_n \in P} \chi_a\big(f_{r_i}(x_2, \ldots, x_n) - a_2 x_2 - \ldots - a_n x_n\big).$$

Получаем

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{i=1}^{q} \chi_a(-a_1 r_i) C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n). \tag{8}$$

Утверждение 1) следует из равенства

$$C_a(f, 0) = C_a(f_{r_1}, 0) + \ldots + C_a(f_{r_q}, 0)$$

и следствия 1.

Докажем утверждение 2). Согласно теореме 2 достаточно доказать, что для всех $a \in P^*$ и $\vec{a} = (a_1, \ldots, a_n) \in P^n$, таких что $1 \leqslant \|\vec{a}\| \leqslant k$, выполнено $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Если $a_1 = 0$, то $1 \leqslant \|(a_2, \ldots, a_n)\| \leqslant k$, и по теореме 2

$$C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n) = 0, \quad i = 1, \ldots, q.$$

Значит, $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Если $a_1 \neq 0$ и $1 \leqslant \|(a_2, \ldots, a_n)\| \leqslant k - 1$, то по теореме 2

$$C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n) = 0, \quad i = 1, \ldots, q,$$

и $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Осталось рассмотреть случай, когда $a_1 \neq 0$ и $(a_2, \ldots, a_n) = \vec{0}$. В этом случае согласно (8)

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{i=1}^{q} \chi_a(-a_1 r_i) C_a(f_{r_i}, 0).$$

Так как $C_a(f_{r_1}, 0) = \ldots = C_a(f_{r_q}, 0)$, то

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = C_a(f_{r_1}, 0) \sum_{i=1}^{q} \chi_a(-a_1 r_i).$$

Из соотношений (4) следует, что

$$\sum_{i=1}^{q} \chi_a(-a_1 r_i) = 0,$$

поэтому $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$.

Утверждение 3) непосредственно следует из утверждений 1), 2) и следствий 1, 2.

Утверждение 4) вытекает из соотношений

$$|C_a(f, \langle \vec{a}, \vec{x} \rangle)| \leqslant \sum_{i=1}^{q} |\chi_a(-a_1 r_i) C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n)| =$$
$$= \sum_{i=1}^{q} |C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n)| \leqslant \sum_{i=1}^{q} C(f_{r_i}),$$

справедливых для всех $a \in P^*$ и $\vec{a} \in P^n$.

Используя интерполяционную формулу Лагранжа, получим

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{q} \delta_{x_1, r_i} f_{r_i}(x_2, \ldots, x_n) =$$
$$= \sum_{i=1}^{q} \frac{(x_1 - r_1) \ldots (x_1 - r_{i-1})(x_1 - r_{i+1}) \ldots (x_1 - r_q)}{(r_i - r_1) \ldots (r_i - r_{i-1})(r_i - r_{i+1}) \ldots (r_i - r_q)} f_{r_i}(x_2, \ldots, x_n).$$

Непосредственно из этого равенства следуют утверждения 5) и 6). ▲

Впервые аналогичная конструкция для булевых функций была рассмотрена в работе [27], где были доказаны аналоги утверждений 2) и 3) теоремы 3.

В случае $f_{r_1} = \ldots = f_{r_q}$ функция f, построенная по правилу (7), удовлетворяет равенству $f(x_1, \ldots, x_n) = f_{r_1}(x_2, \ldots, x_n)$. Если $r_1 = 0$, $f_{r_2} = \ldots = f_{r_q} = f_1$, $f_0 \neq f_1$, то

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} f_0(x_2, \ldots, x_n), & \text{если } x_1 = 0, \\ f_1(x_2, \ldots, x_n), & \text{если } x_1 \neq 0, \end{cases}$$

и функция f будет задаваться формулой

$$f(x_1, x_2, \ldots, x_n) = x_1^{q-1} f_1(x_2, \ldots, x_n) + (e - x_1^{q-1}) f_0(x_2, \ldots, x_n).$$

Рассмотрим теперь важную с практической точки зрения конструкцию разветвления бент-функций. Пусть $n = 2k$, $\vec{x}, \vec{y} \in P^k$, $f_{r_i}(\vec{x}, \vec{y}) = \langle \pi_i(\vec{x}), \vec{y} \rangle + h_i(\vec{y})$ – бент-функция из класса Майораны – Макфарланда, где $i = 1, \ldots, q$. Рассмотрим функцию

$$f(x, \vec{x}, \vec{y}) = \sum_{i=1}^{q} \delta_{x, r_i} f_{r_i}(\vec{x}, \vec{y}), \quad x \in P, \tag{9}$$

построенную по правилу (7) из функций $f_{r_1}, \ldots, f_{r_q}$.

Теорема 4. *Пусть функция f построена по правилу* (9). *Тогда*:

1) *Функция f сбалансирована тогда и только тогда, когда все элементы*

$$h_1(\pi_1^{-1}(\vec{0})), \ldots, h_q(\pi_q^{-1}(\vec{0}))$$

попарно различны;

2) *Линейная характеристика функции f удовлетворяет неравенству*

$$C(f) \leqslant q^{\frac{n}{2}+1}.$$

Доказательство. Докажем утверждение 1). Согласно теореме 1 для всех $a \in P^*$ выполнено

$$C_a(f_{r_i}, 0) = q^k \chi_a(h_i(\pi_i^{-1}(\vec{0}))), \quad i = 1, \ldots, q.$$

По теореме 3 и следствию 1 функция f сбалансирована тогда и только тогда, когда

$$C_a(f, 0) = \sum_{i=1}^{q} C_a(f_{r_i}, 0) = q^k \sum_{i=1}^{q} \chi_a(h_i(\pi_i^{-1}(\vec{0}))) = 0$$

для всех $a \in P^*$. Из предложения 4 следует, что это равносильно сбалансированности последовательности $h_1(\pi_1^{-1}(\vec{0})), \ldots, h_q(\pi_q^{-1}(\vec{0}))$.

Утверждение 2) непосредственно следует из теоремы 3 и равенств

$$C(f_{r_i}) = q^{n/2}, \quad i = 1, \ldots, q. \quad ▲$$

§ 5. Конструкция Майораны – Макфарланда

Применим конструкцию Майораны – Макфарланда для построения сбалансированных функций. Пусть $n = 2k$, и пусть φ – линейное преобразование на множестве P^k с координатными функциями $\varphi_1, \ldots, \varphi_k$, определенное по правилу

$$\varphi(\vec{x}) = \vec{x} M,$$

где $M = (m_{ij})_{k\times k}$ – матрица размера $k \times k$ над полем P, имеющая ранг $k-1$. Для произвольной функции $h\colon P^k \to P$ и всех $\vec{x}, \vec{y} \in P^k$ определим функцию $f\colon P^n \to P$ равенством

$$f(\vec{x},\vec{y}) = \langle\varphi(\vec{x}),\vec{y}\rangle + h(\vec{x}) = \varphi_1(\vec{x})y_1 + \ldots + \varphi_k(\vec{x})y_k + h(\vec{x}). \tag{10}$$

Множество $\varphi^{-1}(\vec{0})$ является линейным пространством размерности 1, порожденным некоторым ненулевым вектором $\vec{c} \in P^n$, т.е.

$$\varphi^{-1}(\vec{0}) = \{r\vec{c}\colon\ r \in P\}.$$

Отметим, что в классической конструкции Майораны – Макфарланда в качестве отображения φ берется произвольная подстановка на множестве P^k. В этом случае функция f, задаваемая равенством (10), является бент-функцией.

Т е о р е м а 5. *Пусть функция f определена равенством* (10). *Тогда*:

1) *f – сбалансированная функция тогда и только тогда, когда $h(a\vec{c}) \neq h(b\vec{c})$ для всех различных $a, b \in P$;*
2) *Если* $\deg h \geqslant 3$, *то* $\deg f = \deg h$;
3) *Если* $\mathrm{dl}\, h \geqslant 3$, *то* $\mathrm{dl}\, f = \mathrm{dl}\, h$;
4) $C(f) \leqslant q^{\frac{n}{2}+1}$.

Д о к а з а т е л ь с т в о. Обозначим через L линейное пространство, порожденное системой всех строк матрицы M. Тогда, если $\vec{b} \notin L$, то $\varphi^{-1}(\vec{b}) = \varnothing$, а если $\vec{b} \in L$, то

$$\varphi^{-1}(\vec{b}) = \vec{d} + \varphi^{-1}(\vec{0}), \tag{11}$$

где $\vec{d}$ – фиксированный вектор, такой что $\vec{d}M = \vec{b}$. Рассмотрим для всех $\vec{a}, \vec{b} \in P^k$ и $a \in P^*$ коэффициент кросс-корреляции

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = \sum_{\vec{x}\in P^k} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) \sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}),\vec{y}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \sum_{\vec{x}\in P^k} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) \sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}) - \vec{b},\vec{y}\rangle).$$

Заметим, что

$$\sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}) - \vec{b},\vec{y}\rangle) = \begin{cases} q^k, & \text{если } \varphi(\vec{x}) = \vec{b}, \\ 0, & \text{если } \varphi(\vec{x}) \neq \vec{b}, \end{cases}$$

поэтому если $\vec{b} \notin L$, то $C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = 0$, а если $\vec{b} \in L$, то

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = q^k \sum_{\vec{x}\in\varphi^{-1}(\vec{b})} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) =$$

$$= q^k \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a},\vec{d} + r\vec{c}\rangle) =$$

$$= q^k \chi_a(-\langle\vec{a},\vec{d}\rangle) \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a}, r\vec{c}\rangle).$$

В частности,

$$|C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)| = q^k \left| \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a}, r\vec{c}\rangle) \right|. \tag{12}$$

Докажем утверждение 1). Согласно следствию 1 функция f сбалансирована тогда и только тогда, когда $C_a(f,0)=0$ для всех $a\in P^*$. Из равенства (11) следует, что при $\vec{a}=\vec{b}=\vec{0}$ выполнено $\vec{d}=\vec{0}$, поэтому с использованием равенства (12) получим, что $C_a(f,0)=0$ для всех $a\in P^*$ тогда и только тогда, когда

$$\sum_{r\in P}\chi_a(h(\vec{0}+r\vec{c}))=0,$$

для всех $a\in P^*$. Согласно предложению 4 полученные соотношения равносильны сбалансированности последовательности, составленной из элементов $h(r\vec{c})$, $r\in P$, т.е. условию $h(a\vec{c})\neq h(b\vec{c})$ для всех различных $a,b\in P$.

Докажем утверждения 2) и 3). Имеем равенство

$$f(\vec{x},\vec{y})=y_1\vec{x}M_1^{\downarrow}+\ldots+y_k\vec{x}M_k^{\downarrow}+h(\vec{x})=\sum_{i,j=1}^{k}m_{ij}x_iy_j+h(\vec{x}),$$

из которого получаем

$$\deg f=\begin{cases}2, & \text{если } \deg h\leqslant 2,\\ \deg h, & \text{если } \deg h\geqslant 3,\end{cases}$$

$$\mathrm{dl}\, f=\begin{cases}2, & \text{если } \mathrm{dl}\, h\leqslant 2,\\ \mathrm{dl}\, h, & \text{если } \mathrm{dl}\, h\geqslant 3.\end{cases}$$

Утверждение 4) непосредственно следует из равенства (12). ▲

§ 6. Аналог конструкции Доббертина

Пусть $n=2k$, $\vec{x},\vec{y}\in P^k$, $h(\vec{x},\vec{y})$ – бент-функция над полем P от n переменных. По аналогии с работой [1] назовем бент-функцию h нормальной, если существует линейное многообразие $M=\vec{\alpha}+L$, где $\vec{\alpha}\in P^n$, а L – линейное пространство размерности k над полем P, такое что ограничение h на множество M является константой. Пусть эта константа равна c. Отметим, что бент-функции из класса Майораны – Макфарланда являются нормальными. Пример булевой бент-функции, не являющейся нормальной, был построен нетривиальным методом в работе [28].

Для построения сбалансированных функций используем нормальную бент-функцию. Рассмотрим $L_0=\{(\vec{0},\vec{y}):\ \vec{y}\in P^k\}$. Выберем обратимое линейное преобразование $\tau\colon P^n\to P^n$, такое что $\tau(L)=L_0$. Рассмотрим бент-функцию

$$\varphi(\vec{x},\vec{y})=h(\tau^{-1}(\vec{x},\vec{y})).$$

Ясно, что

$$\varphi(\tau(\vec{\alpha})+L_0)=h(\tau^{-1}(\tau(\vec{\alpha})+L_0))=h(\alpha+L)=c.$$

Пусть $\tau(\vec{\alpha})=(\vec{x}_0,\vec{y}_0)$, тогда $\tau(\vec{\alpha})+L_0=(\vec{x}_0,\vec{0})+L_0$ и $\varphi((\vec{x}_0,\vec{0})+L_0)=c$. Выберем произвольную функцию $g\colon P^k\to P$ и построим функцию $f(\vec{x},\vec{y})$ по правилу

$$f(\vec{x},\vec{y})=\begin{cases}g(\vec{y}), & \text{если } \vec{x}=\vec{x}_0,\\ \varphi(\vec{x},\vec{y}), & \text{если } \vec{x}\neq\vec{x}_0.\end{cases}\tag{13}$$

Впервые эта конструкция для булевых функций (при $q=2$) и в более частном виде, когда $c=0$, $\vec{x}_0=\vec{0}$, была предложена Г. Доббертином в работе [1]. Следующая теорема обобщает результаты этой работы на случай произвольного поля из q элементов.

Теорема 6. *Пусть функция f определена равенством* (13). *Тогда*:

1) *f – сбалансированная функция тогда и только тогда, когда g – сбалансированная функция*;
2) $C(f) \leqslant q^{\frac{n}{2}} + C(g)$;
3) *Если* $\deg\varphi \leqslant (q-1)n/2$ *и* $g(\vec{y}) \neq \text{const}$, *то* $\deg f = (q-1)n/2 + \deg g$;
4) *Если* $\operatorname{dl}\varphi \leqslant t(p-1)n/2$ *и* $g(\vec{y}) \neq \text{const}$, *то* $\operatorname{dl} f = t(p-1)n/2 + \operatorname{dl} g$.

Доказательство. Найдем для всех $a \in P^*$ и $\vec{a}, \vec{b} \in P^k$ коэффициент кросс-корреляции:

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = \sum_{\vec{x},\vec{y}\in P^k} \chi_a(f(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \sum_{\vec{y}\in P^k} \chi_a(g(\vec{y}) - \langle\vec{a},\vec{x}_0\rangle - \langle\vec{b},\vec{y}\rangle) + \sum_{\substack{\vec{x},\vec{y}\in P^k \\ \vec{x}\neq\vec{x}_0}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \chi_a(-\langle\vec{a},\vec{x}_0\rangle) C_a(g, \langle\vec{b},\vec{y}\rangle) + S(\vec{a},\vec{b}).$$

Вычислим величину

$$S(\vec{a},\vec{b}) = \sum_{\substack{\vec{x}\neq\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle).$$

Для этого изучим

$$\sum_{\substack{\vec{x}=\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) = \sum_{\vec{y}\in P^k} \chi_a(c - \langle\vec{a},\vec{x}_0\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) \sum_{\vec{y}\in P^k} \chi_a(-\langle\vec{b},\vec{y}\rangle).$$

Так как

$$\sum_{\vec{y}\in P^k} \chi_a(-\langle\vec{b},\vec{y}\rangle) = \begin{cases} 0, & \text{если } \vec{b} \neq \vec{0}, \\ q^k, & \text{если } \vec{b} = \vec{0}, \end{cases}$$

что равно $q^k\delta_{\vec{b},\vec{0}}$, то

$$\sum_{\substack{\vec{x}=\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) = \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) q^k \delta_{\vec{b},\vec{0}}.$$

Следовательно,

$$S(\vec{a},\vec{b}) + \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) q^k \delta_{\vec{b},\vec{0}} = C_a(\varphi, \langle\vec{a},\vec{x}\rangle + \langle\vec{b},\vec{y}\rangle),$$

и справедливо равенство

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) =$$
$$= \chi_a(-\langle\vec{a},\vec{x}_0\rangle) \left(C_a(g, \langle\vec{b},\vec{y}\rangle) + \chi_a(\langle\vec{a},\vec{x}_0\rangle) C_a(\varphi, \langle\vec{a},\vec{x}\rangle + \langle\vec{b},\vec{y}\rangle) - \chi_a(c) q^k \delta_{\vec{b},\vec{0}} \right).$$

Рассмотрим величину

$$\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)=$$
$$=\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0\rangle)\sum_{\vec{x},\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{a},\vec{x}\rangle-\langle\vec{b},\vec{y}\rangle)=$$
$$=\sum_{\vec{x},\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{b},\vec{y}\rangle)\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0-\vec{x}\rangle)=$$
$$=\sum_{\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{b},\vec{y}\rangle)q^k\delta_{\vec{x},\vec{x}_0}=q^k\sum_{\vec{y}\in P^k}\chi_a(\varphi(\vec{x}_0,\vec{y})-\langle\vec{b},\vec{y}\rangle)=$$
$$=q^k\sum_{\vec{y}\in P^k}\chi_a(c-\langle\vec{b},\vec{y}\rangle)=q^k\chi_a(c)\sum_{\vec{y}\in P^k}\chi_a(-\langle\vec{b},\vec{y}\rangle)=q^{2k}\chi_a(c)\delta_{\vec{b},\vec{0}}.$$

Подставим в полученную формулу значение $\vec{b}=\vec{0}$. Получим что сумма q^k слагаемых каждое из которых по модулю не превосходит q^k дает число, имеющее модуль равный q^{2k}. Это возможно только если каждое слагаемое рассматриваемой суммы равно $\chi_a(c)q^k$, т.е.

$$\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle)=\chi_a(c)q^k.$$

Таким образом,

$$C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)=$$
$$=\begin{cases}\chi_a(-\langle\vec{a},\vec{x}_0\rangle)\left(C_a(g,\langle\vec{b},\vec{y}\rangle)+\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)\right), & \text{если } \vec{b}\neq\vec{0},\\ \chi_a(-\langle\vec{a},\vec{x}_0\rangle)C_a(g,0), & \text{если } \vec{b}=\vec{0},\end{cases}$$

и для модуля коэффициента кросс-корреляции справедливы равенства

$$|C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)|=$$
$$=\begin{cases}\left|C_a(g,\langle\vec{b},\vec{y}\rangle)+\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)\right|, & \text{если } \vec{b}\neq\vec{0},\\ |C_a(g,0)|, & \text{если } \vec{b}=\vec{0}.\end{cases}\qquad(14)$$

Докажем утверждение 1). Согласно следствию 1 функция f является сбалансированной тогда и только тогда, когда $C_a(f,0)=0$ для всех $a\in P^*$. Из равенств (14) следует, что это равносильно условию $C_a(g,0)=0$, $a\in P^*$, т.е. сбалансированности функции g.

Утверждение 2) следует из равенств (14), предложения 3 и соотношений

$$|C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)|\leqslant|C_a(g,\langle\vec{b},\vec{y}\rangle)|+|C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)|\leqslant C(g)+q^k.$$

Докажем утверждения 3) и 4). Пусть $\vec{x}_0=(c_1,\ldots,c_k)$, тогда

$$f(\vec{x},\vec{y})=\delta_{\vec{x},\vec{x}_0}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y})=\prod_{i=1}^{k}\delta_{x_i,c_i}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y})=$$
$$=\prod_{i=1}^{k}\frac{\prod\limits_{a\in P\setminus\{c_i\}}(x_i-a)}{\prod\limits_{a\in P\setminus\{c_i\}}(c_i-a)}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y}).$$

Справедливость утверждений 3) и 4) теперь очевидна. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Dobbertin H.* Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity // Fast Software Encryption (Proc. 2nd Int. Workshop FSE 1994. Leuven, Belgium. Dec. 14–16, 1994). Lect. Notes Comput. Sci. V. 1008. Berlin: Springer, 1995. P. 61–74. https://doi.org/10.1007/3-540-60590-8_5
2. *Chee S., Lee S., Kim K.* Semi-bent Functions // Advances in Cryptology—ASIACRYPT'94 (Proc. 4th Int. Conf. on the Theory and Applications of Cryptology. Wollongong, Australia. Nov. 28 – Dec. 1, 1994). Lect. Notes Comput. Sci. V. 917. Berlin: Springer, 1995. P. 107–118. https://doi.org/10.1007/BFb0000428
3. *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge Univ. Press, 2010. P. 257–397.
4. *Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО. 2012.
5. *Токарева Н.Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64. http://mi.mathnet.ru/da599
6. Амбросимов А.С. Свойства бент-функций q-значной логики над конечными полями. Дискр. математика. 1994. Т. 6. № 3. С. 50–60. http://mi.mathnet.ru/dm639
7. *Солодовников В.И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискрет. матем. 2002. Т. 14. № 1. С. 99–113. https://doi.org/10.4213/dm234
8. *Кузьмин А.С., Марков В.Т., Нечаев А.А., Шишкин В.А., Шишков А.Б.* Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информ. 2008. Т. 44. № 1. С. 15–37. http://mi.mathnet.ru/ppi1263
9. *Кузьмин А.С., Нечаев А.А., Шишкин В.А.* Бент- и гипербент-функции над конечным полем // Тр. по дискр. матем. Т. 10. М.: Физматлит, 2007. С. 97–122.
10. *Бугров А.Д.* Кусочно-аффинные подстановки конечных полей // Прикл. дискр. матем. 2015. № 4 (30). С. 5–23. https://doi.org/10.17223/20710410/30/1
11. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
12. *Golomb S.W., Gong G.* Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. New York: Cambridge Univ. Press, 2005.
13. *Рябов В.Г.* Нелинейность функций над конечными полями // Дискр. матем. 2021. Т. 33. № 4. С. 110–131. https://doi.org/10.4213/dm1674
14. *McFarland R.L.* A Family of Difference Sets in Non-cyclic Groups // J. Combin. Theory Ser. A. 1973. V. 15. № 1. P. 1–10. https://doi.org/10.1016/0097-3165(73)90031-9
15. *Carlet C., Ding C.* Highly Nonlinear Mappings // J. Complexity. 2004. V. 20. № 2–3. P. 205–244. https://doi.org/10.1016/j.jco.2003.08.008
16. *Nyberg K.* Construction of Bent Functions and Difference Sets // Advances in Cryptology—EUROCRYPT'90 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Aarhus, Denmark. May 21–24, 1990). Lect. Notes Comput. Sci. V. 473. Berlin: Springer, 1991. P. 151–160. https://doi.org/10.1007/3-540-46877-3_13
17. *Kumar P.V., Scholtz R., Welch L.R.* Generalized Bent Functions and Their Properties // J. Combin. Theory Ser. A. 1985. V. 40. № 1. P. 90–107. https://doi.org/10.1016/0097-3165(85)90049-4
18. *Кейперс Л., Нидеррайтер Г.* Равномерное распределение последовательностей. М.: Наука, 1985.
19. *Camion P., Canteaut A.* Correlation-Immune and Resilient Function over a Finite Alphabet and Their Applications in Cryptography // Designs Codes Cryptogr. 1999. V. 16. № 2. P. 121–149. https://doi.org/10.1023/A:1008337029047
20. *Панков К.Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Матем. вопр. криптогр. 2014. Т. 5. № 4. С. 73–97. https://doi.org/10.4213/mvk136

21. *Bennett C.H., Brassard G., Robert J.-M.* Privacy Amplification by Public Discussion // SIAM J. Comput. 1988. V. 17. № 2. P. 210–229. https://doi.org/10.1137/0217014
22. *Xiao G.-Z., Massey J.L.* A Spectral Characterization of Correlation-Immune Combining Functions // IEEE Trans. Inform. Theory. 1988. V. 34. № 3. P. 569–571. https://doi.org/10.1109/18.6037
23. *Pankov K.N.* Improved Asymptotic Estimates for the Numbers of Correlation-Immune and k-Resilient Vectorial Boolean Functions // Discrete Math. Appl. 2019. V. 29. № 3. P. 195–213. https://doi.org/10.1109/18.6037
24. *Панков К.Н.* Рекуррентные формулы для числа k-эластичных и корреляционно-имунных двоичных отображений // Прикл. дискрет. матем. Приложение. 2019. № 12. С. 62–66. https://doi.org/10.17223/2226308X/12/19
25. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Т. 2. М.: Гелиос АРВ, 2003.
26. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикл. дискр. матем. 2010. № 2 (8). С. 22–33. http://mi.mathnet.ru/pdm174
27. *Camion P., Carlet C., Charpin P., Sendrier N.* On Correlation-Immune Functions // Advances in Cryptology—CRYPTO'91 (Proc. 11th Annu. Int. Cryptology Conf. Santa Barbara, CA, USA. Aug. 11–15, 1991). Lect. Notes Comput. Sci. V. 576. Berlin: Springer, 1992. P. 86–100. https://doi.org/10.1007/3-540-46766-1_6
28. *Canteaut A., Daum M., Dobbertin H., Leander G.* Finding Nonnormal Bent Functions // Discrete Appl. Math. 2006. V. 154. № 2. P. 202–218. https://doi.org/10.1016/j.dam.2005.03.027

Камловский Олег Витальевич
МТУСИ, кафедра теории вероятностей
и прикладной математики
ov-kam@yandex.ru
Панков Константин Николаевич
МТУСИ, кафедра информационной безопасности
pankov_kn@mtuci.ru

Поступила в редакцию
25.08.2022
После доработки
08.11.2022
Принята к публикации
10.11.2022

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

Оригинал-макет подготовил *Д.Ю. Ногин*
по контракту с ООО «Тематическая редакция»

Москва
ООО «Тематическая редакция»