ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 1**

УДК 621.391 : 519.725

© 2021 г. **В.А. Зиновьев, Д.В. Зиновьев**

ОБ ОБОБЩЕННОЙ КАСКАДНОЙ КОНСТРУКЦИИ КОДОВ В МОДУЛЬНОЙ МЕТРИКЕ И МЕТРИКЕ ЛИ[1,2]

Рассмотрена обобщенная каскадная конструкция кодов над q-ичным алфавитом в модульной метрике L_1 и метрике Ли L. Результирующие коды имеют произвольную длину, произвольное расстояние (независимо от размера алфавита) и могут исправлять как независимые ошибки, так и пакеты ошибок в обеих метриках. В частности, для любой длины 2^m построены коды над $\mathbb{Z}_4$ с расстоянием Ли, равным 4, которые при отображении Грея приводят к расширенным двоичным совершенным кодам длины 2^{m+1} (с кодовым расстоянием 4). Построены коды над $\mathbb{Z}_4$ длины n с расстоянием Ли, равным n, которые при отображении Грея приводят к матрицам Адамара порядка $2n$ (при дополнительном условии, что существует матрица Адамара порядка n). Построенные новые коды в метрике Ли часто лучше по своим параметрам, чем ранее известные коды, в частности, значительно лучше, чем ранее построенные коды Астолы.

Ключевые слова: блоковый корректирующий код, корректирующий код в метрике Ли, корректирующий код в модульной метрике, обобщенная каскадная конструкция, корректирующий код над $\mathbb{Z}_4$.

DOI: 10.31857/S0555292321010046

§ 1. Введение

Пусть $E = \{0, 1, \ldots, q-1\}$. Блоковым q-ичным кодом C называется любое подмножество множества E^n. Будем называть такой код $(n, N, d)_q$-кодом, где n – *длина* кода, N – число кодовых слов, т.е. *мощность* кода C, а d – *минимальное расстояние Хэмминга*

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

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

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

Для случая, когда q – степень простого числа, а q-ичный $(n, N = q^k, d)_q$-код C является линейным пространством размерности k над $\mathbb{F}_q$, используется стандартное обозначение $[n, k, d]_q$. В случае $q = 2$ символ q в обозначениях $(n, N, d)_q$ и $[n, k, d]_q$ опускается.

Расстоянием Ли $d_L(i, j)$ между символами i и j из E мы называем минимальную разность между этими символами:

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

[1] Исследование выполнено в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

[2] Результаты статьи были доложены на конференции ACCT'2018 и опубликованы в ее трудах [1].

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:

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

Нам понадобится еще одно расстояние, а именно *модульное расстояние* d_{L_1}, равное для символов x_i и x_j из E модулю разности между этими элементами: $d_{L_1}(x_i, x_j) = |x_i - x_j|$, и доопределяемое на векторы над E аналогичным образом:

$$d_{L_1}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n} d_{L_1}(x_i, y_i).$$

Коды, исправляющие ошибки, для обеих метрик являются важным случаем корректирующих кодов и имеют применения в системах связи и системах хранения информации (см., например, работы [2–8] и библиографию в них).

Цель настоящей работы – описать обобщенную каскадную конструкцию для кодов в метриках L и L_1. Этот подход позволяет построить широкий класс кодов с хорошей корректирующей способностью (с точки зрения таких существующих кодов) для исправления как независимых ошибок, так и пакетов ошибок. Метод построения кодов основан на хорошо известном обобщенном каскадном методе построения корректирующих кодов для евклидовой метрики [9] и метрики Хэмминга [10], который мы применили для метрик L и L_1. Для случая $q = 4$ наша конструкция дает коды над $\mathbb{Z}_4$ произвольной длины и с произвольным расстоянием, которые часто лучше, чем известные коды. В частности, для длины $n = 2^m$ мы получаем коды с расстоянием Ли $d_L = 4$, так что преобразование Грея приводит к двоичным расширенным совершенным кодам длины $2n$ с кодовым расстоянием (уже в хэмминговой метрике), равным 4. Таким образом, мы получаем, что каждый двоичный расширенный совершенный код длины $n = 2^m$ индуцирует $\mathbb{Z}_4$-код той же длины n с расстоянием Ли $d_L = 4$, который дает (при преобразовании Грея) двоичный расширенный совершенный код длины $2n$. Тем самым мы получаем дважды экспоненциальное число взаимно не эквивалентных расширенных двоичных совершенных кодов с $d = 4$, имеющих $\mathbb{Z}_4$-представление. Эта же конструкция дает коды над $\mathbb{Z}_4$ с расстоянием Ли, равным n, которые при отображении Грея приводят к (двоичным) матрицам Адамара порядка $2n$, имеющих $\mathbb{Z}_4$-представление (при дополнительном условии, что существует матрица Адамара порядка n). Как показывают сравнения построенных кодов с уже существующими кодами конечной длины, новые коды в метрике Ли лучше по своим параметрам, чем ранее известные коды.

Статья организована следующим образом. Построение кодов рассмотрено в § 2. Комбинаторные свойства таких кодов приведены в § 3. Следующий § 4 посвящен важному частному случаю кодов, а именно $\mathbb{Z}_4$-кодам. В § 5 рассмотрены коды над $\mathbb{Z}_q$, где $q = p^s$, с фиксированным расстоянием, а § 6 посвящен сравнению новых кодов небольшой длины с ранее построенными кодами в метрике Ли.

§ 2. Построение кодов

Перенумеруем элементы алфавита $E = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ размера q. 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 множества E, а именно: каждому элементу a ставится во взаимно-однозначное соответствие его номер, или *индексный вектор*, $L(a) = (i_1, \ldots, i_s)$ длины s над $\mathbb{Z}_{q_1}, \mathbb{Z}_{q_2}, \ldots, \mathbb{Z}_{q_s}$ (сим-

волы j-й позиции принимают значения из $\mathbb{Z}_{q_j}$). Определим числа Q_j, $j = 1, \ldots, s$:

$$q = q_1 \ldots q_j \times Q_j, \quad j = 1, \ldots, s, \quad \text{где} \quad Q_s = 1.$$

Сначала разобьем E на q_1 подмножеств E_i размера Q_1:

$$E = E_0 \cup \ldots \cup E_{q_1 - 1},$$

где

$$E_i = \{i + jq_1 : \ j = 0, 1, \ldots, Q_1 - 1\}.$$

Затем сделаем то же самое для каждого множества E_i, т.е. каждое E_i разобьем на q_2 подмножеств $E_{i,j}$ размера Q_2:

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

где

$$E_{i,j} = \{i + jq_1 + kq_1q_2 : \ k = 0, 1, \ldots, Q_2 - 1\},$$

и так далее. На ℓ-м шаге будем иметь

$$E_{i_1,\ldots,i_{\ell-1}} = E_{i_1,\ldots,i_{\ell-1},0} \cup \ldots \cup E_{i_1,\ldots,i_{\ell-1},q_\ell - 1},$$

где $E_{i_1,\ldots,i_{\ell-1},j}$ – следующее множество:

$$E_{i_1,\ldots,i_{\ell-1},j} = \\ = \{i_1 + i_2q_1 + \ldots + i_{\ell-1}q_1 \ldots q_{\ell-2} + jq_1 \ldots q_{\ell-1} + kq_1 \ldots q_\ell : \ k = 0, 1, \ldots, Q_\ell - 1\}$$

для $j = 0, 1, \ldots, q_\ell - 1$. Эту процедуру мы повторяем в течение s шагов, в результате которых получаем подмножества $E_{i_1,\ldots,i_{s-1}}$ размера $Q_{s-1} = q_s$, а именно получаем следующее разбиение:

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

так что каждое множество $E_{i_1,\ldots,i_{s-1}}$ содержит q_s элементов. Каждому элементу a из алфавита E размера q с разложением $q = q_1q_2 \ldots q_s$ приписывается номер, а именно его индексный вектор $L(a)$, определяемый следующим образом: если элемент a принадлежит подмножеству $E_{i_1,\ldots,i_{s-1}}$ и имеет индекс i_s в множестве $E_{i_1,\ldots,i_{s-1}}$, то a имеет индексный вектор $L(a) = (i_1, i_2, \ldots, i_{s-1}, i_s)$. Индекс i_s элемента a – это его номер в множестве элементов $E_{i_1,\ldots,i_{s-1}}$, когда эти элементы упорядочены обычным образом по возрастанию (индекс i_s элемента a растет с ростом a). Если $E_{i_1,\ldots,i_{s-1}} = \{a_1, a_2, \ldots, a, \ldots, a_{q_s}\}$, где

$$a_1 < a_2 < \ldots < a = a_j < \ldots < a_{q_s},$$

то в множестве $E_{i_1,\ldots,i_{s-1}}$ элемент a имеет индекс j.

Таким образом, каждому элементу из E ставится в соответствие его номер, представляющий собой целочисленный вектор $(i_1, \ldots, i_s)$ длины s, обладающий следующим свойством: *j-й индекс i_j принадлежит множеству* $\{0, 1, \ldots, q_j - 1\}$. Легко видеть, что вектор $L(a)$ является $(q_1, \ldots, q_s)$-разложением числа a, а именно: если $L(a)$ – индексный вектор a, т.е.

$$L(a) = (i_1, i_2, \ldots, i_s),$$

то

$$a = i_1 + i_2 q_1 + i_3 q_1 q_2 + \ldots + i_s q_1 \ldots q_{s-1}. \tag{2}$$

В случае, когда $q = p^s$ является степенью простого числа p, а элементами E_q являются элементы конечного поля $\mathbb{F}_q$, условимся, что элементы E_q упорядочиваются лексикографически, используя естественное представление элементов поля $\mathbb{F}_q$ как элементов векторного пространства размерности s над $\mathbb{F}_p$.

Следующее простое утверждение необходимо нам в дальнейшем.

Лемма 1. *Пусть E – алфавит размера q, где q представлено в виде произведения чисел $q = q_1 q_2 \ldots q_s$. Пусть a и b из E имеют номера $L(a) = (i_1, \ldots, i_s)$ и $L(b) = (j_1, \ldots, j_s)$. Пусть*

$$\ell = \min\{h : \ h = 1, \ldots, s, \ i_h \neq j_h\}.$$

Тогда

$$d_L(a,b) \geqslant q_1 \ldots q_{\ell-1} \min\Big\{|i_\ell - j_\ell|, \ \frac{q}{q_1 \ldots q_{\ell-1}} - |i_\ell - j_\ell|\Big\} \geqslant q_1 \ldots q_{\ell-1}$$

и

$$d_{L_1}(a,b) \geqslant q_1 \ldots q_{\ell-1} |i_\ell - j_\ell| \geqslant q_1 \ldots q_{\ell-1},$$

где $q_0 = 1$.

Доказательство. Предположим, что два разных элемента a и b принадлежат множеству $E_{i_1,\ldots,i_{\ell-1}}$, где ℓ – максимально возможное для заданных a и b число, обладающее этим свойством. Из выражения (2) получаем, что

$$a - b = (i_1 - j_1) + (i_2 - j_2) q_1 + (i_3 - j_3) q_1 q_2 + \ldots + (i_s - j_s) q_1 \ldots q_{s-1}. \tag{3}$$

Так как a и b принадлежат множеству $E_{i_1,\ldots,i_{\ell-1}}$, то $i_h = j_h$ для $h = 1, \ldots, \ell - 1$, и мы заключаем, что a и b сравнимы по модулю $q_1 \ldots q_{\ell-1}$. Так как $i_\ell \neq j_\ell$, для модульного расстояния получаем

$$d_{L_1}(a,b) \geqslant q_1 \ldots q_{\ell-1} |i_\ell - j_\ell| \geqslant q_1 \ldots q_{\ell-1}.$$

Аналогично для расстояния Ли получаем

$$d_L(a,b) = q_1 \ldots q_{\ell-1} \min\Big\{|i_\ell - j_\ell|, \frac{q}{q_1 \ldots q_{\ell-1}} - |i_\ell - j_\ell|\Big\} \geqslant q_1 \ldots q_{\ell-1}.$$

Обе оценки для произвольных a и b, принадлежащих множеству $E_{i_1,\ldots,i_{\ell-1}}$, очевидно, не улучшаемы, так как обе достигаются. Конечно, они могут быть улучшены в условиях леммы с помощью выражения (3), если мы знаем какие-то из индексов i_h и j_h для значений $h \geqslant \ell + 1$. ▲

Опишем построение кодов обобщенным каскадным методом. Пусть задан алфавит E (который мы называем *внутренним кодом*) размера q, где $q = q_1 q_2 \ldots q_s$ и где все элементы алфавита E перенумерованы, так что каждому элементу a сопоставлен его индексный вектор $L(a)$. Предположим, что имеется s кодов A_j, $j = 1, \ldots, s$ (одной и той же длины), 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). Коды A_j мы называем *внешними кодами*. Из каждого кода A_j выберем по произвольному кодовому слову $\boldsymbol{a}^{(j)} = (a_1^{(j)}, \ldots, a_n^{(j)})$. По s выбранным словам $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)}$ построим матрицу B размера $s \times n$, выбирая в качестве j-й строки выбранное нами слово $\boldsymbol{a}^{(j)}$ кода A_j. Пусть $\boldsymbol{b}_i$ обозначает i-й столбец матрицы B. По построению этой матрицы элемент $b_{i,j}$, стоящий в j-й позиции вектора-столбца $\boldsymbol{b}_i$, принадлежит алфавиту E_{q_j} размера q_j, т.е. $b_{i,j} \in \{0, 1, \ldots, q_j - 1\}$.

Отсюда следует, что каждый столбец $\boldsymbol{b}_i$ является индексным вектором $L(a)$ некоторого элемента a из множества E, т.е.

$$L(a) = (i_1, \ldots, i_s) = (b_{i,1}, \ldots, b_{i,s}), \quad i_j \in \{0, 1, \ldots, q_j - 1\}, \quad j = 1, \ldots, s.$$

С помощью полученной матрицы B мы задаем кодовое слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ над алфавитом E нового результирующего кода C, заменяя каждый i-й вектор-столбец $\boldsymbol{b}_i$ элементом $a = a(\boldsymbol{b}_i)$, индексным вектором которого является вектор-столбец $\boldsymbol{b}_i$. Это означает, что на i-й позиции кодового слова $\boldsymbol{c} = (c_1, \ldots, c_n)$ стоит элемент a, т.е. что $c_i = a = a(\boldsymbol{b}_i)$. Тем самым, каждому выбору $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)}$ слов по одному из каждого внешнего кода A_j соответствует одно слово $\boldsymbol{c}$ результирующего кода C. 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 C.

Теорема 1. *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 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*

$$n, \quad N = \prod_{j=1}^{s} N_j, \quad d_{L_1} \geqslant d_L \geqslant \min\{d_1,\, q_1 d_2,\, q_1 q_2 d_3,\, \ldots,\, q_1 q_2 \ldots q_{s-1} d_s\}.$$

Доказательство. Значения параметров q, n и N нового кода вполне очевидны по построению кода. Докажем, что результирующий код C имеет расстояние Ли d_L и модульное расстояние d_{L_1}, указанные в утверждении теоремы. Пусть $\boldsymbol{c}^{(1)} = (c_1^{(1)}, \ldots, c_n^{(1)})$ и $\boldsymbol{c}^{(2)} = (c_1^{(2)}, \ldots, c_n^{(2)})$ – два различных кодовых слова, и пусть $\boldsymbol{a}^{(j,1)} = (a_1^{(j,1)}, \ldots, a_n^{(j,1)})$ и $\boldsymbol{a}^{(j,2)} = (a_1^{(j,2)}, \ldots, a_n^{(j,2)})$, $j = 1, \ldots, s$, – кодовые слова внешних кодов, на которых основаны соответствующие слова кода C. Так как $\boldsymbol{c}^{(1)}$ и $\boldsymbol{c}^{(2)}$ различны, то имеется ℓ, такое что слова $\boldsymbol{a}^{(\ell,1)}$ и $\boldsymbol{a}^{(\ell,2)}$ различны, но все предыдущие слова $\boldsymbol{a}^{(j,1)}$ и $\boldsymbol{a}^{(j,2)}$, где $j = 1, \ldots, \ell - 1$, совпадают. Далее, $\boldsymbol{a}^{(\ell,1)}$ и $\boldsymbol{a}^{(\ell,2)}$ (как кодовые слова A_ℓ) находятся друг от друга на расстоянии (Хэмминга) d_ℓ или больше. Это означает, что имеется по крайней мере d_ℓ позиций с номерами $r \in \{1, \ldots, n\}$, в которых индексные векторы $L^{(1)}(c_r^{(1)}) = (i_1, \ldots, i_s)$ и $L^{(2)}(c_r^{(2)}) = (j_1, \ldots, j_s)$ элементов $c_r^{(1)}$ и $c_r^{(2)}$ совпадают в первых $\ell - 1$ позициях и отличаются в ℓ-й позиции. Поэтому в силу леммы 1 элементы $c_r^{(1)}$ и $c_r^{(2)}$ находятся друг от друга на расстоянии Ли

$$d_L(c_r^{(1)}, c_r^{(2)}) \geqslant q_1 \ldots q_{\ell-1}.$$

Учитывая, что число таких позиций не менее d_ℓ, а кодовые слова $\boldsymbol{c}^{(1)}$ и $\boldsymbol{c}^{(2)}$ находятся друг от друга на расстоянии не менее чем $(q_1 \ldots q_{\ell-1})d_\ell$, получаем требуемое выражение для минимального расстояния d_L кода C. Тот же результат, очевидно, справедлив и для модульного расстояния, которое всегда не меньше расстояния Ли. ▲

Замечание 1. Заметим, что код, полученный по теореме 1, может быть декодирован алгоритмом, предложенным в работе [11], который реализует минимальное расстояние кода, а также допускает мягкое декодирование. Построенные обобщенные каскадные коды в метриках d_L и d_{L_1}, так же как и для метрики Хэмминга (см. [10–12]) и евклидовой метрики [9], позволяют исправлять как независимые ошибки, так и пакеты ошибок. Кроме того, они обладают важным свойством неравной защиты информационных символов [13]. Все эти свойства реализуются одним и

тем же алгоритмом декодирования по минимуму обобщенного расстояния, предложенным в указанной работе [11].

§ 3. Комбинаторные и алгебраические свойства

Пусть S_n обозначает полную группу всех перестановок на множестве из n элементов. Два кода C и C' в E_q^n с одними и теми же параметрами эквивалентны, если найдутся вектор $\boldsymbol{x} \in E_q^n$ и перестановка $\sigma \in S_n$ (которая действует на координатных позициях множества E_q^n), такие что

$$C + \boldsymbol{x} = \sigma(C').$$

Теорема 2. *Пусть коды C и C' над алфавитом E получены по теореме* 1 *из внешних кодов $A_1, A_2, \ldots, A_s$ и $A'_1, A'_2, \ldots, A'_s$ соответственно. Пусть найдется по крайней мере одно i, такое что коды A_i и A'_i не эквивалентны. Тогда результирующие коды C и C' также не эквивалентны.*

Доказательство. Предположим, что коды $A_1, A_2, \ldots, A_s$ эквивалентны кодам $A'_1, A'_2, \ldots, A'_s$, т.е. существует перестановка $\pi \in S_n$ и векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s$, такие что $A_i + \boldsymbol{x}_i = \pi(A'_i)$ для $i = 1, \ldots, s$. По построению кодов это означает, что множество матриц B под действием сдвига каждой i-й строки на вектор $\boldsymbol{x}_i$, $i = 1, \ldots, s$, и перестановки π на столбцы матриц B переходит в множество матриц B' (определяющих слова кода C'). Но это означает, что коды C и C' эквивалентны. Наоборот, пусть код C' эквивалентен коду C, т.е. существует перестановка $\pi \in S_n$ и вектор $\boldsymbol{x} \in E_q^n$, такие что $C + \boldsymbol{x} = \pi(C')$. Тогда $\pi(A'_i) = A_i + \boldsymbol{x}_i$ (здесь $\boldsymbol{x}_i$ индуцируются вектором $\boldsymbol{x}$) для всех $i = 1, \ldots, s$, т.е. коды A_i и A'_i эквивалентны. Если же коды A_i и A'_i не эквивалентны хотя бы для одного i, то результирующие коды C и C' не могут быть эквивалентны. ▲

Для произвольного кода C обозначим через $\mathrm{Sym}(C)$ множество перестановок, стабилизирующих этот код. Два кода C и C' назовем *симметрично эквивалентными*, если найдется перестановка $\tau \in \mathrm{Sym}(C)$, такая что $C = \tau(C') = \{\tau(\boldsymbol{v}) : \boldsymbol{v} \in C'\}$. Скажем, что код $C \subset E_q^n$ *симметрично транзитивен*, если для любых двух слов $\boldsymbol{u}$ и $\boldsymbol{v}$ кода C, имеющих одну и ту же композицию, существует перестановка $\tau \in \mathrm{Sym}(C)$, такая что $\tau(\boldsymbol{u}) = \boldsymbol{v}$.

Теорема 3. *Пусть $q = q_1 q_2$ и заданы коды A_1 и A_2. Пусть код C над алфавитом E_q получен по теореме* 1 *из кодов A_1 и A_2. Предположим, что код A_1 симметрично транзитивен, а код A_2 таков, что $\mathrm{Sym}(A_2) = S_n$. Тогда код C также симметрично транзитивен.*

Доказательство. Пусть $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ – произвольные кодовые слова из C, имеющие одну и ту же композицию, и пусть слово $\boldsymbol{c}_1$ получено из $\boldsymbol{a}_1 \in A_1$ и $\boldsymbol{b}_1 \in A_2$, а $\boldsymbol{c}_2$ – из $\boldsymbol{a}_2 \in A_1$ и $\boldsymbol{b}_2 \in A_2$. Так как по построению

$$\boldsymbol{c}_j = \boldsymbol{a}_j + q_1 \boldsymbol{b}_j, \quad j = 1, 2,$$

то слова $\boldsymbol{b}_1$ и $\boldsymbol{b}_2$ (а также $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$) имеют одну и ту же композицию и поэтому могут быть переставлены некоторой перестановкой из S_n. Поскольку код A_1 симметрично транзитивен, найдется перестановка $\pi \in \mathrm{Sym}(A_1)$, такая что $\pi(\boldsymbol{a}_1) = \boldsymbol{a}_2$. Так как заведомо $\pi \in S_n$, положим $\pi(b_1) = b_2$, и тогда получим

$$\pi(\boldsymbol{c}_1) = \pi(\boldsymbol{a}_1 + q_1 \boldsymbol{b}_1) = \pi(\boldsymbol{a}_1) + q_1 \pi(\boldsymbol{b}_1) = \boldsymbol{a}_2 + q_1 \boldsymbol{b}_2 = \boldsymbol{c}_2. \quad ▲$$

Код $C \subseteq E_q^n$ имеет радиус покрытия $\rho = \rho(C)$, если ρ – минимальное число, такое что шары радиуса ρ с центрами в кодовых словах кода C покрывают все пространство E_q^n.

Теорема 4. *Пусть код C получен конструкцией теоремы 1 из s внешних кодов A_i, $i = 1, \dots, s$. Если код A_i для каждого i имеет радиус покрытия ρ_i, то результирующий код C имеет радиус покрытия*

$$\rho(C) \geqslant \max\{\rho_1, q_1\rho_2, \dots, q_1 \dots q_{s-1}\rho_s\}.$$

Доказательство. Заметим, что все слова кода A_1 являются словами кода C (это слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)})$, построенные только из A_1 выбором нулевых слов из всех других кодов A_i с $i \geqslant 2$). Покажем, что вектор $\boldsymbol{x}_1$, который находится на расстоянии ρ_1 от кода A_1, находится от кода C на расстоянии, не меньшем чем ρ_1, т.е. что $d(\boldsymbol{x}_1, C) \geqslant d(\boldsymbol{x}_1, A_1)$. Пусть, например, слово $\boldsymbol{c} \in C$ построено по словам $\boldsymbol{a}^{(1)} = (a_1^{(1)}, \dots, a_n^{(1)})$-кода A_1 и $\boldsymbol{a}^{(2)} = (a_1^{(2)}, \dots, a_n^{(2)})$-кода A_2. Индексные векторы компонент слова $\boldsymbol{c}$ имеют вид $(a_i^{(1)}, a_i^{(2)}, 0, \dots, 0)$, $i = 1, 2, \dots, n$. Пусть $j_1, \dots, j_{\rho_1}$ – номера позиций, в которых $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$ различаются. В наихудшем для нас случае все ненулевые символы слова $\boldsymbol{a}^{(2)}$ расположены в тех же позициях, что и ненулевые символы слова $\boldsymbol{a}^{(1)}$. Но индексные векторы элементов $\boldsymbol{x}_1$ имеют только первую ненулевую компоненту (а все остальные равны нулю). Поэтому любая компонента j_h, в которой $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$ различаются и в которой $a_{j_h}^{(2)} \neq 0$, увеличивает расстояние Ли между $\boldsymbol{x}_1$ и $\boldsymbol{c}$ (по крайней мере на q_1) по сравнению с расстоянием Хэмминга между $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$, равным ρ_1. Тем самым мы доказали, что $\rho(C) \geqslant \rho_1$.

Следующее неравенство $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2\}$ доказывается совершенно аналогично. Рассмотрим все слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)})$, полученные выбором ненулевого слова $\boldsymbol{a}^{(2)} = (a_1^{(2)}, \dots, a_n^{(2)})$ кода A_2, а всех остальных слов – нулевыми. Индексные векторы компонент таких слов $\boldsymbol{c}$ имеют вид $(0, a_i^{(2)}, 0, \dots, 0)$, $i = 1, 2, \dots, n$. Если вектор $\boldsymbol{x}_2$ находится на расстоянии ρ_2 от кода A_2, то он находится на расстоянии, не меньшем чем $q_1\rho_2$, от всех слов $\boldsymbol{c}$ кода C указанного вида (действительно, координатные позиции таких слов кратны q_1). Можем ли мы приблизиться к $\boldsymbol{x}_2$, рассматривая слова $\boldsymbol{c}$ другого типа? Ясно, что это невозможно при выборе ненулевыми слов $\boldsymbol{a}^{(3)}$. Соответствующие слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)}, \boldsymbol{a}^{(2)})$ (полученные выбором ненулевых слов $\boldsymbol{a}^{(2)}$ и $\boldsymbol{a}^{(3)}$) имеют новые координатные позиции, которые не пересекаются с позициями слов $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)})$ и которые кратны уже q_1q_2. Тем самым, расстояние между $\boldsymbol{x}_2$ и кодом C только увеличивается. Если же выбирать ненулевыми слова $\boldsymbol{a}^{(1)}$, то мы окажемся в условиях предыдущего случая, для которого $\rho(C) \geqslant \rho_1$. Это дает оценку $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2\}$.

Следующее неравенство $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2, q_1q_2\rho_3\}$ устанавливается аналогичным образом, и так далее. ▲

§ 4. $\mathbb{Z}_4$-коды

Пусть $E = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$. Любой элемент a из E имеет индексный вектор (i_1, i_2), являющийся двоичным представлением a, т.е. $a = i_1 + 2i_2$. Положим $n = 2^m$ и выберем следующие два внешних кода: двоичный расширенный совершенный $(n, 2^{n-m-1}, 4)$-код в качестве кода A_1 и $(n, 2^{n-1}, 2)$-код, полученный проверкой на четность или на нечетность по модулю 2, в качестве кода A_2. Пусть

$$\boldsymbol{a}^{(1)} = \left(a_1^{(1)}, a_2^{(1)}, \dots, a_n^{(1)}\right) \in A_1 \quad \text{и} \quad \boldsymbol{a}^{(2)} = \left(a_1^{(2)}, a_2^{(2)}, \dots, a_n^{(2)}\right) \in A_2.$$

Тогда

$$\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \boldsymbol{a}^{(2)}) = (c_1, c_2, \dots, c_n) \in C,$$

где

$$L(c_i) = \big(a_i^{(1)}, a_i^{(2)}\big), \quad \text{так что} \quad c_i = a_i^{(1)} + 2a_i^{(2)} \in \mathbb{Z}_4.$$

Результирующий $(n, N, d_L)_4$-код C над $\mathbb{Z}_4$ имеет следующие параметры:

$$n = 2^m, \quad N = 2^{2n-m-2}, \quad d_L = \min\{4 \cdot 1, 2 \cdot 2\} = 4, \quad q = 4.$$

Напомним отображение Грея φ из $\mathbb{Z}_4$ на $\mathbb{Z}_2 \times \mathbb{Z}_2$:

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

которое продолжается на векторы над $\mathbb{Z}_4$ очевидным образом:

$$\varphi(c_1, \ldots, c_n) = (\varphi(c_1), \ldots, \varphi(c_n)).$$

Определим теперь новый код $\mathcal{C}$ как образ кода C с помощью отображения Грея:

$$\mathcal{C} = \{\varphi(\boldsymbol{c}) : \ \boldsymbol{c} \in C\}.$$

Так как при отображении Грея из $\mathbb{Z}_4$ в $\mathbb{Z}_2 \times \mathbb{Z}_2$ расстояние Ли переходит в расстояние Хэмминга [14], так что

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = d(\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})),$$

то заключаем, что новый $(n', N', d')_2$-код $\mathcal{C}$ имеет параметры

$$n' = 2^{m+1}, \quad N' = 2^{n'-m-2}, \quad d' = 4.$$

Таким образом, $\mathcal{C}$ представляет собой двоичный расширенный совершенный код, допускающий $\mathbb{Z}_4$-представление, иначе говоря, $\mathbb{Z}_4$-код. Это означает, что произвольный двоичный расширенный совершенный код A_1 длины n индуцирует двоичный расширенный совершенный $\mathbb{Z}_4$-код C длины $2n$.

Итак, с учетом теоремы 2 имеет место следующая

Теорема 5. *Двоичный расширенный совершенный код A_1 длины n индуцирует двоичный расширенный совершенный $\mathbb{Z}_4$-код C длины $2n$. При этом, если два таких кода A_1 и A_1' не эквивалентны (соответственно, различны), то результирующие $\mathbb{Z}_4$-коды C и C' длины $2n$ также не эквивалентны (соответственно, различны).*

Напомним, что все $\mathbb{Z}_4$-линейные совершенные коды перечислены в [15].

Следствие 1. *Число взаимно неэквивалентных расширенных двоичных совершенных кодов длины $n = 2^m$, имеющих $\mathbb{Z}_4$-представление, не меньше $2^{2^{n/4}}$.*

Доказательство. Этот результат непосредственно вытекает из известной конструкции удвоения Васильева [16], из которой следует, что число взаимно неэквивалентных расширенных двоичных совершенных кодов длины $n = 2^m$ не меньше $2^{2^{n/2}}$. ▲

Снова рассмотрим алфавит $E = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$. Пусть n – натуральное число, такое что существует матрица Адамара порядка n. Таким образом, в качестве A_1 мы берем $(n, 2, n)$-код с повторением, а в качестве кода A_2 – $(n, 2n, n/2)$-код Адамара.

Тогда результирующий $(n, N, d_L)_4$-код C над $\mathbb{Z}_4$ имеет параметры

$$n, \quad N = 4n, \quad d_L = \min\Big\{n \cdot 1, 2 \cdot \frac{n}{2}\Big\} = n, \quad q = 4.$$

Теперь, если определить новый код длины $2n$ как образ кода C под действием отображения Грея, мы получим двоичный $(2n, 4n, n)$-код Адамара. Таким образом, каждый код Адамара длины n порождает код Адамара длины $2n$, имеющий $\mathbb{Z}_4$-представление. Коды Адамара, имеющие $\mathbb{Z}_{2^s}$-представления, активно изучаются (см., например, работу [17] и библиографию в ней).

Теорема 6. *Пусть A_2 – двоичный код Адамара длины n, т.е. код с параметрами $(n, 2n, n/2)$. Тогда этот код вместе с $(n, 2, n)$-кодом A_1 индуцирует двоичный $(2n, 4n, n)$-код Адамара C, имеющий $\mathbb{Z}_4$-представление. При этом, если два таких кода A_2 и A_2' не эквивалентны (соответственно, различны), то результирующие $\mathbb{Z}_4$-коды C и C' длины $2n$ также не эквивалентны (соответственно, различны).*

Из этого утверждения непосредственно вытекает

Следствие 2. *Число взаимно неэквивалентных двоичных $(n, 2n, n/2)$-кодов Адамара длины n, имеющих $\mathbb{Z}_4$-представление, не меньше числа взаимно неэквивалентных двоичных $(n/2, n, n/4)$-кодов Адамара.*

§ 5. Коды над $\mathbb{Z}_{p^s}$

Рассмотрим алфавит $E_q = \mathbb{Z}_q$, где $q = p^s$, а $p \geqslant 2$ – простое. Если использовать в качестве внешних кодов A_i двоичные расширенные примитивные (в узком смысле) коды БЧХ, то имеет место следующая

Теорема 7. *Пусть m, s, u – произвольные натуральные числа, такие что $m \geqslant 3$, $s \geqslant 2$, $u \geqslant 2$. Тогда конструкция теоремы 1 дает (n, N, d_L)-код C над $\mathbb{Z}_q$ с параметрами $n = 2^m$, $N = 2^k$, $d_L = d_{L_1} = 2^u$, $q = 2^s$, где*

$$k \geqslant \begin{cases} sn - s - m(2^u - 2^{u-s} - s), & \text{если } q \leqslant d, \\ sn - u - m(2^u - u - 1), & \text{если } q > d. \end{cases} \tag{4}$$

Доказательство. Как известно, для любых натуральных m и t, таких что $tm \leqslant 2^m - 2$ и $t \leqslant 2^{m-2} - 1$, существует расширенный двоичный примитивный $[n, k, d]$-код БЧХ (в узком смысле), такой что

$$n = 2^m, \quad k \geqslant n - 1 - mt, \quad d \geqslant 2t + 2.$$

В описанной выше конструкции выберем в качестве i-го внешнего кода A_i расширенный двоичный примитивный код БЧХ (в узком смысле) с параметрами

$$n = 2^m, \quad d_i = 2^{u-i+1}, \quad k_i \geqslant n - 1 - m(2^{u-i} - 1), \quad i = 1, 2, \ldots, s.$$

В зависимости от соотношения между s и u непосредственно из теоремы 1 получаем следующие два выражения для нижней оценки числа информационных символов $k = k_1 + \ldots + k_s$ результирующего кода: если $s \leqslant u$, то

$$k \geqslant (n - 1 - m(2^{u-1} - 1)) + (n - 1 - m(2^{u-2} - 1)) + \ldots + (n - 1 - m(2^{u-s} - 1)),$$

а если $s \geqslant u + 1$, то

$$k \geqslant (n - 1 - m(2^{u-1} - 1)) + (n - 1 - m(2^{u-2} - 1)) + \ldots + (n - 1) + n(s - u).$$

Учитывая, что

$$\sum_{i=u-s}^{u-1} (2^i - 1) = 2^u - 2^{u-s} - s$$

и

$$\sum_{i=1}^{u-1}(2^i-1)=2^u-u-1,$$

получаем две соответствующие оценки на число k, приведенные в утверждении теоремы. ▲

Покажем теперь как можно построить код C с произвольными параметрами q, n и d_L, где $q=p^s$ – произвольная степень простого числа $p\geqslant 2$, а n и d_L – натуральные числа, удовлетворяющие следующему условию: найдется целое число i, $1\leqslant i\leqslant s$, такое что

$$\frac{d_L}{p^{i-1}}\leqslant n. \tag{5}$$

Обозначим через $h=h(s,p,n,d_L)$ минимальное i, для которого имеет место неравенство (5). Параметр h – это индекс начала нетривиальных внешних кодов A_i. Построим $s-h+1$ внешних $(n,N_i,d_i)_p$-кодов A_i над $\mathbb{F}_p$ для $i=h,\ldots,s$. Положим $d_1=d_L$. Для каждого $i=h,\ldots,s$ определим параметр ℓ_i, а именно натуральное число, которое задает параметры внешнего кода A_i (и которое надо оптимизировать). Код A_i строится с помощью (простой) каскадной конструкции из двух кодов: внешнего $(n_{v,i},k_{v,i},d_{v,i})$-кода V_i над $\mathbb{F}_{q^{\ell_i}}$, где $d_{v,i}=n_{v,i}+1-k_{v,i}$, являющегося МДР-кодом, и внутреннего $(n_{u,i},N_{u,i},d_{u,i})_p$-кода U_i над $\mathbb{F}_p$, мощность которого определяется размером алфавита внешнего кода V_i, т.е. $N_{u,i}=q^{\ell_i}$, длина которого $n_{u,i}$ должна удовлетворять условию $n_{v,i}n_{u,i}\geqslant n$ для всех $i=h,\ldots,s$. Для каждого $i=h,\ldots,s$ введем еще один параметр, а именно целое неотрицательное число $\chi_i=n_{v,i}n_{u,i}-n$. Длины $n_{v,i}$ и $n_{u,i}$ должны выбираться так, чтобы χ_i было минимальным. Каждый символ каждого кодового слова V_i заменяем на кодовое слово кода U_i, которое поставлено ему во взаимно-однозначное соответствие. В результате получаем внешний (уже для обобщенной каскадной конструкции теоремы 1) код A_i над $\mathbb{F}_p$ с параметрами (n,N_i,d_i):

$$n=n_{v,i}n_{u,i}-\chi_i,\quad N_i=p^{k_i},\quad d_i=d_{v,i}d_{u,i}-\chi_i^{(d)}, \tag{6}$$

где

$$k_i=s\ell_i(n_{v,i}+1-d_{v,i})-\chi_i^{(k)}, \tag{7}$$

а целочисленные (неотрицательные) параметры $\chi_i^{(d)}$ и $\chi_i^{(k)}$ выбираются произвольно так, чтобы выполнялось равенство

$$\chi_i=\chi_i^{(k)}+\chi_i^{(d)}.$$

Используя построенные коды A_i для всех $i=h,\ldots,s$, в соответствии с теоремой 1 получаем код C над $\mathbb{F}_q$ с параметрами $(n,N,d_L)_q$, где

$$n,\quad N=p^k,\quad k=\sum_{i=h}^{s}k_i,\quad d_L=\min\bigl\{p^{i-1}d_{v,i}d_{u,i}:\ i=h,\ldots,s\bigr\}. \tag{8}$$

При $i\leqslant h-1$ код A_i представляет собой формально тривиальный код (т.е. одно кодовое слово), не дающий вклада в мощность результирующего кода C. В этих случаях в алфавите E_q размера q можно использовать только числа, кратные p^{h-1}.

В частном случае, когда $\ell_i=\ell$ для всех $i=h,\ldots,s$ для некоторого $\ell\geqslant 1$, все внешние коды V_i имеют одинаковую длину n_v, все внутренние коды U_i имеют одни

и те же параметры $(n_u, p^{s\ell}, d_u)_p$, и когда $\chi_i = 0$ для всех $i = h, \ldots, s$, параметры n, $N = p^k$ и d_L кода C принимают следующий вид:

$$n = n_v n_u, \quad k = s\ell \sum_{i=h}^{s} (n_v + 1 - d_{v,i}) \tag{9}$$

и

$$d_L = d_u \min\bigl\{p^{i-1} d_{v,i} : \ i = h, \ldots, s\bigr\}. \tag{10}$$

Таким образом, имеет место следующая

Теорема 8. *Пусть $q = p^s$ – произвольная степень простого числа p, и пусть m, d_L – натуральные числа, причем m – любое, а d_L – такое, что имеется число h в диапазоне $1 \leqslant h \leqslant s-1$, для которого справедливо неравенство* (5), *не справедливое при этом для $h-1$. Тогда теорема* 1 *гарантирует построение указанным выше способом (n, k, d_L)-кода C над $\mathbb{F}_q$ с параметрами, удовлетворяющими соотношениям* (9), (10).

Чтобы написать явные выражения для параметров q, n, d_L и $N = p^k$, нужно выбрать конкретный внутренний код U. Как показывают приводимые ниже примеры кодов, удобно использовать код с проверкой на четность, т.е. код U с параметрами $n_u = s\ell + 1$, $N_u = p^{s\ell}$ и $d_u = 2$. Для этого очень частного (вообще говоря, не всегда оптимального) выбора кода U справедливо

Следствие 3. *Пусть $q = p^s$ – произвольная степень простого числа p, а числа n, d_L и h удовлетворяют условиям теоремы* 8. *Тогда теорема* 1 *гарантирует, что (n, N, d_L)-код C над $\mathbb{F}_q$, построенный указанным выше способом, имеет следующие параметры*:

$$N = q^k = p^{sk}, \quad \text{где} \quad k \geqslant n\frac{2(s-h+1)}{2s+1} - d_L \frac{p^{s-h}-1}{(p-1)p^{s-1}}. \tag{11}$$

Доказательство. Из (9), учитывая, что $n = n_v(\ell s+1)$ и $d_L = d_{v,1} d_{u,1} = 2d_{v,1}$, имеем

$$\begin{aligned} k &= \ell \sum_{i=h}^{s} (n_v + 1 - d_{v,i}) = \ell \sum_{i=h}^{s} \left(n_v + 1 - \left\lceil \frac{d_{v,1}}{p^{i-1}} \right\rceil \right) \geqslant \ell \sum_{i=h}^{s} \left(n_v - \frac{d_{v,1}}{p^{i-1}} \right) = \\ &= \ell(s-h+1)n_v - \frac{\ell d_{v,1}}{p^{s-1}} \frac{(p^{s-h}-1)}{p-1} = \ell(s-h+1)\frac{n}{\ell s+1} - \frac{\ell d_{v,1}}{p^{s-1}} \frac{(p^{s-h}-1)}{p-1} = \\ &= n\frac{\ell(s-h+1)}{\ell s+1} - \frac{d_L}{2} \frac{\ell(p^{s-h}-1)}{(p-1)p^{s-1}}. \end{aligned}$$

Результирующий код C над $\mathbb{F}_q$ имеет минимальное расстояние

$$d_L = 2 \min \left\{ p^{i-1} \left\lceil \frac{d_{v,1}}{p^{i-1}} \right\rceil : \ i = 1, \ldots, s \right\} = 2d_{v,1}.$$

Получаем следующее выражение для k, которое зависит от выбора ℓ:

$$k \geqslant \max \left\{ n\frac{\ell(s-h+1)}{\ell s+1} - d_L \frac{\ell(p^{s-h}-1)}{2(p-1)p^{s-1}} : \ \ell \geqslant 1 \right\}. \quad \blacktriangle \tag{12}$$

§ 6. Сравнения с каскадными кодами

Как упоминалось, Астола [5] предложил каскадную конструкцию для кодов в метрике Ли, в которой он использовал известные идеи Юстесена для построения

Таблица 1

$(n_a, k_a, d_a)_q$ [5]	$(n_a, k, d)_q$ (теорема 8)	ℓ	h	$A_i(n, k_i, d_i)_p$	$V_i(n_{v,i}, k_{v,i}, d_{v,i})_{q^\ell}$	$U_i(n_{u,i}, k_{u,i}, d_{u,i})_p$
$(48, 2, 80)_{5^2}$	$(48, 2, 200)_{5^2}$	1	2	$A_2(48, 2, 40)_5$		
$(48, 2, 80)_{5^2}$	$(48, 21, 80)_{5^2}$	1	2	$A_2(48, 21, 16)_5$		
$(48, 4, 70)_{5^2}$	$(48, 4, 180)_{5^2}$	2	2	$A_2(48, 4, 36)_5$		
$(48, 4, 70)_{5^2}$	$(48, 24, 75)_{5^2}$	2	2	$A_2(48, 24, 15)_5$		
$(48, 8, 54)_{5^2}$	$(48, 8, 150)_{5^2}$	2	2	$A_2(48, 8, 30)_5$		
$(48, 8, 54)_{5^2}$	$(48, 28, 55)_{5^2}$	2	2	$A_2(48, 28, 11)_5$		
$(2496, 62, 2696)_{5^2}$	$(2496, 63, 6040)_{5^2}$	3	2	$A_2(2496, 63, 1208)_5$	$V_2(624, 21, 604)_{5^6}$	$U_2(4, 3, 2)_5$
$(2496, 62, 2696)_{5^2}$	$(2496, 474, 2700)_{5^2}$	2	2	$A_2(2496, 948, 540)_5$	$V_2(416, 237, 180)_{5^4}$	$U_2(6, 4, 3)_5$
$(2496, 124, 2510)_{5^2}$	$(2496, 126, 5830)_{5^2}$	3	2	$A_2(2496, 126, 1166)_5$	$V_2(624, 42, 583)_{5^6}$	$U_2(4, 3, 2)_5$
$(2496, 124, 2510)_{5^2}$	$(2496, 498, 2520)_{5^2}$	2	2	$A_2(2496, 996, 504)_5$	$V_2(416, 249, 168)_{5^4}$	$U_2(6, 4, 3)_5$
$(160, 4, 412)_{3^4}$	$(160, 4, 2268)_{3^4}$	1	4	$A_4(160, 4, 84)_3$		
$(160, 4, 412)_{3^4}$	$(160, 161/4, 414)_{3^4}$	1 1 1	2 2 2	$A_2(160, 1, 160)_3$ $A_3(160, 49, 46)_3$ $A_4(160, 111, 16)_3$		
$(160, 20, 300)_{3^4}$	$(160, 20, 864)_{3^4}$	1 1	3 3	$A_3(160, 10, 96)_3$ $A_4(160, 70, 33)_3$		
$(160, 20, 300)_{3^4}$	$(160, 201/4, 306)_{3^4}$	1 1 1	2 2 2	$A_2(160, 7, 102)_3$ $A_3(160, 69, 34)_3$ $A_4(160, 125, 12)_3$		
$(160, 40, 174)_{3^4}$	$(160, 40, 405)_{3^4}$	1 1 1	2 2 2	$A_2(160, 1, 480)_3$ $A_3(160, 45, 48)_3$ $A_4(160, 114, 15)_3$		
$(160, 40, 174)_{3^4}$	$(160, 275/4, 174)_{3^4}$	1 1 1	2 2 2	$A_2(160, 36, 58)_3$ $A_3(160, 99, 20)_3$ $A_4(160, 140, 7)_3$		
$(26240, 656, 49810)_{3^4}$	$(26240, 656, 212706)_{3^4}$	2	4	$A_4(26240, 2624, 7878)_3$	$V_4(1640, 328, 1313)_{3^8}$	$U_4(16, 8, 6)_3$
$(26240, 656, 49810)_{3^4}$	$(26240, 11045/2, 49815)_{3^4}$	2 2	3 3	$A_3(26250, 6142, 5535)_3$ $A_4(26244, 15348, 1846)_3$	$V_3(1875, 769, 1107)_{3^8}$ $V_4(2916, 1994, 923)_{3^8}$	$U_3(14, 8, 5)_3$ $U_4(9, 8, 2)_3$

Таблица 1 (продолжение)

$(n_a, k_a, d_a)_q$ [3]	$(n_a, k, d)_q$ (теорема 8)	ℓ	h	$A_i(n, k_i, d_i)_p$	$V_i(n_{v,i}, k_{v,i}, d_{v,i})_{q^\ell}$	$U_i(n_{u,i}, k_{u,i}, d_{u,i})_p$
$(26240, 5248, 28154)_{3^4}$	$(26240, 5250, 43304)_{3^4}$	2	3	$A_3(26244, 4080, 4812)_3$	$V_3(2916, 510, 2406)_{3^8}$	$U_3(9, 8, 2)_3$
		2	3	$A_4(26244, 16920, 1604)_3$	$V_4(2916, 2115, 802)_{3^8}$	$U_4(9, 8, 2)_3$
$(26240, 5248, 28154)_{3^4}$	$(26240, 8032, 28157)_{3^4}$	2	2	$A_2(26240, 2160, 9387)_3$	$V_2(1312, 270, 1043)_{3^8}$	$U_3(20, 8, 9)_3$
		2	2	$A_3(26244, 10812, 3130)_3$	$V_3(2916, 1352, 1565)_{3^8}$	$U_3(9, 8, 2)_3$
		2	2	$A_4(26244, 19156, 1044)_3$	$V_4(2916, 2395, 522)_{3^8}$	$U_4(9, 8, 2)_3$
$(484, 12, 1942)_{3^5}$	$(484, 12, 6318)_{3^5}$	2	5	$A_5(484, 60, 78)_3$	$V_5(44, 6, 39)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 12, 1942)_{3^5}$	$(484, 84, 1942)_{3^5}$	2	5	$A_3(495, 20, 224)_3$	$V_3(9, 2, 8)_{3^{10}}$	$U_3(55, 10, 28)_3$
		2	5	$A_4(486, 160, 72)_3$	$V_4(27, 16, 12)_{3^{10}}$	$U_4(18, 10, 6)_3$
		2	5	$A_5(486, 240, 24)_3$	$V_5(27, 24, 4)_{3^{10}}$	$U_5(18, 10, 6)_3$
$(484, 60, 1394)_{3^5}$	$(484, 60, 2430)_{3^5}$	2	5	$A_5(484, 300, 30)_3$	$V_5(44, 30, 15)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 60, 1394)_{3^5}$	$(484, 591/5, 1404)_{3^5}$	2	2	$A_2(484, 1, 484)_3$		
		2	2	$A_3(484, 40, 168)_3$	$V_3(11, 4, 8)_{3^{10}}$	$U_3(44, 10, 21)_3$
		2	2	$A_4(484, 190, 52)_3$	$V_4(44, 19, 26)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	2	$A_5(484, 360, 18)_3$	$V_5(44, 36, 9)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 120, 796)_{3^5}$	$(484, 120, 1188)_{3^5}$	2	4	$A_4(484, 230, 44)_3$	$V_4(44, 23, 22)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(484, 370, 16)_3$	$V_5(44, 37, 8)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 120, 796)_{3^5}$	$(484, 851/5, 798)_{3^5}$	2	2	$A_2(484, 16, 270)_3$		
		2	2	$A_3(486, 130, 90)_3$	$V_3(27, 13, 15)_{3^{10}}$	$U_3(18, 10, 6)_3$
		2	2	$A_4(484, 300, 30)_3$	$V_4(44, 30, 15)_{3^{10}}$	$U_4(11, 10, 2)_3$
		3	2	$A_5(496, 405, 10)_3$	$V_5(31, 27, 5)_{3^{15}}$	$U_5(16, 15, 2)_3$
$(236192, 5904, 768402)_{3^5}$	$(236192, 5904, 3000402)_{3^5}$	2	5	$A_5(236192, 29520, 37042)_3$	$V_5(21472, 2952, 18521)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(236192, 5904, 768402)_{3^5}$	$(236192, 49923, 768442)_{3^5}$	2	3	$A_3(236192, 12500, 85383)_3$	$V_3(10736, 1250, 9487)_{3^{10}}$	$U_3(22, 10, 9)_3$
		2	3	$A_4(236197, 86830, 28461)_3$	$V_4(18169, 8683, 9487)_{3^{10}}$	$U_4(13, 10, 3)_3$
		2	3	$A_5(236192, 150285, 9488)_3$	$V_5(14762, 10019, 4744)_{3^{15}}$	$U_5(16, 15, 2)_3$
$(236192, 59046, 344430)_{3^5}$	$(236192, 59046, 543618)_{3^5}$	2	4	$A_4(236192, 29520, 37042)_3$	$V_4(21472, 2952, 18521)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(236192, 181170, 6712)_3$	$V_5(21472, 18117, 3356)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(236192, 59046, 344430)_{3^5}$	$(236192, 411856/5, 344462)_{3^5}$	2	4	$A_2(236192, 16, 114810)_3$		
		2	4	$A_3(236196, 67440, 38274)_3$	$V_3(13122, 6744, 6379)_{3^{10}}$	$U_3(18, 10, 6)_3$
		2	4	$A_4(236192, 150940, 12758)_3$	$V_4(21472, 15094, 6379)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(236192, 193460, 4254)_3$	$V_5(21472, 19346, 2127)_{3^{10}}$	$U_5(11, 10, 2)_3$

каскадных кодов в метрике Хэмминга. Кроме того, Астола привел в [5] таблицу параметров каскадных кодов в метрике Ли для значений $q \in \{25, 81, 243\}$. Коды были построены каскадным способом на основе известной конструкции Юстесена (см. ссылки в [5]). В табл. 1 приведены параметры кодов из [5], а также параметры кодов, построенных с помощью теоремы 8. Для построения внешних кодов A_i использовались либо коды с наилучшими известными параметрами [18], либо коды A_i, построенные простой каскадной конструкцией из внешних кодов V_i с параметрами $(n_{v,i}, N_{v,i}, d_{v,i})_{q^\ell}$ и внутренних кодов U_i с параметрами $(n_{u,i}, k_{u,i}, d_{u,i})_p$. Под простой каскадной конструкцией на основе $(n_v, N_v, d_v)_{q_v}$-кода V и $(n_u, N_u, d_u)_{q_u}$-кода U понимается замена в каждом слове кода V каждого символа алфавита кода V на слово кода U, которое поставлено ему во взаимно-однозначное соответствие. В результате получается новый код A над алфавитом кода U мощности $N = N_v$ и длины $n = n_v n_u$ с минимальным расстоянием (Хэмминга) $d \geqslant d_v d_u$. В табл. 1 для построения внешних кодов A_i в основном использовались МДР-коды и коды из [18]. Для каждого кода Астолы [5] с параметрами $(n_a, N_a = q^{k_a}, d_a)_q$ мы строим два кода: код с параметрами $(n_a, k_a, d)_q$, фиксируя k_a при заданном n_a, и код с параметрами $(n_a, k, d_a)_q$, фиксируя d_a при заданном n_a. Для всех новых кодов приведены все внешние коды A_i, а также коды V_i и U_i, на основе которых строятся эти коды A_i. В случаях, когда $n_v n_u$ больше, чем нужное нам n, мы используем общеизвестные методы укорочения кодов: выбрасывание лишних позиций (уменьшая n и d) или укорочение фиксированием символов выбранных позиций (уменьшая n и k). Если результирующий код C над $\mathbb{F}_{p^s}$ имеет мощность $N = p^k$, где k не делится на s, то для удобства сравнения с кодами из [5] в табл. 1 используются дробные числа k/s для числа информационных символов кода C.

СПИСОК ЛИТЕРАТУРЫ

1. *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.
2. *Berlekamp E.R.* Negacyclic Codes for the Lee Metric // Proc. Conf. on Combinatorial Mathematics and Its Applications. Chapel Hill, NC. Apr. 10–14, 1967. Chapel Hill: Univ. of North Carolina Press, 1968. Ch. 17. P. 298–316. Reprinted in: *Berlekamp E.R.* Algebraic Coding Theory. Rev. Ed. Singapore: World Sci., 2015. Ch. 9. P. 207–217. https://doi.org/10.1142/9789814635905_0009
3. *Chiang J.C., Wolf J.K.* On Channels and Codes for the Lee Metric // Inform. Control. 1971. V. 19. № 2. P. 159–174. https://doi.org/10.1016/S0019-9958(71)90791-1
4. *Мазур Л.Е.* Коды, исправляющие ошибки большого веса в метрике Ли // Пробл. передачи информ. 1973. Т. 9. № 4. С. 11–16. http://mi.mathnet.ru/ppi917
5. *Astola J.* Concatenated Codes for the Lee Metric // IEEE Trans. Inform. Theory. 1982. V. 28. № 5. P. 778–779. https://doi.org/10.1109/TIT.1982.1056550
6. *Racsmány A.* On Constructing Codes with Given Distance in Lee-Metric // Probl. Control Inform. Theory. 1986. V. 15. № 5. P. 377–384.
7. *Давыдов В.А.* Коды, исправляющие ошибки в модульной метрике, метрике Ли и ошибки оператора // Пробл. передачи информ. 1993. Т. 29. № 3. С. 10–20. http://mi.mathnet.ru/ppi184
8. *Давыдов В.А.* О применении модульной метрики к решению задачи декодирования по минимуму евклидового расстояния // Пробл. передачи информ. 2019. Т. 55. № 2. С. 50–57. https://doi.org/10.1134/S0134347519020037
9. *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
10. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670

11. *Dumer I., Zinoviev V., Zyablov V.* Concatenated Decoding According to Minimal Generalized Distance // Probl. Control Inform. Theory. 1981. V. 10. № 1. P. 3–19.
12. *Зиновьев В.А., Зяблов В.В.* Исправление пакетов ошибок и независимых ошибок обобщенными каскадными кодами // Пробл. передачи информ. 1979. Т. 15. № 2. С. 58–70. http://mi.mathnet.ru/ppi1488
13. *Зиновьев В.А., Зяблов В.В.* Коды с неравной защитой информационных символов // Пробл. передачи информ. 1979. Т. 15. № 3. С. 50–60. http://mi.mathnet.ru/ppi1499
14. *Hammons A.R., 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
15. *Krotov D.S.* Z_4-Linear Hadamard and Extended Perfect Codes // Electron. Notes Discrete Math. 2001. V. 6. P. 107–112. https://doi.org/10.1016/S1571-0653(04)00161-1
16. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
17. *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
18. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available online at http://www.codetables.de (accessed on Oct. 9, 2018).

Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
28.12.2019
После доработки
10.02.2021
Принята к публикации
10.02.2021