ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 2**

УДК 621.291 : 519.725

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

КОНСТРУКЦИИ И ИНВАРИАНТЫ ОПТИМАЛЬНЫХ КОДОВ В МЕТРИКЕ ЛИ[1]

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

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

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

§ 1. Введение

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

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

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

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

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

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

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

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

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

§ 2. Обозначения, определения и основные свойства

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Аналогичные рассуждения имеют место и для ядра кода C. ▲

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 3. Каскадная конструкция совершенного кода в декартовом произведении графов

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

M является кодом с минимальным расстоянием 2; (1)

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

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

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

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

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

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

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

Рассмотрим несколько случаев.

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

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

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

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

§ 4. Каскадная конструкция совершенного кода в метрике Ли

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Таким образом, в коде D имеется

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

кодовых слов.

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

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

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

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

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

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

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

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

$$\begin{pmatrix}\frac{q}{p_{j_0}} & \frac{2q}{p_{j_0}} & \dots & \frac{(p_{j_0}-1)q}{2p_{j_0}}\end{pmatrix},$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство. Мощность кода C^λ равна

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

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

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

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

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

Имеем следующее равенство:

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

Рассмотрим два случая.

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

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

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

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

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

для метрики Ли в случае, когда

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

Имеем следующие оценки:

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

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

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

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

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

параметрами приведена в примере в конце статьи) получим не менее

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

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

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

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

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

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

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

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

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

Таким образом, получаем следующее утверждение.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

СПИСОК ЛИТЕРАТУРЫ

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

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

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

Поступила в редакцию
07.06.2023
После доработки
20.10.2023
Принята к публикации
23.10.2023