ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 2022 Вып. 3

УДК 621.391.1 : 519.725

 Ф.И. Соловьева

РАЗБИЕНИЯ НА СОВЕРШЕННЫЕ КОДЫ В МЕТРИКАХ ХЭММИНГА И ЛИ[1]

Предложены новые комбинаторные конструкции разбиений на совершенные коды в метриках Хэмминга и Ли. Кроме того, приведен новый комбинаторный метод построения диаметральных совершенных кодов в метрике Ли, который развит для построения разбиений на такие коды. Для метрики Ли улучшены известные нижние оценки числа совершенных и диаметральных совершенных кодов Ли, предложенные Этционом в 2011 г.

Ключевые слова: совершенный код, совершенный код в метрике Хэмминга, совершенный код в метрике Ли, диаметральный совершенный код в метрике Ли, разбиения, разбиения на совершенные коды.

DOI: 10.31857/S0555292322030056, **EDN:** EAJWAD

§ 1. Введение

Целью данной статьи является развитие новых комбинаторных методов построения разбиений на совершенные коды в метриках Хэмминга и Ли, а также конструкций диаметральных совершенных кодов Ли и разбиений на такие коды. Оказалось, что идеи некоторых подходов для построения совершенных q-ичных кодов, $q \geqslant 2$, в метрике Хэмминга могут быть развиты для построения кодов и разбиений на совершенные коды Ли и диаметральные совершенные коды Ли. Приведенные конструкции позволяют существенно улучшить известные нижние оценки числа совершенных и диаметральных совершенных кодов Ли, предложенные Этционом в 2011 г. (см. [1]).

В отличие от метрики Хэмминга, для которой получено большое число различных свитчинговых и каскадных методов построения совершенных кодов и разбиений, для построения кодов и разбиений в метрике Ли предложено лишь незначительное число конструкций. Мотивация исследования совершенных и диаметральных совершенных кодов Ли и основательный обзор полученных по данной тематике результатов могут быть найдены в работе [1], где представлены две конструкции совершенных и диаметральных совершенных кодов Ли, и поэтому они не приводятся в настоящей статье. Алгебраические методы построения совершенных и диаметральных совершенных кодов Ли см. также в работах [2, 3]. Гипотеза о несуществовании совершенных кодов, исправляющих две ошибки, была выдвинута в 1970 г. в работе [4]. О совершенных кодах Ли, исправляющих две ошибки, см. также в [5]; о существовании и некоторых необходимых условиях для квазисовершенных кодов в метрике Ли см. [6].

Упор в данной статье сделан на построение разбиений, поскольку этот вопрос оставался недостаточно глубоко изученным как для метрики Ли, так и для метрики Хэмминга. Кроме того, это дает возможность строить коды, используя эти

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

разбиения, что позволило получить новые нижние оценки числа совершенных и диаметральных совершенных кодов Ли. Отметим также, что все конструкции кодов и разбиений в данной статье являются комбинаторными, что может представлять интерес с практической точки зрения.

Статья имеет следующую структуру: в § 2 приводятся необходимые определения и понятия, § 3 посвящен построению разбиений на совершенные коды над полем Галуа $\mathbb{F}_q$, $q > 2$. В § 4 приведена конструкция построения разбиений на совершенные коды Ли, идейно восходящая к подходу, использованному для построения разбиений в § 3. В § 5 предложены новые диаметральные совершенные коды Ли и разбиения на такие коды. В каждом из последних трех параграфов приводятся нижние оценки числа кодов и разбиений и сравнение их с полученными ранее нижними оценками.

§ 2. Совершенные и диаметральные совершенные коды в метрике Ли

Векторное пространство размерности n над полем Галуа $\mathbb{F}_q$ по отношению к метрике Хэмминга обозначается через $\mathbb{F}_q^n$. Основные определения, касающиеся кодов в метрике Хэмминга, см. в [7].

В данном параграфе приведем необходимые определения и понятия для метрики Ли. Сначала рассмотрим определения для совершенных кодов Ли, затем для диаметральных совершенных кодов Ли.

Через $\mathbb{Z}_s^n$ обозначим множество слов длины n над кольцом вычетов $\mathbb{Z}_s$ по модулю s. *Вес Ли* $w_L(x)$ слова x из множества слов $\mathbb{Z}_s^n$ определяется как сумма весов Ли его координатных позиций. *Расстояние Ли*, обозначаемое через $d_L(x, y)$, для произвольных слов $x, y \in \mathbb{Z}_s^n$ определяется как

$$d_L(x, y) = \sum_{i=1}^{n} \min(|x_i - y_i|, s - |x_i - y_i|).$$

В настоящей статье рассматриваются совершенные коды Ли с минимальным расстоянием Ли $d_L = 3$. Такой код длины n над кольцом вычетов $\mathbb{Z}_s$ имеет мощность $s^n/(2n+1)$, где $2n+1$ – размер сферы Ли радиуса 1, а $s \geqslant 2n+1$. Код в $\mathbb{Z}_s^n$ *линеен*, если он образует подгруппу кольца $\mathbb{Z}_s^n$. Линейный совершенный код Ли длины n с минимальным расстоянием 3 над кольцом вычетов $\mathbb{Z}_s$ существует согласно [2] тогда и только тогда, когда $\tau \,|\, s$, где τ равно произведению всех простых делителей числа $2n+1$. При этом наименьшее s, для которого существует совершенный код Ли с минимальным расстоянием 3 над $\mathbb{Z}_s$, равно τ. В случаях $s = 2$ и $s = 3$ метрика Ли совпадает с метрикой Хэмминга для двоичных и троичных кодов, что неверно при $s > 3$.

Как и совершенные коды в метрике Хэмминга, совершенные коды в метрике Ли с минимальным расстоянием 3 разбивают множество слов $\mathbb{Z}_s^n$ на смежные классы посредством сдвигов на слова веса Ли, равного единице.

В случае диаметральных совершенных кодов Ли важным является понятие антикода, как и для диаметральных совершенных кодов в метриках Хэмминга, Джонсона и Грассмана (см. [8, 9]). Антикод с максимальным расстоянием $d-1$ (подмножество слов A в $\mathbb{Z}_s^n$, таких что $d_L(x, y) < d$, где $x, y \in A$), удовлетворяет неравенству Дельсарта [8]

$$|C||A| \leqslant s^n,$$

здесь C – код с минимальным расстоянием d в $\mathbb{Z}_s^n$. Если оценка в неравенстве Дельсарта точна, то C называется *диаметральным совершенным кодом Ли*. В статье рассматриваются диаметральные совершенные коды Ли только с $d_L = 4$, объем такого кода равен $|C| = s^n/4n$, где $4n$ – размер антикода. Пусть

$$n = 2^i p_1^{i_1} \dots p_k^{i_k}$$

– разложение числа n в произведение степеней простых сомножителей, где $p_r > 2$, $r = 1, \dots, k$, и может быть, $i = 0$. Тогда согласно [3, теорема 13] линейный диаметральный совершенный код Ли длины n с минимальным расстоянием 4 существует над кольцом $\mathbb{Z}_s$ тогда и только тогда, когда

$$s = 2^{i'} p_1^{i'_1} \dots p_k^{i'_k}, \quad \text{где } 2 \leqslant i' \leqslant i+2 \text{ и } 1 \leqslant i'_r \leqslant i_r.$$

Наименьшее s, для которого существует диаметральный совершенный код Ли длины n с минимальным расстоянием 4 над $\mathbb{Z}_s$, равно 4τ, где $\tau = p_1 \dots p_k$, т.е. s четно. Длина кода не обязательно равна степени числа 2.

Аналогично расширенным совершенным кодам в метрике Хэмминга диаметральные совершенные коды Ли разбивают множество слов четного и нечетного весов в $\mathbb{Z}_s^n$ на смежные классы. Существенная разница между двоичными совершенными кодами в метрике Хэмминга и диаметральными совершенными кодами Ли состоит в следующем. Произвольный двоичный совершенный код в метрике Хэмминга можно расширить посредством общей проверки на четность, в результате чего получится диаметральный совершенный код (и наоборот при выкалывании последнего). При этом минимальное расстояние кода увеличится на единицу. Подобная процедура в случае диаметральных совершенных кодов Ли невозможна.

Для q-ичных совершенных кодов, $q > 2$, задача о расширении кодов с минимальным расстоянием 3 до кодов с расстоянием 4 все еще остается нерешенной. Беспалов в [10] доказал несуществование q-ичных расширенных совершенных кодов в метрике Хэмминга в случаях, когда $q = 3$, 4, а $n > q+2$, или оба числа n и q нечетны, а также доказал несуществование нелинейных МДР-кодов с параметрами $(q+2, q^{q-1}, 4)_q$ в случае, когда q нечетно.

§ 3. Разбиения $\mathbb{F}_q^n$ на совершенные коды

В этом параграфе рассмотрим коды в метрике Хэмминга и применение конструкции Думера [11] для построения разбиений на q-ичные совершенные коды в $\mathbb{F}_q^n$, $q > 2$.

Пусть $P_1 = \{C_1, C_2, \dots, C_{q^r}\}$ – произвольное разбиение на q-ичные совершенные коды в $\mathbb{F}_q^n$, $q > 2$, с параметрами $(n, q^{n-r}, 3)_q$, где $n = \dfrac{q^r-1}{q-1}$. Пусть D – произвольный q^r-ичный совершенный код в $\mathbb{F}_{q^r}^\ell$, $q > 2$, где

$$\ell = \frac{q^{rs}-1}{q^r-1}, \quad |D| = q^{r(\ell-s)},$$

т.е. код, имеющий параметры $(\ell, q^{r(\ell-s)}, 3)_{q^r}$. Множество векторов

$$C = \bigcup_{(x_1,x_2,\dots,x_\ell)\in D} C_{x_1} \times C_{x_2} \times \dots \times C_{x_\ell} \tag{1}$$

является q-ичным совершенным кодом, имеющим параметры $(n\ell, |D||C_1|^\ell, 3)_q$, где длина кода равна $n\ell = \dfrac{q^{rs}-1}{q-1}$. Эта каскадная конструкция является спецификацией обобщенной каскадной конструкции Зиновьева [12] для q-ичных кодов, а также непосредственным обобщением каскадной конструкции для двоичных совершенных кодов из [13,14]. Заметим, что автор работы [1] (см. теорему 10 в ней) ошибочно полагает, что эта конструкция является новой. В отличие от оригинальной конструкции

Думера [11], где рассматривается разбиение на классы смежности совершенного кода C_1, в (1) используются произвольные разбиения на q-ичные совершенные коды в $\mathbb{F}_q^n$, $q > 2$.

Кроме того, к кодам C_{x_i}, $i \in \{1, 2, \ldots, \ell\}$, где $x = (x_1, x_2, \ldots, x_\ell) \in D$, можно применить произвольные ℓ подстановок π_t, $t \in \{1, 2, \ldots, \ell\}$, на алфавите кода D, т.е. на $\mathbb{F}_{q^r}$. Пусть $C_{\pi(x_i)}$ – результат действия подстановки π на коде C_{x_i}. Без ограничения общности первую подстановку можно положить тождественной, т.е. $C_{\pi_1(x_1)} = C_{x_1}$. В этом случае конструкция (1) преобразуется в следующую:

$$C = \bigcup_{x=(x_1,x_2,\ldots,x_\ell)\in D} C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)}. \qquad (2)$$

Перейдем к построению разбиений посредством конструкции (2). Для этой цели рассмотрим помимо произвольного разбиения P_1, введенного выше, произвольное разбиение $P_2 = \{D_1, D_2, \ldots, D_{q^{rs}}\}$ на q^r-ичные совершенные коды D_i длины ℓ, $i \in \{1, 2, \ldots, q^{rs}\}$. Для построения кодов C_i^* применим конструкцию (2) к кодам D_i и разбиению P_1, а именно

$$C_i^* = \bigcup_{x=(x_1,x_2,\ldots,x_\ell)\in D_i} C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)}, \quad i = 1, 2, \ldots, q^{rs}. \qquad (3)$$

Теорема 1. *Совокупность кодов* (3) *образует разбиение пространства* $\mathbb{F}_q^{n\ell}$, $q > 2$, *на q-ичные совершенные коды длины $n\ell$, где* $n\ell = \dfrac{q^{rs} - 1}{q - 1}$.

Доказательство. Число совершенных кодов длины $n\ell$ в разбиении пространства $\mathbb{F}_q^{n\ell}$ на совершенные коды должно быть равно q^{rs}, что совпадает с числом кодов, построенных в (3). Убедимся, что $C_i^* \cap C_j^* = \varnothing$, где

$$C_j^* = \bigcup_{(x_1,x_2,\ldots,x_\ell)\in D_j} C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)},$$

$i \neq j$, $i, j \in \{1, 2, \ldots, q^{rs}\}$. Поскольку D_i и D_j являются элементами разбиения P_2, то $D_i \cap D_j = \varnothing$. Отсюда $x \neq x'$ для любых x, x', таких что $x \in D_i$, $x' \in D_j$. Следовательно, найдется $k \in \{1, 2, \ldots, \ell\}$, такое что $x_k \neq x'_k$, откуда

$$C_{x_k} \cap C_{x'_k} = \varnothing \quad \text{и} \quad C_{\pi_k(x_k)} \cap C_{\pi_k(x'_k)} = \varnothing.$$

А значит, выполняется

$$C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)} \cap C_{x'_1} \times C_{\pi_2(x'_2)} \times \ldots \times C_{\pi_\ell(x'_\ell)} = \varnothing,$$

и как следствие, имеем $C_i^* \cap C_j^* = \varnothing$ для любых i, j из множества $\{1, 2, \ldots, q^{rs}\}$, где $i \neq j$. ▲

Пусть $M_{n,q}^H$ и $\widetilde{M}_{\ell,q}^H$ обозначают числа различных разбиений на q- и q^r-ичные совершенные коды длины n и ℓ соответственно, где верхний индекс H указывает, что разбиения рассматриваются в метрике Хэмминга. Число подстановок π_t в силу произвольности их выбора равно $(\ell - 1)!$. Из конструкции разбиений, приведенной в теореме 1, легко найти нижнюю оценку числа таких разбиений.

Следствие 1. *Число различных разбиений пространства $\mathbb{F}_q^{n\ell}$ на совершенные коды, полученных конструкцией* (3), *не меньше*

$$M_{n\ell,q}^H \geqslant M_{n,q}^H \widetilde{M}_{\ell,q}^H (\ell - 1)!. \qquad (4)$$

В работе [15] была представлена наилучшая дважды экспоненциальная нижняя оценка числа различных разбиений на q-ичные, $q > 2$, совершенные коды длины

$$N = (q^m - 1)/(q^m - 1), \quad q = p^m, \quad m > 1.$$

Конструкция основана на свитчинговом методе так называемых простых i-компонент кода Хэмминга, с использованием латинских квадратов. Было показано, что число различных разбиений пространства $\mathbb{F}_q^N$ на q-ичные совершенные коды при $p \to \infty$ не меньше, чем

$$p^{p^{n(2m-1)+m+1}(1-o(1))}. \tag{5}$$

Множитель в нижней оценке числа различных разбиений, который дают подстановки π_t в конструкции (2), всего лишь экспоненциальный, поскольку

$$(\ell - 1)^{\ell-1+\frac{1}{2}} e^{-\ell+1} \leqslant (\ell - 1)! \leqslant (\ell - 1)^{\ell-1+\frac{1}{2}} e^{-\ell+2}.$$

Отсюда и из того факта, что с ростом r величина q^r растет существенно быстрее, чем q, величина $M^H_{\ell,q}$ больше, чем $M^H_{n,q}(\ell - 1)!$. Таким образом, имеем

$$\widetilde{M}^H_{n\ell,q} > M^H_{n,q}(\ell - 1)!.$$

Очевидно, что оценка (4) с использованием (5) для $\widetilde{M}^H_{\ell,q}$ является дважды экспоненциальной по числу $\ell m r$, где ℓ – длина q^r-ичных кодов в разбиении P_2, $q = p^m$. Однако, как нетрудно убедиться, она уступает оценке из [15], которая по-прежнему является лучшей на сегодняшний день.

§ 4. Разбиения на совершенные коды Ли

Построение разбиений на совершенные коды Ли основано на конструкции Этциона для совершенных кодов Ли из [1]. Для полноты изложения приведем этот метод построения кодов. Он в свою очередь основан на конструкции (2), благодаря чему легко проследить связь результатов настоящего параграфа с результатами, приведенными в § 3.

Пусть $P_1 = \{C_1, C_2, \ldots, C_{q^r}\}$ – произвольное разбиение множества слов $\mathbb{Z}^n_{\tau(2n+1)}$ на совершенные коды Ли длины $n = \dfrac{q^r - 1}{2}$ над алфавитом из $\tau(2n + 1)$ символов, где q нечетно и равно p^m, $m > 2$. Напомним, что здесь $q^r = 2n + 1$ – размер шара Ли радиуса 1 в $\mathbb{Z}^n_{\tau(2n+1)}$, где τ равно произведению всех простых делителей числа $2n + 1$, т.е. $\tau = p$. Минимальное расстояние кода C_i равно 3, а его мощность

$$|C_i| = (\tau(2n + 1))^n/(2n + 1).$$

Пусть D – произвольный q^r-ичный совершенный код в $\mathbb{F}^\ell_{q^r}$, $q > 2$, где

$$\ell = \frac{q^{rs} - 1}{q^r - 1}, \quad |D| = q^{r(\ell - s)},$$

т.е. D имеет параметры $(\ell, q^{r(\ell-s)}, 3)_{q^r}$. Подчеркнем, что здесь код D рассматривается в метрике Хэмминга.

Пусть $x = (x_1, x_2, \ldots, x_\ell)$ – произвольное кодовое слово кода D. К кодам C_{x_i}, $i \in \{1, 2, \ldots, \ell\}$, применим произвольные ℓ подстановок π_t на множестве $\{1, 2, \ldots, q^r\}$, где $t \in \{1, 2, \ldots, \ell\}$. Пусть π_t являются подстановками на элементах алфавита кода D. Таким образом, имеем ℓ подстановок, первую из которых без ограничения общности полагаем тождественной, т.е. $C_{\pi_1(x_1)} = C_{x_1}$. Множество слов

$$C = \bigcup_{x=(x_1,x_2,\ldots,x_\ell)\in D} C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)} \tag{6}$$

является совершенным кодом Ли в алфавите из $\tau(2n+1)$ символов, имеющим мощность

$$|C| = (\tau(2n+1))^{n\ell}/(2n\ell+1) \tag{7}$$

и длину $n\ell$. В отличии от конструкции Этциона [1], где P_1 является разбиением лишь на сдвиги совершенного кода Ли C_1, для построения кода C в (6) были взяты более широкие классы разбиений $\mathbb{Z}^n_{\tau(2n+1)}$ на совершенные коды Ли. Ниже убедимся, что такие нетривиальные разбиения существуют.

Разбиения на совершенные коды Ли построим, в свою очередь, с помощью конструкции (6). Рассмотрим помимо разбиения P_1, упомянутого выше, любое разбиение

$$P_2 = \{D_1, D_2, \ldots, D_{q^{rs}}\}$$

пространства $\mathbb{F}^\ell_{q^r}$ на q^r-ичные совершенные коды D_i длины ℓ, $i \in \{1,2,\ldots,q^{rs}\}$. Для построения кодов C_i^*, $i \in \{1,2,\ldots,q^{rs}\}$, применим конструкцию (6) к кодам D_i и разбиению P_1:

$$C_i^* = \bigcup_{x=(x_1,x_2,\ldots,x_\ell)\in D_i} C_{x_1} \times C_{\pi_2(x_2)} \times \ldots \times C_{\pi_\ell(x_\ell)}, \quad i = 1,2,\ldots,q^{rs}. \tag{8}$$

Т е о р е м а 2. *Совокупность кодов* (8) *образует разбиение множества* $\mathbb{Z}^{n\ell}_{\tau(2n+1)}$ *на совершенные коды Ли длины* $n\ell = (q^{rs}-1)/2$ *над алфавитом из* $\tau(2n+1)$ *символов.*

Д о к а з а т е л ь с т в о. Согласно [1, теорема 14] все коды C_i^*, $i \in \{1,2,\ldots,q^{rs}\}$, являются совершенными кодами Ли длины $n\ell = (q^{rs}-1)/2$. По построению число таких кодов в каждом разбиении равно q^{rs}. Следовательно, с учетом (7) и того, что $2n\ell+1 = q^{rs}$, имеем

$$|C_i^*|q^{rs} = \frac{\tau^{n\ell}(2n+1)^{n\ell}}{2n\ell+1}q^{rs} = \tau^{n\ell}(2n+1)^{n\ell} = \left|\mathbb{Z}^{n\ell}_{\tau(2n+1)}\right|,$$

что соответствует необходимому числу совершенных кодов Ли в разбиении множества $\mathbb{Z}^{n\ell}_{\tau(2n+1)}$.

Доказательство того факта, что любые два кода C_i^* и C_j^*, где $i \neq j$, не пересекаются, идентично факту непересечения аналогичных кодов в метрике Хэмминга (см. теорему 1), и поэтому опущено. ▲

Пусть $M^L_{n,q}$ обозначает число различных разбиений длины n на совершенные коды Ли. Подчеркнем, что верхний индекс L указывает на то, что разбиения рассматриваются в метрике Ли. Из конструкции разбиений (8) получаем нижнюю оценку числа разбиений на совершенные коды Ли, аналогичную полученной для q-ичных совершенных кодов в $\mathbb{F}^{n\ell}_q$ (см. следствие 1).

С л е д с т в и е 2. *Для числа различных разбиений множества* $\mathbb{Z}^{n\ell}_{\tau(2n+1)}$ *на совершенные коды Ли длины* $n\ell$, *полученных конструкцией* (8), *справедлива оценка снизу*

$$M^L_{n\ell,q} \geqslant M^L_{n,q}\widetilde{M}^H_{\ell,q}((q^r)!)^{\ell-1}. \tag{9}$$

Поскольку второй сомножитель $\widetilde{M}^H_{\ell,q}$, $q = p^m$, в (9) отражает число разбиений на q^r-ичные совершенные коды длины ℓ в метрике Хэмминга, которое является дважды экспоненциальным от числа ℓmr (см. конец § 3 настоящей статьи), то и результирующая оценка для разбиений на совершенные коды в метрике Ли является дважды экспоненциальной от числа ℓmr. Подставляя ее в конструкцию (6) для совершенных кодов Ли, получаем число различных совершенных кодов Ли, большее чем в [1], где при оценке числа различных совершенных кодов Ли рассматриваются только тривиальные разбиения на совершенные коды Ли. Поскольку оценка Этциона явно представлена не была (см. [1, раздел V]), уточним ее. Она имеет вид

$$N^L_{n\ell,q} \geqslant N^H_{\ell,q}((q^r)!)^{\ell-1}, \tag{10}$$

где $N^L_{n\ell,q}$ и $N^H_{\ell,q}$ обозначают число различных совершенных кодов Ли и совершенных кодов в $\mathbb{F}^\ell_{q^r}$ в метрике Хэмминга длин $n\ell$ и ℓ соответственно.

Используя для построения совершенных кодов Ли конструкцию (6), получаем оценку снизу

$$N^L_{n\ell,q} \geqslant M^L_{n,q} N^H_{\ell,q}((q^r)!)^{\ell-1},$$

что существенно больше оценки Этциона (10) в силу дважды экспоненциальной оценки от числа nm в (9), вычисленной для $M^L_{n,q}$ – числа различных разбиений длины n на совершенные коды Ли.

§ 5. Построение диаметральных совершенных кодов Ли и разбиений

Настоящий параграф посвящен построению диаметральных совершенных кодов Ли и разбиений на такие коды. Сначала рассмотрим построение кодов, а затем на их основе разовьем конструкцию разбиений. Конструкция диаметральных совершенных кодов Ли основана на идее каскадной конструкции Фелпса 1984 г. для двоичных расширенных совершенных кодов (см. [16]). Отметим, что конструкция из [16] является частным случаем обобщенной каскадной конструкции [12]. При построении разбиений используется предложенная конструкция диаметральных совершенных кодов Ли и подход, развитый в работе [17].

5.1. Построение диаметральных совершенных кодов Ли. Пусть $C^0_1, C^0_2, \ldots, C^0_{2r}$ и $C^1_1, C^1_2, \ldots, C^1_{2r}$ – произвольные разбиения множеств четно- и нечетновесовых слов в множестве слов $\mathbb{Z}^r_s$ на диаметральные совершенные коды Ли длины r с минимальным расстоянием $d_L = 4$ над кольцом $\mathbb{Z}_s$, где s четно. Пусть C^m – произвольный расширенный двоичный совершенный код длины $m = 2^p$ в $\mathbb{F}^m_2$ с минимальным расстоянием $d_H = 4$. Далее код C^m будем называть *базовым кодом.* Для каждого вектора μ из C^m рассмотрим $2r$-ичный МДР-код C_μ с минимальным расстоянием Хэмминга 2 длины m и мощности

$$|C_\mu| = (2r)^{m-1}$$

над алфавитом из $2r$ символов. Отметим, что как и в конструкции из § 3, в данной конструкции для построения диаметральных совершенных кодов используются коды над различными алфавитами и метриками.

Т е о р е м а 3. *Множество*

$$\mathcal{C} = \bigcup_{\mu\in C^m} \bigcup_{j\in C_\mu} C^{\mu_1}_{j_1} \times C^{\mu_2}_{j_2} \times \ldots \times C^{\mu_m}_{j_m} \tag{11}$$

является диаметральным совершенным кодом Ли длины $n = mr$ над кольцом $\mathbb{Z}_s$.

Доказательство. Очевидно, что длина кода $\mathcal{C}$ равна $n = mr$. Также, с учетом того, что мощности входящих в построение кодов равны

$$|C_{j_i}^{\mu_i}| = \frac{s^r}{4r}, \quad |C_\mu| = (2r)^{m-1}, \quad |C^m| = 2^{m-\log m-1},$$

несложно вычислить мощность кода:

$$|\mathcal{C}| = |(C_{j_i}^{\mu_i})|^m |C_\mu||C^m| = \left(\frac{s^r}{4r}\right)^m (2r)^{m-1} 2^{m-\log m-1} = \frac{s^n}{4n}.$$

Убедимся, что минимальное расстояние Ли в коде $\mathcal{C}$ равно 4.

По построению для двух различных кодовых слов u и u' кода $\mathcal{C}$, таких что $\mu = \mu'$ и $j = j'$, выполняется неравенство $d_L(u, u') \geqslant 4$.

Докажем, что для любых $\mu, \mu' \in C^m$, $j, j' \in C_\mu$, таких что пары (μ, μ') и (j, j') различны, выполняется

$$d_L\big(C_{j_1}^{\mu_1} \times \ldots \times C_{j_m}^{\mu_m}, C_{j'_1}^{\mu'_1} \times \ldots \times C_{j'_m}^{\mu'_m}\big) \geqslant 4. \tag{12}$$

Возможны следующие случаи.

1. Пусть $\mu = \mu'$, $j \neq j'$.

Тогда $d_H(j, j') \geqslant 2$, и найдутся координаты a, b, такие что $j_a \neq j'_a$, $j_b \neq j'_b$. Отсюда, учитывая, что $C_{j_a}^{\mu_a}$ и $C_{j'_a}^{\mu_a}$ одновременно являются четно- или нечетновесовыми диаметральными совершенными кодами Ли (аналогичное верно для кодов $C_{j_b}^{\mu_b}$ и $C_{j'_b}^{\mu_b}$), имеем $d_L(C_{j_a}^{\mu_a}, C_{j'_a}^{\mu_a}) \geqslant 2$ и $d_L(C_{j_b}^{\mu_t}, C_{j'_b}^{\mu_b}) \geqslant 2$. Следовательно,

$$d_L\big(C_{j_1}^{\mu_1} \times \ldots \times C_{j_a}^{\mu_a} \times C_{j_b}^{\mu_b} \times \ldots \times C_{j_m}^{\mu_m}, C_{j'_1}^{\mu_1} \times \ldots \times C_{j'_a}^{\mu_a} \times C_{j'_b}^{\mu_b} \times \ldots \times C_{j'_m}^{\mu_m}\big) \geqslant 4.$$

2. Пусть $\mu \neq \mu'$.

Векторы μ и μ' принадлежат базовому коду C^m, т.е. $d_H(\mu, \mu') \geqslant 4$, и найдутся четыре координаты a, b, a' и b', в которых различаются μ и μ'. Следовательно, имеются четыре пары диаметральных совершенных кодов Ли $C_{j_i}^{\mu_i}$ и $C_{j'_i}^{\mu'_i}$, $i \in \{a, b, a', b'\}$, удовлетворяющие

$$d_L\big(C_{j_i}^{\mu_i}, C_{j'_i}^{\mu'_i}\big) \geqslant 1.$$

Отсюда справедливо (12), и как следствие, минимальное расстояние Ли диаметрального совершенного кода $\mathcal{C}$ длины n равно 4. ▲

Обозначим через $N_{n,s}^L$, $\widetilde{D}_{r,s}^L$, N_m^H и R_m^H, соответственно, число различных диаметральных совершенных кодов Ли длины n над $\mathbb{Z}_s$, разбиений на диаметральные совершенные коды Ли длины r над $\mathbb{Z}_s$, число различных двоичных совершенных кодов и число различных МДР-кодов с кодовым расстоянием 2 длины m; здесь верхние индексы L и H указывают на метрики Ли и Хэмминга. Из конструкции диаметральных кодов, приведенной выше, получаем следующую нижнюю оценку числа диаметральных совершенных кодов Ли.

Следствие 3. *Для числа различных диаметральных совершенных кодов Ли длины n, полученных конструкцией* (11), *справедлива оценка снизу*

$$N_{n,s}^L \geqslant \widetilde{D}_{r,s}^L N_m^H R_m^H. \tag{13}$$

Как второй N_m^H, так и третий R_m^H сомножители в (13) являются дважды экспоненциальными от чисел $m/2$ и $r \log_2(m-2)$ в силу [18] и [19] соответственно. Следовательно, эта нижняя оценка существенно лучше нижней оценки числа различных диаметральных кодов Этциона длины $2^{t-1}n$ в [1], которая имеет вид

$$\prod_{i=1}^{t}(2^i\frac{n}{2}-1)!^{2^{t-i}} \tag{14}$$

и, как несложно убедиться, не превосходит

$$2^t\cdot 2^{n2^{t-1}\log_2\frac{n}{2}}.$$

Оценку (13) можно дополнительно усилить, используя широкие классы разбиений $\widetilde{D}^L_{2r,s}$, построение которых рассмотрим ниже.

5.2. Построение разбиений на диаметральные совершенные коды Ли. Пусть $C^0_{i,1}$, $C^0_{i,2},\dots,C^0_{i,2r}$ и $C^1_{i,1},C^1_{i,2},\dots,C^1_{i,2r}$, $i=1,\dots,m$, – произвольные разбиения множеств четно- и нечетновесовых слов в множестве $\mathbb{Z}^r_s$ на диаметральные совершенные коды Ли длины r с минимальным расстоянием $d_L=4$ над алфавитом $\mathbb{Z}_s$, где s четно. Как и выше, в этой конструкции будут рассмотрены коды в разных алфавитах.

Рассмотрим два разбиения множеств четно- и нечетновесовых слов в пространстве $\mathbb{F}^m$, $m=2^p$, на смежные классы базового двоичного расширенного совершенного кода C^m длины m с минимальным расстоянием $d_H=4$:

$$C^0_i=C^m+e_i+e_m,\quad C^1_i=C^m+e_i,\quad i=1,2,\dots,m;$$

здесь все кодовые слова кода C^0_i имеют четный вес, а кодовые слова C^1_i – нечетный. Для каждого вектора μ из C^m возьмем $2r$-ичный МДР-код C_μ с кодовым расстоянием 2 длины m и мощности $|C_\mu|=(2r)^{m-1}$ над алфавитом из $2r$ символов.

Кроме того, для каждого вектора μ из базового кода C^m рассмотрим латинский квадрат L_μ порядка $2r$, k-я строка которого равна

$$\left(\ell^\mu_{k,1},\ell^\mu_{k,2},\dots,\ell^\mu_{k,2r}\right),\quad k=1,2,\dots,2r.$$

Латинские квадраты и МДР-коды могут быть взяты как различными, так и совпадающими. Определим коды над $\mathbb{Z}_s$ длины $n=mr$ следующим образом:

$$\mathcal{C}_{i,k}=\bigcup_{\mu\in C^0_i}\bigcup_{j\in C_\mu}C^{\mu_1}_{i,j_1}\times\dots\times C^{\mu_{m-1}}_{i,j_{m-1}}\times C^{\mu_m}_{i,\ell^\mu_{k,j_m}},\quad i=1,2,\dots,m,\quad k=1,2,\dots,2r, \tag{15}$$

$$\mathcal{D}_{i,k}=\bigcup_{\mu\in C^1_i}\bigcup_{j\in C_\mu}C^{\mu_1}_{i,j_1}\times\dots\times C^{\mu_{m-1}}_{i,j_{m-1}}\times C^{\mu_m}_{i,\ell^\mu_{k,j_m}},\quad i=1,2,\dots,m,\quad k=1,2,\dots,2r. \tag{16}$$

Идея конструкции, описанной в (15) и (16), перекликается с одним из методов построения разбиений на двоичные расширенные совершенные коды из [17].

Теорема 4. *Совокупность кодов $\mathcal{C}_{i,k}$ и $\mathcal{D}_{i,k}$, где $i=1,2,\dots,m$, $k=1,2,\dots,2r$, из (15), (16) образует разбиение множества $\mathbb{Z}^n_s$, $n=mr$, на диаметральные совершенные коды Ли длины n над алфавитом $\mathbb{Z}_s$.*

Доказательство. Согласно теореме 3 все коды $\mathcal{C}_{i,k}$ и $\mathcal{D}_{i,k}$, $i=1,2,\dots,m$, $k=1,2,\dots,2r$, являются диаметральными совершенными кодами Ли над алфавитом $\mathbb{Z}_s$, имеющими длину $n=mr$. По построению число таких кодов в разбиении равно $4mr$. Следовательно,

$$|\mathcal{C}_{i,k}| \cdot 4mr = \frac{s^n}{4mr} \cdot 4mr = s^n = |\mathbb{Z}_s^n|,$$

что соответствует необходимому числу диаметральных совершенных кодов Ли в разбиении множества $\mathbb{Z}_s^n$.

Очевидно, что четновесовые коды $\mathcal{C}_{i,k}$ и нечетновесовые $\mathcal{D}_{i',k'}$ не пересекаются. Докажем, что любые два кода $\mathcal{C}_{i,k}$ и $\mathcal{C}_{i',k'}$, где $(i,k) \neq (i',k')$, не пересекаются.

Возможны следующие случаи.

1. Пусть $i \neq i'$. Помимо кода $\mathcal{C}_{i,k}$ рассмотрим код $\mathcal{C}_{i',k}$, где

$$\mathcal{C}_{i',k} = \bigcup_{\mu' \in C_{i'}^0} \ \bigcup_{j' \in C_{\mu'}} C_{i'j_1'}^{\mu_1'} \times \ldots \times C_{i',j_{m-1}'}^{\mu'_{m-1}} \times C_{i',\ell_{k,j_m'}^{\mu'}}^{\mu_m'}.$$

Так как $i \neq i'$, то $C_i^0 \neq C_{i'}^0$. Отсюда в силу того, что оба кода C_i^0 и $C_{i'}^0$ четновесовые, получаем, что существуют $\mu \in C_i^0$ и $\mu' \in C_{i'}^0$, такие что

$$d_H(\mu, \mu') = d_H\big((\mu_1, \ldots, \mu_m), (\mu_1', \ldots, \mu_m')\big) \equiv 0 \pmod 2,$$

т.е. $d_H(\mu, \mu') \geqslant 2$. Значит, найдутся по крайней две координаты a и b, в которых различаются слова μ и μ', т.е. $\mu_a \neq \mu_a'$, $\mu_b \neq \mu_b'$. Следовательно, имеются две пары диаметральных совершенных кодов Ли $(C_{i,j_a}^{\mu_a}, C_{i',j_a'}^{\mu_a'})$ и $(C_{i,j_b}^{\mu_b}, C_{i',j_b'}^{\mu_b'})$, такие что

$$d_L\big(C_{i,j_a}^{\mu_a}, C_{i',j_a'}^{\mu_a'}\big) \geqslant 1 \quad \text{и} \quad d_L\big(C_{i,j_b}^{\mu_b}, C_{i',j_b'}^{\mu_b'}\big) \geqslant 1.$$

Как следствие, имеем

$$\mathcal{C}_{i,k} \cap \mathcal{C}_{i',k} = \varnothing.$$

2. Пусть $i = i'$ и $k \neq k'$. Пусть

$$\mathcal{C}_{i,k'} = \bigcup_{\mu' \in C_i^0} \ \bigcup_{j' \in C_{\mu'}} C_{ij_1'}^{\mu_1'} \times \ldots \times C_{i,j_{m-1}'}^{\mu'_{m-1}} \times C_{i,\ell_{k',j_m'}^{\mu'}}^{\mu_m'}.$$

При $\mu \neq \mu'$ рассуждения идентичны проведенным в случае 1.

Пусть $\mu = \mu'$ и пересечение кодов $\mathcal{C}_{i,k}$ и $\mathcal{C}_{i,k'}$ непусто. В этом случае найдутся два вектора j и j' в МДР-коде C_μ, такие что они совпадают в первых $m-1$ координатных позициях и выполняется

$$\ell_{k,j_m}^{\mu} = \ell_{k',j_m'}^{\mu}. \tag{17}$$

Так как код C_μ имеет минимальное расстояние 2, то это возможно, только если $j_m = j_m'$. Отсюда и из (17) с учетом того, что L_μ – латинский квадрат, имеем $k = k'$, т.е. $\mathcal{C}_{i,k} = \mathcal{C}_{i,k'}$, противоречие.

Для нечетновесовых кодов $\mathcal{D}_{i,k}$, $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, 2r$, доказательство аналогично, поэтому оно опущено. Как следствие, получаем разбиение множества слов $\mathbb{Z}_s^n$, $n = mr$, на диаметральные совершенные коды Ли длины n. ▲

Оценим снизу число $\widetilde{D}_{r,s}^L$ разбиений множества слов $\mathbb{Z}_s^r$, $r = m'r'$, на диаметральные совершенные коды Ли длины r. Пусть $\widetilde{D}_{r',s}^L$, $N_{m'}^H$, $R_{m'}^H$ и $N_{2r,\mathrm{Lat}}$ – соответственно, число различных разбиений $\mathbb{Z}_s^{r'}$ на диаметральные совершенные коды Ли длины r' над $\mathbb{Z}_s$, число различных двоичных расширенных совершенных кодов длины m', различных МДР-кодов с кодовым расстоянием 2 длины m' и различных латинских квадратов порядка $2r$. Здесь, как и ранее, верхние индексы L и H указывают на принадлежность к метрикам Ли и Хэмминга. Из конструкции теоремы 4 имеем следующую нижнюю оценку числа разбиений множества слов $\mathbb{Z}_s^r$, $r = m'r'$, на диаметральные совершенные коды Ли длины r.

С л е д с т в и е 4. *Для числа разбиений множества слов* $\mathbb{Z}_s^r$, $r = m'r'$, *на диаметральные совершенные коды Ли длины* r *справедлива оценка снизу*

$$\widetilde{D}_{r,s}^L \geqslant \left(\widetilde{D}_{r',s}^L\right)^{2m'} N_{m'}^H \left(R_{m'}^H N_{2r,\mathrm{Lat}}\right)^{2|C^{m'}|}. \tag{18}$$

Все сомножители в оценке (18) можно оценить снизу, как и в предыдущих параграфах, что, очевидно, при подстановке $\widetilde{D}_{r,s}^L$ в формулу (13) еще больше усиливает нижнюю оценку числа $N_{n,s}^L$ диаметральных совершенных кодов Ли длины $n = mr$ по сравнению с оценкой, предложенной Этционом в [1].

СПИСОК ЛИТЕРАТУРЫ

1. *Etzion T.* Product Construction for Perfect Lee Codes // IEEE Trans. Inform. Theory. 1994. V. 57. № 11. P. 7473–7481. https://doi.org/10.1109/TIT.2011.2161133
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. *Horak P., AlBdaiwi B.* Diameter Perfect Lee Codes // IEEE Trans. Inform. Theory. 2012. V. 58. № 8. P. 5490–5499. https://doi.org/10.1109/TIT.2012.2196257
4. *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
5. *Kim D.* Nonexistence of Perfect 2-Error-Correcting Lee Codes in Certain Dimensions // European J. Combin. 2017. V. 63. P. 1–5. https://doi.org/10.1016/j.ejc.2017.01.007
6. *Mesnager S., Tang C., Qi Y.* 2-Correcting Lee Codes: (Quasi)-Perfect Spectral Conditions and Some Constructions // IEEE Trans. Inform. Theory. 2018. V. 64. № 4. P. 3031–3041. https://doi.org/10.1109/TIT.2018.2789921
7. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
8. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10 (97 pp.).
9. *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
10. *Bespalov E.* On the Non-existence of Extended 1-Perfect Codes and MDS Codes // J. Combin. Theory Ser. A. 2022. V. 189. Article ID 105607 (11 pp.). https://doi.org/10.1016/j.jcta.2022.105607
11. *Cohen G., Honkala I., Listyn S., Lobstein A.* Covering Codes. Amsterdam: Elsevier, 1997.
12. *Zinoviev V.A.* On Generalized Concatenated Codes // Topics in Information Theory (Proc. 2nd Colloq. on Information Theory. Keszthely, Hungary. August 25–29, 1975). Colloq. Math. Soc. János Bolyai. V. 16. Amsterdam: North-Holland, 1977. P. 587–592.
13. *Зиновьев В.А.* Комбинаторные методы построения и анализа нелинейных корректирующих кодов: Дисс. ... докт. ф.-м.н.: 01.01.09. М., 1987.
14. *Соловьева Ф.И.* Класс двоичных плотно упакованных кодов, порождаемых q-ичными кодами // Методы дискретного анализа в изучении булевых функций и графов. Вып. 48. Новосибирск: Ин-т матем. СО АН СССР, 1989. С. 70–72.
15. *Соловьева Ф.И., Лось А.В.* О построении разбиений F_q^N на совершенные q-значные коды // Дискретн. анализ и исслед. опер. 2009. V. 16. № 3. P. 63–73. http://mi.mathnet.ru/da574

16. *Phelps K.T.* A General Product Construction for Error Correcting Codes // SIAM J. Algebr. Discrete Methods. 1984. V. 5. № 2. P. 224–228. https://doi.org/10.1137/0605023
17. *Avgustinovich S.V., Lobstein A.C., Soloveva F.I.* Intersection Matrices for Partitions by Binary Perfect Codes // IEEE Trans. Inform. Theory. 2001. V. 47. № 4. P. 1621–1624. https://doi.org/10.1109/18.923749
18. *Krotov D.S., Avgustinovich S.V.* On the Number of 1-Perfect Binary Codes: A Lower Bound // IEEE Trans. Inform. Theory. 2008. V. 54. № 4. P. 1760–1765. https://doi.org/10.1109/TIT.2008.917692
19. *Потапов В.Н., Кротов Д.С.* О числе n-арных квазигрупп конечного порядка // Дискретная математика. 2012. Т. 24. № 1. С. 60–69. https://doi.org/10.4213/dm1172

Соловьева Фаина Ивановна
(15.08.1952 – 09.08.2022)

Поступила в редакцию
06.06.2022
После доработки
06.06.2022
Принята к публикации
24.08.2022