ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2019. Т. 26, № 4. С. 5–15

УДК 519.725 DOI 10.33048/daio.2019.26.669

МАКСИМАЛЬНОЕ ПЕРЕСЕЧЕНИЕ ЛИНЕЙНЫХ И ЭКВИВАЛЕНТНЫХ ИМ КОДОВ *)

С. В. Августинович[1,2,a], *Е. В. Горкунов*[1,2,b]

[1] Институт математики им. С. Л. Соболева,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия

[2] Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия

E-mail: [a] avgust@math.nsc.ru, [b] gorkunov@math.nsc.ru

Аннотация. Рассматриваются линейные коды в пространстве над конечным полем, наделённом метрикой Хэмминга. Код, являющийся образом линейного кода под действием изометрического преобразования пространства, называется псевдолинейным. Получена достижимая при $q \geqslant 3$ верхняя граница $(q-2)M/q$ для мощности пересечения двух различных псевдолинейных кодов одинаковой мощности M. Библиогр. 10.

Ключевые слова: линейный код, псевдолинейный код, МДР-код, пересечение кодов, эквивалентный код, изометрия, изотопия, конечное поле.

Введение

Рассмотрим n-мерное линейное пространство $V = \mathbb{F}^n$ над конечным полем $\mathbb{F} = GF(q)$ и его координатное представление в стандартном базисе $\{e_i\}_{i=1}^n$. Произвольное подмножество $C \subseteq V$ будем называть *кодом* длины n. Код, образующий подпространство в V, называется *линейным*. Элементы кода называются *кодовыми словами*.

Напомним, что расстояние Хэмминга $d(x, y)$ между векторами $x, y \in V$ полагается равным количеству координат, в которых различаются x и y, а число $w(x) = d(0, x)$ называется *весом* вектора $x \in V$. Минимальное ненулевое расстояние $d(C)$ между кодовыми словами кода $C \in V$ называется *кодовым расстоянием* C. Стоит отметить, что кодовое расстояние

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 19–01–00682) и Программы фундаментальных научных исследований СО РАН № I.5.1 (проект № 0314–2019–0016).

линейного кода совпадает с минимальным ненулевым весом его кодовых слов.

Известно (см., например, [1]), что группа изометрий метрического пространства Хэмминга исчерпывается композициями преобразований двух видов. Первое преобразование — произвольная перестановка мест координат каждого вектора. Формально действие перестановки $\pi \in S_n$ на произвольном векторе $x = (x_1, x_2, \ldots, x_n) \in V$ определяется таким образом:

$$\pi(x) = \sum_{i=1}^{n} x_i e_{\pi(i)} = \sum_{i=1}^{n} x_{\pi^{-1}(i)} e_i. \tag{1}$$

Второй вид изометрий пространства V строится на основе перестановок из симметрической группы S_q, действующей на элементах поля $\mathbb{F}$. Пусть $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in S_q^n$ — набор таких перестановок. Преобразование $\sigma\colon V \to V$, заданное по правилу

$$\sigma(x) = (\sigma_1(x_1), \sigma_2(x_2), \ldots, \sigma_n(x_n))$$

для произвольного вектора $x \in V$, является изометрией пространства V. Изометрию такого вида будем называть *изотопией*.

Таким образом, изометрия пространства V представима парой $(\pi; \sigma)$, образованной перестановкой $\pi \in S_n$ и изотопией $\sigma \in S_q^n$. Композиция двух изометрий $(\pi; \sigma)$ и $(\pi'; \sigma')$ выполняется по правилу

$$(\pi; \sigma)(\pi'; \sigma') = (\pi\pi'; \pi'(\sigma)\sigma'),$$

где действие перестановки π' на изотопию $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ аналогично действию перестановки порядка n на вектор длины n. Иначе говоря, перестановка π' меняет местами перестановки σ_i, $i = 1, 2, \ldots, n$, в наборе σ.

Два кода *эквивалентны,* если один из них может быть преобразован в другой некоторой изометрией пространства V. При этом если изометрия является перестановкой координат, то коды *изоморфны,* а если изотопией, то *изотопны.* Код, изотопный линейному, назовём *псевдолинейным.*

Отметим, что код, эквивалентный линейному, также является псевдолинейным. Действительно, легко проверить непосредственно, что преобразование (1) пространства V линейно. Поэтому если коды $C, C' \subseteq V$ эквивалентны и $C' = (\pi; \sigma)C$ для некоторой изометрии $(\pi; \sigma)$, то код C' изотопен линейному коду $\pi(C)$, получающемуся из C под действием перестановки π.

Далее в разд. 1 обратим внимание в целом на задачу о пересечениях в комбинаторике и связанные с ней вопросы, сформулируем основной результат статьи. В разд. 2 приступим к доказательству теоремы и сведём его к рассмотрению частного случая, касающегося МДР-кодов. Окончательно оценку на мощность пересечения двух равномощных псевдолинейных кодов установим в разд. 3.

1. Задачи о пересечении и восстановлении кодов

Задачи о пересечении комбинаторных объектов, таких как коды, схемы, носители функций, графы, латинские квадраты, групповые таблицы и многие другие, широко распространены и привлекают пристальное внимание исследователей. Этому есть несколько объяснений. Наиболее простое состоит в том, что зачастую подобные задачи естественным образом возникают при решении более общих проблем.

Вместе с тем информация о пересечении кодов (или других объектов) проясняет вопрос о степени их отличия друг от друга в силу очевидной связи пересечения и симметрической разности. При этом мощность симметрической разности может служить для измерения расстояния между объектами. Таким образом, рассматривая класс объектов в качестве «кода» и исследуя пересечения его представителей, можно судить о «кодовом» расстоянии внутри этого класса.

Опять же в силу упомянутой связи поиск максимального пересечения можно заменить поиском минимальной симметрической разности. Точнее, в такой постановке вопроса принято говорить о минимальной компоненте. Для двух объектов C_1 и C_2 некоторого класса под компонентой понимается одна из непересекающихся частей $C_1 \setminus C_2$ и $C_2 \setminus C_1$ их симметрической разности. Замена компоненты в рассматриваемом объекте её альтернативой позволяет строить новые объекты того же класса. Например, из C_1 получаем C_2.

Наконец, задача о максимальном пересечении может быть переформулирована в виде задачи о восстановлении, и наоборот. Например, пусть мощность пересечения двух кодов некоторого класса не может превосходить числа M. Это эквивалентно тому, что произвольный код в рамках этого класса однозначно определяется любым своим подмножеством мощности $M+1$ и более.

В работе [2] исследованы спектры возможных размерностей для пересечений изоморфных линейных кодов. Вопрос о пересечении совершенных кодов поставлен в [3] (совершенный код имеет ровно одну вершину в любом шаре радиуса 1 пространства V). В [4] рассмотрены спектры мощностей компонент или пересечений корреляционно-иммунных функций, бент-функций, совершенных раскрасок и совершенных кодов. Там же содержится хороший обзор литературы по этой теме.

Знания о пересечении линейных кодов и их смежных классов применены к построению разбиений пространства V на неэквивалентные совершенные коды в [5] и аффинно неэквивалентные — в [6]. В этой статье рассмотрим линейные и эквивалентные им коды и найдём максимально возможную мощность их пересечений.

В случае $q \in \{2, 3\}$ произвольная изотопия пространства V представима композицией умножения на подходящую невырожденную диагональную $(n \times n)$-матрицу D и сдвига на некоторый вектор $x \in V$, т. е. $\sigma(V) = x + VD$. Таким образом, двоичные и троичные псевдолинейные коды суть не что иное, как смежные классы линейных кодов, поэтому вопрос об их пересечениях разрешается тривиально. Смежные классы различных линейных кодов $C_1, C_2 \in V$ либо не пересекаются, либо имеют пересечение, мощность которого совпадает с мощностью подпространства $C_1 \cap C_2$. Последнее, вообще говоря, справедливо для пространства над любым конечным полем.

Всюду далее полагаем $q \geqslant 4$. Рассмотрим линейный код $C \leqslant V$ с кодовым расстоянием не меньше 2 и подействуем, например, на первую координату кодовых слов транспозицией (01). Образ кода C при таком отображении обозначим через C'. Поскольку код C линейный, для каждого элемента $a \in \mathbb{F}$ в коде содержится одинаковое количество кодовых слов со значением первой координаты, равным a, поэтому $|C \cap C'| = \frac{q-2}{q}|C|$.

Оказывается, что число в правой части полученного равенства отражает максимальную мощность пересечения двух различных псевдолинейных кодов одинаковой мощности. Причём это справедливо как для эквивалентных кодов, так и для тех, которые не являются таковыми.

Теорема 1. *Для различных псевдолинейных кодов $C_1, C_2 \subseteq V$ одинаковой мощности имеет место неравенство*

$$|C_1 \cap C_2| \leqslant \frac{q-2}{q}|C_1|.$$

Доказательство теоремы 1 является основной целью статьи.

2. Сведе́ние к МДР-кодам

Для фиксированных элементов $a_1, a_2, \ldots, a_r \in \mathbb{F}$ и индексов $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, n\}$ множество векторов $\Gamma = \{y \in V \mid y_{i_j} = a_j,\ j = 1, 2, \ldots, r\}$ называется *гранью* размерности $k = n - r$ в пространстве V. Грань размерности $n - 1$ называется *гипергранью*. Грань размерности 1 будем называть *линией*, а номер её свободной координаты — *направлением* линии.

Лемма 1. *Пересечение $C \cap \Gamma$ псевдолинейного кода $C \subseteq V$ с гранью $\Gamma \subseteq V$ представляет собой псевдолинейный код.*

Лемма 2. *Произвольный псевдолинейный код $C \subseteq V$ в любой линии пространства V имеет* 0, 1 *или q кодовых слов. Если некоторая линия содержит q кодовых слов кода C, то для любой линии L этого направления либо $L \cap C = \varnothing$, либо $L \subseteq C$.*

Если для некоторого $i \in \{1, 2, \ldots, n\}$ псевдолинейный код C вместе с каждым кодовым словом $x \in C$ содержит всю линию направления i, проходящую через x, то будем называть i-ю координату *фиктивной* для кода C. Следующие утверждения очевидны.

Утверждение 1. *Координата с номером $i \in \{1, 2, \ldots, n\}$ фиктивна для псевдолинейного кода C тогда и только тогда, когда линейный код, являющийся прообразом C, содержит вектор стандартного базиса e_i.*

Утверждение 2. *Координата с номером $i \in \{1, 2, \ldots, n\}$ фиктивна для псевдолинейного кода C тогда и только тогда, когда некоторая пара кодовых слов кода C лежит в одной линии направления i.*

Имея целью доказательство основной теоремы от противного, рассмотрим пару псевдолинейных кодов наименьшей длины n, для которых теорема не выполняется. Будем говорить, что эти коды образуют *минимальный контрпример.* Положим $\alpha = \frac{q-2}{q}$, так что если псевдолинейные коды $C_1, C_2 \subset V$ образуют контрпример к утверждению теоремы 1, то $|C_1 \cap C_2| > \alpha |C_1|$. Далее установим некоторые свойства кодов минимального контрпримера.

Лемма 3. *Псевдолинейные коды, образующие минимальный контрпример, не имеют фиктивных координат.*

Доказательство. Пусть коды $C_1, C_2 \subset V$ образуют минимальный контрпример и i-я координата фиктивна для C_1, $i \in \{1, 2, \ldots, n\}$. Последнее означает, что для любой линии направления i код C_1 либо не пересекается с этой линией, либо содержит её полностью. Тем самым код C_1 разбивается на линии i-го направления.

Положим $M = C_1 \cap C_2$. Поскольку $|M| > \alpha |C_1|$, найдётся линия L направления i такая, что $|M \cap L| > \alpha |L| = q - 2 \geqslant 2$. Отсюда следует, что в L содержится не менее трёх кодовых слов кода C_2 и координата с номером i фиктивна для C_2.

Удалим фиктивную i-ю координату из кодов C_1, C_2. В результате получим коды меньшей длины, образующие контрпример, что противоречит минимальности исходного контрпримера. Лемма 3 доказана.

Для кода $C \subseteq V$ с кодовым расстоянием d известна граница Синглтона (см., например, [7]), согласно которой $\log_q |C| \leqslant n - d + 1$. Отметим, что в случае линейного кода $\log_q |C| = \dim C$. Код, достигающий границы Синглтона, называется МДР-*кодом.* Следующая лемма сводит поиск контрпримера к теореме 1 к рассмотрению МДР-кодов.

Лемма 4. *Псевдолинейные коды, образующие минимальный контрпример, являются* МДР-*кодами с кодовым расстоянием* 2.

Доказательство. Вновь рассмотрим коды $C_1, C_2 \subset V$, образующие минимальный контрпример, и выберем кодовое слово $x \in C_1 \setminus C_2$. Пусть найдётся линия L, проходящая через x и не содержащая кодовых слов кода C_2. Если L имеет направление i, то удалим координату с номером i в кодах C_1, C_2. В результате получим контрпример с кодами меньшей длины.

Действительно, так как коды C_1, C_2 не содержат фиктивных координат, удаление любой из них сохраняет мощность кодов. Вместе с тем мощность их пересечения может только увеличиться. Поэтому в результате получатся коды меньшей длины, образующие контрпример, что противоречит минимальности исходного контрпримера. Это означает, что в любой линии, проходящей через вектор x, содержится ровно одно кодовое слово кода C_2.

Из проведённых рассуждений следует, что в линейном прообразе C кода C_2 имеется $n-1$ линейно независимых векторов. С другой стороны, $C_2 \neq V$, так что $\dim C = n-1$. Из границы Синглтона получаем, что $d(C) \leqslant n - \dim C + 1 = 2$. В то же время в коде C отсутствуют фиктивные координаты, поэтому $d(C) \geqslant 2$. Таким образом, коды C, C_1 и C_2 имеют мощность q^{n-1}, кодовое расстояние 2 и достигают границы Синглтона, т. е. являются МДР-кодами. Лемма 4 доказана.

3. Максимальное пересечение МДР-кодов

В этом разделе покажем, что теорема 1 выполняется для МДР-кодов с кодовым расстоянием 2, и тем самым получим её полное доказательство. Всюду кодовое расстояние обсуждаемых кодов подразумевается равным 2, если не оговорено иное. Линейный МДР-код длины n имеет размерность $n-1$. Любой такой код подходящей изотопией пространства V можно отобразить в код

$$C_0 = \{x \in V \mid x_n = x_1 + x_2 + \cdots + x_{n-1}\}. \qquad (2)$$

Таким образом, все псевдолинейные МДР-коды длины n с кодовым расстоянием 2 изотопны коду C_0.

В случае $n = 3$ код C_0 принимает вид $C_0 = \{(x_1, x_2, x_3) \in V \mid x_3 = x_1 + x_2\}$, и его можно представить в виде таблицы Кэли аддитивной группы поля $\mathbb{F}$. Эта таблица представляет собой $(q \times q)$-таблицу, строки и столбцы которой индексированы элементами поля $\mathbb{F}$, а на пересечении строки $a \in \mathbb{F}$ и столбца $b \in \mathbb{F}$ находится элемент $a + b$.

Ввиду этого существенной является работа [8], в которой исследуется минимально возможное количество отличий между двумя групповыми таблицами. Под групповой таблицей понимается любая таблица, полученная из таблицы Кэли некоторой группы произвольными перестановками строк, столбцов и элементов группы.

Теорема 2 [8, теорема 1]. *Две различные групповые таблицы произвольных групп порядка q отличаются друг от друга минимум в $2q$ позициях. Исключением являются пары групп $\left(\mathbb{Z}_2^2, \mathbb{Z}_4\right)$, $(\mathbb{Z}_4, \mathbb{Z}_4)$ и $(\mathbb{Z}_6, \mathbb{Z}_6)$, для которых минимальное отличие составляет* 4, 7 *и* 8 *позиций соответственно.*

Из теоремы 2 следует, что два псевдолинейных МДР-кода длины 3 с кодовым расстоянием 2 имеют в пересечении не более $q^2 - 2q$ кодовых слов. Иначе говоря, для таких кодов справедлива теорема 1, и контрпример к ней нужно искать среди кодов большей длины.

Однако ниже докажем, что теорема 1 справедлива для всех МДР-кодов. С этой целью примем во внимание результаты работы [9] и тот факт, что имеется взаимно однозначное соответствие между МДР-кодами с кодовым расстоянием 2 и квазигруппами. Определения и достаточные сведения о связи МДР-кодов и квазигрупп можно найти в [10]. Несколько огрубляя формулировки, обозначим здесь основные положения.

Функция $f\colon \mathbb{F}^{n-1} \to \mathbb{F}$ называется *квазигруппой*, если она обратима по каждому из $n-1$ своих аргументов. В терминах настоящей статьи в каждой линии пространства V квазигруппа имеет q попарно различных значений. График $C(f) = \{(x_1, x_2, \ldots, x_n) \in V \mid x_n = f(x_1, x_2, \ldots, x_{n-1})\}$ квазигруппы f представляет собой МДР-код длины n в пространстве V. Верно и обратное: из МДР-кода можно легко построить квазигруппу, приняв одну из координат кодовых слов в качестве значения соответствующей функции. Например, для кода C_0, определённого в (2), квазигруппа может быть записана в виде $x_n = \ell(x_1, x_2, \ldots, x_{n-1}) = x_1 + x_2 + \cdots + x_{n-1}$.

Теорема 3 [9, лемма 1]. *Если квазигруппы f, g и h таковы, что $f(x,y,z) \equiv h(g(x,y),z)$ для $x \in \mathbb{F}$, $y \in \mathbb{F}^{m-1}$, $z \in \mathbb{F}^{n-m-1}$, $n-1 > m \geqslant 2$, и для некоторых $a \in \mathbb{F}^{m-1}$ и $b \in \mathbb{F}^{n-m-1}$ значения f на гранях $y = a$ и $z = b$ известны, то квазигруппа f однозначно определена на всём пространстве V.*

Следствие 1. *Если* МДР-*код C длины $n \geqslant 4$ с кодовым расстоянием* 2 *совпадает с кодом $C_0 = \{x \in V \mid x_n = x_1 + x_2 + \cdots + x_{n-1}\}$ в некоторых двух гипергранях пространства V, то $C = C_0$.*

Доказательство. Заметим, что квазигруппа $x_n = x_1 + x_2 + \cdots + x_{n-1}$ представима в виде

$$x_n = (x_1 + x_2) + x_3 + \cdots + x_{n-1} = h(g(x_1, x_2), x_3, \ldots, x_{n-1})$$

для некоторых квазигрупп g и h. Поскольку коды C и C_0 изотопны, квазигруппа f, соответствующая коду C, имеет аналогичное представление, скажем, $x_n = h'(g'(x_1, x_2), x_3, \ldots, x_{n-1})$ для некоторых квазигрупп g' и h'.

Эти рассуждения наводят на очевидный путь выбора подходящих к условиям теоремы 3 граней, в которых коды C_0 и C совпадают, а следовательно, совпадают значения соответствующих им квазигрупп. При таких условиях квазигруппа f определена однозначно, поэтому $x_n = f(x_1, x_2, \dots, x_{n-1}) = x_1 + x_2 + \dots + x_{n-1}$, что эквивалентно равенству $C = C_0$. Следствие 1 доказано.

Теорема 4. *Если для псевдолинейных* МДР-*кодов* $C_1, C_2 \subseteq V$ *длины* $n \geqslant 3$ *с кодовым расстоянием* 2 *имеет место* $|C_1 \cap C_2| > \frac{q-2}{q}|C_1|$, *то* $C_1 = C_2$.

Доказательство проведём индукцией по длине n. Базу индукции составляют псевдолинейные МДР-коды длины 3, для которых, как отмечено выше, теорема верна в силу результатов работы [8]. Рассмотрим коды $C_1, C_2 \subseteq V$ длины $n \geqslant 4$, удовлетворяющие условиям теоремы, и предположим, что для псевдолинейных МДР-кодов длины меньше n утверждение теоремы выполняется. Без ограничения общности можем считать, что один из кодов C_1, C_2 линейный, так что положим $C_2 = C_0$ и докажем равенство $C_1 = C_0$.

Отметим, что при пересечении МДР-кода с любой гипергранью пространства V образуется МДР-код на единицу меньшей длины (без учёта координаты, фиксированной в выбранной гиперграни).

Для каждого $i \in \{1, 2, \dots, n\}$ рассмотрим разбиение V на q гиперграней Γ_{ij}, $j = 0, 1, \dots, q-1$, с фиксированным значением по направлению i. Среди них найдётся такая гипергрань Γ_i, что

$$|C_0 \cap C_1 \cap \Gamma_i| > \frac{q-2}{q}|C_1 \cap \Gamma_i|.$$

В противном случае, поскольку гиперграни Γ_{ij}, $j = 0, 1, \dots, q-1$, попарно не пересекаются, имеем

$$|C_0 \cap C_1| = \sum_{j=0}^{q-1} |C_0 \cap C_1 \cap \Gamma_{ij}| \leqslant \frac{q-2}{q} \sum_{j=0}^{q-1} |C_1 \cap \Gamma_{ij}| = \frac{q-2}{q}|C_1|,$$

что противоречит условию теоремы.

По предположению индукции получаем $C_0 \cap \Gamma_i = C_1 \cap \Gamma_i$. Иначе говоря, коды C_0 и C_1 совпадают в гиперграни Γ_i. Таким образом, для каждого $i \in \{1, 2, \dots, n\}$ существует гипергрань $\Gamma_i \subset V$ с фиксированным значением по направлению i, в которой коды C_0 и C_1 совпадают. В силу следствия 1 заключаем, что $C_1 = C_0$. Теорема 4 доказана.

Доказательство теоремы 1 получается объединением леммы 4 и теоремы 4. Теорема 1 доказана.

Авторы выражают благодарность Д. С. Кротову и В. Н. Потапову за плодотворные обсуждения по теме настоящей статьи.

ЛИТЕРАТУРА

1. **Марков А. А.** О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
2. **Bar-Yahalom E., Etzion T.** Intersection of isomorphic linear codes // J. Comb. Theory., Ser. A. 1997. Vol. 80, No. 1. P. 247–256.
3. **Etzion T., Vardy A.** Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. Vol. 11, No. 2. P. 205–223.
4. **Потапов В. Н.** Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информации. 2012. Т. 48, № 1. С. 54–63.
5. **Августинович С. В., Соловьёва Ф. И., Хеден У.** О разбиениях n-куба на неэквивалентные совершенные коды // Пробл. передачи информации. 2007. Т. 43, № 4. С. 45–50.
6. **Лось А. В., Соловьёва Ф. И.** О разбиениях пространства F_q^N на аффинно неэквивалентные совершенные q-значные коды // Сиб. электрон. мат. изв. 2010. Т. 7. С. 425–434.
7. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
8. **Frisch S.** On the minimal distance between group tables // Acta Sci. Math. (Szeged). 1997. Vol. 63. P. 341–351.
9. **Krotov D. S., Potapov V. N., Sokolova P. V.** On reconstructing reducible n-ary quasigroups and switching subquasigroups // Quasigr. Relat. Syst. 2008. Vol. 16. P. 55–67.
10. **Потапов В. Н., Кротов Д. С.** Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. журн. 2006. Т. 47, № 4. С. 873–887.

Августинович Сергей Владимирович
Горкунов Евгений Владимирович

Статья поступила
23 июля 2019 г.

После доработки —
27 августа 2019 г.

Принята к публикации
28 августа 2019 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2019. Vol. 26, No. 4. P. 5–15

UDC 519.725 DOI 10.33048/daio.2019.26.669

MAXIMUM INTERSECTION OF LINEAR CODES AND CODES EQUIVALENT TO LINEAR [*)]

S. V. Avgustinovich[1,2,a] and *E. V. Gorkunov*[1,2,b]

[1] Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue, 630090 Novosibirsk, Russia

[2] Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia

E-mail: [a] `avgust@math.nsc.ru`, [b] `gorkunov@math.nsc.ru`

Abstract. We consider linear codes in a space over a finite field with the Hamming metric. A code is called pseudolinear if it is the image of a linear code under an isometric transformation of the space. We derive an upper bound $(q-2)M/q$ attainable for $q \geqslant 3$ for the size of the intersection of two different pseudolinear codes of the same size M. Bibliogr. 10.

Keywords: linear code, pseudolinear code, MDS-code, code intersection, equivalent codes, isometry, isotopy, finite field.

REFERENCES

1. **A. A. Markov,** On transformations without error propagation, in *Selected Works,* Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Information Science and Related Topics (MTsNMO, Moscow, 2003), pp. 70–93 [Russian].
2. **E. Bar-Yahalom** and **T. Etzion,** Intersection of isomorphic linear codes, *J. Comb. Theory, Ser. A* **80** (1), 247–256 (1997).
3. **T. Etzion** and **A. Vardy,** Perfect binary codes and tilings: Problems and solutions, *SIAM J. Discrete Math.* **11** (2), 205–223 (1998).
4. **V. N. Potapov,** Cardinality spectra of components of correlation immune functions, bent functions, perfect colorings, and codes, *Probl. Peredachi Inf.* **48** (1), 54–63 (2012) [Russian] [*Probl. Inf. Transm.* **48** (1), 47–55 (2012)].

[*)] This research is supported by the Russian Foundation for Basic Research (Project 19–01–00682) and the Programme for Fundamental Scientific Research of SB RAS No. I.5.1 (Project 0314–2019–0016).

5. **S. V. Avgustinovich, F. I. Solov'eva,** and **O. Heden,** Partitions of an n-cube into nonequivalent perfect codes, *Probl. Peredachi Inf.* **43** (4), 45–50 (2007) [Russian] [*Probl. Inf. Transm.* **43** (4), 310–315 (2007)].
6. **A. V. Los'** and **F. I. Solov'eva,** On partitions of the space F_q^N into affine nonequivalent perfect q-ary codes, *Sib. Elektron. Mat. Izv.* **7**, 425–434 (2010) [Russian].
7. **F. J. MacWilliams** and **N. J. A. Sloane,** The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977; Svyaz', Moscow, 1979 [Russian]).
8. **S. Frisch,** On the minimal distance between group tables, *Acta Sci. Math. (Szeged)* **63**, 341–351 (1997).
9. **D. S. Krotov, V. N. Potapov,** and **P. V. Sokolova,** On reconstructing reducible n-ary quasigroups and switching subquasigroups, *Quasigr. Relat. Syst.* **16**, 55–67 (2008).
10. **V. N. Potapov** and **D. S. Krotov,** Asymptotics for the number of n-quasigroups of order 4, *Sib. Mat. Zh.* **47** (4), 873–887 (2006) [Russian] [*Sib. Math. J.* **47** (4), 720–731 (2006)].

Sergey V. Avgustinovich
Evgeny V. Gorkunov

Received July 23, 2019
Revised August 27, 2019
Accepted August 28, 2019