S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 11, стр. 771–776 (2014) УДК 519.725
MSC 11T71, 94B05

О ЛИНЕЙНОЙ ЖЕСТКОСТИ $[n, n-1, 2]$-КОДОВ В ПРОСТРАНСТВЕ НАД ПРОСТЫМ ПОЛЕМ

Е. В. ГОРКУНОВ, Е. В. СОТНИКОВА

Abstract. In this paper a notion of linear rigidity of codes is introduced and discussed. We recall several examples of codes those are linearly rigid as well as those are not. Linear rigidity of MDS-codes with minimum distance 2 in the vector space over the prime field is proved.

Keywords: linear code, MDS-code, linear rigidity of codes, code automorphism, code symmetry, prime field, finite field.

1. Введение

Пусть натуральное число q является положительной степенью простого числа p. Рассмотрим n-мерное векторное пространство $\mathbb{F}_q^n$ над конечным полем $\mathbb{F}_q = GF(q)$. Для координатного представления $\mathbb{F}_q^n$ выберем стандартный базис, элементы которого будем обозначать $e_i, i = 1, \ldots, n$. *Кодом* длины n называется произвольное подмножество $C \subseteq \mathbb{F}_q^n$, а элементы кода — *кодовыми словами*. Код C *линейный*, если он образует подпространство в $\mathbb{F}_q^n$.

Расстояние Хэмминга между векторами $x, y \in \mathbb{F}_q^n$ определяется по числу координат, в которых эти векторы отличаются. *Кодовым расстоянием* кода $C \subseteq \mathbb{F}_q^n$ называется минимальное расстояние между его различными кодовыми словами.

Положим $[n] = \{1, \ldots, n\}$. Множество $\operatorname{supp}(x) = \{i \in [n] \mid x_i \neq 0\}$ есть *носитель* вектора $x \in \mathbb{F}_q^n$, а его мощность называется *весом* x и обозначается $w(x)$. В силу линейности, кодовое расстояние линейного кода равняется минимальному ненулевому весу его кодовых слов.

Gorkunov, E. V., Sotnikova, E. V. On linear rigidity of a class of codes.

Поступила 3 октября 2014 г., опубликована 16 октября 2014 г.

Преобразование $\mathbb{F}_q^n$, сохраняющее расстояние между векторами, называется *изометрией*. Метрические свойства кода определяют его возможности по исправлению ошибок. Коды, обладающие одинаковой метрической структурой, с этой точки зрения одинаковы. Более точно, два кода *эквивалентны*, если существует изометрия пространства $\mathbb{F}_q^n$, отображающая один из них в другой.

А. А. Марков [1] показал, что произвольная изометрия пространства $\mathbb{F}_q^n$ может быть представлена в виде композиции перестановки $\pi \in S_n$, меняющей местами координаты вектора, и *изотопии* — набора перестановок $\sigma = (\sigma_1, \ldots, \sigma_n)$ из S_q^n, которые действуют на значения соответствующих координат вектора. Иными словами, группа изометрий пространства $\mathbb{F}_q^n$ представляется полупрямым произведением

$$\mathrm{Aut}(\mathbb{F}_q^n) = S_n \leftthreetimes S_q^n = \left\{(\pi;\sigma) \mid \pi \in S_n,\, \sigma \in S_q^n\right\}.$$

Действие изометрии $(\pi;\sigma) \in \mathrm{Aut}(\mathbb{F}_q^n)$ на вектор $x \in \mathbb{F}_q^n$ задается равенствами

$$x(\pi;\sigma) = (x\pi)\sigma,\ y = x\pi = (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}}),$$
$$y\sigma = (y_1\sigma_1, \ldots, y_n\sigma_n).$$

Группа $\mathrm{Aut}(C)$, образованная изометриями $\mathbb{F}_q^n$, отображающими код C в себя, называется *группой автоморфизмов* кода C. Знание о структуре группы автоморфизмов кода позволяет лучше понять строение самого кода, выделить в нем сходные или, наоборот, различные части, что на практике находит применение в создании новых конструкций кодов, а также повышении эффективности алгоритмов кодирования и декодирования. С другой стороны, невозможно исследовать группу автоморфизмов кода без минимальных знаний о его строении.

Через e обозначим тождественную перестановку из S_n. Автоморфизм $(e;\sigma) \in \mathrm{Aut}(C)$ назовем *автотопией* кода C. Группу автотопий кода C обозначим $\mathrm{Atp}(C)$. Вместо записи $(e;\sigma) \in \mathrm{Atp}(C)$ будем писать кратко $\sigma \in \mathrm{Atp}(C)$.

Автоморфизмы кода C, оставляющие на месте нулевой вектор, образуют его *группу симметрий* $\mathrm{Sym}(C)$. Заметим, что биекция пространства $\mathbb{F}_q^n$ является симметрией тогда и только тогда, когда она сохраняет вес произвольного вектора. Изучение группы автоморфизмов линейного кода сводится к исследованию его группы симметрий, поскольку произвольный автоморфизм линейного кода естественным образом представляется в виде композиции симметрии этого кода и сдвига на некоторое его кодовое слово.

Предложение 1. *Для линейного кода $C \subseteq \mathbb{F}_q^n$ имеет место изоморфизм*

$$\mathrm{Aut}(C) \cong \mathrm{Sym}(C) \leftthreetimes C.$$

Умножение всех векторов пространства $\mathbb{F}_q^n$ на мономиальную $(n\times n)$-матрицу представляет собой изометрию $\mathbb{F}_q^n$, которую назовем *мономиальной*. Будем говорить, что коды $C_1, C_2 \subseteq \mathbb{F}_q^n$ *мономиально эквивалентны*, если существует мономиальная изометрия $\mathbb{F}_q^n$, отображающая один из них в другой. Ф. Дж. Мак-Вильямс [2] доказала, что линейные коды мономиально эквивалентны тогда и только тогда, когда между ними существует линейный изоморфизм, сохраняющий вес каждого кодового слова. Из теоремы Мак-Вильямс вытекает, что *группа мономиальных автоморфизмов* $\mathrm{MAut}(C)$ кода C совпадает с группой линейных симметрий этого кода.

Обозначим через $\mathrm{Gal}(\mathbb{F}_q)$ группу Галуа поля $\mathbb{F}_q$. Функция $f\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ называется *полулинейной* с сопутствующим автоморфизмом $\gamma \in \mathrm{Gal}(\mathbb{F}_q)$, если равенство $f(\alpha x + \beta y) = \gamma(\alpha) f(x) + \gamma(\beta) f(y)$ выполняется для любых $\alpha, \beta \in \mathbb{F}_q$ и $x, y \in \mathbb{F}_q^n$. Таким образом, полупрямое произведение $\mathrm{Gal}(\mathbb{F}_q) \leftthreetimes \mathrm{MAut}(\mathbb{F}_q^n)$ исчерпывает в точности все полулинейные симметрии $\mathbb{F}_q^n$.

Все симметрии пространств $\mathbb{F}_2^n$ и $\mathbb{F}_3^n$ линейны. В случае $q \geqslant 4$ полулинейные симметрии образуют собственную подгруппу группы $\mathrm{Sym}(\mathbb{F}_q^n)$. Если у пространства $\mathbb{F}_q^n$ есть симметрии, не являющиеся полулинейными, то возникает естественный вопрос, могут ли линейные коды в нем обладать такими симметриями. Как будет видно далее, ответ на этот вопрос положительный, однако имеющиеся примеры либо тривиальны, либо связаны с тем, что расширение поля образует линейное пространство над своим подполем.

Назовем линейный код *линейно жестким*, если все его симметрии полулинейны. Это определение можно расширить на случай произвольного кода, например, следующим образом: код линейно жесткий, если все симметрии его линейной оболочки полулинейны. В такой формулировке вопрос о линейной жесткости нелинейных кодов сводится к случаю линейных. В [3] доказано, что код Хэмминга линейно жесткий. Представляется интересным получить характеризацию линейно жестких кодов. В настоящей статье доказана линейная жесткость МДР-кодов с кодовым расстоянием 2 в пространстве над простым полем. Поскольку пространства $\mathbb{F}_2^n$ и $\mathbb{F}_3^n$ являются линейно жесткими, далее будем полагать $q \geqslant 4$.

2. Примеры линейно нежестких кодов

В этом разделе присмотримся более пристально к понятию линейной жесткости. Наряду с примерами линейно жестких кодов укажем некоторые коды, не обладающие этим свойством, а также докажем некоторые простые утверждения о линейной жесткости.

1) Коды с несущественными координатами. Если в некоторой фиксированной координате кодовые слова кода C имеют одно и то же значение, назовем ее *несущественной*. Заметим, что если линейный код имеет несущественную координату, то ее значение может быть только 0. Нетрудно видеть, что множества существенных и несущественных координат кода инвариантны относительно его автоморфизмов.

Предложение 2. *Произвольный автоморфизм кода отображает существенные координаты в существенные, а несущественные в несущественные.*

Наличие несущественной координаты у кода значительно влияет на его группу автоморфизмов, так как к такой координате может быть применена любая перестановка из стабилизатора ее значения.

Предложение 3. *Код, имеющий несущественные координаты, является линейно нежестким.*

2) Коды с кодовым расстоянием 1 представляют собой другой пример линейно нежестких кодов.

Предложение 4. *Код с кодовым расстоянием* 1 *линейно нежесткий.*

Доказательство. Пусть код $C \subseteq \mathbb{F}_q^n$ имеет кодовое расстояние 1. Поскольку взятие линейной оболочки не увеличивает кодовое расстояние кода, то, без

ограничения общности, можно считать, что C линеен. По определению, в коде с расстоянием 1 существуют два кодовых слова, отличающиеся ровно в одной, например, i-й координате. Тогда $e_i \in C$. Это означает, что C обладает следующим свойством. Для любого вектора $x \in C$ в коде C найдутся $q-1$ различных векторов, каждый из которых отличается от x только в i-й координате.

Из сказанного следует, что изотопия, действующая произвольно в i-й координате и тождественно по всем остальным, является автотопией кода C. Любая автотопия такого вида, отличная от мономиальной, не является полулинейной. Тем самым утверждение доказано. □

3) Коды с проверочной матрицей, элементы которой содержатся в некотором подполе поля $\mathbb{F}_q$, дают еще один широко известный пример линейно нежестких кодов. Рассмотрим линейный код C с проверочной матрицей H, элементы которой содержатся в собственном подполе $\mathbb{F} < \mathbb{F}_q$. Для определенности, положим $\mathbb{F} = \mathbb{F}_p$ — простое подполе. Из теории полей известно, что в случае $q = p^r$ и $r > 1$, поле $\mathbb{F}_q$ образует линейное пространство размерности r над $\mathbb{F}_p$. Выберем подстановку $\sigma \in S_q$, которая является линейным преобразованием $\mathbb{F}_q$ над подполем $\mathbb{F}_p$. Тогда справедливо равенство

$$H(x^{\mathsf{T}}\sigma) = (Hx^{\mathsf{T}})\sigma,$$

где предполагается, что σ действует на каждую координату вектора $x \in \mathbb{F}_q^n$. Вместе с тем, $0\sigma = 0$. Отсюда получаем, что векторы x и $(x_1\sigma, \ldots, x_n\sigma)$ являются или не являются кодовыми словами кода C одновременно. Следовательно, $(\sigma, \ldots, \sigma) \in \mathrm{Atp}(C)$. Легко убедиться, что при $q \geqslant 8$ перестановка σ может быть выбрана так, чтобы она не являлась умножением на ненулевой элемент поля $\mathbb{F}_q$ и не принадлежала группе $\mathrm{Gal}(\mathbb{F}_q)$. При этом выборе указанная автотопия кода C не является полулинейной, и код оказывается линейно нежестким.

3. Линейная жесткость МДР-кодов с расстоянием 2 в $\mathbb{F}_p^n$

В этом разделе изучим на предмет линейной жесткости класс МДР-кодов с кодовым расстоянием 2 в пространстве $\mathbb{F}_p^n$ над простым полем $\mathbb{F}_p$. Такой код имеет размерность $n-1$, и никакие два его кодовых слова не являются смежными.

Теорема 1. *Линейный код длины $n \geqslant 3$ размерности $n-1$ с кодовым расстоянием 2 над простым полем линейно жесткий.*

Доказательство. Рассмотрим линейный код $C < \mathbb{F}_p^n$ размерности $n-1$ с кодовым расстоянием $d = 2$. Предположим, что проверочная матрица этого кода имеет вид $H = [h_1 \ldots h_n]$. Иначе говоря, C является пространством решений уравнения $h_1x_1 + \ldots + h_nx_n = 0$. Поскольку $d = 2$, то все элементы матрицы H отличны от нуля.

Пусть $\mathbb{F}_p^*$ обозначает мультипликативную группу поля $\mathbb{F}_p$. Зададимся произвольной симметрией $(\pi;\sigma) \in \mathrm{Sym}(C)$ и покажем, что она линейна. Тем самым будет доказана линейная жесткость кода C.

По определению, произвольная симметрия оставляет на месте нулевую вершину, что означает $0\sigma_i = 0$ для всех $i \in [n]$. Отсюда, в частности, следует, что вектор $x \in \mathbb{F}_p^n$ и его образ $x(\pi;\sigma)$ имеют одинаковый вес, то есть $w(x(\pi;\sigma)) = w(x)$.

Выберем произвольную позицию $i \in [n]$ и пусть $s\pi = i$. Заметим, что каждое из множеств векторов

$$B_s = \{e_s + a_t e_t \mid a_t = -h_s h_t^{-1}, t \in [n] \setminus \{s\}\} \quad \text{и}$$
$$B_i = \{e_i + b_j e_j \mid b_j = -h_i h_j^{-1}, j \in [n] \setminus \{i\}\}$$

представляет собой базис кода C (в случае $i\pi = i$ эти множества совпадают). Поэтому произвольное кодовое слово $x \in C$ и его образ $y = x(\pi;\sigma) \in C$ можно представить в виде

$$x = \sum_{t \neq s} \alpha_t \cdot e_s + \sum_{t \neq s} \alpha_t a_t e_t,$$
$$y = \sum_{j \neq i} \beta_j \cdot e_i + \sum_{j \neq i} \beta_j b_j e_j \tag{1}$$

для подходящих $\alpha_t \in \mathbb{F}_p, t \in [n] \setminus \{s\}$, и $\beta_j \in \mathbb{F}_p, j \in [n] \setminus \{i\}$.

Отследим, каким образом симметрия $(\pi;\sigma)$ действует на x при таком представлении. Это позволит получить необходимые условия на σ. Положим $t_j\pi = j$ при $j \in [n] \setminus \{i\}$. Тогда запишем

$$x\pi = \sum_{t \neq s} \alpha_t \cdot e_i + \sum_{t \neq s} \alpha_t a_t e_{t\pi} = \sum_{j \neq i} \alpha_{t_j} \cdot e_i + \sum_{j \neq i} \alpha_{t_j} a_{t_j} e_j,$$
$$y = x(\pi;\sigma) = (x\pi)\sigma = (\sum_{j \neq i} \alpha_{t_j})\sigma_i e_i + \sum_{j \neq i} (\alpha_{t_j} a_{t_j})\sigma_j e_j. \tag{2}$$

Сравнивая (1) и (2) и помятуя о единственности представления кодового слова y в базисе B_i, приходим к соотношению

$$(\sum_{j \neq i} \alpha_{t_j})\sigma_i = \sum_{j \neq i} (\alpha_{t_j} a_{t_j})\sigma_j b_j^{-1} \quad \text{для произвольных } \alpha_{t_j} \in \mathbb{F}_p, j \in [n] \setminus \{i\}. \tag{3}$$

Поочередно приравнивая в последнем равенстве один из коэффициентов α_{t_j} некоторому $\alpha \in \mathbb{F}_p^*$, а остальные — нулю, найдем, что

$$\alpha\sigma_i = (\alpha a_{t_j})\sigma_j b_j^{-1} \quad \text{для всех } \alpha \in \mathbb{F}_p^* \text{ и } j \in [n] \setminus \{i\}. \tag{4}$$

Отметим, что эти равенства остаются верными и при $\alpha = 0$.

Теперь перейдем непосредственно к доказательству линейности перестановки σ_i. Так как $n \geqslant 3$, то число варьируемых коэффициентов α_{t_j} не меньше 2. Выберем два из них. Для определенности и упрощения записи, будем считать, что $i \notin \{1, 2\}$. Тогда $1, 2 \in [n] \setminus \{i\}$ и можем выбрать, например, α_{t_1} и α_{t_2}.

Сначала в (3) положим $\alpha_{t_1} = \alpha_{t_2} = 1$, а оставшиеся коэффициенты приравняем нулю. С учетом (4) получаем

$$2\sigma_i = a_{t_1}\sigma_1 b_1^{-1} + a_{t_2}\sigma_2 b_2^{-1} = 1\sigma_i + 1\sigma_i = 2(1\sigma_i).$$

Далее индукцией по $\alpha_{t_1} = \alpha \in \mathbb{F}_p^*$ при неизменных остальных коэффициентах имеем:

$$\alpha\sigma_i = (\alpha - 1 + 1)\sigma_i = ((\alpha - 1)a_{t_1})\sigma_1 b_1^{-1} + a_{t_2}\sigma_2 b_2^{-1} =$$
$$= (\alpha - 1)\sigma_i + 1\sigma_i = (\alpha - 1)(1\sigma_i) + 1\sigma_i = \alpha(1\sigma_i).$$

Таким образом, для любого $\alpha \in \mathbb{F}_p^*$ справедливо $\alpha\sigma_i = \alpha(1\sigma_i)$. При этом $0\sigma_i = 0$ — по определению симметрии. Из сказанного следует, что σ_i является перестановкой умножения на элемент $1\sigma_i \in \mathbb{F}_p^*$, которая, очевидно, линейна.

Из произвольности выбора позиции $i \in [n]$ следует, что все перестановки из набора σ линейны. Это означает, что σ действует линейно на всем пространстве $\mathbb{F}_p^n$. В совокупности с линейностью действия π получаем, что симметрия $(\pi;\sigma) \in \mathrm{Sym}(C)$ линейна, а код C линейно жесткий. □

Замечания. 1. К настоящему времени в классе кодов с кодовым расстоянием 2 в пространстве над простым полем авторам известны лишь примеры линейно жестких кодов. Поэтому представляется интересным выяснить, все ли такие коды являются линейно жесткими.

2. Стоит подчеркнуть, что в пространстве над конечным полем, отличным от простого, существует семейство линейно *не*жестких МДР-кодов с кодовым расстоянием 2. Это семейство является подмножеством третьей группы кодов, рассмотренных в разделе 2. Вместе с тем остается открытым вопрос, существуют ли в $\mathbb{F}_q^n$ линейно жесткие МДР-коды с кодовым расстоянием 2 в случае $q = p^r$ и $r > 1$.

Авторы выражают глубокую благодарность С. В. Августиновичу за ценные замечания и вопросы, которые способствовали более стройному изложению статьи.

Список литературы

[1] А. А. Марков, *О преобразованиях, не распространяющих искажения,* Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы, МЦНМО, Москва, (2003), 70–93. MR2086689

[2] F. J. MacWilliams, *Combinatorial problems of elementary Abelian groups,* Doctoral thesis, Harvard University, Cambridge, 1962. MR2939359

[3] Е. В. Горкунов, *Группа автоморфизмов q-ичного кода Хэмминга,* Дискретн. анализ и исслед. опер., **17**:6 (2010), 50–55. MR2797615

[4] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки,* М.: Связь, 1979. Zbl 0447.94016

Евгений Владимирович Горкунов
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090, Новосибирск, Россия
Новосибирский государственный университет,
ул. Пирогова, 2,
630090, Новосибирск, Россия
E-mail address: gorkunov@math.nsc.ru

Евгения Вадимовна Сотникова
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090, Новосибирск, Россия
E-mail address: lucernavesper@gmail.com