S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

Том 14, стр. 210–217 (2017) УДК 519.725
DOI 10.17377/semi.2017.14.021 MSC 11T71, 94B05

ОБ АВТОМОРФИЗМАХ ЛИНЕЙНЫХ КОДОВ НАД ПРОСТЫМ ПОЛЕМ

С. В. АВГУСТИНОВИЧ, Е. В. ГОРКУНОВ

Abstract. We discuss linearity of code automorphisms for codes in a space over a finite field. We introduce a concept of minimal supports and minimal codewords, which in some cases are turned out useful to prove that an automorphism of a linear code is linear. Also we construct a graph on the set of minimal supports of a code as a vertex set. In this paper for a linear code in a space over a prime field it is shown that all its autotopies fixing the zero vector are linear if and only if the graph of minimal supports of the code does not contain any isolated vertices. We also characterize the autotopy group of a linear code over a prime field.

Keywords: linear code, code automorphism, linear automorphism, linearly rigid code, minimal codeword, graph of minimal supports, finite field, prime field.

1. Введение

Структура математического объекта тесно связана с его группой автоморфизмов. Если один объект имеет естественное вложение в другой, то вопрос о том, как соотносятся их группы автоморфизмов, возникает столь же естественно, однако не всегда является простой задачей. В одном случае рассматриваемый объект жестко привязан к структуре объемлющего пространства, в другом — нет. Настоящая заметка имеет своей целью охарактеризовать границу между этими двумя ситуациями для случая линейных подпространств в линейных пространствах над простым полем.

Avgustinovich, S.V., Gorkunov, E.V., On automorphisms of linear codes over a prime field.

Работа второго автора выполнена при поддержке Российского фонда фундаментальных исследований (грант 16-01-00499).

Поступила 7 декабря 2016 г., опубликована 14 марта 2017 г.

Рассмотрим n-мерное векторное пространство $\mathbb{F}_q^n$ над конечным полем $\mathbb{F}_q$. В общем случае $q = p^r$ является степенью простого числа p. Мультипликативную группу поля обозначим через $\mathbb{F}_q^*$. Некоторые утверждения, доказываемые в настоящей статье, справедливы для произвольного конечного поля; однако основной результат имеет отношение к случаю простого поля $\mathbb{F}_p$.

Кодом длины n называется произвольное подмножество $C \subseteq \mathbb{F}_q^n$; элементы кода — *кодовые слова*. Код *линейный*, если он образует подпространство в $\mathbb{F}_q^n$. Матрица размеров $|C| \times n$, строками которой являются все кодовые слова C, называется *кодовой*. Если произвольный базис линейного кода, записать в виде строк матрицы, то получится *порождающая матрица* этого кода.

Векторы пространства $\mathbb{F}_q^n$ будем записывать в стандартном базисе и обозначать через $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Множество $\operatorname{supp}(x) = \{i \mid x_i \neq 0\}$ называется *носителем* вектора x; число $w(x) = |\operatorname{supp}(x)|$ называется *весом* x. Носитель кода $C \subseteq \mathbb{F}_q^n$ равен объединению носителей его кодовых слов, то есть $\operatorname{supp}(C) = \bigcup\limits_{x \in C} \operatorname{supp}(x)$.

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

Биекция пространства $\mathbb{F}_q^n$ на себя, сохраняющая расстояния между векторами, называется *изометрией*. Изометрии $\mathbb{F}_q^n$, отображающие код $C \subseteq \mathbb{F}_q^n$ в себя, образуют его *группу автоморфизмов* $\operatorname{Aut}(C)$.

Хорошо известно [1], что каждая изометрия $\mathbb{F}_q^n$ является композицией подстановки порядка n и изотопии. Подстановка $\pi \in S_n$ меняет местами координаты вектора, а *изотопия* представима набором $\sigma = (\sigma_1, \ldots, \sigma_n)$ подстановок из S_q, каждая из которых действует на элементах поля $\mathbb{F}_q$ и изменяет значение в соответствующей координате вектора $x \in \mathbb{F}_q^n$.

Иными словами, группа изометрий пространства $\mathbb{F}_q^n$ представляется полупрямым произведением

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

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

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

Отметим следующие подгруппы группы автоморфизмов кода $C \subseteq \mathbb{F}_q^n$. Автоморфизмы, оставляющие нулевой вектор неподвижным, образуют *группу симметрий* $\operatorname{Sym}(C)$. Автоморфизм, являющийся изотопией, назовем *автотопией* кода C; группу автотопий обозначим через $\operatorname{Atp}(C)$. Автотопию, являющуюся симметрией кода C, будем называть *топосимметрией*. Топосимметрии кода образуют группу $\operatorname{TSym}(C) = \operatorname{Sym}(C) \cap \operatorname{Atp}(C)$.

Обозначим через $M_n(q)$ группу мономиальных матриц над полем $\mathbb{F}_q$. Согласно теореме Мак-Вильямс [2], если симметрия $(\pi; \sigma) \in \operatorname{Sym}(C)$ линейна, найдется матрица $M \in M_n(q)$ такая, что $C(\pi; \sigma) = CM = \{xM \mid x \in C\}$. Поскольку преобразование пространства $\mathbb{F}_q^n$ умножением всех векторов на некоторую мономиальную матрицу является симметрией, вместе с теоремой Мак-Вильямс это означает, что группа линейных симметрий пространства $\mathbb{F}_q^n$ и группа его мономиальных преобразований суть одно и то же.

Все симметрии пространств $\mathbb{F}_2^n$ и $\mathbb{F}_3^n$ линейны. В случае простого $p \geqslant 5$ пространство $\mathbb{F}_p^n$ обладает нелинейными симметриями. Линейный код в $\mathbb{F}_p^n$ назовем *линейно жестким*, если все его симметрии линейны. В [3] доказано, что код Хэмминга линейно жесткий. Линейная жесткость МДР-кодов с кодовым расстоянием 2 в пространстве над простым полем показана в [4]. Там же аккумулированы известные примеры линейно нежестких кодов, в число которых входят коды с несущественными координатами. С учетом последнего, в дальнейшем будем полагать, что все координаты кода существенны. Иначе говоря, в кодовой матрице кода отсутствуют нулевые столбцы.

В этой статье исследуются автотопии произвольных линейных кодов. В случае простого поля $\mathbb{F}_p$ получены необходимые и достаточные условия, при которых все топосимметрии линейного кода линейны. Полностью охарактеризована группа автотопий линейного кода из $\mathbb{F}_p^n$. Статья организована следующим образом. В разд. 2 вводятся понятия минимального слова и графа минимальных носителей кода из $\mathbb{F}_q^n$. Линейные коды со связным графом минимальных носителей рассматриваются в разд. 3. Группа автотопий линейного кода с несвязным графом минимальных носителей обсуждается в разд. 4. Там же сформулирован основной результат.

2. Минимальные слова линейного кода

Обратим внимание на различные носители ненулевых кодовых слов кода $C \subseteq \mathbb{F}_q^n$. По включению их совокупность образует частично упорядоченное множество $\mathcal{S}$. Среди элементов $\mathcal{S}$ есть минимальные по указанному порядку. Носитель кодового слова $x \in C$ назовем *минимальным носителем* кода C, если $\operatorname{supp}(x)$ является минимальным элементом в $\mathcal{S}$.

Кодовое слово $x \in C$, $x \neq 0$, с минимальным носителем будем также называть *минимальным.* Отметим, что x минимальное в том и только том случае, если для любого кодового слова $y \in C$, отличного от нуля, отношение $\operatorname{supp}(y) \subseteq \operatorname{supp}(x)$ влечет равенство $\operatorname{supp}(y) = \operatorname{supp}(x)$.

Известна теорема Глаголева [5, лемма Глаголева] о том, что для любого линейного кода $C \leqslant \mathbb{F}_q^n$ существует линейный код $C' \leqslant \mathbb{F}_q^n$ с такими же размерностью и кодовым расстоянием (возможно, совпадающий с C), базис которого может быть выбран среди слов минимального веса. Следующее утверждение в определенном смысле обобщает эту теорему.

Предложение 1. *Базис произвольного линейного кода может быть выбран среди его минимальных слов.*

Доказательство. Рассмотрим линейный код $C \leqslant \mathbb{F}_q^n$ и через M обозначим множество его минимальных слов. Заметим, что если в C имеются кодовые слова, отличные от нуля, то $M \neq \varnothing$. В случае, когда линейная оболочка C_M множества M совпадает с кодом C, доказательство очевидно. Покажем, что это единственно возможный случай.

Предположим, что $\overline{C}_M = C \setminus C_M \neq \varnothing$. Выберем кодовое слово $x \in \overline{C}_M$, которое является минимальным в коде $\overline{C}_M$. Поскольку x не является минимальным в $C = C_M \cup \overline{C}_M$, найдется кодовое слово $y \in C_M$, $y \neq 0$, такое, что $\operatorname{supp}(y) \subset \operatorname{supp}(x)$. Пусть $i \in \operatorname{supp}(y)$. Тогда для $z = x - x_i y_i^{-1} y$ имеем $z \in \overline{C}_M$ и $\operatorname{supp}(z) \subset \operatorname{supp}(x)$, что противоречит минимальности слова x в коде $\overline{C}_M$. Следовательно, $\overline{C}_M = \varnothing$. □

На множестве минимальных носителей кода C определим граф $G_{\min}(C)$. Минимальные носители $S_1 \neq S_2$ смежны в $G_{\min}(C)$, если $S_1 \cap S_2 \neq \varnothing$. Назовем граф $G_{\min}(C)$ *графом минимальных носителей* кода C.

Заметим, что все ненулевые кодовые слова одномерного кода являются минимальными и их носители совпадают. Это означает, что одномерный код имеет одновершинный граф минимальных носителей. Группа автотопий одномерного кода находится тривиально.

Предложение 2. *Для одномерного линейного кода $C \leqslant \mathbb{F}_q^n$ справедливы соотношения* $\mathrm{TSym}(C) \cong S_{q-1}$ *и* $\mathrm{Atp}(C) \cong S_q$.

Доказательство. Для доказательства достаточно заметить, что код C при умножении на подходящую диагональную матрицу преобразуется в код с повторением, а именно в код $C' = \{(\alpha, \ldots, \alpha) \in \mathbb{F}_q^n \mid \alpha \in \mathbb{F}_q\}$. Соответствующие группы автотопий кодов C и C' являются сопряженными указанным линейным преобразованием. После этого утверждение становится очевидным. □

Аналогично упорядочению носителей кодовых слов можем упорядочить по включению носители всех линейных подкодов кода C некоторой фиксированной размерности. Среди элементов такого частично упорядоченного множества также будут минимальные.

Линейный подкод $V \leqslant C$ размерности $t \leqslant \dim C$ назовем *минимальным,* если для любого другого линейного подкода $U \leqslant C$ размерности t из отношения $\mathrm{supp}(U) \subseteq \mathrm{supp}(V)$ следует $\mathrm{supp}(U) = \mathrm{supp}(V)$.

Предложение 3. *Если в линейном коде $C \leqslant \mathbb{F}_q^n$ минимальные подкоды одной размерности имеют совпадающие носители, то они равны.*

Доказательство. Рассмотрим в коде C минимальные подкоды U и V одной размерности такие, что $\mathrm{supp}(U) = \mathrm{supp}(V)$. Предположим, $U \neq V$. Следовательно, найдется вектор $u \in U$ такой, что $u \notin V$. Поскольку в этом случае $u \neq 0$, одна из его координат отлична от нуля, например, i-я.

Далее выберем произвольный базис B подкода V. Вычитая из каждого базисного вектора $v \in B$ вектор u, умноженный на подходящий коэффициент, занулим i-ю координату всех векторов из B. В результате получим базис B'. Очевидно, для линейного кода W, порожденного базисом B', имеют место соотношения $W \leqslant C$, $\dim W = \dim V$ и $\mathrm{supp}(W) \subset \mathrm{supp}(V)$. В совокупности, это противоречит минимальности кодов U и V. □

Следствие 1. *Если носители двух минимальных слов линейного кода $C \leqslant \mathbb{F}_q^n$ совпадают, то одно из них получается из другого умножением на некоторый ненулевой коэффициент.*

3. Коды со связным графом минимальных носителей

Минимальные слова кода представляют собой весьма сильный инструмент для того, чтобы отследить, какими автотопиями может обладать этот код. Покажем, что если одна из подстановок, задающих автотопию кода, является умножением на ненулевой элемент поля и в коде существует минимальное слово с соответствующей ненулевой координатой, то автотопия необходимо действует таким же умножением на всем носителе этого слова.

Лемма 1. *Пусть $C \leqslant \mathbb{F}_q^n$ — линейный код, $x \in C$ — минимальное кодовое слово и $\sigma = (\sigma_1, \ldots, \sigma_n) \in \mathrm{TSym}(C)$. Если для некоторого $i \in \mathrm{supp}(x)$ подстановка σ_i является умножением на элемент из $\mathbb{F}_q^*$, то $\sigma_j = \sigma_i$ для любого $j \in \mathrm{supp}(x)$.*

Доказательство. Предположим, σ_i есть умножение на элемент $\mu \in \mathbb{F}_q^*$. Поскольку $\mu x \in C$, вектор $z = x\sigma - \mu x$ также является кодовым. При этом $\mathrm{supp}(z) \subset \mathrm{supp}(x)$, так как $z_i = 0$. Тогда если $z \neq 0$, приходим к противоречию с минимальностью слова x. Значит, $x\sigma = \mu x$.

Вместе с x минимальными словами кода C являются все векторы вида λx для $\lambda \in \mathbb{F}_q^*$. Поочередно рассматривая эти минимальные слова в качестве вектора x в рассуждениях выше, делаем вывод, что для любого $j \in \mathrm{supp}(x)$ и любого $\alpha \in \mathbb{F}_q$ справедливо $\alpha\sigma_j = \mu\alpha$. Следовательно, $\sigma_j = \sigma_i$. □

Лемма 1 помогает установить тот факт, что в пространстве над простым полем коды с нетривиальным связным графом минимальных носителей имеют относительно бедную группу топосимметрий, изоморфную $\mathbb{F}_p^*$.

Лемма 2. *Если у линейного кода $C \leqslant \mathbb{F}_p^n$ отсутствуют нулевые координаты, а его граф минимальных носителей связен и не является одновершинным, то $\mathrm{TSym}(C) \cong \mathbb{F}_p^*$.*

Доказательство. По условию, в графе $G_{\min}(C)$ минимальных носителей кода C не менее двух вершин. Это означает, что в C существует не менее двух минимальных слов с попарно различными носителями. Любые два из них линейно независимы, так что $\dim C \geqslant 2$.

Все столбцы кодовой матрицы C ненулевые, поэтому каждая из n координатных позиций входит хотя бы в один минимальный носитель кода C. Выберем любые две из них и допустим, что выбранные позиции принадлежат некоторым минимальным носителям S_1 и S_2 кода C, причем $S_1 \neq S_2$. Поскольку граф $G_{\min}(C)$ связен, в нем найдется простая цепь P, соединяющая вершины S_1 и S_2. Отметим, что каждые два носителя, соседние в P, имеют непустое пересечение.

Рассмотрим произвольную автотопию $\sigma = (\sigma_1, \ldots, \sigma_n) \in \mathrm{TSym}(C)$. В силу леммы 1 и связности графа $G_{\min}(C)$, чтобы доказать, что все подстановки σ_i, $i = 1, \ldots, n$, являются умножением на $\lambda \in \mathbb{F}_p^*$ (один и тот же для всех σ_i), достаточно показать это хотя бы для одной из них.

Пусть $x, y \in C$ — минимальные слова кода C с различными носителями $S_1 = \mathrm{supp}(x)$ и $S_2 = \mathrm{supp}(y)$, смежными в $G_{\min}(C)$. Без ограничения общности, положим $S_1 \setminus S_2 = \{1, \ldots, n_1\}$, $S_1 \cap S_2 = \{n_1{+}1, \ldots, n_2\}$, $S_2 \setminus S_1 = \{n_2{+}1, \ldots, n_3\}$ для некоторых $1 < n_1 < n_2 < n_3 \leqslant n$. То есть кодовые слова x, y имеют вид

$$\begin{aligned} x &= x' \,|\, x'' \,|\, 0 \,|\, 0, \\ y &= 0 \,|\, y'' \,|\, y''' \,|\, 0. \end{aligned}$$

Здесь $x' = (x_1, \ldots, x_{n_1})$, $x'' = (x_{n_1+1}, \ldots, x_{n_2})$, аналогично $y'' = (y_{n_1+1}, \ldots, y_{n_2})$, $y''' = (y_{n_2+1}, \ldots, y_{n_3})$. Выделим соответствующие части автотопии σ и обозначим через $\sigma' = (\sigma_1, \ldots, \sigma_{n_1})$, $\sigma'' = (\sigma_{n_1+1}, \ldots, \sigma_{n_2})$, $\sigma''' = (\sigma_{n_2+1}, \ldots, \sigma_{n_3})$.

Тогда имеем

$$\begin{aligned} x\sigma &= x'\sigma' \,|\, x''\sigma'' \,|\, 0 \,|\, 0, \\ y\sigma &= 0 \,|\, y''\sigma'' \,|\, y'''\sigma''' \,|\, 0, \\ x\sigma + y\sigma &= x'\sigma' \,|\, x''\sigma'' + y''\sigma'' \,|\, y'''\sigma''' \,|\, 0, \\ (x+y)\sigma &= x'\sigma' \,|\, (x''+y'')\sigma'' \,|\, y'''\sigma''' \,|\, 0. \end{aligned}$$

Заметим, что векторы $z_1 = (x+y)\sigma$, $z_2 = x\sigma + y\sigma$ и $z = z_1 - z_2$ принадлежат C, так как код линеен и $\sigma \in \mathrm{TSym}(C)$. При этом, если $(x'' + y'')\sigma'' \neq x''\sigma'' + y''\sigma''$, то $z \neq 0$ и $\mathrm{supp}(z) \subset \mathrm{supp}(x)$, что противоречит минимальности x. Значит, $(x+y)\sigma = x\sigma + y\sigma$. В частности, фиксируя координатную позицию $i \in S_1 \cap S_2$, запишем $(x_i + y_i)\sigma_i = x_i\sigma_i + y_i\sigma_i$.

Код C линейный, поэтому пару минимальных слов $x, y \in C$ с носителями S_1, S_2 можно выбрать с произвольно заданными $x_i = \alpha$, $y_i = \beta \in \mathbb{F}_p^*$. Следовательно,

$$(\alpha + \beta)\sigma_i = \alpha\sigma_i + \beta\sigma_i \quad \text{для любых } \alpha, \beta \in \mathbb{F}_p.$$

Далее имеем $2\sigma_i = (1+1)\sigma_i = 1\sigma_i + 1\sigma_i = 2 \cdot 1\sigma_i$ и по индукции выводим, что

$$\mu\sigma_i = \mu \cdot 1\sigma_i \quad \text{для любого } \mu \in \mathbb{F}_p^*.$$

Таким образом, σ_i есть умножение на элемент $\lambda = 1\sigma_i \in \mathbb{F}_p^*$, и для произвольного $x \in \mathbb{F}_p^n$ справедливо $x\sigma = (x_1\sigma_1, \ldots, x_n\sigma_n) = (\lambda x_1, \ldots, \lambda x_n) = \lambda x$.

С другой стороны, для любого $\mu \in \mathbb{F}_p^*$ преобразование линейного кода по правилу $\varphi_\mu \colon x \mapsto \mu x$ является автотопией этого кода. С учетом доказанного, это означает, что $\mathrm{TSym}(C)$ исчерпывается $p-1$ автотопиями φ_μ. Естественная биекция между $\mathrm{TSym}(C)$ и $\mathbb{F}_p^*$ задает искомый изоморфизм. □

4. Коды с несвязным графом минимальных носителей

Рассмотрим линейные коды с несвязным графом минимальных носителей. Большая часть рассуждений ниже будет справедлива для кодов над произвольным конечным полем $\mathbb{F}_q$. В конце раздела сформулируем основной результат статьи — необходимые и достаточные условия линейности всех топосимметрий линейного кода в пространстве над простым полем $\mathbb{F}_p$.

Предположим, граф $G_{\min}(C)$ линейного кода $C \leqslant \mathbb{F}_q^n$ имеет $s > 1$ компонент связности. Каждая из них покрывает подмножество координатных позиций, которое не пересекается с подмножествами позиций, покрываемыми другими компонентами связности.

Выберем базис B кода C среди его минимальных слов. Несвязность $G_{\min}(C)$ означает, что этот базис может быть разбит на подмножества B_i, $i = 1, \ldots, s$, носители которых попарно не пересекаются. Рассмотрим порождающую матрицу G кода C, образованную векторами базиса B. Будем полагать, что строки матрицы G сгруппированы по подмножествам B_i. Так как носители кодовых слов из разных подмножеств B_i не пересекаются, найдется подходящая перестановка столбцов матрицы G, преобразующая ее к блочно-диагональной матрице

$$G' = \begin{pmatrix} G_1 & 0 & \ldots & 0 \\ 0 & G_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & G_s \end{pmatrix}.$$

Такая блочная матрица содержит одинаковое количество блоков по строкам и столбцам, причем блоки вне главной диагонали нулевые. В строки блока G_i, $i = 1, \ldots, s$, записаны векторы из подмножества B_i, так что блок имеет размеры $|B_i| \times |\mathrm{supp}(B_i)|$.

Рассмотрим случай двух блоков, хотя в общем случае их может быть вплоть до $k = \dim C$. Пусть порождающая матрица кода C подходящей перестановкой столбцов представляется в виде

$$G' = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}.$$

Если блок G_i, $i = 1, 2$, имеет размеры $k_i \times n_i$, он порождает некоторый линейный код C_i размерности k_i длины n_i. В этом случае линейный код, порождаемый матрицей G', можно рассмотреть в качестве декартова произведения $C_1 \times C_2 = \{(x', x'') \in \mathbb{F}_q^n \mid x' \in C_1, x'' \in C_2\}$.

Код $C \subseteq \mathbb{F}_q^n$ назовем *разложимым в произведение* кодов C_i, $i = 1, \ldots, s$, если подходящей перестановкой координат C представляется в виде декартова произведения $C_1 \times \ldots \times C_s$. Сомножители такого произведения назовем также *сомножителями* кода C.

Группа автотопий кода, разложимого в произведение, очевидным образом распадается в декартово произведение подгрупп, изоморфных группам автотопий сомножителей этого кода.

Лемма 3. *Пусть код $C \subseteq \mathbb{F}_q^n$ разложим в произведение $C = C_1 \times C_2$. Тогда* $\mathrm{Atp}(C) \cong \mathrm{Atp}(C_1) \times \mathrm{Atp}(C_2)$.

Объединяя леммы 2 и 3, получаем следующие результаты.

Теорема 1. *Пусть $C \leqslant \mathbb{F}_p^n$ — линейный код без нулевых координат. Все топосимметрии кода C линейны тогда и только тогда, когда среди его сомножителей отсутствуют одномерные коды, или, что то же, в его графе минимальных носителей отсутствуют изолированные вершины.*

Теорема 2. *Если линейный код $C \leqslant \mathbb{F}_p^n$ без нулевых координат разложим в произведение неразложимых линейных кодов C_i, $i = 1, \ldots, s$, среди которых отсутствуют одномерные, то все автотопии кода C аффинны и образуют группу*

$$\mathrm{Atp}(C) \cong (\mathbb{F}_p^*)^s \leftthreetimes C.$$

В заключение обратим внимание на нетривиальность проблемы линейной жесткости кодов. Если порядок поля отличен от простого, определение линейно жесткого кода расширяется, и такой код допускает полулинейные симметрии. Имеется [6, разд. 7] характеризация полулинейных симметрий для линейных кодов с кодовым расстоянием $d \geqslant 3$ в пространстве $\mathbb{F}_q^n$. Вопрос о том, существуют ли у некоторого кода нелинейные автоморфизмы (другими словами, является ли код линейно нежестким) остается открытым, в том числе для кодов над полем составного порядка. В случае кода Хэмминга общее решение удалось получить [3] во многом благодаря исключительным комбинаторным свойствам этого кода.

References

[1] A. A. Markov, *On transformations without error propagation,* in: Selected Works, Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, p. 70–93, MTsNMO, Moscow, 2003 [Russian].

[2] F. J. MacWilliams, *Combinatorial Problems of Elementary Abelian Groups,* Doctoral thesis, Harvard University, Cambridge, 1962. MR2939359

[3] E. V. Gorkunov, *The automorphism group of a q-ary Hamming code,* Diskretn. Analiz Issled. Oper., **17**:6 (2010), 50–55 [Russian]. MR2797615

[4] E. V. Gorkunov, E. V. Sotnikova, *On linear rigidity of* $[n, n-1, 2]$*-codes in a space over a prime field,* Sib. Elektron. Mat. Izv., **11** (2014), 771–776 [Russian]. Zbl 1354.94064
[5] Ya. M. Kurlyandchik, *On logarithmic asymptotic behavior of length of a maximal cycle with spread* $r > 2$*,* in: Discrete Analysis, **19**, 48–55, Inst. Mat. SO AN SSSR, Novosibirsk, 1971 [Russian].
[6] W. C. Huffman, *Codes and Groups,* in: Handbook of Coding Theory, Ch. 17, Elsevier Science, Amsterdam, 1998. MR1667953

Sergey Vladimirovich Avgustinovich
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090 Novosibirsk, Russia;
Novosibirsk State University,
ul. Pirogova, 2,
630090 Novosibirsk, Russia
E-mail address: avgust@math.nsc.ru

Evgeny Vladimirovich Gorkunov
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090 Novosibirsk, Russia;
Novosibirsk State University,
ul. Pirogova, 2,
630090 Novosibirsk, Russia
E-mail address: gorkunov@math.nsc.ru