ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391.1 : 519.725

© 2022 г. **И.Ю. Могильных**

О q-ИЧНЫХ ПРОПЕЛИНЕЙНЫХ СОВЕРШЕННЫХ КОДАХ НА ОСНОВЕ РЕГУЛЯРНЫХ ПОДГРУПП ОБЩЕЙ АФФИННОЙ ГРУППЫ[1]

Код называется пропелинейным, если его группа автоморфизмов содержит подгруппу, действующую регулярно на кодовых словах кода. Подгруппа группы аффинных преобразований $GA(r,q)$ называется регулярной, если она действует регулярно на векторах $\mathbb{F}_q^r$. Всякий автоморфизм регулярной подгруппы общей линейной группы $GA(r,q)$ индуцирует перестановку на смежных классах по коду Хэмминга длины $\frac{q^r-1}{q-1}$. На основе этой перестановки в статье предложена конструкция q-ичных пропелинейных совершенных кодов длины $\frac{q^{r+1}-1}{q-1}$. В частности, для любого простого q получена бесконечная серия q-ичных пропелинейных совершенных кодов предполного ранга.

Ключевые слова: пропелинейный код, совершенный код, регулярное действие, аффинная группа, ранг.

DOI: 10.31857/S0555292322010041

§ 1. Введение

Понятие пропелинейного кода было введено в [1]. Эти коды обобщают такие классы кодов как линейные, $\mathbb{Z}_4$-линейные и пр. Отметим, что многие известные конструкции двоичных совершенных кодов позволяют строить пропелинейные коды. В частности, к таким относятся пропелинейные коды из оригинальных конструкций Васильева [2] и Соловьевой [3], предложенные в работах [4–6]. Помимо пропелинейных двоичных совершенных кодов известны также конструкции других оптимальных кодов. Например, все известные на сегодняшний день конструкции кодов Препараты являются пропелинейными [7–9].

В отличие от двоичного случая, работ, посвященных q-ичным, $q \geqslant 3$, оптимальным пропелинейным кодам относительно немного. Транзитивные и пропелинейные МДР-коды исследовались в работе [10]. В работе [5] была предложена конструкция совершенных q-ичных кодов ранга на единицу больше размерности кода Хэмминга на основе конструкции Шонхейма.

В данной статье рассмотрена конструкция q-ичных совершенных кодов, использующая автоморфизмы регулярных подгрупп группы $GA(r,q)$ и конструкцию Моллара [11] (см. также [12]). При $q = 2$ эта конструкция является частным случаем конструкции Соловьевой для двоичных совершенных кодов и расширенных совершенных из [3] и была рассмотрена в работах [6, 13].

Двоичные пропелинейные коды из работы [6] имеют относительно большое ядро, ранги этих кодов принимают все значения от размерности кода Хэмминга до предполного ранга. В работе [13] показано существование бесконечной серии двоичных

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

расширенных совершенных кодов, чья группа автоморфизмов действует транзитивно на коде, а также транзитивно на множестве векторов на расстоянии 1 от кода. Коды с таким свойством известны как транзитивные на соседях (neighbor transitive), см. [14]. В [13] установлено, что эквивалентность расширенных совершенных пропелинейных кодов из [6] равносильна изоморфизму их систем четверок Штейнера, что позволяет решать проблему эквивалентности этих кодов, имеющих длину 32, с помощью персонального компьютера.

Опишем содержание данной статьи, которое идейно восходит к [6]. В § 2 приводятся определения и обозначения. Конструкция пропелинейных кодов дана в § 3. В исходной конструкции Моллара [11] для построения совершенного кода длины $\frac{q^{r+1}-1}{q-1}$ используются смежные классы двух кодов – кода Хэмминга длины $\frac{q^r-1}{q-1}$ и кода, проверочная матрица которого состоит из всех векторов длины r, а также перестановка τ на векторах $\mathbb{F}_q^r$. Каждый автоморфизм всякой регулярной подгруппы $GA(r,q)$ – это перестановка на множестве векторов $\mathbb{F}_q^r$. В § 3 показано, что если τ – такая перестановка, то соответствующий код Моллара пропелинеен. Заметим, что эта конструкция, помимо кодов Хэмминга и кодов из работы [5], является единственным методом построения q-ичных пропелинейных совершенных кодов для $q \geqslant 3$, известным на сегодняшний день.

В § 4 рассматривается проблема рангов q-ичных пропелинейных кодов, полученных в § 3. Для всякого простого q показано существование перестановки τ, такой что код S_τ длины q^2+q+1 является пропелинейным и имеет предполный ранг. С использованием конструкции прямого произведения для регулярных подгрупп $GA(r,q)$ (см. [15]) этот результат обобщается следующим образом: для всякого простого q и любых ℓ, r, $0 \leqslant \ell \leqslant r/2$, $r \geqslant 2$, существует q-ичный совершенный пропелинейный код длины $\frac{q^{r+1}-1}{q-1}$ ранга $\frac{q^{r+1}-1}{q-1} - r - 1 + 2\ell$. В частности, этот класс содержит бесконечную серию кодов предполного ранга растущей длины. Так как при $q = 3$ ранг является инвариантом класса эквивалентности кодов, то имеется $\left\lfloor \frac{r}{2} \right\rfloor + 1$ троичных кодов попарно различных рангов длины $\frac{3^{r+1}-1}{2}$, не эквивалентных кодам из [5], так как последние имеют ранг, на единицу превосходящий ранг кода Хэмминга.

Результаты, изложенные в этой статье, были анонсированы в препринте [16] без доказательств.

§ 2. Определения и обозначения

Через $\mathbb{F}_q^n$ обозначим пространство всех векторов над полем $\mathbb{F}_q$. Нулевой элемент векторного пространства и вектор из одних единиц будем обозначать через $\mathbf{0}$ и $\mathbf{1}$, и их длина будет очевидна из контекста. Конкатенацию векторов x и y обозначаем через $x\,|\,y$. Если C и D – q-ичные коды, то

$$C \times D = \{(x\,|\,y) :\ x \in C,\ y \in D\}.$$

Совершенным называется q-ичный код с кодовым расстоянием 3, мощность которого достигает границы Хэмминга.

Пусть f, f' – перестановки векторов в пространствах $\mathbb{F}_q^n$ и $\mathbb{F}_q^{n'}$ соответственно. Обозначим через $(f\,|\,f')$ перестановку, которая действует на конкатенациях векторов x из $\mathbb{F}_q^n$ и y из $\mathbb{F}_q^{n'}$ следующим образом:

$$(f\,|\,f')(x\,|\,y) = (f(x)\,|\,f'(y)). \tag{1}$$

Отметим, что в § 3 в частном случае, когда f, f' являются автоморфизмами (например, перестановками позиций) $\mathbb{F}_q^n$ и $\mathbb{F}_q^{n'}$, определенное в (1) обозначение трактуется как автоморфизм $\mathbb{F}_q^{n+n'}$.

Перестановка π координатных позиций $\{1, 2, \ldots, n\}$ действует следующим образом:

$$\pi(x) = \pi(x_1, \ldots, x_n) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}).$$

Рассмотрим n перестановок σ_i, $i \in \{1, \ldots, n\}$, элементов поля $\mathbb{F}_q$. *Посимвольной перестановкой* пространства $\mathbb{F}_q^n$ называется отображение $\sigma = (\sigma_1, \ldots, \sigma_n)$, переставляющее символы в каждой из позиций:

$$(\sigma_1, \ldots, \sigma_n)(x_1, \ldots, x_n) = (\sigma_1(x_1), \ldots, \sigma_n(x_n)).$$

Композиция $\sigma\sigma'$ двух перестановок σ и σ' такого типа – это посимвольная перестановка $(\sigma_1\sigma'_1, \ldots, \sigma_n\sigma'_n)$, где $\sigma_i\sigma'_i$ – композиция $\sigma_i\sigma'_i(\cdot) = \sigma_i(\sigma'_i(\cdot))$ для любого $i \in \{1, 2, \ldots, n\}$.

Под *автоморфизмом* $\mathbb{F}_q^n$ будем понимать изометрию пространства, т.е. биективное отображение на себя, сохраняющее попарное расстояние между векторами. Всякий автоморфизм $\mathbb{F}_q^n$ можно описать парой $(\sigma; \pi)$, где π – перестановка позиций $\{1, \ldots, n\}$, σ – посимвольная перестановка, а образ вектора x определяется следующим образом:

$$(\sigma; \pi)(x) = \sigma(\pi(x)).$$

Композиция двух изометрий $(\sigma; \pi)$ и $(\delta; \pi')$ определяется как

$$(\sigma; \pi)(\delta; \pi') = (\sigma\delta'; \pi\pi'), \tag{2}$$

где $\delta' = \left(\delta_{\pi^{-1}(1)}, \ldots, \delta_{\pi^{-1}(n)}\right)$. Совокупность всех автоморфизмов $\mathbb{F}_q^n$ относительно операции композиции образует группу, обозначаемую $\mathrm{Aut}(\mathbb{F}_q^n)$.

Для всякой перестановки позиций π автоморфизм $(\sigma; \pi)$ называется *мономиальным*, если для каждого $i \in \{1, \ldots, n\}$ найдется ненулевой элемент α_i поля $\mathbb{F}_q$, такой что $\sigma_i(\gamma) = \alpha_i * \gamma$ для всякого $\gamma \in \mathbb{F}_q$, где через $*$ обозначено умножение в $\mathbb{F}_q$. Отметим, что всякий мономиальный автоморфизм является линейным. Пусть u – вектор из $\mathbb{F}_q^n$. Через σ_u обозначим посимвольную перестановку, такую что для всякого $x \in \mathbb{F}_q^n$

$$\sigma_u(x) = u + x, \tag{3}$$

где через $+$ обозначено сложение векторов в $\mathbb{F}_q^n$. Такие перестановки будем называть *трансляциями*.

Утверждение 1. *Для мономиального автоморфизма m пространства $\mathbb{F}_q^n$ и любого вектора и пространства $\mathbb{F}_q^n$ имеет место равенство*

$$m\sigma_u = \sigma_{m(u)}m.$$

Доказательство. В силу определения (3) трансляции σ_u и линейности мономиального автоморфизма m образ всякого вектора $x \in \mathbb{F}_q^n$ под действием автоморфизма $m\sigma_u$ равен

$$m\sigma_u(x) = m(u + x) = m(u) + m(x).$$

Вектор $m(u) + m(x)$ можно записать как $\sigma_{m(u)}m(x)$, откуда получаем требуемое. ▲

Группой автоморфизмов кода C называется стабилизатор кода C как множества в группе $\mathrm{Aut}(\mathbb{F}_q^n)$. Напомним, что действие группы на множестве M называется *регулярным*, если оно транзитивно и порядок группы совпадает с мощностью M. *Пропелинейным* (см. [17]; оригинальное определение было дано в [1]) называется q-ичный код, чья группа автоморфизмов содержит подгруппу, действующую регулярно на его кодовых словах. Два кода длины n называются *эквивалентными*, если найдется автоморфизм (изометрия) пространства $\mathbb{F}_q^n$, переводящий один код в другой.

Общей линейной группой $GL(r,q)$ называется группа невырожденных $(r \times r)$-матриц над $\mathbb{F}_q$. *Общей аффинной группой* $GA(r,q)$ называется группа преобразований (a,M), где a – вектор-столбец из $\mathbb{F}_q^r$, $M \in GL(r,q)$, действующих на векторах-столбцах $b \in \mathbb{F}_q^r$ следующим образом:

$$(a,M)(b) = a + Mb,$$

относительно композиции

$$(a,M)(b,M') = (a + Mb, MM'). \tag{4}$$

Подгруппа G группы $GA(r,q)$ называется *регулярной*, если она действует транзитивно на векторах из $\mathbb{F}_q^r$ и имеет порядок q^r. Другими словами, для всякого вектора $a \in \mathbb{F}_q^r$ найдется единственное аффинное преобразование g из G, такое что $g = (a,M)$ для некоторой матрицы $M \in GL(r,q)$. Очевидно, что группа трансляций на векторы из $\mathbb{F}_q^r$ является регулярной подгруппой $GA(r,q)$. Существует также большое число других регулярных подгрупп $GA(r,q)$ с разнообразными свойствами. В п. 4.2 рассмотрена регулярная подгруппа $GA(2,q)$, при простых q изоморфная группе трансляций, но не сопряженная с ней.

Через $\langle C \rangle$ обозначим линейную оболочку, натянутую на векторы кода C. Через $\dim(C)$ обозначим размерность линейного пространства C. Через $\mathrm{rank}(M)$ обозначим ранг матрицы M. *Рангом* кода C называется $\dim(\langle C \rangle)$, т.е. ранг его кодовой матрицы. Ранг кода длины n называется *полным* (*предполным*), если он равен n ($n-1$ соответственно).

В силу того, что при $q = 2, 3$ всякий автоморфизм является композицией мономиального автоморфизма и трансляции, имеем следующее (см., например, [18]):

Утверждение 2. *Если q равно 2 или 3, то ранг любого кода, содержащего нулевой вектор, является инвариантом класса эквивалентности этого кода.*

Замечание 1. Ситуацию при $q \geqslant 4$ проиллюстрируем на следующем примере. Пусть C – код Хэмминга с проверочной матрицей $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 \end{pmatrix}$, где α – примитивный элемент поля $\mathbb{F}_4$. Векторы $(00\alpha\alpha^2 1)$, $(00\alpha^2 1\alpha)$ принадлежат коду C. Рассмотрим посимвольную перестановку $\sigma = (\mathrm{Id}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}, (1\alpha))$. Заметим, что код $\sigma(C)$ содержит векторы $(00\alpha\alpha^2\alpha)$, $(00\alpha^2 11)$. Отсюда заключаем, что в линейной оболочке $\sigma(C)$ содержится вектор (00001) веса 1.

Таким образом, $\sigma(C)$ и C имеют ранги 4 и 3 соответственно. Отметим, что применяя подобные перестановки к q-ичному коду Хэмминга любой длины, можно строить коды, эквивалентные кодам Хэмминга, произвольных рангов от размерности кода до полного при любом $q \geqslant 4$. Таким образом, в случае $q \geqslant 4$ ранг кода, содержащего нулевой вектор, не является инвариантом класса эквивалентности.

§ 3. Пропелинейные совершенные коды из автоморфизмов регулярных подгрупп $GA(r,q)$

В данном параграфе приводится основная конструкция кодов. Построение базируется на методе Моллара, однако будет использовано более подходящее для нас из-

ложение Романова из [12], чему посвящен п. 3.1. Конструкция использует разбиение пространства предыдущей кодовой длины на коды Хэмминга. В п. 3.2 приводятся известные факты о действии общей линейной группы на смежных классах этого разбиения. Конструкция пропелинейных кодов приведена в п. 3.3, где мы воспользуемся автоморфизмами регулярных подгрупп $GA(r,q)$ для построения пропелинейных кодов.

3.1. Каскадная конструкция q-ичных совершенных кодов. Пусть H_C – проверочная матрица q-ичного кода Хэмминга C с r проверочными символами, H' – матрица размера $r \times q^r$, столбцами которой являются все векторы из $\mathbb{F}_q^r$. Построим проверочную матрицу q-ичного кода Хэмминга с $r+1$ проверками. Пусть в ее первой строке первые $\dfrac{q^r-1}{q-1}$ элементов являются нулевыми, а оставшиеся q^r элементов – единицы поля $\mathbb{F}_q$. Несложно видеть, что матрица

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} \\ H_C & H' \end{pmatrix} \tag{5}$$

является проверочной для q-ичного кода Хэмминга длины $\dfrac{q^{r+1}-1}{q-1}$.

Для $a \in \mathbb{F}_q^r$ через C_a обозначим смежный класс по коду C, синдром которого равен a:

$$C_a = \{x : \, x \in \mathbb{F}_q^{\frac{q^r-1}{q-1}}, \, H_C x^T = a\}. \tag{6}$$

Обозначим через D линейный код длины q^r с проверочной матрицей

$$H_D = \begin{pmatrix} \mathbf{1} \\ H' \end{pmatrix}, \tag{7}$$

где H', как и ранее, – матрица размера $r \times q^r$, столбцами которой являются все векторы из $\mathbb{F}_q^r$. Позиции кода D пронумеруем столбцами проверочной матрицы H_D: позиция имеет номер $a \in \mathbb{F}_q^r$, если $\begin{pmatrix} 1 \\ a \end{pmatrix}$ – соответствующий столбец проверочной матрицы H_D. Для $a \in \mathbb{F}_q^r$ через D_a обозначим смежный класс $D + e_{\mathbf{0}} - e_a$, где e_a – вектор с единицей только в позиции, занумерованной вектором a, в остальных позициях e_a равен нулю. Для перестановки τ на множестве векторов $\mathbb{F}_q^r$ рассмотрим следующий код:

$$S_\tau = \bigcup_{a \in \mathbb{F}_q^r} C_a \times D_{\tau(a)}.$$

Теорема 1 [11, 12]. *Для любой степени простого числа q и произвольной перестановки τ векторов $\mathbb{F}_q^r$ код S_τ является q-ичным совершенным кодом длины* $\dfrac{q^{r+1}-1}{q-1}$.

Заметим, что в силу определения C_a и D_a код Хэмминга $\bigcup\limits_{a \in \mathbb{F}_q^r} C_a \times D_a$ имеет проверочную матрицу (5), поэтому является частным случаем этой конструкции.

3.2. Действие $GL(r,q)$ на смежных классах по C и D. Следующие свойства кодов Хэмминга являются широко известными (см., например, [19, теорема 7.1]) или напрямую вытекают из обозначения для смежного класса C_a.

Утверждение 3. *Пусть C – код Хэмминга длины $\dfrac{q^r-1}{q-1}$ с проверочной матрицей H_C, и пусть C_a – смежный класс* (6). *Тогда*

1. *Для любых двух векторов a и b из $\mathbb{F}_q^r$ выполнено $C_a + C_b = C_{a+b}$;*
2. [19, теорема 7.1] *Для всякой матрицы $M \in GL(r,q)$ найдется мономиальный автоморфизм $m_M \in \mathrm{Aut}(C)$, такой что для любого вектора x выполнено*

$$H_C(m_M(x))^T = MH_Cx^T.$$

Отображение $M \to m_M$ является инъективным гомоморфизмом $GL(r,q)$ в группу $\mathrm{Aut}(C)$;
3. *Для всякого $a \in \mathbb{F}_q^r$ имеет место равенство $m_M(C_a) = C_{Ma}$.*

Рассмотрим гомоморфизм $GL(r,q)$ в группу автоморфизмов кода D. Если M – невырожденная $(r \times r)$-матрица над $\mathbb{F}_q$, то через π_M обозначим перестановку координатных позиций D, действующую следующим образом:

$$\pi_M(e_a) = e_{Ma}. \tag{8}$$

Очевидно, π_M является автоморфизмом кода D, проверочная матрица которого состоит из всех векторов из $\mathbb{F}_q^r$. Отметим также, что группа $\{\pi_M : M \in GL(r,q)\}$ также действует на множестве смежных классов D_a, $a \in \mathbb{F}_q^r$.

Утверждение 4. *Справедливо следующее*:
1. *Для любых векторов $a, b \in \mathbb{F}_q^r$ имеем $D_a + D_b = D_{a+b}$;*
2. *Отображение $M \to \pi_M$ является инъективным гомоморфизмом $GL(r,q)$ в группу* $\mathrm{Aut}(D)$. *Для любого $b \in \mathbb{F}_q^r$ имеет место*

$$\pi_M(D_b) = D_{Mb}.$$

Доказательство. 1. Заметим, что $D_a + D_b = D + 2e_{\mathbf{0}} - e_a - e_b$. Для доказательства равенства $D_a + D_b = D + e_{\mathbf{0}} - e_{a+b}$ достаточно показать, что вектор $2e_{\mathbf{0}} - e_a - e_b - (e_{\mathbf{0}} - e_{a+b}) = e_{\mathbf{0}} + e_{a+b} - e_a - e_b$ принадлежит коду D. В свою очередь, это вытекает из нумерации столбцов проверочной матрицы H_D кода D векторами из $\mathbb{F}_q^r$, а именно

$$H_D(e_{\mathbf{0}} + e_{a+b} - e_a - e_b)^T = \begin{pmatrix}1\\ \mathbf{0}\end{pmatrix} + \begin{pmatrix}1\\ a+b\end{pmatrix} - \begin{pmatrix}1\\ a\end{pmatrix} - \begin{pmatrix}1\\ b\end{pmatrix} = \begin{pmatrix}0\\ \mathbf{0}\end{pmatrix}.$$

2. Из того, что π_M – автоморфизм кода D, и из (8) имеем

$$\pi_M(D_b) = \pi_M(D + e_{\mathbf{0}} - e_b) = D + e_0 - e_{Mb} = D_{Mb}. \quad \blacktriangle$$

3.3. Пропелинейные коды из регулярных подгрупп $GA(r,q)$. Пусть G – регулярная подгруппа общей аффинной группы $GA(r,q)$. Тогда в силу определения регулярного действия для любого $a \in \mathbb{F}_q^r$ найдется единственное аффинное преобразование из группы G, обозначаемое везде далее через g_a, которое отображает вектор $\mathbf{0}$ в вектор a. Заметим, что так как $g_a(\mathbf{0}) = a$, то аффинное преобразование g_a принимает вид

$$g_a = (a, M_a) \tag{9}$$

для некоторой невырожденной матрицы M_a. Таким образом, q^r элементов всякой регулярной подгруппы группы $GA(r,q)$ занумерованы векторами из $\mathbb{F}_q^r$.

Используя введенную нумерацию, получим несколько равенств. Рассмотрим композицию преобразований g_a и g_b:

$$g_ag_b = (a, M_a)(b, M_b) = (a + M_ab, M_aM_b).$$

Аффинное преобразование $g_a g_b$ принадлежит группе G и отображает $\mathbf{0}$ в $a+M_a b$, что вытекает из приведенного выше выражения для $g_a g_b$. В силу регулярности действия G на векторах из $\mathbb{F}_q^r$ найдется единственное аффинное преобразование, переводящее $\mathbf{0}$ в вектор $g_a(b) = a+M_a b$. Используя введенную в (9) нумерацию элементов G через векторы $\mathbb{F}_q^r$, это преобразование обозначается $g_{g_a(b)}$.

Итак,

$$g_a g_b = (a + M_a b, M_a M_b) = g_{g_a(b)} = (a + M_a b, M_{g_a(b)}), \tag{10}$$

откуда

$$M_a M_b = M_{g_a(b)} = M_{a+M_a b}. \tag{11}$$

Пусть T – автоморфизм группы G, тогда перестановка τ векторов $\mathbb{F}_q^r$ вида $g_{\tau(a)} = T(g_a)$ для всякого $a \in \mathbb{F}_q^r$ называется перестановкой, *индуцированной автоморфизмом* T. Заметим, что всякий автоморфизм оставляет на месте нейтральный элемент группы, поэтому для всякой перестановки τ, индуцированной автоморфизмом, имеет место $\tau(\mathbf{0}) = \mathbf{0}$.

В силу определения индуцированной перестановки, а также учитывая преобразование $g_{g_a(b)} = g_a g_b$ (см. (10)), имеем

$$g_{\tau(g_a(b))} = (\tau(g_a(b)), M_{\tau(g_a(b))}) = T(g_{g_a(b)}) = T(g_a g_b).$$

Так как T автоморфизм, то $T(g_a g_b) = T(g_a)T(g_b)$, и следовательно,

$$T(g_a g_b) = T(g_a)T(g_b) = g_{\tau(a)} g_{\tau(b)} = (g_{\tau(a)}(\tau(b)), M_{\tau(a)} M_{\tau(b)}).$$

Отсюда можно заключить, что преобразования $(\tau(g_a(b)), M_{\tau(g_a(b))})$ и $(g_{\tau(a)}(\tau(b)), M_{\tau(a)} M_{\tau(b)})$ равны, а следовательно,

$$\tau(g_a(b)) = g_{\tau(a)}(\tau(b)), \tag{12}$$

$$M_{\tau(g_a(b))} = M_{\tau(a)} M_{\tau(b)}. \tag{13}$$

Т е о р е м а 2. *Пусть τ – перестановка векторов $\mathbb{F}_q^r$, индуцированная автоморфизмом регулярной подгруппы $GA(r,q)$. Тогда S_τ – пропелинейный q-ичный совершенный код длины $\dfrac{q^{r+1}-1}{q-1}$.*

Д о к а з а т е л ь с т в о. Пусть τ – перестановка, индуцированная автоморфизмом регулярной подгруппы G группы $GA(r,q)$. Напомним, что для всякого $a \in \mathbb{F}_q^r$ преобразование g_a – преобразование вида (9) из группы G.

Покажем, что следующее множество автоморфизмов $\mathbb{F}_q^r$ является группой:

$$\Gamma = \bigcup_{a \in \mathbb{F}_q^r} \big\{ (\sigma_x \,|\, \sigma_y)(m_{M_a} \,|\, \pi_{M_{\tau(a)}}) : (x \,|\, y) \in C_a \times D_{M_{\tau(a)}} \big\},$$

где σ_x, σ_y – трансляции, отвечающие векторам x и y (см. (3)), M_a – матричная часть преобразования $g_a \in G$ (см. (9)), m_{M_a} – мономиальный автоморфизм кода Хэмминга C, отвечающий матрице M_a, а $\pi_{M_{\tau(a)}}$ – перестановочный автоморфизм кода D, отвечающий матрице $M_{\tau(a)}$ (см. п. 3.2). Напомним, что $(x \,|\, y)$ – конкатенация векторов, на которой действует автоморфизм $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$, где операция $\cdot\,|\,\cdot$ определена в (1). Заметим, что для каждого фиксированного a в выражении для Γ, приведенном выше, $(x \,|\, y)$ пробегает код $C_a \times D_{\tau(a)}$, однозначно задавая трансляции $(\sigma_x \,|\, \sigma_y)$. При этом автоморфизм $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$ зависит лишь от a, поэтому $|\Gamma| = |S_\tau|$.

Рассмотрим композицию двух автоморфизмов из Γ и покажем, что автоморфизм

$$(\sigma_x \,|\, \sigma_y)(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v)(m_{M_b} \,|\, \pi_{M_{\tau(b)}}) \tag{14}$$

принадлежит Γ, где $x \in C_a$, $y \in D_{\tau(a)}$ и $u \in C_b$, $v \in D_{\tau(b)}$ для некоторых векторов a и b из $\mathbb{F}_q^r$. Преобразуем

$$(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v). \tag{15}$$

Так как $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})$ – мономиальный автоморфизм, а $(\sigma_u \,|\, \sigma_v)$ – трансляция, то в силу утверждения 1 имеем

$$(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(\sigma_u \,|\, \sigma_v) = (m_{M_a}\sigma_u \,|\, \pi_{M_{\tau(a)}}\sigma_v) = (\sigma_{m_{M_a}(u)} \,|\, \sigma_{\pi_{M_{\tau(a)}}(v)})(m_{M_a} \,|\, \pi_{M_{\tau(a)}}).$$

Обозначим векторы $m_{M_a}(u)$ и $\pi_{M_{\tau(a)}}(v)$ через u' и v' соответственно. Выражение (14) преобразуется в

$$(\sigma_x \,|\, \sigma_y)(\sigma_{u'} \,|\, \sigma_{v'})(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}}). \tag{16}$$

Вектор u принадлежит C_b, поэтому в силу п. 3 утверждения 3 имеем $m_{M_a}(u) \in$ $\in C_{M_a b}$, т.е.

$$u' \in C_{M_a b}. \tag{17}$$

В свою очередь, вектор v принадлежит $D_{\tau(b)}$, откуда в силу п. 2 утверждения 4 для $v' = \pi_{M_{\tau(a)}}(v)$ выполняется

$$v' \in D_{M_{\tau(a)}\tau(b)}. \tag{18}$$

Очевидно, что трансляции (перестановки вида (3)) коммутируют, поэтому для трансляций автоморфизма (16) выполнены следующие равенства: $\sigma_x\sigma_{u'} = \sigma_{x+u'}$ и $\sigma_y\sigma_{v'} = \sigma_{y+v'}$. Напомним, что $x \in C_a$, а также согласно (17) вектор $u' \in C_{M_a b}$, поэтому в силу п. 1 утверждения 3 вектор $x + u'$ принадлежит $C_{a+M_a(b)}$. Отсюда, учитывая, что аффинное преобразование g_a равно (a, M_a), имеем $g_a(b) = a + M_a(b)$. Следовательно, $C_{a+M_a(b)} = C_{g_a(b)}$ и

$$x + u' \in C_{g_a(b)}. \tag{19}$$

Имеем $y \in D_{\tau(a)}$, и в силу (18) $v' \in D_{M_{\tau(a)}\tau(b)}$. Тогда согласно п. 1 утверждения 4 получаем следующее:

$$y + v' \in D_{\tau(a)} + D_{M_{\tau(a)}\tau(b)} = D_{\tau(a)+M_{\tau(a)}\tau(b)}.$$

Заметим, что аффинное преобразование $g_{\tau(a)}$ равно $(\tau(a), M_{\tau(a)})$, и так как согласно (12) выполняется $g_{\tau(a)}(\tau(b)) = \tau(g_a(b))$, то

$$y + v' \in D_{\tau(a)+M_{\tau(a)}\tau(b)} = D_{g_{\tau(a)}(\tau(b))} = D_{\tau(g_a(b))}. \tag{20}$$

Итак, (16) преобразуется в

$$(\sigma_{x+u'} \,|\, \sigma_{y+v'})(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}}), \tag{21}$$

где $(x + u' \,|\, y + v') \in C_{g_a(b)} \times D_{\tau(g_a(b))}$ в силу (19) и (20).

Рассмотрим мономиальную часть $(m_{M_a} \,|\, \pi_{M_{\tau(a)}})(m_{M_b} \,|\, \pi_{M_{\tau(b)}})$ автоморфизма (21). Согласно п. 2 утверждения 3 отображение $M \to m_M$ является гомоморфизмом

$GL(r,q)$ в $\mathrm{Aut}(C)$, поэтому выполнено следующее:

$$m_{M_a} m_{M_b} = m_{M_a M_b}.$$

В свою очередь, в силу (11) выполняется $m_{M_a M_b} = m_{g_a(b)}$, поэтому

$$m_{M_a} m_{M_b} = m_{g_a(b)}. \tag{22}$$

Так как в силу п. 2 утверждения 4 отображение $M \to \pi_M$ является гомоморфизмом $GL(r,q)$ в $\mathrm{Aut}(D)$, то

$$\pi_{M_{\tau(a)}} \pi_{M_{\tau(b)}} = \pi_{M_{\tau(a)} M_{\tau(b)}}.$$

Согласно (13) справедливо $M_{\tau(a)} M_{\tau(b)} = M_{\tau(g_a(b))}$, и следовательно,

$$\pi_{M_{\tau(a)}} \pi_{M_{\tau(b)}} = \pi_{M_{\tau(g_a(b))}}. \tag{23}$$

Итак, автоморфизм (21) и, соответственно, исходная композиция автоморфизмов (14) преобразуется в

$$(\sigma_{x+u'} \,|\, \sigma_{y+v'})(m_{g_a(b)} \,|\, \pi_{M_{\tau(g_a(b))}}),$$

где $(x + u' \,|\, y + v') \in C_{g_a(b)} \times D_{\tau(g_a(b))}$, т.е. принадлежит Γ. Отсюда заключаем, что Γ является группой. Отметим, что трансляции $(\sigma_x \,|\, \sigma_y)$ в выражении для Γ таковы, что $(x \,|\, y)$ пробегают весь код S_τ, поэтому орбита нулевого вектора под действием Γ совпадает с кодом S_τ. Другими словами, группа Γ – подгруппа группы автоморфизмов кода S_τ, действующая транзитивно на его кодовых словах. Более того, так как порядок Γ совпадает с мощностью кода S_τ, то Γ также регулярна, а код S_τ пропелинеен. ▲

§ 4. Ранги кодов, полученных каскадной конструкцией

Пусть τ – перестановка векторов $\mathbb{F}_q^r$, оставляющая на месте $\mathbf{0}$. Так как позиции кода D занумерованы векторами $\mathbb{F}_q^r$, то τ также будем трактовать как перестановку позиций кода D. *Дефектом* перестановки τ будем называть разность $\dim(D) - \dim(D \cap \tau(D))$. Через $D^\perp$ обозначим код, дуальный к D. Заметим, что

$$\dim(D) - \dim(D \cap \tau(D)) = \dim((D \cap \tau(D))^\perp) - \dim(D^\perp).$$

В силу выражения для размерности суммы и пересечения подпространств имеем

$$\dim((D \cap \tau(D))^\perp) - \dim(D^\perp) = \dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - \dim(D^\perp) =$$
$$= \dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - r - 1.$$

Лемма 1. *Пусть $\mathbf{0}, a^2, \ldots, a^{q^r}$ – все векторы пространства $\mathbb{F}_q^r$, τ – любая перестановка этих векторов, $\tau(\mathbf{0}) = \mathbf{0}$, D – код с проверочной матрицей $H_D = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \mathbf{0} & a^2 & \ldots & a^{q^r} \end{pmatrix}$. Тогда дефект τ равен*

$$\mathrm{rank} \begin{pmatrix} a^2 & \ldots & a^{q^r} \\ \tau(a^2) & \ldots & \tau(a^{q^r}) \end{pmatrix} - r.$$

Доказательство. По определению дефект τ равен $\dim(\langle D^\perp \cup (\tau(D))^\perp \rangle) - r - 1$.

Размерность кода $\langle D^\perp \cup (\tau(D))^\perp \rangle$ можно выразить как $\mathrm{rank} \begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix}$, где $\tau(H_D)$ – проверочная матрица кода $\tau(D)$.

Подействовав перестановкой τ^{-1} на столбцы матрицы $\begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix}$, получим равенство $\operatorname{rank}\begin{pmatrix} H_D \\ \tau(H_D) \end{pmatrix} = \operatorname{rank}\begin{pmatrix} H_D \\ \tau^{-1}(H_D) \end{pmatrix}$. Матрица $\begin{pmatrix} H_D \\ \tau^{-1}(H_D) \end{pmatrix}$ равна

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \mathbf{0} & a^2 & \dots & a^{q^r} \\ 1 & 1 & \dots & 1 \\ \mathbf{0} & \tau(a^2) & \dots & \tau(a^{q^r}) \end{pmatrix},$$

и пространство ее строк раскладывается в прямую сумму ее первой строки и подматрицы $\begin{pmatrix} \mathbf{0} & a^2 & \dots & a^{q^r} \\ \mathbf{0} & \tau(a^2) & \dots & \tau(a^{q^r}) \end{pmatrix}$, откуда имеем требуемое выражение для дефекта. ▲

Отметим, что в следующей теореме код S_τ не обязательно является пропелинейным.

Теорема 3 [16]. *Пусть τ – перестановка векторов $\mathbb{F}_q^r$ с дефектом ℓ, такая что $\tau(\mathbf{0}) = \mathbf{0}$. Тогда ранг кода S_τ длины $\dfrac{q^{r+1}-1}{q-1}$ равен $\dfrac{q^{r+1}-1}{q-1} - r - 1 + \ell$.*

В п. 4.1 введем подход, позволяющий строить перестановки векторов пространства $\mathbb{F}_q^r$ с увеличивающимся дефектом из существующих перестановок пространств $\mathbb{F}_q^{r'}$ и $\mathbb{F}_q^{r-r'}$. Этот подход позволяет строить коды с растущей прибавкой ранга по отношению к размерности кода Хэмминга. В п. 4.2 рассмотрим конструкцию перестановки τ, индуцированной автоморфизмом регулярной подгруппы, дающую бесконечную серию пропелинейных совершенных кодов S_τ растущей длины.

4.1. Дефект итерации перестановок. Пусть τ и σ – биекции (перестановки) на себя множеств векторов из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$ соответственно, $\tau(\mathbf{0}) = \mathbf{0}$, $\sigma(\mathbf{0}) = \mathbf{0}$. Всякий вектор-столбец из $\mathbb{F}_q^{r_1+r_2}$ представляет собой конкатенацию $\begin{pmatrix} a \\ b \end{pmatrix}$ некоторых векторов-столбцов $a \in \mathbb{F}_q^{r_1}$ и $b \in \mathbb{F}_q^{r_2}$. В соответствии с (1) определим *итерацию перестановок* τ и σ как перестановку $\tau \,|\, \sigma$, которая отображает вектор-столбец $\begin{pmatrix} a \\ b \end{pmatrix}$ пространства $\mathbb{F}_q^{r_1+r_2}$, где a и b – векторы-столбцы из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$, следующим образом:

$$(\tau \,|\, \sigma)\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau(a) \\ \sigma(b) \end{pmatrix}. \tag{24}$$

Утверждение 5. *Пусть τ и σ – перестановки множеств векторов из $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$ соответственно, индуцированные автоморфизмами некоторых регулярных подгрупп $GA(r_1, q)$ и $GA(r_2, q)$ соответственно. Тогда $\tau \,|\, \sigma$ – подстановка, индуцированная автоморфизмом некоторой регулярной подгруппы $GA(r_1 + r_2, q)$.*

Доказательство. Пусть G_1 и G_2 – регулярные подгруппы групп $GA(r_1, q)$ и $GA(r_2, q)$. Для элементов $(a, M) \in G_1$ и $(b, M') \in G_2$ рассмотрим следующее аффинное преобразование из $GA(r_1 + r_2, q)$, которое обозначим через $(a, M) \times (b, M')$:

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} M & 0 \\ 0 & M' \end{pmatrix}\right).$$

Заметим, что $\{(a, M) \times (b, M') : (a, M) \in G_1,\ (b, M') \in G_2\}$ является прямым произведением групп G_1 и G_2 и, более того, является регулярной подгруппой $GA(r_1 + r_2, q)$ (см., например, [15, § 6]). Обозначим эту группу через $G_1 \times G_2$.

Пусть T и S – автоморфизмы групп G_1 и G_2 с индуцированными перестановками τ и σ соответственно. Автоморфизмы T и S являются перестановками элементов

групп G_1 и G_2 соответственно. Определим перестановку $T \times S$ элементов группы $G_1 \times G_2$, действующую на аффинных преобразованиях из $G_1 \times G_2$ следующим образом: $(T \times S)(g_1 \times g_2) = T(g_1) \times S(g_2)$. Очевидно, что $T \times S$ является автоморфизмом группы $G_1 \times G_2$ и индуцированная перестановка автоморфизма $T \times S$ есть $\tau \,|\, \sigma$, определенная ранее в (24). ▲

Теорема 4. *Пусть τ и φ – перестановки векторов пространств $\mathbb{F}_q^{r_1}$ и $\mathbb{F}_q^{r_2}$, $q \geqslant 2$, с дефектами ℓ_1 и ℓ_2 соответственно, $\tau(\mathbf{0}) = \mathbf{0}$, $\varphi(\mathbf{0}) = \mathbf{0}$. Тогда дефект перестановки $\tau \,|\, \varphi$ равен $\ell_1 + \ell_2$.*

Доказательство. Рассмотрим следующую нумерацию всех q-ичных векторов длины $r_1 + r_2$. Всякий вектор-столбец длины $r_1 + r_2$ является конкатенацией двух векторов длин r_1 и r_2. Пусть векторы длин r_1 и и r_2 занумерованы в некотором порядке, начиная с нулевых векторов: $\mathbf{0}, a^2, \ldots, a^{q^{r_1}}$ и $\mathbf{0}, b^2, \ldots, b^{q^{r_2}}$. Перечислим $q^{r_1+r_2}$ векторов длины $r_1 + r_2$ в следующем порядке: вначале перечислим все векторы (q^{r_2} штук), первые r_1 позиций которых равны нулевому вектору $\mathbf{0}$, потом все векторы, первые r_1 позиций которых равны a^2, и т.д.

Применяя лемму 1 для указанной нумерации векторов из $\mathbb{F}_q^{r_1+r_2}$, получаем, что дефект перестановки $(\tau \,|\, \varphi)$ равен

$$\operatorname{rank}(M) - r_1 - r_2, \tag{25}$$

где M – матрица

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}}) \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

Ранг матрицы M равен рангу следующей матрицы:

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}}) \\
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

В силу расположения нулевых векторов в этой матрице, пространство ее строк раскладывается в прямую сумму пространств строк следующих двух ее подматриц:

$$\begin{pmatrix}
\mathbf{0} & \ldots & \mathbf{0} & a^2 & a^2 & \ldots & a^2 & \ldots & a^{q^{r_1}} & a^{q^{r_1}} & \ldots & a^{q^{r_1}} \\
\mathbf{0} & \ldots & \mathbf{0} & \tau(a^2) & \tau(a^2) & \ldots & \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) & \tau(a^{q^{r_1}}) & \ldots & \tau(a^{q^{r_1}})
\end{pmatrix},$$
$$\begin{pmatrix}
b^2 & \ldots & b^{q^{r_2}} & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} & \ldots & \mathbf{0} & b^2 & \ldots & b^{q^{r_2}} \\
\varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) & \ldots & \mathbf{0} & \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}})
\end{pmatrix}.$$

Удалив повторяющиеся и нулевые столбцы из матриц, получаем следующее:

$$\operatorname{rank}(M) = \operatorname{rank}\begin{pmatrix} a^2 & \ldots & a^{q^{r_1}} \\ \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) \end{pmatrix} + \operatorname{rank}\begin{pmatrix} b^2 & \ldots & b^{q^{r_2}} \\ \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) \end{pmatrix}.$$

По лемме 1 ранги матриц $\begin{pmatrix} a^2 & \ldots & a^{q^{r_1}} \\ \tau(a^2) & \ldots & \tau(a^{q^{r_1}}) \end{pmatrix}$ и $\begin{pmatrix} b^2 & \ldots & b^{q^{r_2}} \\ \varphi(b^2) & \ldots & \varphi(b^{q^{r_2}}) \end{pmatrix}$ равны $\ell_1 + r_1$ и $\ell_2 + r_2$ соответственно, где ℓ_1 и ℓ_2 –дефекты перестановок τ и φ соответственно, поэтому $\operatorname{rank}(M) = r_1 + r_2 - \ell_1 - \ell_2$. Отсюда из (25) получаем, что дефект $(\tau \,|\, \varphi)$ равен $\ell_1 + \ell_2$. ▲

Замечание 2. Отметим, что частный случай теоремы 4 при $q = 2$ был доказан в [6, лемма 3], однако доказательство содержит ошибку.

4.2. Бесконечная серия пропелинейных совершенных кодов различных рангов над простым алфавитом.

Пример 1. Пусть q – простое число, $q > 2$. Ниже мы рассмотрим регулярную подгруппу $GA(2, q)$, изоморфную $\mathbb{Z}_q^2$, но не сопряженную с подгруппой трансляций на векторы из $\mathbb{F}_q^2$ в группе $GA(2, q)$. Покажем, что существует автоморфизм этой группы, такой что дефект индуцированной им перестановки равен 2.

Рассмотрим следующие аффинные преобразования:

$$g = \left(\begin{pmatrix}1\\0\end{pmatrix}, \mathrm{Id}\right), \quad h = \left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right).$$

По индукции покажем, что для любого i имеет место

$$h^i = \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\right). \tag{26}$$

Предположим, что для некоторого i выполнено равенство (26), тогда по определению композиции (4) имеем

$$\begin{aligned}
h^{i+1} &= \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}i(i-1)\\ i\end{pmatrix} + \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2i\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}i(i-1)+2i\\ i+1\end{pmatrix}, \begin{pmatrix}1 & 2i+2\\0 & 1\end{pmatrix}\right) = \left(\begin{pmatrix}i(i+1)\\ i+1\end{pmatrix}, \begin{pmatrix}1 & 2i+2\\0 & 1\end{pmatrix}\right).
\end{aligned}$$

Таким образом, формула (26) выполнена для любого i. Из (26) вытекает, что h имеет порядок q.

Заметим, что $gh = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right)$. Более того,

$$\begin{aligned}
hg &= \left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}1\\0\end{pmatrix}, \mathrm{Id}\right) = \left(\begin{pmatrix}0\\1\end{pmatrix} + \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right) = \\
&= \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}\right).
\end{aligned}$$

Таким образом, g и h коммутируют и имеют порядок q, поэтому группа, порожденная этими элементами, изоморфна $\mathbb{Z}_q^2$. Покажем, что эта группа является регулярной подгруппой $GA(2, q)$. Учитывая формулу (26), имеем

$$g^i h^j = \left(\begin{pmatrix}i\\0\end{pmatrix}, \mathrm{Id}\right)\left(\begin{pmatrix}j(j-1)\\ j\end{pmatrix}, \begin{pmatrix}1 & 2j\\0 & 1\end{pmatrix}\right) = \left(\begin{pmatrix}i+j(j-1)\\ j\end{pmatrix}, \begin{pmatrix}1 & 2j\\0 & 1\end{pmatrix}\right). \tag{27}$$

Если упорядоченная пара (i, j) не равна паре (i', j'), то векторы $\begin{pmatrix}i+j(j-1)\\ j\end{pmatrix}$ и $\begin{pmatrix}i'+j'(j'-1)\\ j'\end{pmatrix}$ различны. Поэтому группа, порожденная g и h, является регулярной подгруппой $GA(2, q)$.

Так как группа, порожденная g и h, изоморфна $\mathbb{Z}_q^2$, то перестановка T ее элементов, такая что

$$T(g^i h^j) = h^i g^j$$

для всех $i, j \in \{0, \ldots, q-1\}$, является автоморфизмом этой группы порядка 2. Заметим, что в силу формулы (27) выполняется

$$g^i h^j = \left(\begin{pmatrix} i + j(j-1) \\ j \end{pmatrix}, \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix} \right)$$

и, так как g и h коммутируют,

$$h^i g^j = \left(\begin{pmatrix} j + i(i-1) \\ i \end{pmatrix}, \begin{pmatrix} 1 & 2i \\ 0 & 1 \end{pmatrix} \right).$$

Рассмотрим перестановку τ, индуцированную автоморфизмом T. По определению перестановки τ, индуцированной автоморфизмом T, имеем $T((a, M)) = (\tau(a), M')$, где (a, M) – элемент рассматриваемой регулярной группы. Поэтому, учитывая данные выше выражения для $g^i h^j$ и $h^i g^j$, для произвольных $i, j \in \{0, \ldots, q-1\}$ справедливо

$$\tau \begin{pmatrix} i + j(j-1) \\ j \end{pmatrix} = \begin{pmatrix} j + i(i-1) \\ i \end{pmatrix}.$$

В частности, когда пары (i, j) равны $(1, 0)$, $(0, 1)$, $(-1, -2)$, $(0, 2)$, имеем

$$\tau \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \tau \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \tau \begin{pmatrix} 5 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \tau \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}. \tag{28}$$

Покажем, что дефект перестановки τ равен 2. Так как $r = 2$, то по лемме 1 дефект τ равен $\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} - 2$, где $a^2, \ldots, a^{q^2}$ – ненулевые векторы $\mathbb{F}_q^2$. Покажем, что $\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(a^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} = 4$, т.е. перестановка τ имеет дефект 2.

Возьмем следующие векторы $a^2, \ldots, a^5$: $a^2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $a^3 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $a^4 = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$, $a^5 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$. Учитывая равенства (28), производя невырожденные линейные преобразования со строками матрицы, убеждаемся, что ее строки линейно независимы:

$$\operatorname{rank} \begin{pmatrix} a^2 & \ldots & a^{q^2} \\ \tau(b^2) & \ldots & \tau(a^{q^2}) \end{pmatrix} =$$

$$= \operatorname{rank} \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 1 & 0 & 2 & \ldots \\ 1 & 0 & -1 & 0 & \ldots \end{pmatrix} = \operatorname{rank} \begin{pmatrix} 1 & 0 & 5 & 2 & \ldots \\ 0 & 1 & -2 & 2 & \ldots \\ 0 & 0 & 2 & 0 & \ldots \\ 0 & 0 & 6 & 2 & \ldots \end{pmatrix} = 4.$$

Следовательно, τ имеет дефект 2.

Т е о р е м а 5. *Для всякого простого q, $q \geqslant 3$, и любых $r \geqslant 2$, $i \in \{0, \ldots, \lfloor r/2 \rfloor\}$ существует пропелинейный q-ичный совершенный код S_φ длины $\dfrac{q^{r+1}-1}{q-1}$ ранга $\dfrac{q^{r+1}-1}{q-1} - r - 1 + 2i$.*

Д о к а з а т е л ь с т в о. Пусть τ – перестановка векторов $\mathbb{F}_q^2$ с дефектом 2, индуцированная автоморфизмом регулярной подгруппы из примера 1. Рассмотрим пере-

становку

$$\varphi = \tau \,|\, \ldots \,|\, \tau \,|\, \mathrm{id} \,|\, \ldots \,|\, \mathrm{id}$$

векторов $\mathbb{F}_q^r$, где τ взята i раз, а тождественная перестановка взята $r - 2i$ раз. По утверждению 5 эта перестановка индуцирована автоморфизмом, поэтому по теореме 2 код S_φ – пропелинейный. По теореме 4 дефект перестановки φ равен $2i$, откуда в силу теоремы 3 имеем требуемое значение для ранга S_φ. ▲

Замечание 3. Отметим, что при $q = 3$ ранг является инвариантом, поэтому все $\lfloor r/2 \rfloor + 1$ кодов, описанных в теореме 5, попарно неэквивалентны. Следовательно, все из них, кроме линейного, отличаются от кодов, построенных в работе [5], так как последние либо линейные, либо имеют ранг, на единицу превосходящий размерность кода Хэмминга той же длины. При $q \geqslant 4$ коды из классов эквивалентности кодов из доказательства теоремы 5, скорее всего, также не могут иметь ранг, на единицу превосходящий размерность кода Хэмминга той же длины. Однако показать это представляется технически трудным.

Автор выражает благодарность Ф.И. Соловьевой, в дискуссиях с которой появилась часть утверждений и подходов данной статьи, а также рецензенту за ценные замечания и предложения, позволившие улучшить изложение материала.

СПИСОК ЛИТЕРАТУРЫ

1. *Rifà J., Basart J.M., Huguet L.* On Completely Regular Propelinear Codes // Proc. 6th Int. Conf. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-6). Rome, Italy. July 4–8, 1988. Lect. Notes Comp. Sci. V. 357. Berlin: Springer, 1989. P. 341–355. https://doi.org/10.1007/3-540-51083-4_71
2. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
3. *Соловьева Ф.И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск: Ин-т матем. СО АН СССР, 1981. С. 65–76.
4. *Borges J., Mogilnykh I.Yu., Rifà J., Solov'eva F.I.* Structural Properties of Binary Propelinear Codes // Adv. Math. Commun. 2012. V. 6. № 3. P. 329–346. https://doi.org/10.3934/amc.2012.6.329
5. *Krotov D.S., Potapov V.N.* Propelinear 1-Perfect Codes from Quadratic Functions // IEEE Trans. Inform. Theory. 2014. V. 60. № 4. P. 2065–2068. https://doi.org/10.1109/TIT.2014.2303158
6. *Mogilnykh I.Yu., Solov'eva F.I.* A Concatenation Construction for Propelinear Perfect Codes from Regular Subgroups of $GA(r, 2)$ // Сиб. электрон. матем. изв. 2019. Т. 16. С. 1689–1702. https://doi.org/10.33048/semi.2019.16.119
7. *Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319. https://doi.org/10.1109/18.312154
8. *Borges J., Phelps K.P., Rifà J., Zinoviev V.A.* On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 11. P. 2834–2843. https://doi.org/10.1109/TIT.2003.819329
9. *Зиновьев В.А., Зиновьев Д.В.* Обобщенные коды Препараты и 2-разрешимые системы четверок Штейнера // Пробл. передачи информ. 2016. V. 52. № 2. С. 15–36. http://mi.mathnet.ru/ppi2201
10. *Krotov D.S., Potapov V.N.* Constructions of Transitive Latin Hypercubes // European J. Combin. 2016. V. 54. P. 51–64. https://doi.org/10.1016/j.ejc.2015.12.001
11. *Mollard M.* Une novelle famille de 3-codes parfaits sur $GF(q)$ // Discrete Math. 1984. V. 49. № 2. P. 209–212. https://doi.org/10.1016/0012-365X(84)90121-3
12. *Romanov A.M.* On Non-Full-Rank Perfect Codes over Finite Fields // Des. Codes Cryptogr. 2019. V. 87. № 5. P. 995–1003. https://doi.org/10.1007/s10623-018-0506-1

13. *Mogilnykh I.Yu., Solov'eva F.I.* Coordinate Transitivity of a Class of Extended Perfect Codes and Their SQS // Сиб. электрон. матем. изв. 2020. Т. 17. С. 1451–1462. https://doi.org/10.33048/semi.2020.17.101
14. *Gillespie N.I., Praeger C.E.* New Characterisations of the Nordstrom–Robinson Codes // Bull. London Math. Soc. 2017. V. 49. № 2. P. 320–330. https://doi.org/10.1112/blms.12016
15. *Pellegrini M.A., Tamburini Bellani M.C.* More on Regular Subgroups of the Affine Group // Linear Algebra Appl. 2016. V. 505. P. 126–151. https://doi.org/10.1016/j.laa.2016.04.031
16. *Mogilnykh I.Yu.* q-ary Propelinear Perfect Codes from the Regular Subgroups of the $GA(r, q)$ and Their Ranks, https://arXiv.org/abs/2112.08659 [math.CO], 2021.
17. *Phelps K.T., Rifà J.* On Binary 1-Perfect Additive Codes: Some Structural Properties // IEEE Trans. Inform. Theory. 2002. V. 48. № 9. P. 2587–2592. https://doi.org/10.1109/TIT.2002.801474
18. *Горкунов Е.В.* Группы автоморфизмов кодов Хэмминга и их компонент: Дис. ... канд. физ.-мат. наук: 01.01.09. Новосибирск: НГУ, 2010.
19. *Huffman W.C.* Codes and Groups // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. Ch. 6. P. 1345–1440.

Могильных Иван Юрьевич
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
ivmog@math.nsc.ru

Поступила в редакцию
17.12.2021
После доработки
10.02.2022
Принята к публикации
12.02.2022