

УДК 621.391.15

МОНОМИАЛЬНЫЕ АВТОМОРФИЗМЫ ЛИНЕЙНОЙ И ПРОСТОЙ КОМПОНЕНТ КОДА ХЭММИНГА *)

Е. В. Горкунов

Аннотация. Линейная и простая компоненты кода Хэмминга — это линейные оболочки множества кодовых слов веса три с фиксированной координатой, равной 1, взятые над конечным полем \mathbb{F}_q и простым подполем \mathbb{F}_p соответственно. Дано описание групп мономиальных автоморфизмов этих компонент. Вычислен порядок группы мономиальных автоморфизмов линейной компоненты.

Ключевые слова: линейная компонента, простая компонента, код Хэмминга, группа мономиальных автоморфизмов.

Введение

В статье исследуются группы мономиальных автоморфизмов двух схожих по структуре подкодов q -ичного кода Хэмминга — линейной и простой компонент. Эти подкоды являются линейными оболочками множества кодовых троек кода Хэмминга, имеющих в фиксированной координате 1, взятыми над конечным полем и его простым подполем соответственно. На основе сдвигов линейной компоненты С. В. Августинович и Ф. И. Соловьёва [1] разработали методы построения новых совершенных кодов, названные методами i - и $\tilde{\alpha}$ -компонент. Развитием этих подходов стал метод простых компонент, используя который, А. В. Лось [6] построил семейство различных совершенных q -ичных кодов, являющееся при $q > 2$ наиболее мощным из известных в настоящее время. Перечисленные методы оказались также плодотворными для исследования свойств совершенных q -ичных кодов (см., например, Фелпс и др. [18], А. В. Лось [5]). Основным результатом настоящей статьи являются теоремы о строении групп мономиальных автоморфизмов линейной и простой компонент. Для линейной компоненты получен порядок указанной группы.

*) Исследование выполнено при частичной поддержке Лаборатории НГУ–Интел (Новосибирск).

Приведём основные определения. Пусть $\mathbb{F}_q = GF(q)$ — поле Галуа порядка q , где q — степень простого числа. Через \mathbb{F}_q^* обозначим мультипликативную группу поля \mathbb{F}_q . Расстояние Хэмминга $d(x, y)$ между векторами $x, y \in \mathbb{F}_q^n$ определяется как число координат, в которых эти векторы различаются. Расстояние $d(x, 0)$ до нулевого вектора 0 называется *весом Хэмминга* $x \in \mathbb{F}_q^n$ и обозначается через $w(x)$. *Носителем вектора* $x = (x_1, \dots, x_n)$ из \mathbb{F}_q^n называется множество

$$\text{supp}(x) = \{i \mid x_i \neq 0\}.$$

Произвольное подмножество $C \subseteq \mathbb{F}_q^n$ называется *q -ичным кодом* длины n . Код, образующий k -мерное линейное подпространство в пространстве \mathbb{F}_q^n , называется *линейным* или $[n, k]$ -кодом. Элементы кода суть *кодированные слова*. Кодовые слова веса 3 назовём *тройками*. *Носителем* $\text{supp}(C)$ кода C называется объединение носителей его кодовых слов, *кодowym расстоянием* — число

$$d = d(C) = \min_{x, y \in C, x \neq y} d(x, y).$$

Если шары заданного радиуса $t \geq 0$ с центрами в кодовых словах C образуют разбиение пространства \mathbb{F}_q^n , то код C называется *совершенным*. Широко известно (см., например, Мак-Вильямс и Слоэн [7]), что произвольный нетривиальный совершенный код над конечным полем либо исправляет одну ошибку, либо является двоичным или троичным кодом Голея, исправляющим 3 или 2 ошибки соответственно. Всюду далее термин *совершенный* относится к коду, исправляющему *одну* ошибку. Такой код должен иметь длину $N = (q^m - 1)/(q - 1)$ и мощность q^{N-m} . Единственным линейным совершенным кодом является код Хэмминга \mathcal{H} . Этот код существует для любого $m \geq 2$ и является единственным с точностью до изометрии пространства \mathbb{F}_q^N . Тем не менее, существует множество нелинейных совершенных q -ичных кодов, впервые построенных Ю. Л. Васильевым [3], а позднее — Шёнхаймом [19], Линдстрёмом [15] и многими другими авторами (см., например, [21]).

1. Автоморфизмы кода

В этом разделе приведём определения групп автоморфизмов кодов и некоторые известные результаты по исследованию этих групп.

Отображение $\varphi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ называется *изометрией* пространства \mathbb{F}_q^n , если φ сохраняет расстояние между любыми векторами $x, y \in \mathbb{F}_q^n$, т. е. $d(x, y) = d(\varphi(x), \varphi(y))$.

Пусть S_n — симметрическая группа подстановок порядка n на множестве $\{1, 2, \dots, n\}$. Образ произвольного вектора $x = (x_1, \dots, x_n)$ из пространства \mathbb{F}_q^n под действием подстановки $\pi \in S_n$ определяется равенством

$$x\pi = (x_{1\pi^{-1}}, \dots, x_{n\pi^{-1}}). \quad (1)$$

Например, для случая $n = 3$ и подстановки $\pi = (123)$ имеем

$$(x_1, x_2, x_3)(123) = (x_3, x_1, x_2).$$

Следуя Константиnescу и Хайзе [13], назовём *конфигурацией* изометрию $\sigma: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, заданную правилом

$$x\sigma = (x_1\sigma_1, \dots, x_n\sigma_n), \quad (2)$$

где $\sigma = (\sigma_1, \dots, \sigma_n)$ — набор подстановок из симметрической группы S_q , действующий на элементах поля \mathbb{F}_q .

А. А. Марков [9] в 1956 г. доказал, что группа изометрий \mathbb{F}_q^n является полупрямым произведением группы S_n на группу S_q^n всех конфигураций этого пространства, т. е.

$$\text{Aut}(\mathbb{F}_q^n) = S_n \ltimes S_q^n = \{(\pi; \sigma) \mid \pi \in S_n, \sigma = (\sigma_1, \dots, \sigma_n) \in S_q^n\}. \quad (3)$$

Групповая операция между двумя элементами $(\pi; \sigma)$ и $(\tau; \delta)$ в полупрямом произведении $S_n \ltimes S_q^n$ определяется формулой

$$(\pi; \sigma)(\tau; \delta) = (\pi\tau; \sigma\tau \cdot \delta), \quad (4)$$

где действие подстановки τ на конфигурации σ определяется аналогично (1), а умножение между конфигурациями $\sigma\tau$ и δ производится покомпонентно.

Группа всех изометрий пространства \mathbb{F}_q^n , отображающих код C в себя, называется *группой автоморфизмов* кода C и обозначается через

$$\text{Aut}(C) = \{(\pi; \sigma) \in \text{Aut}(\mathbb{F}_q^n) \mid C(\pi; \sigma) = C\}.$$

Необходимо отметить, что приведённое определение группы автоморфизмов кода согласуется с определением Константиnescу и Хайзе [13] и отличается от традиционного. Например, у Мак-Вильямс и Слоэна [7], Хаффмана [14], а также у других авторов она определяется как группа *полулинейных* изометрий пространства, отображающих код в себя. При $q \geq 4$ полулинейные изометрии пространства \mathbb{F}_q^n составляют собственную подгруппу группы $\text{Aut}(\mathbb{F}_q^n)$ (см. (3)).

Пусть α — примитивный элемент поля \mathbb{F}_q . Если все элементы \mathbb{F}_q умножить на некоторый фиксированный элемент $\lambda \in \mathbb{F}_q^*$, то получим подстановку

$$\begin{pmatrix} 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \\ 0 & \alpha^0 \lambda & \alpha^1 \lambda & \dots & \alpha^{q-2} \lambda \end{pmatrix} \quad (5)$$

из S_q , которую назовём *подстановкой умножения*. Через S_q^* обозначим подгруппу, порождённую всеми подстановками умножения. Заметим, что $S_q^* \cong \mathbb{F}_q^*$. Элемент поля $\lambda \in \mathbb{F}_q$ и соответствующую подстановку умножения (5) будем обозначать одинаково, подчёркивая при необходимости о чём идёт речь.

Группой мономиальных автоморфизмов кода C называется множество

$$\text{MAut}(C) = \{(\pi; \sigma) \in \text{Aut}(C) \mid \sigma \in (S_q^*)^n\}.$$

Конфигурацию $(\lambda, \dots, \lambda)$, все компоненты которой равны одной подстановке умножения λ , обозначим через Λ . Например, под записью $\sigma\Lambda$, где $\sigma = (\sigma_1, \dots, \sigma_n)$ — некоторая конфигурация, подразумевается

$$\sigma\Lambda = (\sigma_1, \dots, \sigma_n) \cdot (\lambda, \dots, \lambda) = (\sigma_1\lambda, \dots, \sigma_n\lambda).$$

Полупрямое произведение $S_n \ltimes (S_q^*)^n$ является группой всех мономиальных автоморфизмов пространства \mathbb{F}_q^n . Имеется естественный изоморфизм между $S_n \ltimes (S_q^*)^n$ и группой $M_n(q)$ мономиальных матриц порядка n над полем \mathbb{F}_q . Напомним, что *мономиальной* называется матрица, у которой в каждой строке и в каждом столбце имеется ровно один ненулевой элемент из \mathbb{F}_q . Любая такая матрица единственным образом представляется в виде произведения матрицы подстановки и диагональной матрицы. Мономиальному автоморфизму $(\pi; (\lambda_1, \dots, \lambda_n))$ соответствует мономиальная матрица $M = PD$, где P — матрица подстановки π , а $D = D(\lambda_1, \dots, \lambda_n)$ — диагональная матрица с элементами $\lambda_1, \dots, \lambda_n$ на главной диагонали. Действие мономиального автоморфизма $(\pi; \sigma) \in \text{MAut}(\mathbb{F}_q^n)$ на произвольном векторе $x \in \mathbb{F}_q^n$, заданное в (1) и (2), согласовано с обычным умножением этого вектора на матрицу M :

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

Пусть ε обозначает конфигурацию, все компоненты которой являются тождественными подстановками. *Группой перестановочных автоморфизмов* кода C называется множество

$$\text{PAut}(C) = \{(\pi; \varepsilon) \in \text{Aut}(C)\}.$$

Нетрудно видеть, что проекции групп $\text{Aut}(C)$ и $\text{MAut}(C)$ на S_n являются группами. Следуя Хаффману [14], обозначим их через

$$\begin{aligned}\text{Aut}_{\text{pr}}(C) &= \{\pi \mid \exists (\pi; \sigma) \in \text{Aut}(C)\}, \\ \text{MAut}_{\text{pr}}(C) &= \{\pi \mid \exists (\pi; \sigma) \in \text{MAut}(C)\}.\end{aligned}$$

Вместе с тем для любого кода C группа перестановочных автоморфизмов $\text{PAut}(C)$ и её проекция на S_n изоморфны. Поэтому произвольная изометрия вида $(\pi; \varepsilon)$ естественно отождествляется с подстановкой π , а группа перестановочных автоморфизмов кода также определяется как множество подстановок

$$\text{PAut}(C) = \{\pi \in S_n \mid (\pi; \varepsilon) \in \text{Aut}(C)\}.$$

Широко известен результат Фелпса [17]: каждая конечная группа изоморфна группе перестановочных автоморфизмов некоторого совершенного двоичного кода. Однако структура *всей* группы автоморфизмов этого кода при этом остаётся неизвестной. Пусть C — некоторый совершенный двоичный код. Из свойства антиподальности [20] кода C следует, что группа автоморфизмов $\text{Aut}(C)$ содержит тождественную подстановку координат e и сдвиг на вектор $\mathbf{1}$, состоящий из всех единиц. Если группа $\text{Aut}(C)$ состоит только из указанных двух преобразований, она называется *тривиальной*. С. В. Августинович и Ф. И. Соловьёва [12], а также С. А. Малюгин [16] доказали существование систематических и несистематических (соответственно) совершенных двоичных кодов с тривиальными группами автоморфизмов.

В [2] исследована структура группы перестановочных автоморфизмов кодов Васильева. Там же, в частности, доказано, что группа перестановочных автоморфизмов линейной компоненты двоичного кода Хэмминга \mathcal{H} длины $N = 2^m - 1$ изоморфна полупрямому произведению $S_n \ltimes S_2^n$, где $n = 2^{m-1} - 1$.

Известно (см., например, [7]), что группа перестановочных автоморфизмов двоичного кода Хэмминга \mathcal{H} длины $N = 2^m - 1$ изоморфна общей линейной группе $GL_m(2)$ невырожденных матриц. Поскольку код Хэмминга линейен, его группа автоморфизмов (в двоичном случае) представима в виде

$$\text{Aut}(\mathcal{H}) \cong GL_m(2) \ltimes \mathcal{H}.$$

Ф. И. Соловьёва и С. Т. Топалова сначала в [10] показали максимальность порядка группы $\text{Aut}(\mathcal{H})$ среди групп автоморфизмов совершенных двоичных кодов одинаковой длины, а затем в [11] доказали, что указанный максимальный порядок группы автоморфизмов имеет только код

Хэмминга. Одновременно С. А. Малюгин [8] для произвольного нелинейного совершенного двоичного кода C установил, что

$$|\text{Aut}(C)| \leq \frac{1}{2} |\text{Aut}(\mathcal{H})|.$$

Общую структуру группы мономиальных автоморфизмов линейного q -ичного кода с кодовым расстоянием $d \geq 3$ описывает

Теорема 1 [14, теорема 7.1]. *Группа мономиальных автоморфизмов линейного кода C с кодовым расстоянием $d \geq 3$ и проверочной $(m \times n)$ -матрицей H изоморфна подгруппе группы $GL_m(q)$.*

В частности, хорошо известно [14, теорема 7.2], что группа мономиальных автоморфизмов кода Хэмминга изоморфна общей линейной группе

$$\text{MAut}(\mathcal{H}) \cong GL_m(q). \quad (6)$$

В [4] доказано, что если код Хэмминга имеет проверочную матрицу, состоящую из всех столбцов вида $(0 \dots 0 1 * \dots *)^T$, то

$$\text{PAut}(\mathcal{H}) \cong UT_m(q),$$

где $UT_m(q)$ — группа унитреугольных $(m \times m)$ -матриц.

2. Представление линейной компоненты в виде прямой суммы подкодов Хэмминга

В этом разделе рассмотрим линейную компоненту кода Хэмминга \mathcal{H} длины $N = \frac{q^m - 1}{q - 1}$ и покажем, что она представима в виде прямой суммы подкодов Хэмминга размерности $q - 1$. Пусть множество T_i состоит из кодовых троек кода \mathcal{H} , имеющих 1 в i -й координате, $i \in \{1, 2, \dots, N\}$, т. е.

$$T_i = \{x \in \mathcal{H} \mid w(x) = 3, x_i = 1\}.$$

Линейная оболочка $R_i = \langle T_i \rangle$ называется *линейной компонентой* кода Хэмминга \mathcal{H} .

По определению линейная компонента образует подпространство кода \mathcal{H} и при $m = 2$ совпадает с ним. Таким образом, при $m = 2$ группа мономиальных автоморфизмов линейной компоненты изоморфна $GL_2(q)$. Далее будем полагать, что $m \geq 3$, т. е. $N > q + 1$. При этих значениях m и N выполняется строгое включение $R_i \subset \mathcal{H}$.

Проверочная матрица H_m кода Хэмминга \mathcal{H} состоит из всех попарно линейно независимых столбцов длины m . Поэтому для произвольного

столбца h_j матрицы H_m , отличного от h_i , однозначно определяются $q-1$ различных столбцов h_{k_s} и $q-1$ элементов $\beta_s \in \mathbb{F}_q^*$ таких, что справедливы равенства

$$h_i + \alpha^s h_j + \beta_s h_{k_s} = 0, \quad s = 0, 1, \dots, q-2. \quad (7)$$

Как и ранее, α является примитивным элементом поля \mathbb{F}_q , так что

$$\mathbb{F}_q^* = \{\alpha^0, \dots, \alpha^{q-2}\}.$$

Заметим, что не существует других линейных комбинаций столбцов h_i и h_j с некоторым третьим столбцом, имеющих коэффициент 1 при h_i .

Известно (см., например, [7]), что между столбцами проверочной матрицы H_m и точками $(m-1)$ -мерной проективной геометрии $PG(m-1, q)$ имеется взаимно однозначное соответствие. При этом три точки в проективной геометрии $PG(m-1, q)$ лежат на прямой тогда и только тогда, когда соответствующие столбцы линейно зависимы. Таким образом на столбцах проверочной матрицы H_m задаётся структура проективной геометрии.

Применяя геометрическую терминологию, назовём *прямой* множество столбцов, определённых через (7), т.е. множество

$$L = \{h_i, h_j, h_{k_0}, \dots, h_{k_{q-2}}\}.$$

Заметим, что, как и прежде, три столбца принадлежат одной прямой (лежат на прямой) тогда и только тогда, когда они линейно зависимы. Если необходимо подчеркнуть, что прямая задаётся столбцами h_i и h_j , будем обозначать её $L(i, j)$. Имея в виду некоторую аналогию с носителем вектора, назовём *носителем прямой* L множество $\text{supp}(L) = \{j \mid h_j \in L\}$.

Докажем, что прямая однозначно определяется любыми двумя своими столбцами.

Утверждение 1. Если L — прямая и $h_k, h_l \in L$, то $L = L(k, l)$.

ДОКАЗАТЕЛЬСТВО. Пусть $L = L(i, j)$ для некоторых $i, j \in \{1, \dots, N\}$. Это означает по определению, что тройки столбцов h_i, h_j, h_k и h_i, h_j, h_l линейно зависимы. В силу этого для любого другого столбца h_t справедливо, что h_i, h_j, h_t линейно зависимы тогда и только тогда, когда линейно зависимы h_k, h_l, h_t . При $h_k, h_l \in L$ это эквивалентно равенству $L = L(k, l)$. Утверждение 1 доказано.

Пусть e_j , $j \in \{1, \dots, N\}$, обозначает вектор с 1 в j -й координате и 0 в остальных позициях. Равенства (7) эквивалентны тому, что тройки

$$x^s = e_i + \alpha^s e_j + \beta_s e_{k_s}, \quad s = 0, 1, \dots, q-2, \quad (8)$$

принадлежат коду Хэмминга \mathcal{H} , или, что то же самое, множеству T_i . Причём только эти тройки в множестве T_i имеют ненулевые i -ю и j -ю координаты одновременно.

Линейная оболочка троек (8) представляет собой подкод $\mathcal{H}_j \subset R_i \subset \mathcal{H}$ размерности $q - 1$, называемый *подкодом Хэмминга*, т. е. линейный код такой, что

$$\mathcal{H}_j = \{x \in \mathcal{H} \mid \text{supp}(x) \subseteq \text{supp}(L(i, j))\}. \quad (9)$$

Если подкод \mathcal{H}_j укоротить, оставив только координаты его носителя, то получится код Хэмминга длины $q + 1$.

Лемма 1. *Линейная компонента R_i кода Хэмминга длины $N = \frac{q^m - 1}{q - 1}$ представляется в виде прямой суммы подкодов Хэмминга \mathcal{H}_{j_t} , $t = 1, \dots, n$, размерность которых равна $q - 1$, т. е.*

$$R_i = \mathcal{H}_{j_1} \oplus \mathcal{H}_{j_2} \oplus \dots \oplus \mathcal{H}_{j_n}, \quad (10)$$

где $n = \frac{q^{m-1} - 1}{q - 1}$. Это представление единственно с точностью до порядка слагаемых.

ДОКАЗАТЕЛЬСТВО. Носитель любой тройки из множества T_i является подмножеством носителя некоторой прямой, содержащей столбец h_i . Рассмотрим все прямые, содержащие столбец h_i . Из утверждения 1 следует, что условия (i) $L(i, j) = L(i, k)$; (ii) $h_j \in L(i, k)$ и (iii) $h_k \in L(i, j)$ эквивалентны. Это означает, что для различных $j_1, j_2 \in \{1, 2, \dots, N\} \setminus \{i\}$ справедливо

$$\text{либо } L(i, j_1) = L(i, j_2), \quad \text{либо } L(i, j_1) \cap L(i, j_2) = \{h_i\}, \quad (11)$$

а для соответствующих подкодов Хэмминга —

$$\text{либо } \mathcal{H}_{j_1} = \mathcal{H}_{j_2}, \quad \text{либо } \mathcal{H}_{j_1} \cap \mathcal{H}_{j_2} = \{0\}. \quad (12)$$

Число различных прямых равно

$$n = \frac{N - 1}{q} = \frac{q^m - 1 - (q - 1)}{q(q - 1)} = \frac{q^{m-1} - 1}{q - 1}.$$

Пусть $L(i, j_1), \dots, L(i, j_n)$ — все различные прямые. Соотношения (11) и (12) позволяют разбить множество троек T_i на n непересекающихся подмножеств, которые содержатся в некоторых подкодах Хэмминга \mathcal{H}_{j_t} , а носители их троек — в носителе $\text{supp}(L(i, j_t))$ соответствующей прямой.

Из включений $T_i \subset \bigcup_{t=1}^n \mathcal{H}_{j_t} \subset R_i$ получаем $R_i = \mathcal{H}_{j_1} + \mathcal{H}_{j_2} + \dots + \mathcal{H}_{j_n}$. Поскольку в этой сумме все подкоды различны, с учётом (11) и (12) для

любого $t \in \{1, \dots, n\}$ имеем соотношение $(\sum_{u \neq t} \mathcal{H}_{j_u}) \cap \mathcal{H}_{j_t} = \{0\}$. Отсюда следует (10).

Для доказательства единственности достаточно убедиться, что других подкодов Хэмминга размерности $q - 1$ в линейной компоненте R_i не существует. Действительно, базис B такого кода может быть составлен из троек множества T_i . При этом $|\text{supp}(B)| = q + 1$. Множество столбцов $\{h_j \mid j \in \text{supp}(B)\}$ проверочной матрицы H_m , очевидно, содержит столбец h_i . Кроме того, среди них найдётся только два линейно независимых, поскольку пространство решений системы

$$\sum_{j \in \text{supp}(B)} x_j h_j = 0$$

имеет размерность $q - 1$. Таким образом, подкод Хэмминга размерности $q - 1$ в компоненте R_i определяет прямую, содержащую столбец h_i , и, следовательно, совпадает с некоторым подкодом \mathcal{H}_{j_t} . Лемма 1 доказана.

Подкоды \mathcal{H}_j , $j = j_1, \dots, j_n$, входящие в прямую сумму (10), назовём базовыми подкодами Хэмминга линейной компоненты R_i . Очевидно, $\text{supp}(\mathcal{H}_j) = \text{supp}(L(i, j))$.

Построим линейную компоненту R'_1 некоторого кода Хэмминга \mathcal{H}' , эквивалентную исходной компоненте R_i и имеющую в некотором смысле регулярный вид. «Регулярность» заключается в том, что если укоротить базовые подкоды Хэмминга компоненты R'_1 до их носителей, то получим n равных кодов Хэмминга длины $q + 1$. Для этого построим проверочную матрицу H'_m следующим образом. В качестве первого столбца матрицы H'_m возьмём h_i — i -й столбец матрицы H_m ; в качестве второго — любой другой столбец h_{j_1} . Следующие $q - 1$ столбцов матрицы H'_m определим как линейные комбинации h_i и h_{j_1} вида (сравните эти выражения с равенствами (7))

$$h_i + \alpha^s h_{j_1}, \quad s = 0, 1, \dots, q - 2. \quad (13)$$

В качестве $(q + 2)$ -го столбца берём произвольный столбец h_{j_2} , попарно линейно независимый с уже выбранными, и аналогично (13) определяем следующие $q - 1$ столбцов как линейные комбинации h_i и h_{j_2} . Действуем так, пока не выпишем все N столбцов матрицы H'_m , которая является проверочной для некоторого кода Хэмминга \mathcal{H}' , эквивалентного коду \mathcal{H} . При этом важно отметить, что коды \mathcal{H} и \mathcal{H}' могут быть получены друг из друга некоторым мономиальным автоморфизмом пространства \mathbb{F}_q^N , отображающим линейную компоненту $R_i \subset \mathcal{H}$ в линейную компоненту

$R'_1 \subset \mathcal{H}'$. Это означает, что группы $\text{MAut}(R_i)$ и $\text{MAut}(R'_1)$ изоморфны. Вместе с тем регулярный вид линейной компоненты $R'_1 \subset \mathcal{H}'$ упрощает часть рассуждений, изложенных ниже.

Для иллюстрации приведём пример. Рассмотрим в качестве \mathcal{H} трогичный код Хэмминга длины $N = 13$ с проверочной матрицей

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

Пусть $i = 2$ и в качестве первого столбца матрицы H'_3 взят $h_2 = (0, 1, 0)^\top$, а в качестве второго — например, $h_{j_1} = h_1 = (0, 0, 1)^\top$. Согласно (13) имеем следующие два столбца: $(0, 1, 1)^\top$ и $(0, 1, 2)^\top$. Далее выберем столбец $h_{j_2} = h_5 = (1, 0, 0)^\top$ и аналогично (13) найдём столбцы $(1, 1, 0)^\top$ и $(2, 1, 0)^\top$. Продолжая так, в итоге получим матрицу

$$H'_3 = \left(\begin{array}{c|ccc|ccc|ccc|ccc} 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & 1 \end{array} \right)$$

эквивалентного кода Хэмминга \mathcal{H}' . Очевидно, что $H_3 = H'_3 M$ для некоторой мономиальной матрицы M . Порождающая матрица линейной компоненты $R'_1 \subset \mathcal{H}'$ в этом случае имеет размер 8×13 и может быть записана в виде

$$\begin{pmatrix} 1 & & & & & & & & & & & & \\ 1 & A & & & & & & & & & & & 0 \\ \vdots & & A & & & & & & & & & & \\ \vdots & & & A & & & & & & & & & \\ 1 & & 0 & & & & & & & & & & \\ 1 & & & & A & & & & & & & & \end{pmatrix}, \quad \text{где } A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}.$$

3. Мономиальные автоморфизмы линейной компоненты

В этом разделе исследуем мономиальные автоморфизмы линейной компоненты R_i кода Хэмминга \mathcal{H} . Сначала докажем, что мономиальные автоморфизмы пространства \mathbb{F}_q^n отображают произвольный линейный код в линейный код той же размерности. Затем рассмотрим ряд свойств автоморфизмов из группы $\text{MAut}(R_i)$, которые в конечном итоге позволят полностью описать эту группу.

Утверждение 2. Если $(\pi; \sigma) \in \text{MAut}(\mathbb{F}_q^n)$ и C — произвольный $[n, k]$ -код, то образ $C(\pi; \sigma)$ является линейным кодом размерности k .

ДОКАЗАТЕЛЬСТВО. Поскольку найдётся мономиальная матрица M такая, что $x(\pi; \sigma) = xM$ для любого $x \in \mathbb{F}_q^n$, можно записать

$$(\lambda x + \mu y)(\pi; \sigma) = (\lambda x + \mu y)M = \lambda xM + \mu yM = \lambda x(\pi; \sigma) + \mu y(\pi; \sigma), \quad (14)$$

где $x, y \in \mathbb{F}_q^n$ и $\lambda, \mu \in \mathbb{F}_q$. Отсюда следует, что код $C(\pi; \sigma)$ линейен.

Очевидно, имеет место равенство $0(\pi; \sigma) = 0$. Тогда из (14) получаем, что любые k линейно независимых кодовых слов из C отображаются автоморфизмом $(\pi; \sigma)$ в k линейно независимых кодовых слов из $C(\pi; \sigma)$. Утверждение 2 доказано.

Нетрудно убедиться, что все мономиальные автоморфизмы кода Хэмминга \mathcal{H} , оставляющие неподвижной координату i , образуют подгруппу в $\text{MAut}(R_i)$.

Утверждение 3. Пусть $(\pi; \sigma) \in \text{MAut}(\mathcal{H})$ и $i\pi = i$. Тогда

$$(\pi; \sigma) \in \text{MAut}(R_i).$$

ДОКАЗАТЕЛЬСТВО. Заметим, что множество $\bigcup_{\lambda \in \mathbb{F}_q^*} \lambda T_i$ включает в себя все тройки кода \mathcal{H} , имеющие ненулевую i -ю координату. Из утверждения 2 следует, что образ $R_i(\pi; \sigma)$ является линейным кодом. При этом если σ_i — подстановка умножения на некоторый элемент $\lambda \in \mathbb{F}_q^*$, то множество T_i отображается в множество λT_i . Тогда

$$R_i(\pi; \sigma) = \langle T_i \rangle (\pi; \sigma) = \langle \lambda T_i \rangle = \lambda \langle T_i \rangle = R_i,$$

т. е. $(\pi; \sigma)$ является мономиальным автоморфизмом R_i . Утверждение 3 доказано.

Из утверждения 3 следует, что группа $\text{MAut}_{\text{pr}}(R_i)$ транзитивно действует на множестве координатных позиций, отличных от i -й.

Утверждение 4. Группа $\text{MAut}_{\text{pr}}(R_i)$ действует транзитивно на множестве координатных позиций $\{1, 2, \dots, N\} \setminus \{i\}$.

ДОКАЗАТЕЛЬСТВО. Как было замечено выше, группа $\text{MAut}(\mathcal{H})$ изоморфна общей линейной группе $GL_m(q)$. Как известно [7], группа $GL_m(q)$ дважды транзитивна на множестве столбцов проверочной матрицы H_m кода Хэмминга и тем самым на множестве координатных позиций его кодовых слов. Отсюда следует, что для произвольных j и k , отличных от i , найдётся автоморфизм $(\pi; \sigma) \in \text{MAut}(\mathcal{H})$ такой, что $i\pi = i$, $j\pi = k$. В силу утверждения 3 этот автоморфизм принадлежит группе $\text{MAut}(R_i)$. Утверждение 4 доказано.

Несколько технических утверждений, приведённых ниже, описывают мономиальные автоморфизмы компоненты R_i . По лемме 1 в линейной компоненте не существует подкодов Хэмминга размерности $q - 1$, отличных от базовых. С учётом утверждения 2 отсюда следует

Лемма 2. *Произвольный автоморфизм $(\pi; \sigma) \in \text{MAut}(R_i)$ отображает базовые подкоды Хэмминга линейной компоненты R_i друг в друга.*

ДОКАЗАТЕЛЬСТВО. Образ базового подкода Хэмминга $\mathcal{H}_j(\pi; \sigma) \subset R_i$ является подкодом Хэмминга размерности $q - 1$. Этим подкодом может быть либо сам \mathcal{H}_j , либо некоторый другой базовый подкод Хэмминга компоненты R_i . Лемма 2 доказана.

Следующая лемма показывает, что произвольный мономиальный автоморфизм линейной компоненты R_i оставляет координату i неподвижной.

Лемма 3. *Если $(\pi; \sigma) \in \text{MAut}(R_i)$ и $N > q + 1$, то $i\pi = i$.*

ДОКАЗАТЕЛЬСТВО. Поскольку $0(\pi; \sigma) = 0$, для произвольного вектора $x \in \mathbb{F}_q^N$ справедливо

$$\text{supp}(x(\pi; \sigma)) = \text{supp}(x\pi).$$

Отсюда следует, что для всякого базового подкода Хэмминга \mathcal{H}_j компоненты R_i выполняется равенство

$$\text{supp}(\mathcal{H}_j(\pi; \sigma)) = \text{supp}(\mathcal{H}_j\pi). \quad (15)$$

При $N > q + 1$ в линейной компоненте содержится не менее 2 базовых подкодов Хэмминга. Из леммы 2 с учётом (15) следует, что носители базовых подкодов подстановкой π отображаются друг в друга. Так как попарные пересечения этих носителей равны $\{i\}$, то $i\pi = i$. Лемма 3 доказана.

Утверждение 5. *Если кодовые слова x, y из $[n, k]$ -кода C с кодовым расстоянием 3 таковы, что $w(x) = w(y) = 3$ и $\text{supp}(x) = \text{supp}(y)$, то $y = \mu x$ для некоторого $\mu \in \mathbb{F}_q^*$.*

ДОКАЗАТЕЛЬСТВО. Без потери общности считаем, что

$$\text{supp}(x) = \text{supp}(y) = \{1, 2, 3\}.$$

Очевидно, что векторы $x_1^{-1}x$ и $y_1^{-1}y$ принадлежат коду C , имеют 1 в первой координате и их носители равны $\{1, 2, 3\}$. Следовательно,

$$d(x_1^{-1}x, y_1^{-1}y) \leq 2.$$

Поскольку $d(C) = 3$, имеем $x_1^{-1}x = y_1^{-1}y$. Отсюда получаем

$$\frac{y_1}{x_1} = \frac{y_2}{x_2} = \frac{y_3}{x_3} = \mu.$$

Поэтому $y = \mu x$, где $\mu \in \mathbb{F}_q^*$. Утверждение 5 доказано.

Лемма 4. Если $(e; \sigma) \in \text{Aut}(R_i)$ и $0\sigma = 0$, то существует $\lambda \in \mathbb{F}_q^*$ такой, что $\sigma = \Lambda$.

ДОКАЗАТЕЛЬСТВО. Так как конфигурация σ оставляет на месте нулевой вектор, она сохраняет вес произвольного вектора $x \in \mathbb{F}_q^N$. Более того, носители вектора x и его образа $x(e; \sigma) = x\sigma$ совпадают:

$$\text{supp}(x) = \text{supp}(x\sigma). \quad (16)$$

Напомним, что множество T_i образовано всеми тройками кода Хэмминга, i -я координата которых равна 1. Для фиксированной координаты $j \neq i$ рассмотрим тройки (8), принадлежащие множеству T_i , т. е. $x^s = e_i + \alpha^s e_j + \beta_s e_{k_s}$, $s = 0, 1, \dots, q-2$. Из линейности R_i следует, что для всех $r = 0, 1, \dots, q-2$ коду R_i принадлежат тройки $\alpha^r x^s$.

Пусть

$$\sigma_i = \begin{pmatrix} 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \\ 0 & \lambda_0 & \lambda_1 & \dots & \lambda_{q-2} \end{pmatrix}. \quad (17)$$

В силу равенства (16) для любых $r, s \in \{0, 1, \dots, q-2\}$ к вектору $\alpha^r x^s$ и его образу $(\alpha^r x^s)\sigma$ можно применить утверждение 5. Множитель, связывающий эти два вектора, найдём, поделив i -ю координату образа на i -ю координату прообраза, т. е. этот множитель равен λ_r/α^r . Таким образом, получаем

$$\begin{aligned} (\alpha^r x^s)\sigma &= (\alpha^r \sigma_i) e_i + (\alpha^{r+s} \sigma_j) e_j + ((\alpha^r \beta_s) \sigma_{k_s}) e_{k_s} \\ &= \frac{\lambda_r}{\alpha^r} \alpha^r x^s = \lambda_r e_i + \lambda_r \alpha^s e_j + \lambda_r \beta_s e_{k_s}. \end{aligned}$$

Отсюда следует, что для произвольных $r, s \in \{0, 1, \dots, q-2\}$ выполняется

$$\alpha^{r+s} \sigma_j = \lambda_r \alpha^s. \quad (18)$$

В частности, $\alpha^s \sigma_j = \lambda_0 \alpha^s$, т. е. σ_j является подстановкой умножения на элемент $\lambda = \lambda_0$.

Далее, из (18) получаем

$$\lambda_r = \alpha^{-s} (\alpha^{r+s} \sigma_j) = \alpha^{-s} \lambda_0 \alpha^{r+s} = \lambda_0 \alpha^r.$$

Иначе говоря, и σ_i является подстановкой умножения на $\lambda = \lambda_0$. В силу произвольности выбора $j \in \{1, \dots, N\} \setminus \{i\}$ получаем требуемое. Лемма 4 доказана.

Следствие 1. Если $(\pi; \sigma), (\pi; \delta) \in \text{Aut}(R_i)$, то $\delta = \sigma\Lambda$ для некоторого $\lambda \in \mathbb{F}_q^*$.

ДОКАЗАТЕЛЬСТВО. Поскольку $(\pi; \sigma), (\pi; \delta) \in \text{Aut}(R_i)$, произведение $(\pi; \sigma)^{-1}(\pi; \delta)$ также является автоморфизмом кода R_i . По определению операции умножения в полупрямом произведении (см. (4)) получаем $(\pi; \sigma)^{-1} = (\pi^{-1}; \sigma^{-1}\pi^{-1})$. С учётом этого записываем

$$(\pi; \sigma)^{-1}(\pi; \delta) = (\pi^{-1}; \sigma^{-1}\pi^{-1})(\pi; \delta) = (e; \sigma^{-1}\delta).$$

Таким образом, автоморфизм $(e; \sigma^{-1}\delta)$ принадлежит группе $\text{Aut}(R_i)$. Из леммы 4 следует, что $\sigma^{-1}\delta = \Lambda$ для некоторого $\lambda \in \mathbb{F}_q^*$, т. е. конфигурация $\sigma^{-1}\delta$ умножает произвольный вектор $x \in \mathbb{F}_q^N$ на элемент поля λ . Отсюда $\delta = \sigma\Lambda$. Следствие 1 доказано.

Лемма 5. Для линейной компоненты R_i справедливо

$$\text{MAut}(R_i) \cong \text{MAut}_{\text{pr}}(R_i) \times \mathbb{F}_q^*. \quad (19)$$

ДОКАЗАТЕЛЬСТВО. По следствию 1 для произвольной подстановки $\pi \in \text{MAut}_{\text{pr}}(R_i)$ в группе $\text{MAut}(R_i)$ существует не более одного автоморфизма $(\pi; \sigma)$ такого, что $\sigma_i = \lambda$.

С другой стороны, так как R_i — линейный код, то для любого кодового слова $x \in R_i$ и произвольного $\lambda_0 \in \mathbb{F}_q^*$ выполняется $\lambda_0 x \in R_i$. Следовательно, если $(\pi; \delta) \in \text{MAut}(R_i)$, то и автоморфизм $(\pi; \delta\Lambda_0)$ принадлежит группе $\text{MAut}(R_i)$ для произвольного $\lambda_0 \in \mathbb{F}_q^*$. В частности, найдётся такой автоморфизм $(\pi; \sigma)$, что $\sigma_i = \delta_i\lambda_0 = \lambda$.

Таким образом, для любых $\pi \in \text{MAut}_{\text{pr}}(R_i)$ и $\lambda \in \mathbb{F}_q^*$ в $\text{MAut}(R_i)$ существует ровно один автоморфизм $(\pi; \sigma)$ такой, что $\sigma_i = \lambda$. Иными словами, между $\text{MAut}(R_i)$ и $\text{MAut}_{\text{pr}}(R_i) \times \mathbb{F}_q^*$ существует биекция φ , заданная по правилу $\varphi: (\pi; \sigma) \mapsto (\pi, \lambda)$, если $\sigma_i = \lambda$.

По определению прямого произведения для двух элементов группы из правой части (19) имеет место равенство $(\pi, \lambda)(\tau, \mu) = (\pi\tau, \lambda\mu)$. Отсюда, используя лемму 3, нетрудно показать, что φ является изоморфизмом, а именно,

$$\varphi((\pi; \sigma)(\tau; \delta)) = \varphi(\pi\tau, (\sigma\tau)\delta) = (\pi\tau, \lambda\mu) = (\pi, \lambda)(\tau, \mu) = \varphi(\pi; \sigma)\varphi(\tau; \delta),$$

где по предположению $(\pi; \sigma), (\tau; \delta) \in \text{MAut}(R_i)$, $\sigma_i = \lambda$, $\delta_i = \mu$. Лемма 5 доказана.

Перейдём к описанию группы $\text{MAut}_{\text{pr}}(R_i)$. Для этого введём некоторые обозначения. Учитывая, что линейная компонента R_i раскладывается в прямую сумму (10) подкодов Хэмминга, положим

$$I_j = \text{supp}(\mathcal{H}_j) \setminus \{i\}, \quad j = j_1, \dots, j_n. \quad (20)$$

Во избежание громоздких индексов обозначим j_t через t , $t = 1, \dots, n$. Отметим, что $I_j \cap I_k = \emptyset$ при $j \neq k$, причём $I_j = \{j, k_0, k_1, \dots, k_{q-2}\}$ согласно (7)–(9).

Для наглядности запишем координатные позиции $\{1, \dots, N\} \setminus \{i\}$ в виде элементов $(n \times q)$ -матрицы W . В j -ю строку матрицы W поместим элементы множества I_j . Обозначим

$$W = \begin{pmatrix} i_{11} & i_{12} & \dots & i_{1q} \\ i_{21} & i_{22} & \dots & i_{2q} \\ \vdots & \vdots & \dots & \vdots \\ i_{n1} & i_{n2} & \dots & i_{nq} \end{pmatrix}.$$

Из лемм 2 и 3 следует, что подстановка π из $\text{MAut}_{\text{pr}}(R_i)$ отображает множества I_j друг в друга. Тем самым для произвольной подстановки $\pi \in \text{MAut}_{\text{pr}}(R_i)$ однозначно определяется базовая подстановка $\pi' \in S_n$ такая, что

$$j\pi' = k, \quad \text{если } I_j \pi = I_k; \quad j = 1, \dots, n. \quad (21)$$

Далее, для произвольной подстановки $\Delta \in S_n$ определим подстановку $\mathfrak{d}(\Delta) \in S_N$ следующим образом:

$$i\mathfrak{d}(\Delta) = i, \quad i_{js}\mathfrak{d}(\Delta) = i_{ks}, \quad \text{если } j\Delta = k; \quad j = 1, \dots, n; \quad s = 1, \dots, q, \quad (22)$$

$$\text{т. е. } \mathfrak{d}(\Delta) = \left(i \mid \dots \mid i_{j1} \quad \dots \quad i_{jq} \mid \dots \right).$$

Следуя С. В. Августиновичу и др. [2], подстановку $\mathfrak{d}(\Delta)$ будем называть *дубликатором*.

Заметим, что дубликатор $\mathfrak{d}(\pi')$, являющийся образом подстановки $\pi \in \text{MAut}_{\text{pr}}(R_i)$, отображает множество I_j в то же множество I_k , что и подстановка π , т. е. $I_j \pi = I_j \mathfrak{d}(\pi')$. При этом дубликатор сохраняет порядок элементов множества I_j , в котором они записаны в матрице W .

Нетрудно видеть, что отображение $\mathfrak{b}: \pi \mapsto \pi'$ является гомоморфизмом из $\text{MAut}_{\text{pr}}(R_i)$ в S_n . Отображение $\mathfrak{d}: \Delta \mapsto \mathfrak{d}(\Delta)$ есть изоморфизм между S_n и группой всех дубликаторов. Образ подстановки π под действием композиции $\mathfrak{b} \circ \mathfrak{d}$ будем обозначать через $\bar{\pi}$, т. е. $\bar{\pi} = \mathfrak{d}(\pi')$.

С учётом принятых обозначений из лемм 2 и 3 следует, что любая подстановка $\pi \in \text{MAut}_{\text{pr}}(R_i)$ однозначно представляется в виде композиции

$$\pi = \bar{\pi} \gamma_1 \gamma_2 \dots \gamma_n, \quad (23)$$

где $\gamma_1, \dots, \gamma_n$ — независимые подстановки порядка q на множествах I_1, \dots, I_n соответственно.

Используя запись координат $\{1, \dots, N\} \setminus \{i\}$, заданную матрицей W , можно иначе интерпретировать сомножители в правой части (23). Подстановка $\bar{\pi}$ переставляет строки этой матрицы, оставляя элементы в тех же столбцах. Произвольная из подстановок γ_j , $j = 1, \dots, n$, переставляет между собой элементы в j -й строке матрицы W . Подстановки $\gamma_1, \dots, \gamma_n$ независимы и, вообще говоря, различны. Однако будем считать, что место подстановки γ_j в записи правой части (23) задаёт номер строки матрицы W , на элементах которой она действует.

Без ограничения общности доказательство следующей леммы проведём для линейной компоненты R'_1 , построенной выше (см. разд. 2). Пусть $G = \text{MAut}_{\text{pr}}(\mathcal{H}^{q+1})$, где \mathcal{H}^{q+1} — код Хэмминга длины $q + 1$.

Лемма 6. *Для линейной компоненты R_i справедливо*

$$\text{MAut}_{\text{pr}}(R_i) \cong S_n \ltimes (\text{St}_G(i))^n. \quad (24)$$

ДОКАЗАТЕЛЬСТВО. Зададим отображение

$$\varphi: \text{MAut}_{\text{pr}}(R_i) \rightarrow S_n \ltimes (\text{St}_G(i))^n$$

по следующему правилу:

$$\varphi: \pi \mapsto (\pi'; (\gamma_1, \dots, \gamma_n)), \quad (25)$$

где подстановки $\pi', \gamma_1, \dots, \gamma_n$ определены в (21)–(23).

Для достижения цели необходимо показать, что φ является изоморфизмом, т. е. биективным отображением между указанными группами, сохраняющим групповую операцию.

ИНЪЕКТИВНОСТЬ очевидна в силу представления (23) и инъективности отображения \mathfrak{d} между S_n и группой всех дубликаторов.

СЮРЪЕКТИВНОСТЬ. Как и для всякой линейной компоненты, для $R_i = R'_1$ справедливо представление (10). По построению R'_1 (см. разд. 2) её базовые подкоды Хэмминга, будучи укороченными до своих носителей, совпадают и равны коду Хэмминга длины $q + 1$, т. е.

$$\mathcal{H}_1^* = \dots = \mathcal{H}_n^* = \mathcal{H}^{q+1}. \quad (26)$$

Рассмотрим два произвольных подкода $\mathcal{H}_j, \mathcal{H}_k$ и дубликатор $\mathfrak{d}(jk)$ подстановки (jk) из S_n . Легко видеть, что $\mathcal{H}_j \mathfrak{d}(jk) = \mathcal{H}_k$ и $R'_1 \mathfrak{d}(jk) = R'_1$. Аналогично рассмотрим произвольную подстановку $\Delta \in S_n$. Из (26) следует, что автоморфизм $(\mathfrak{d}(\Delta); \varepsilon)$, где ε — тождественная конфигурация, принадлежит группе $\text{MAut}(R_i)$, откуда получаем $\mathfrak{d}(\Delta) \in \text{MAut}_{\text{pr}}(R_i)$. При этом по построению выполняется $\mathfrak{d}(\Delta)' = \Delta$.

Далее, возьмём n произвольных подстановок $\gamma_j \in \text{St}_G(i)$, $j = 1, \dots, n$. Для каждой из них в группе $\text{MAut}(\mathcal{H}^{q+1})$ существует мономиальный автоморфизм $(\gamma_j; \sigma^j)$ такой, что σ_1^j равна тождественной подстановке e (код Хэмминга линейен, поэтому конфигурацию σ^j можно домножить на подходящую конфигурацию Λ). Действие автоморфизма $(\gamma_j; \sigma^j)$, $j = 1, \dots, n$, перенесём на соответствующий базовый подкод Хэмминга $\mathcal{H}_j \subset R'_1$, т. е. на координаты из носителя этого кода. Иначе говоря, построим мономиальный автоморфизм пространства \mathbb{F}_q^N такой, что

$$(\tau; \sigma) = (\mathfrak{d}(\Delta) \gamma_1 \dots \gamma_n; \sigma),$$

где $\sigma = (e, \sigma_2^1, \dots, \sigma_{q+1}^1, \dots, \sigma_2^n, \dots, \sigma_{q+1}^n)$.

Если $j\Delta = k$, $j \in \{1, \dots, n\}$, то для базового подкода $\mathcal{H}_j \subset R'_1$ имеем

$$\mathcal{H}_j(\tau; \sigma) = \mathcal{H}_k(\gamma_1 \dots \gamma_n; \sigma) = \mathcal{H}_k(\gamma_k; \sigma^k) = \mathcal{H}_k.$$

Следовательно, $(\tau; \sigma) \in \text{MAut}(R'_1)$, причём $\varphi(\tau; \sigma) = (\Delta; (\gamma_1, \dots, \gamma_n))$. Тем самым сюръективность φ доказана.

СОХРАНЕНИЕ ОПЕРАЦИИ. Пусть $\pi, \tau \in \text{MAut}_{\text{pr}}(R_i)$ и справедливы равенства $\pi = \bar{\pi} \gamma_1 \gamma_2 \dots \gamma_n$ и $\tau = \bar{\tau} v_1 v_2 \dots v_n$, где γ_j, v_j — подстановки порядка q на координатах из множества I_j , $j = 1, \dots, n$. Для вычисления $\varphi(\pi\tau)$ найдём представление вида (23) для $\pi\tau = \bar{\pi} \gamma_1 \dots \gamma_n \bar{\tau} v_1 \dots v_n$.

Для этого сначала рассмотрим, например, дубликатор $\mathfrak{d}(123)$ и композицию подстановок $\gamma_1 \gamma_2 \gamma_3 \mathfrak{d}(123)$. Если применять эти подстановки к матрице W в том порядке, в котором они выписаны, то сначала следует переставить элементы 1-й строки согласно γ_1 , 2-й — согласно γ_2 , 3-й — согласно γ_3 . После чего циклически поменять местами эти первые три строки в соответствии с $\mathfrak{d}(123)$. Однако такой же результат будет достигнут, если сначала поменять местами строки, т. е. первую строку поместить во вторую, вторую — в третью, а третью — в первую; после чего применить подстановки γ_j в порядке $\gamma_3, \gamma_1, \gamma_2$. Иначе говоря, имеем равенство

$$\gamma_1 \gamma_2 \gamma_3 \mathfrak{d}(123) = \mathfrak{d}(123) \gamma_3 \gamma_1 \gamma_2.$$

Аналогично, справедливо $\gamma_1 \dots \gamma_n \bar{\tau} = \bar{\tau} \gamma_{t_1} \dots \gamma_{t_n}$, где по определению $\bar{\tau} = \mathfrak{d}(\tau')$, $t_j = j(\tau')^{-1}$, $j = 1, \dots, n$. Так получаем

$$\pi\tau = \bar{\pi}\gamma_1 \dots \gamma_n \bar{\tau} v_1 \dots v_n = \bar{\pi} \bar{\tau} (\gamma_{t_1} v_1) \dots (\gamma_{t_n} v_n).$$

Отсюда с учётом равенств $\bar{\pi}\bar{\tau} = \mathfrak{d}(\pi')\mathfrak{d}(\tau') = \mathfrak{d}(\pi'\tau') = \mathfrak{d}((\pi\tau)') = \bar{\pi}\bar{\tau}$ и определения групповой операции в полупрямом произведении имеем

$$\begin{aligned} \varphi(\pi\tau) &= ((\pi\tau)'; (\gamma_{t_1} v_1, \dots, \gamma_{t_n} v_n)) = (\pi'\tau'; (\gamma_{t_1}, \dots, \gamma_{t_n}) \cdot (v_1, \dots, v_n)) \\ &= (\pi'\tau'; (\gamma_1, \dots, \gamma_n)\tau' \cdot (v_1, \dots, v_n)) = (\pi'; (\gamma_1, \dots, \gamma_n))(\tau'; (v_1, \dots, v_n)) \\ &= \varphi(\pi)\varphi(\tau). \end{aligned}$$

Лемма 6 доказана.

Непосредственно из лемм 5 и 6 следует

Теорема 2. Пусть $G = \text{MAut}_{\text{pr}}(\mathcal{H}^{q+1})$ и \mathcal{H}^{q+1} — код Хэмминга длины $q+1$. Тогда для линейной компоненты R_i кода Хэмминга \mathcal{H} длины $N = (q^m - 1)/(q - 1)$ при $m \geq 3$ справедливо

$$\text{MAut}(R_i) \cong (S_n \ltimes (\text{St}_G(i))^n) \times \mathbb{F}_q^*,$$

где $n = (q^{m-1} - 1)/(q - 1)$.

Теорема 2 позволяет без труда вычислить порядок группы $\text{MAut}(R_i)$.

Следствие 2. Порядок группы мономиальных автоморфизмов R_i равен

$$|\text{MAut}(R_i)| = n! (q^2 - q)^n (q - 1).$$

Доказательство. Обоснуем равенство $|\text{St}_G(i)| = q^2 - q$, где $G = \text{MAut}_{\text{pr}}(\mathcal{H}^{q+1})$. Вначале заметим, что лемма 4 и следствие 1 справедливы не только для линейной компоненты R_i , но и для кода Хэмминга \mathcal{H} , и для любого линейного кода длины N с кодовым расстоянием $d = 3$, содержащего подмножество кодовых троек T_i . Поэтому для группы $\text{St}_H(i)$, где $H = \text{MAut}(\mathcal{H}^{q+1})$, остаётся справедливой лемма 5, что означает

$$\text{St}_H(i) \cong \text{St}_G(i) \times \mathbb{F}_q^*. \quad (27)$$

Согласно (6) имеем

$$|H| = |GL_2(q)| = (q^2 - 1)(q^2 - q).$$

Группа $GL_m(q)$ действует транзитивно на множестве координатных позиций кодовых слов кода Хэмминга, поэтому $|\text{St}_H(i)| = |H|/(q + 1)$. С учётом (27) получаем

$$|\text{St}_G(i)| = |H|/(q^2 - 1) = q^2 - q.$$

Следствие 2 доказано.

4. Мономиальные автоморфизмы простой компоненты

В этом разделе опишем кратко структуру группы мономиальных автоморфизмов простой компоненты кода Хэмминга. Поскольку во многом она схожа со строением группы $\text{MAut}(R_i)$, часть доказательств опускается. Недостающие рассуждения легко восстанавливаются с использованием аналогичных доказательств для линейной компоненты R_i .

Простой компонентой кода Хэмминга \mathcal{H} называется линейная оболочка множества T_i над простым подполем $\mathbb{F}_p \subseteq \mathbb{F}_q$, которая обозначается через $P_i = \langle T_i \rangle_p$. Напомним, что множество T_i состоит из кодовых троек кода Хэмминга, i -я координата которых равна 1.

Простая компонента является подкодом кода Хэмминга, причём этот подкод нелинеен над полем \mathbb{F}_q , если $q = p^r$ не является простым числом, т. е. $r > 1$. В противном случае если $q = p$, то простая компонента P_i совпадает с линейной компонентой R_i и поэтому является линейным кодом над \mathbb{F}_q . Таким образом, для кода Хэмминга длины $p + 1$ справедливы равенства $P_i = R_i = \mathcal{H}$.

Фелпс и др. [18] доказали, что размерность $\dim_p P_i$ простой компоненты кода Хэмминга над подполем \mathbb{F}_p (иначе, p -размерность) равна

$$\dim_p P_i = \frac{q^{m-1} - 1}{q - 1} (r(q - 2) + 1). \quad (28)$$

В разд. 2 (см. доказательство леммы 1) показано, что множество T_i разбивается на $n = (q^{m-1} - 1)/(q - 1)$ подмножеств. Каждое из этих подмножеств содержит только тройки кода Хэмминга, i -я координата которых равна 1 и носители которых содержатся в носителе одной прямой.

Пусть \mathcal{C}_j обозначает линейную оболочку над подполем \mathbb{F}_p множества троек, носители которых содержатся в $\text{supp}(L(i, j))$, т. е.

$$\mathcal{C}_j = \langle \{x \in T_i \mid \text{supp}(x) \subset \text{supp}(L(i, j))\} \rangle_p. \quad (29)$$

Заметим, что подкод \mathcal{C}_j является простой компонентой подкода Хэмминга \mathcal{H}_j , определённого в (9). С учётом равенства (28) нетрудно видеть, что p -размерность подкода \mathcal{C}_j равна $\dim_p \mathcal{C}_j = r(q - 2) + 1$.

Для простой компоненты P_i справедлива лемма о представлении в виде прямой суммы подкодов \mathcal{C}_j , аналогичная лемме 1 для линейной компоненты R_i . Через $+_p$ и \oplus_p обозначим соответственно сумму и прямую сумму подмножеств из \mathbb{F}_q^N , взятые над подполем \mathbb{F}_p .

Лемма 7. Простая компонента P_i кода Хэмминга длины

$$N = (q^m - 1)/(q - 1)$$

представима в виде прямой суммы подкодов \mathcal{C}_{j_t} , $t = 1, \dots, n$, размерность каждого из которых равна $r(q - 2) + 1$, т. е. справедливо равенство

$$P_i = \mathcal{C}_{j_1} \oplus_p \mathcal{C}_{j_2} \oplus_p \dots \oplus_p \mathcal{C}_{j_n}, \quad (30)$$

где $n = (q^{m-1} - 1)/(q - 1)$. Это представление единственно с точностью до порядка слагаемых.

ДОКАЗАТЕЛЬСТВО аналогично доказательству леммы 1.

Пусть $L(i, j_1), \dots, L(i, j_n)$ — все различные прямые, проходящие через точку h_i . Тогда $T_i \subset \bigcup_{t=1}^n \mathcal{C}_{j_t} \subset P_i$. Отсюда следует, что

$$P_i = \mathcal{C}_{j_1} +_p \mathcal{C}_{j_2} +_p \dots +_p \mathcal{C}_{j_n}.$$

Поскольку в этой сумме все подкоды различны и носители каждой пары из них содержат только один общий элемент i , получаем требуемую прямую сумму (30).

Единственность следует из леммы 1 и того факта, что для произвольного подкода $\mathcal{C} \subset P_i$, обладающего свойствами $\dim_p \mathcal{C} = r(q - 2) + 1$ и $|\text{supp}(\mathcal{C})| = q + 1$, его линейная оболочка над полем \mathbb{F}_q есть подкод Хэмминга размерности $q - 1$. Лемма 7 доказана.

По аналогии с базовыми подкодами линейной компоненты подкоды $\mathcal{C}_{j_1}, \dots, \mathcal{C}_{j_n}$, входящие в прямую сумму (30), назовём *базовыми подкодами простой компоненты* P_i .

В силу равенств (14) заключаем, что для произвольного мономиального автоморфизма $(\pi; \sigma) \in \text{MAut}(\mathbb{F}_q^N)$ множество векторов $B \subset \mathbb{F}_q^N$ линейно зависимо над подполем \mathbb{F}_p тогда и только тогда, когда множество $B(\pi; \sigma)$ линейно зависимо над \mathbb{F}_p . Отсюда следуют

Лемма 8. Произвольный автоморфизм $(\pi; \sigma) \in \text{MAut}(P_i)$ отображает базовые подкоды простой компоненты P_i друг в друга.

Лемма 9. Если $(\pi; \sigma) \in \text{MAut}(P_i)$ и $N > q + 1$, то $i\pi = i$.

Аналогично утверждению 5 доказывается

Утверждение 6. Если $x, y \in P_i$, $w(x) = w(y) = 3$ и $i \in \text{supp}(x) = \text{supp}(y)$, то $y = \mu x$ для некоторого $\mu \in \mathbb{F}_p^*$.

Из утверждения 6 следует

Лемма 10. Если $(e; \sigma) \in \text{MAut}(P_i)$ и $0\sigma = 0$, то существует $\lambda \in \mathbb{F}_p^*$ такой, что $\sigma = \Lambda$.

ДОКАЗАТЕЛЬСТВО этой леммы во многом повторяет доказательство леммы 4 с заменой R_i на P_i и равенства (17) на $\sigma_i = \lambda$.

Аналогично лемме 5 доказывается

Лемма 11. Для простой компоненты P_i справедливо

$$\text{MAut}(P_i) \cong \text{MAut}_{\text{pr}}(P_i) \times \mathbb{F}_p^*.$$

Пусть $\Gamma = \text{MAut}_{\text{pr}}(P_i^{q+1})$, где P_i^{q+1} — простая компонента кода Хэмминга длины $q+1$.

Лемма 12. Для простой компоненты P_i выполняется

$$\text{MAut}_{\text{pr}}(P_i) \cong S_n \ltimes (\text{St}_{\Gamma}(i))^n.$$

Из лемм 11 и 12 следует

Теорема 3. Для простой компоненты P_i кода Хэмминга длины $N = (q^m - 1)/(q - 1)$ при $m \geq 3$ справедливо

$$\text{MAut}(P_i) \cong (S_n \ltimes (\text{St}_{\Gamma}(i))^n) \times \mathbb{F}_p^*,$$

где $n = (q^{m-1} - 1)/(q - 1)$.

Отметим, что вопрос о явном представлении группы мономиальных автоморфизмов простой компоненты кода Хэмминга длины $q+1$, когда q не является простым, остаётся пока открытым.

В заключение автор выражает глубокую благодарность профессору Ф. И. Соловьёвой за внимание к работе и уточнения, внесённые в изложение статьи.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьёва Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\tilde{\alpha}$ -компонент // Пробл. передачи информ. — 1997. — Т. 33, № 3. — С. 15–21.
2. **Августинович С. В., Соловьёва Ф. И., Хеден У.** О структуре группы симметрий кодов Васильева // Пробл. передачи информ. — 2005. — Т. 41, № 2. — С. 42–49.
3. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. Вып. 8. — М.: Физматгиз, 1962. — С. 337–339.
4. **Горкунов Е. В.** Группа перестановочных автоморфизмов q -ичного кода Хэмминга // Пробл. передачи информ. — 2009. — Т. 45, № 4. — С. 18–25.

5. Лось А. В. Построение совершенных q -значных кодов последовательными сдвигами $\tilde{\alpha}$ -компонент // Пробл. передачи информ. — 2004. — Т. 40, № 1. — С. 40–47.
6. Лось А. В. Построение совершенных q -ичных кодов свитчингами простых компонент // Пробл. передачи информ. — 2006. — Т. 42, № 1. — С. 34–42.
7. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
8. Малюгин С. А. О порядке группы автоморфизмов совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 91–100.
9. Марков А. А. О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгоритмов и конструктивная математика, математическая логика, информатика и смежные вопросы. — М.: МЦНМО, 2003. — С. 70–93.
10. Соловьёва Ф. И., Топалова С. Т. О группах автоморфизмов совершенных двоичных кодов и систем троек Штейнера // Пробл. передачи информ. — 2000. — Т. 36, № 4. — С. 3–8.
11. Соловьёва Ф. И., Топалова С. Т. Совершенные двоичные коды и системы троек Штейнера с максимальными порядками групп автоморфизмов // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 101–110.
12. Avgustinovich S. V., Solov'eva F. I. Perfect binary codes with trivial automorphism group // Proc. Int. Workshop on information theory (Killarney, Ireland, June, 1998). — Piscataway: IEEE, 1998. — P. 114–115.
13. Constantinescu I., Heise W. On the concept of code-isomorphy // J. Geom. — 1996. — Vol. 57. — P. 63–69.
14. Huffman W. C. Codes and groups // Handbook of coding theory. Ch. 6. — Amsterdam, New York: Elsevier Science, 1998. — P. 1345–1440.
15. Lindström B. On group and nongroup perfect codes in q symbols // Math. Scand. — 1969. — Vol. 25. — P. 149–158.
16. Malyugin S. A. Perfect codes with trivial automorphism group // Proc. II Int. Workshop "Optimal codes and related topics" (Sozopol, Bulgaria, June 9–15, 1998). — Sofia: Institute of Mathematics and Informatics, 1998. — P. 163–167.
17. Phelps K. T. Every finite group is the automorphism group of some perfect code // J. Comb. Theory. Ser. A. — 1986. — Vol. 43. — P. 45–51.
18. Phelps K. T., Rifà J., Villanueva M. Kernels and p -kernels of p^r -ary 1-perfect codes // Des. Codes Cryptography. — 2005. — Vol. 37, N 2. — P. 243–261.
19. Schönheim J. On linear and nonlinear single-error-correcting q -ary perfect codes // Informatics and Control. — 1968. — Vol. 12. — P. 23–26.
20. Shapiro G. S., Slotnik D. L. On the mathematical theory of error correct-

ing codes // IBM J. Res. Dev. — 1959. — Vol. 3, № 1. — P. 25–34.

- 21. Solov'eva F. I.** On perfect codes and related topics. — Pohang: Pohang Univ. of Science and Technology, 2004. — (Com²MaC Lect. Note Series; Vol. 13).

Горкунов Евгений Владимирович,
e-mail: evgumin@gmail.ru

Статья поступила
27 августа 2009 г.

Переработанный вариант —
23 ноября 2009 г.