

УДК 519.725

ГРУППА АВТОМОРФИЗМОВ q -ИЧНОГО КОДА ХЭММИНГА ^{*)}

Е. В. Горкунов

Аннотация. Известно, что группа полулинейных симметрий кода Хэмминга \mathcal{H} длины $n = \frac{q^m-1}{q-1}$ изоморфна GL_m . Это не проясняет, являются ли все симметрии кода \mathcal{H} полулинейными. Доказано, что любая симметрия кода, образованного тройками из \mathcal{H} , является полулинейной. Отсюда следует полулинейность произвольной симметрии кода Хэмминга. Тем самым показано, что группа автоморфизмов q -ичного кода Хэмминга изоморфна полупрямому произведению $GL_m \ltimes \mathcal{H}$.

Ключевые слова: код Хэмминга, группа автоморфизмов.

Введение

Кодом C длины n называется подмножество n -мерного векторного пространства \mathbb{F}^n над конечным полем $\mathbb{F} = GF(q)$. Если C образует подпространство в \mathbb{F}^n , то код называется *линейным*. Расстояние Хэмминга между векторами $x, y \in \mathbb{F}^n$ измеряется числом координат, в которых эти векторы различаются. Множество $\text{supp}(x) = \{i \mid x_i \neq 0\}$ называется *носителем* вектора $x \in \mathbb{F}^n$, а его мощность $w(x)$ — *весом* x .

Назовём коды C_1 и C_2 *мономиально эквивалентными*, если существует мономиальная $(n \times n)$ -матрица такая, что $C_2 = \{xM \mid x \in C_1\}$. В 1962 г. Мак-Вильямс [4] доказала, что линейные коды мономиально эквивалентны тогда и только тогда, когда между ними существует линейный изоморфизм (как векторных пространств), сохраняющий вес произвольного кодового слова.

Два кода *эквивалентны*, если существует изометрия пространства \mathbb{F}^n , отображающая один код в другой. В 1956 г. А. А. Марков показал, что каждая изометрия пространства \mathbb{F}^n представляется в виде композиции

^{*)}Исследование выполнено в лаборатории НГУ–Интел при частичной поддержке Российского фонда фундаментальных исследований (проект 10–01–00616), а также ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

подстановки $\pi \in S_n$, переставляющей координаты фиксированного вектора, и набора $\sigma = (\sigma_1, \dots, \sigma_n)$ подстановок порядка q , действующих на элементах поля \mathbb{F} , т.е. группа изометрий пространства \mathbb{F}^n представляет собой полупрямое произведение

$$\text{Aut}(\mathbb{F}^n) = S_n \ltimes S_q^n = \{(\pi; \sigma) \mid \pi \in S_n, \sigma \in S_q^n\}.$$

Действие изометрии $(\pi; \sigma)$ на вектор $x \in \mathbb{F}^n$ задаётся равенствами:

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

Группой автоморфизмов кода C называется группа $\text{Aut}(C)$ изометрий пространства \mathbb{F}^n , отображающих код C в себя. Автоморфизм пространства \mathbb{F}^n , заданный умножением векторов на мономиальную матрицу, называется *мономиальным*. Группа мономиальных автоморфизмов кода C обозначается через $\text{MAut}(C)$. Группой симметрий кода C назовём группу его автоморфизмов $(\pi; \sigma)$ таких, что $0(\pi; \sigma) = 0$, и обозначим её через $\text{Sym}(C)$. Отметим, что изометрия пространства \mathbb{F}^n является симметрией тогда и только тогда, когда она сохраняет вес произвольного вектора. Нетрудно доказывается

Утверждение 1. Для любого линейного кода $C \subseteq \mathbb{F}^n$ выполняется

$$\text{Aut}(C) \cong \text{Sym}(C) \ltimes C.$$

Определения других понятий, встречающихся далее, можно найти в [1, 2].

Согласно Хаффману [3] полупрямое произведение $\text{Gal}(\mathbb{F}) \ltimes \text{MAut}(\mathbb{F}^n)$, где $\text{Gal}(\mathbb{F})$ — группа Галуа поля \mathbb{F} , представляет все полулинейные* симметрии пространства \mathbb{F}^n . Если $q \geq 4$, то такие симметрии образуют собственную подгруппу группы $\text{Sym}(\mathbb{F}^n)$. Очевидно, что их доля уменьшается с ростом q . Группа полулинейных симметрий линейного кода C длины n размерности $n - m$ с кодовым расстоянием $d \geq 3$ изоморфна некоторой подгруппе общей полулинейной группы GL_m . В частности, широко известна (см. [3, теорема 7.2])

Теорема 1. Группа полулинейных симметрий кода Хэмминга длины $n = \frac{q^m - 1}{q - 1}$ изоморфна GL_m .

*Функция $f: \mathbb{F}^n \rightarrow \mathbb{F}^n$ называется *полулинейной* с сопутствующим автоморфизмом $\gamma \in \text{Gal}(\mathbb{F})$, если для любых $\alpha, \beta \in \mathbb{F}$ и $x, y \in \mathbb{F}^n$ выполняется $f(\alpha x + \beta y) = \gamma(\alpha)f(x) + \gamma(\beta)f(y)$.

При $q \in \{2, 3\}$ все симметрии \mathbb{F}^n линейны, так как

$$\text{Sym}(\mathbb{F}^n) = \text{MAut}(\mathbb{F}^n).$$

Поэтому $\text{Aut}(\mathcal{H}) \cong GL_m(q) \ltimes \mathcal{H}$. Возникает естественный вопрос: будет ли при любом $q \geq 4$ выполняться $\text{Aut}(\mathcal{H}) \cong GL_m \ltimes \mathcal{H}$? Как показывает следующий пример, существуют нетривиальные линейные коды, которые имеют автоморфизмы, не являющиеся полулинейными.

Пример. Рассмотрим линейный код C (MDP-код) с проверочной матрицей $H = [1 \ 1 \ \dots \ 1]$. Пусть $q = p^r$ и A — подстановка из S_q , заданная некоторым линейным преобразованием поля $\mathbb{F} = GF(q)$ как векторного пространства размерности r над простым подполем $GF(p)$. Тогда для $x \in \mathbb{F}^n$ справедливо $x_1 A + x_2 A + \dots + x_n A = (x_1 + \dots + x_n) A$, а также выполнено $0A = 0$. Отсюда следует, что $x \in C$ эквивалентно $(x_1 A, x_2 A, \dots, x_n A) \in C$. Таким образом, $(e; (A, \dots, A)) \in \text{Aut}(C)$. Если $q \geq 8$, то, очевидно, A можно выбрать так, чтобы оно не являлось умножением на ненулевой элемент поля и не принадлежало группе $\text{Gal}(\mathbb{F})$. Тогда указанный автоморфизм кода C не является полулинейным преобразованием пространства \mathbb{F}^n .

В настоящей статье доказано, что группа автоморфизмов кода Хэмминга \mathcal{H} изоморфна полупрямому произведению $GL_m \ltimes \mathcal{H}$. Показано, что симметрии подкода, состоящего из всех кодовых слов веса 3 кода \mathcal{H} , являются полулинейными. В частности, это означает, что произвольная симметрия кода Хэмминга полулинейна.

1. Автоморфизмы кода Хэмминга

Пусть T — подкод кода Хэмминга, состоящий из кодовых слов веса 3, иначе говоря $T = \{x \in \mathcal{H} \mid w(x) = 3\}$. Стоит отметить, что коду T соответствует так называемая обобщённая система троек Штейнера. Через \mathbb{F}^* обозначим мультипликативную группу поля \mathbb{F} , а через α — её порождающий элемент. Из утверждения 5 [1] следует

Утверждение 2. Если $x, y \in T$ и $\text{supp}(x) = \text{supp}(y)$, то $y = \mu x$ для некоторого $\mu \in \mathbb{F}^*$.

Как замечено выше, любая симметрия пространства \mathbb{F}^n сохраняет вес любого вектора. Поэтому очевидно, что $\text{Sym}(\mathcal{H}) \leq \text{Sym}(T)$. Рассмотрим симметрии кода T и покажем, что они являются полулинейными. Отсюда будет следовать полулинейность симметрий кода Хэмминга. Пусть $N = \{1, 2, \dots, n\}$.

Лемма 1. Если $(\pi; \sigma) \in \text{Sym}(T)$, то существует биекция γ , определённая на \mathbb{F} , такая, что для произвольных $j \in N$ и $\lambda, \beta \in \mathbb{F}$ выполнено

$$(\lambda\beta)\sigma_j = \gamma(\lambda) \cdot \beta\sigma_j. \quad (1)$$

ДОКАЗАТЕЛЬСТВО. Если $\lambda \neq 0$, то для всякого $x \in \mathbb{F}^n$ имеем

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

Отсюда и из утверждения 2 следует, что если $x \in T$, то

$$(\lambda x)(\pi; \sigma) = \mu \cdot x(\pi; \sigma), \quad (2)$$

где $\mu = \mu(\lambda, x) \in \mathbb{F}^*$, вообще говоря, μ зависит от λ и x . Равенство (2) показывает, что произвольная симметрия кода T сохраняет коллинеарность троек. Поскольку $(\lambda x)\pi = \lambda(x\pi)$, обозначив $y = x\pi$, перепишем (2) в виде $(\lambda y)\sigma = \mu \cdot y\sigma$. Пусть $\text{supp}(y) = \{i, j, k\}$. Тогда

$$\frac{(\lambda y_i)\sigma_i}{y_i\sigma_i} = \frac{(\lambda y_j)\sigma_j}{y_j\sigma_j} = \frac{(\lambda y_k)\sigma_k}{y_k\sigma_k} = \mu.$$

Так как код Хэмминга совершенный, для произвольных $i, j \in N$ и $s \in \{0, \dots, q-2\}$ найдётся вектор x^s из T такой, что $y_i^s = (x^s\pi)_i = 1$ и $y_j^s = (x^s\pi)_j = \alpha^s$. Таким образом, фиксируя i , получаем равенства

$$\frac{(\lambda \cdot 1)\sigma_i}{1\sigma_i} = \frac{(\lambda \alpha^s)\sigma_j}{\alpha^s\sigma_j} = \mu(\lambda, x^s) = \mu(\lambda, x^0), \quad j \in N \setminus \{i\}, \quad s \in \{0, \dots, q-2\}.$$

Иначе говоря, для произвольного $\beta \in \mathbb{F}^*$ справедливо

$$(\lambda\beta)\sigma_j = \mu \cdot \beta\sigma_j, \quad j \in N \setminus \{i\}, \quad (3)$$

где $\mu = \mu(\lambda)$, т.е. зависит только от λ . Заметим, что (3) выполняется также и для $\beta = 0$.

Определим отображение $\gamma: \mathbb{F}^* \rightarrow \mathbb{F}^*$ по правилу: $\gamma(\lambda) = \mu$, если выполнено (3). Поскольку σ_j биективно, получим биекцию на \mathbb{F}^* . Доопределив $\gamma(0) = 0$, зададим биекцию на \mathbb{F} такую, что для произвольного $j \neq i$ и любых $\lambda, \beta \in \mathbb{F}$ выполнено (1). В силу произвольности выбора $i \in N$ лемма 1 доказана.

Из леммы 1 следует, что произвольная симметрия кода T сохраняет коллинеарность векторов пространства \mathbb{F}^n . Следующая лемма показывает, что симметрии кода T сохраняют также сумму произвольных векторов из \mathbb{F}^n .

Лемма 2. Если $(\pi; \sigma) \in \text{Sym}(T)$, то для любого $j \in N$ подстановка σ_j сохраняет операцию сложения в поле \mathbb{F} , т. е.

$$(\lambda + \mu)\sigma_j = \lambda\sigma_j + \mu\sigma_j, \quad \lambda, \mu \in \mathbb{F}. \quad (4)$$

ДОКАЗАТЕЛЬСТВО. Пусть сначала $\lambda \neq \mu$ и $\lambda\mu \neq 0$. Поскольку код Хэмминга совершенный, для фиксированных $i, j \in N$ найдутся тройки x^1, x^2 из T такие, что $y_i^1 = y_i^2 = 1$, $y_j^1 = \lambda$, $y_j^2 = \mu$, где $y^1 = x^1\pi$, $y^2 = x^2\pi$. Предположим, что оставшиеся ненулевые координаты векторов y^1 и y^2 равны $y_{k_1} = \beta_1$ и $y_{k_2} = \beta_2$ соответственно, где $k_1 \neq k_2$ (последнее верно, так как $d(y^1, y^2) \geq 3$). Рассмотрим $z^1 = x^1(\pi; \sigma)$, $z^2 = x^2(\pi; \sigma)$ и $z = (x^1 - x^2)(\pi; \sigma)$. В силу линейности \mathcal{H} имеем $x^1 - x^2 \in T$ (что означает $z \in T$), а также $z^1 - z^2 \in T$.

Заметим, что $d(z, z^1 - z^2) \leq 2$, тогда как кодовое расстояние T равно 3. Действительно, $z = (x^1 - x^2)(\pi; \sigma) = (y^1 - y^2)\sigma$, так что $z_i = (z^1 - z^2)_i = 0$ и, следовательно, $\text{supp}(z) = \text{supp}(z^1 - z^2) = \{j, k_1, k_2\}$. Более того, $z_{k_1} = (z^1 - z^2)_{k_1} = \beta_1\sigma_{k_1}$.

Из доказанного следует, что $z = z^1 - z^2$, а значит, $(\lambda - \mu)\sigma_j = \lambda\sigma_j - \mu\sigma_j$. Последовательным применением последнего равенства к $(\lambda + \mu)\sigma_j = (\lambda - (\mu - \lambda))\sigma_j$ получаем (4). Так как $0\sigma_j = 0$, равенство (4) остаётся справедливым и в случае $\lambda\mu = 0$. Наконец, поскольку \mathbb{F} конечно, а σ_j биективно, то $(\lambda + \lambda)\sigma_j = \lambda\sigma_j + \lambda\sigma_j$. В силу произвольности $i, j \in N$ лемма 2 верна.

Используя леммы 1 и 2, покажем, что любая симметрия из $\text{Sym}(T)$ полулинейна.

Лемма 3. Каждая симметрия $(\pi; \sigma)$ из $\text{Sym}(T)$ является полулинейной функцией.

ДОКАЗАТЕЛЬСТВО. Введём обозначение $f(x) = x(\pi; \sigma)$ для $x \in \mathbb{F}^n$. Из лемм 1 и 2 следует, что для произвольных $\lambda, \mu \in \mathbb{F}$ и $x, y \in \mathbb{F}^n$ выполняется

$$f(\lambda x + \mu y) = \gamma(\lambda)f(x) + \gamma(\mu)f(y),$$

где $\gamma: \mathbb{F} \rightarrow \mathbb{F}$ — некоторая биекция.

Докажем, что биекция γ является автоморфизмом поля \mathbb{F} . Действительно, по построению γ (см. доказательство леммы 1) для $x \in \mathbb{F}^n$ и $\lambda_1, \lambda_2 \in \mathbb{F}$ имеем

$$\gamma(\lambda_1\lambda_2)f(x) = f(\lambda_1\lambda_2x) = \gamma(\lambda_1)f(\lambda_2x) = \gamma(\lambda_1)\gamma(\lambda_2)f(x),$$

откуда $\gamma(\lambda_1\lambda_2) = \gamma(\lambda_1)\gamma(\lambda_2)$.

Аналогично,

$$\gamma(\lambda_1 + \lambda_2)f(x) = f((\lambda_1 + \lambda_2)x) = f(\lambda_1x) + f(\lambda_2x) = (\gamma(\lambda_1) + \gamma(\lambda_2))f(x),$$

откуда $\gamma(\lambda_1 + \lambda_2) = \gamma(\lambda_1) + \gamma(\lambda_2)$. Лемма 3 доказана.

Поскольку все симметрии кода Хэмминга \mathcal{H} образуют подгруппу в группе $\text{Sym}(T)$, они являются полулинейными. С другой стороны, теорема 1 описывает все полулинейные симметрии кода \mathcal{H} . Таким образом, из утверждения 1, леммы 3 и теоремы 1 следует

Теорема 2. Для произвольного q -ичного кода Хэмминга \mathcal{H} длины $n = \frac{q^m - 1}{q - 1}$, где $q, m \geq 2$, справедливо

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

Автор выражает глубокую благодарность научному руководителю Ф. И. Соловьёвой за постановку задачи и постоянное внимание к работе и признательность С. В. Августиновичу и Д. С. Кротову за ценные замечания и дискуссии, которые оказали плодотворное влияние на изложение материала.

ЛИТЕРАТУРА

1. Горкунов Е. В. Мономиальные автоморфизмы линейной и простой компонент кода Хэмминга // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 1. — С. 11–32.
2. Горкунов Е. В. Группа перестановочных автоморфизмов q -ичного кода Хэмминга // Пробл. передачи информ. — 2009. — Т. 45, № 4. — С. 18–25.
3. Huffman W. C. Codes and groups // Handbook of coding theory. Ch. 6. — Amsterdam, New York: Elsevier Sci., 1998. — P. 1345–1440.
4. MacWilliams F. J. Combinatorial problems of elementary Abelian groups: Doctoral thesis. — Harvard: Harvard Univ., 1962. — 93 p.

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

Статья поступила
15 февраля 2010 г.