Линейные и групповые совершенные коды над телами и квазителами

С. А. Малюгин

In this paper, we propose a general construction of linear perfect codes over infinite skew fields and quasi skew fields with right (left) unity. A complete classification of such codes over associative skew fields is given. Since the cardinality of the considered skew fields is infinite, the constructed codes have an infinite length. In the previous work, we considered codes over infinite countable fields, the length of which was also countable. We now remove this restriction and consider that the cardinality of the skew field and the length of the codes can be arbitrary (not necessarily countable).

Введение

Квазителом F называется кольцо, в котором для любых ненулевых $a, b \in F$ уравнения $ax = c,\ xb = c$ однозначно разрешимы при любом $c \in F$. Относительно операции умножения множество всех ненулевых элементов $F^* = F \setminus \{0\}$ квазитела F является *квазигруппой* (ассоциативность умножения не предполагается). Квазитело F называется *телом*, если в F существует (двусторонняя) единица $1 \in F$. Если в квазителе F существует правая (левая) единица, то называем F квазителом с *правой* (*левой*) единицей. Наиболее известным примером тела с ассоциативным умножением является тело кватернионов $\mathbb{H}$. Коммутативные тела принято называть полями. Классическим примером неассоциативного тела являются октавы $\mathbb{O}$ или числа Кэли, [1]. Имеется много других конструкций ассоциативных и неассоциативных тел изложенных, например, в [2, 3] (конкретный вид этих примеров в классификации совершенных кодов нам не потребуется). По теореме Веддерберна, любое конечное ассоциативное тело является полем. Также по теореме Артина—Цорна, любое конечное тело, в котором выполняется аксиома альтернативности ($x(xy) = x^2y$, $xy^2 = (xy)y$), тоже является полем (т. е. умножение в таком теле ассоциативно и коммутативно).

В этой работе предлагается общая конструкция линейных совершенных кодов над бесконечными телами и квазителами с правой (левой) единицей. Дается полная классификация таких кодов над ассоциативными телами. Так как мощность рассматриваемых тел бесконечна, то построенные коды будут иметь бесконечную длину. В предыдущей работе рассматривались коды над бесконечными счетными полями, длина которых тоже была счетной. Мы теперь снимаем это ограничение и считаем, что мощность тела и длина кодов может быть любой (не обязательно счетной, вопрос, заданный Д. С. Кротовым). Вся теория линейных кодов базировалась в [4] на аппарате проверочных матриц. В частности, в [4] выяснилось, что один из кодов Хэмминга $H_F^{(\omega)}$ имеет континуум не эквивалентных между собой проверочных матриц. Это одна из причин, поче-

му мы взяли за основу более абстрактный аксиоматический подход, а аппарат проверочных матриц используем только по мере необходимости.

1. Основные определения и предварительные результаты

Пусть F – произвольное квазитело. Абелева группа (по сложению) M называется (*левым*) *модулем* над F, или левым F-модулем, если на M задана (внешняя) операция умножения $\cdot : F \times M \to M$ со следующими аксиомами:

1) $(\alpha + \beta) \cdot \mathbf{x} = \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}$;

2) $\alpha \cdot (\mathbf{x} + \mathbf{y}) = \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}$;

3) $\alpha \cdot \mathbf{x} = \mathbf{0} \Rightarrow \alpha = 0$ или $\mathbf{x} = \mathbf{0}$ $\qquad (\alpha, \beta \in F,\ \mathbf{x}, \mathbf{y} \in M)$.

Если в квазителе F существует левая единица, то требуется выполнения аксиомы

4) $1 \cdot \mathbf{x} = \mathbf{x}$.

Если в квазителе F выполняется закон ассоциативности, то в определении F-модуля требуется выполнение еще одной аксиомы

5) $(\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x})$.

Непустое подмножество $L \subseteq M$ называем *подмодулем* в M, если из $\mathbf{x}, \mathbf{y} \in L$, $\alpha, \beta \in F$ следует $\alpha \cdot \mathbf{x} + \beta \cdot \mathbf{y} \in L$.

Если операция умножения в F коммутативна (т.е. F является полем), то приведенное выше определение является стандартным определением векторного пространства. Если же операция умножения некоммутативна, то аналогичным образом можно определить *правый* модуль (только в аксиомах 1) – 6) следует поменять порядок сомножителей) на обратный. Далее мы всегда будем считать рассматриваемые F-модули левыми.

Основным примером является модуль F^I — всех отображений индексного множества I в тело F. Операции сложения и умножения в F^I задаются покоординатно, т. е. для всех $i \in I$,

$$(\mathbf{x} + \mathbf{y})_i = x_i + y_i,\ (\alpha\mathbf{x})_i = \alpha x_i \quad \alpha \in F,\ \mathbf{x} = (x_i)_{i\in I},\ \mathbf{y} = (y_i)_{i\in I}.$$

Далее нас будет интересовать подмодуль F_0^I всех векторов $\mathbf{x} = (x_i)_{i\in I} \in F^I$, имеющих конечные *носители*, т.е. множество $[\mathbf{x}] = \{i \in I : x_i \neq 0\}$ (носитель вектора $\mathbf{x}$) является конечным. Такие векторы далее будем называть финитными. В пространстве F_0^I определим *норму Хэмминга* $\|\mathbf{x}\|$, как число элементов в носителе $[\mathbf{x}]$. Если в квазителе F есть правая единица, то базисные векторы $(\delta_{i,j})_{j\in I}$(где $\delta_{i,j}$ — символ Кронекера) будем далее обозначать стандартно через $\mathbf{e}_i$.

Определение 1. Подмножество $C \subset F_0^I$ называется *r-совершенным кодом*, если расстояние Хэмминга между различными $\mathbf{x}, \mathbf{y} \in C$ больше $2r$ и объединение всех шаров радиуса r с центрами из C покрывает все пространство F_0^I.

Если r-совершенный код содержит нулевой вектор, то из этого определения очевидно следует, что вес ненулевых векторов такого кода не меньше, чем $2r+1$.

Определение 2. r-совершенный код $C \subset F_0^I$ называем *групповым* (*линейным*), если C является подгруппой (подмодулем) в F_0^I относительно операции сложения (сложения и умножения).

Лемма 1. *Любой ненулевой вектор r-совершенного группового кода C представляется конечной суммой векторов веса $2r+1$ из C.*

Доказательство этой леммы см. [4, 5].

Далее будем рассматривать только 1-совршенные коды ($r = 1$) и будем называть такие коды просто *совершенными кодами*. Это обосновывается тем, что в этом случае имеется естественная конструкция таких кодов.

Рассмотрим еще один левый (ненулевой) модуль L (над тем же телом F). Подмодуль ℓ называем одномерным, если для некоторого ненулевого базисного вектора $\mathbf{a} \in L$ выполняется $\ell = F\mathbf{a} = \{\alpha \cdot \mathbf{a} : \alpha \in F\}$. Рассмотрим семейство $\mathscr{P}$, одномерных подмодулей в L, удовлетворяющее следующим свойствам:

(a) из $\ell_1, \ell_2 \in \mathscr{P}$, $\ell_1 \neq \ell_2$ следует $\ell_1 \cap \ell_2 = \{\mathbf{0}\}$;

(b) $L = \cup\{\ell : \ell \in \mathscr{P}\}$

(так как умножение не предполагается ассоциативным то эти свойства не выполняется автоматически). В каждом одномерном подмодуле $\ell \in \mathscr{P}$ выберем некоторый базисный вектор $\mathbf{a}_\ell$ (с помощью аксиомы выбора, если $\mathscr{P}$ бесконечно). Функцию выбора обозначим через E, т. е. $E : \mathscr{P} \to L \setminus \{\mathbf{0}\}$, $E(\ell) = \mathbf{a}_\ell$ ($\ell \in \mathscr{P}$). В пространстве $F_0^{\mathscr{P}}$ рассмотрим следующее подпространство:

$$\mathscr{H}_E = \left\{ \mathbf{x} = (x_\ell)_{\ell \in \mathscr{P}} : \sum_{\ell \in \mathscr{P}} x_\ell \, \mathbf{a}_\ell = \mathbf{0} \right\}. \tag{1}$$

Все суммы в этом определении являются конечными, в силу финитности векторов $\mathbf{x} \in F_0^{\mathscr{P}}$.

Лемма 2. *Подмножество $\mathscr{H}_E \subset F_0^{\mathscr{P}}$ является совершенным групповым кодом.*

Доказательство. Очевидно, $\mathscr{H}_E$ является аддитивной подгруппой в $F_0^{\mathscr{P}}$. Так как из $\ell \neq \ell'$ следует $F\mathbf{a}_\ell \cap F\mathbf{a}_{\ell'} = \{\mathbf{0}\}$, то вес ненулевых векторов из $\mathscr{H}_E$ не может быть меньше трех. Это означает, что расстояние Хэмминга между различными векторами из $\mathscr{H}_E$ не меньше трех. Поэтому шары радиуса 1, с центрами из $\mathscr{H}_E$ попарно не пересекаются. Чтобы показать, что объединение всех таких шаров покрывает все пространство $F_0^{\mathscr{P}}$, рассмотрим любой вектор $\mathbf{y} = (y_\ell)_{\ell \in \mathscr{P}} \in F_0^{\mathscr{P}} \setminus \mathscr{H}_E$. Следовательно, в пространстве L, вектор $\mathbf{z} = \sum_{\ell \in \mathscr{P}} z_\ell \, \mathbf{a}_\ell \neq \mathbf{0}$. $\mathbf{z} \in \ell_0$ при некотором $\ell_0 \in \mathscr{P}$. Поэтому $\mathbf{z} = \alpha_0 \mathbf{a}_{\ell_0}$ для

некоторого ненулевого $\alpha_0 \in F$. Рассмотрим в пространстве $F_0^{\mathscr{P}}$ вектор $\mathbf{x}$ с координатами $x_\ell = z_\ell$ при $\ell \neq \ell_0$ и $x_{\ell_0} = z_{\ell_0} - \alpha_0$. По построению $\mathbf{x} \in \mathscr{H}_E$ и $\mathbf{x}$ отличается от $\mathbf{y}$ только в одной координате ℓ_0. Поэтому $\|\mathbf{x} - \mathbf{y}\| = 1$ и $\mathbf{x}$ находится в шаре радиуса 1 с центром в $\mathbf{y} \in \mathscr{H}_E$. Лемма доказана.

Определенный таким способом совершенный код $\mathscr{H}_E$ будем далее называть *кодом Хэмминга*, построенным по функции выбора E. Смысл следующей теоремы состоит в том, что так устроен любой совершенный линейный код.

Теорема 1. *Для любого квазмтела F, любого бесконечного множества I, мощность которого $|I| \geqslant |F|$, и любого линейного совершенного кода $C \subset F_0^I$ существует левый модуль L и взаимно однозначное отображение $\psi : I \to \mathscr{P}$, множества I в множество одномерных подмодулей $\mathscr{P}$ модуля L, удовлетворяющее свойствам (a), (b), что для некоторой функции выбора $E : \mathscr{P} \to L\backslash\{\mathbf{0}\}$ $(E(\ell) = \mathbf{a}_\ell,\ \ell \in \mathscr{P})$ имеет место эквивалентность*

$$\mathbf{x} = (x_i)_{i\in I} \in C \iff \sum_{i\in I} x_i \mathbf{a}_{\psi(i)} = \mathbf{0}. \tag{2}$$

Доказательство. Пусть ненулевыми элементами пространства L являются пары (α, i), где $\alpha \in F^*$, $i \in I$. Нулевой элемент пространства L можно отождествить со всеми парами вида $(0, i)$, $i \in I$. Операцию умножения скаляра на вектор определим следующим образом: $\alpha(\beta, i) = (\alpha\beta, i)$, $\alpha, \beta \in F$, $i \in I$. Зададим теперь операцию сложения таких векторов следующим образом: $(\alpha, i) + (\beta, i) = (\alpha + \beta, i)$, $(\alpha, i) + (0, j) = (0, j) + (\alpha, i) = (\alpha, i)$, $\alpha, \beta \in F$, $i, j \in I$. Осталось определить сумму $(\alpha, i) + (\beta, j)$ для $\alpha, \beta \in F^*$, $i \neq j \in I$. Рассмотрим вектор $\mathbf{x} \in F_0^I$ с координатами $x_i = \alpha$, $x_j = \beta$, $x_k = 0$ для всех $k \neq \alpha, \beta$. Из совершенности кода C следует существование единственного вектора $\mathbf{y} \in C$, для которого $\|\mathbf{x} - \mathbf{y}\| = 1$, т. е. $\mathbf{y} = \alpha\mathbf{e}_i + \beta\mathbf{e}_j + \gamma\mathbf{e}_k$ для некоторых $k \in I$, $\gamma \in F^*$. Полагаем $(\alpha, i) + (\beta, j) = (-\gamma, k)$. Необходимо доказать, что так определенные операции сложения и умножения на скаляры задают на множестве таких пар структуру левого модуля. Из определения сразу следует коммутативность сложения $(\alpha, i) + (\beta, j) = (\beta, j) + (\alpha, i)$. Дистрибутивность сложения $\alpha((\beta, i) + (\gamma, j)) = \alpha(\beta, i) + \alpha(\gamma, j)$ следует из линейности кода C. Так как при $i \neq j$, $\beta, \gamma \in F^*$ имеем $\beta\mathbf{e}_i + \gamma\mathbf{e}_j - \delta\mathbf{e}_k \in C$ при некоторых $\delta \in F^*$, $k \in I$, $k \neq i, j$. Тогда тоже $\alpha\beta\mathbf{e}_i + \alpha\gamma\mathbf{e}_j - \alpha\delta\mathbf{e}_k \in C$. Это означает, что $(\alpha\beta, i) + (\alpha\gamma, j) = (\alpha\gamma, k) = \alpha(\gamma, k) = \alpha((\alpha, i) + (\beta, j))$. Из неочевидных проверок является только проверка ассоциативности операции сложения

$$((\alpha, i) + (\beta, j)) + (\gamma, k) = (\alpha, i) + ((\beta, j) + (\gamma, k)) \tag{3}$$

в случае, когда $\alpha, \beta, \gamma \in F^*$, $i, j, k \in I$.

1) Равенство (3) очевидно при $i = j = k$.

2) Пусть $i = j$, $k \neq i$, $\beta = -\alpha$. Левая часть равенства (3) равна (γ, k). В правой части равенства (3) $(-\alpha, i) + (\gamma, k) = (\delta, l)$ для некоторых $l \neq i, k$,

$\delta \in F^*$, при этом $-\alpha\mathbf{e}_i + \gamma\mathbf{e}_k - \delta\mathbf{e}_l \in C$. Далее, $(\alpha, i) + (\delta, l) = (\lambda, m)$, где $\alpha\mathbf{e}_i + \delta\mathbf{e}_l - \lambda\mathbf{e}_m \in C$. Код C является группой по сложению, поэтому вектор $\gamma\mathbf{e}_k - \lambda\mathbf{e}_m \in C$. Вес такого вектора не больше 2, поэтому $m = k$ и $\lambda = \gamma$. Мы доказали, что правая часть равенства (3) равна $(\alpha, i) + ((-\alpha, i) + (\gamma, k)) = (\gamma, k)$ и совпадает с левой частью этого равенства.

3) Пусть теперь $i = j$, $k \neq i$, $\beta \neq -\alpha$. В левой части равенства (3) получаем $(\alpha + \beta, i) + (\gamma, k) = (\delta, l)$ для некоторых $\delta \in F^*$, $l \in I$, $l \neq i, k$. При этом $(\alpha + \beta)\mathbf{e}_i + \gamma\mathbf{e}_k - \delta\mathbf{e}_l \in C$. Выражение в скобках правой части (3) равно $(\beta, i) + (\gamma, k) = (\lambda, m)$ для некоторых $\lambda \in F^*$, $m \in I$, $m \neq i, k$. При этом $\beta\mathbf{e}_i + \gamma\mathbf{e}_k - \lambda\mathbf{e}_m \in C$. Далее, $(\alpha, i) + (\lambda, m) = (\mu, n)$ для некоторых $\mu \in F^*$, $n \in I$, $n \neq i, m$. Причем $\alpha\mathbf{e}_i + \lambda\mathbf{e}_m - \mu\mathbf{e}_n \in C$. Из группового свойства кода C снова получаем $((\alpha+\beta)\mathbf{e}_i+\gamma\mathbf{e}_k-\delta\mathbf{e}_l)-(\beta\mathbf{e}_i+\gamma\mathbf{e}_k-\lambda\mathbf{e}_m)-(\alpha\mathbf{e}_i+\lambda\mathbf{e}_m-\mu\mathbf{e}_n) = \mu\mathbf{e}_n-\delta\mathbf{e}_l \in C$. Снова получили вектор веса не больше 2, принадлежащий коду C. Поэтому $n = l$ и $\mu = \delta$. Правая часть равенства (3) тоже оказалась равной (δ, l).

4) Равенство (3) доказано для $i = j$. Из коммутативности сложения следует, что оно верно также при $j = k$ или $i = k$.

5) Пусть $i, j, k \in I$ все различны, но $(\alpha, i) + (\beta, j) = (\delta, k)$ для некоторого $\delta \in F^*$, причем $\alpha\mathbf{e}_i + \beta\mathbf{e}_j - \delta\mathbf{e}_k \in C$. Тогда левая часть равенства (3) равна $(\gamma + \delta, k)$. Рассмотрим правую часть. Пусть $(\beta, j) + (\gamma, k) = (\lambda, l)$, где $\lambda \in F^*$, $l \in I$, $l \neq j, k$ и $\beta\mathbf{e}_j + \gamma\mathbf{e}_k - \lambda\mathbf{e}_l \in C$. Если $l = i$, то получим $(\alpha\mathbf{e}_i + \beta\mathbf{e}_j - \delta\mathbf{e}_k) - (\beta\mathbf{e}_j + \gamma\mathbf{e}_k - \lambda\mathbf{e}_i) = (\alpha + \lambda)\mathbf{e}_i - (\gamma + \delta)\mathbf{e}_k \in C$. Так как $i \neq k$, то $\lambda = -\alpha$ и $\delta = -\gamma$. При этом правая часть равенства (3) будет равна $(\alpha, i) + (-\alpha, i) = (0, i)$ и левая часть тоже будет равна $(0, i)$. Если же $l \neq i$, то $(\alpha, i)+(\lambda, l) = (\mu, m)$ для некоторых $\mu \in F^*$, $m \in I$, $m \neq i, l$, при этом $\alpha\mathbf{e}_i+\lambda\mathbf{e}_l-\mu\mathbf{e}_m \in C$. Следовательно, $(\alpha\mathbf{e}_i + \beta\mathbf{e}_j - \delta\mathbf{e}_k) - (\beta\mathbf{e}_j + \gamma\mathbf{e}_\mathbf{k} - \lambda\mathbf{e}_l) - (\alpha\mathbf{e}_i + \lambda\mathbf{e}_l - \mu\mathbf{e}_m) = \mu\mathbf{e}_m - (\gamma + \delta)\mathbf{e}_k \in C$. Отсюда, $m = k$ и $\mu = \gamma + \delta$, что означает справедливость равенства (3) при условии $(\alpha, i) + (\beta, j) = (\delta, k)$.

6) Пусть $(\alpha, i) + (\beta, j) = (\delta, l)$ для некоторых $\delta \in F^*$, $l \in I$, $l \neq i, j, k$, при этом $\alpha\mathbf{e}_i + \beta\mathbf{e}_j - \delta\mathbf{e}_l \in C$. Далее, $(\delta, l) + (\gamma, k) = (\lambda, m)$ для некоторых $\lambda \in F^*$, $m \in I$, $m \neq k, l$, причем $\delta\mathbf{e}_l + \gamma\mathbf{e}_k - \lambda\mathbf{e}_m \in C$. Аналогично, вычисление правой части равенства (3) дает $(\beta, j) + (\gamma, k) = (\mu, n)$, где $\mu \in F^*$, $n \in I$, $n \neq j, k$, причем $\beta\mathbf{e}_j+\gamma\mathbf{e}_k-\mu\mathbf{e}_n \in C$. Можно считать, что $n \neq i$ (аналогичный случай был рассмотрен в предыдущем пункте 5)). И на последнем этапе $(\alpha, i)+(\mu, n) = (\nu, p)$ для некоторых $\nu \in F^*$, $p \in I$, $p \neq i, n$, при этом $\alpha\mathbf{e}_i + \mu\mathbf{e}_n - \nu\mathbf{e}_p \in C$. Значит $(\alpha\mathbf{e}_i + \beta\mathbf{e}_j - \delta\mathbf{e}_l) + (\delta\mathbf{e}_l + \gamma\mathbf{e}_k - \lambda\mathbf{e}_m) - (\beta\mathbf{e}_j + \gamma\mathbf{e}_k - \mu\mathbf{e}_n) - (\alpha\mathbf{e}_i + \mu\mathbf{e}_n - \nu\mathbf{e}_p) = \nu\mathbf{e}_p - \lambda\mathbf{e}_m \in C$. Следовательно, $p = m$ и $\nu = \lambda$, что означает справедливость равенства (3) во всех возможных случаях.

Итак, множество всех пар (α, i), $\alpha \in F^*$, $i \in I$, вместе с нулевым элементом (отождествляемым с парами $(0, i)$, $i \in I$) является, относительно введенных выше операций, левым модулем L. Отображение $\psi : I \to L$ зададим формулой

$\psi(i) = (1, i)$ $(i \in I)$.

Доказательство эквивалентности (2) для векторов $\mathbf{x}$ веса 3 сразу следует из определения операции сложения в построенном пространством L. С другой стороны, любой ненулевой вектор $\mathbf{x} \in C$, в силу леммы 1, представляется конечной суммой векторов из C веса 3. Этим обосновывается в (2) импликация $\Rightarrow$. Для доказательства обратной импликации $\Leftarrow$ рассмотрим любой вектор $\mathbf{x} \in F_0^I$ такой, что в пространстве L выполняется

$$\sum_{i \in I} x_i(1, i) = \mathbf{0}(= (0, k), k \in I). \tag{4}$$

Рассмотрим пару ненулевых координат x_{i_1}, x_{i_2}. Так как $x_{i_1}(1, i_1) + (x_{i_2})(1, i_2) = (y, i_3) = y(1, i_3)$ при некотором $i_3 \neq i_1, i_2$, то вектор $\mathbf{z}$, веса 3, с ненулевыми координатами $z_{i_1} = x_{i_1}$, $z_{i_2} = x_{i_2}$, $z_{i_3} = -y$, Принадлежит коду C. Заменив в (4) x_i на $x_i - z_i$, получим равенство нулю суммы с меньшим количеством ненулевых слагаемых. Через конечное число шагов получим, что $\mathbf{x}$ является конечной суммой векторов веса 3 из кода C. Теорема полностью доказана.

Доказательство теоремы 1 (в отличие от леммы 2) является конструктивным. Несмотря на то, что ассоциативность умножения в доказательстве теоремы 1 никак не используется, для совершенных кодов над неассоциативными телами она носит условный характер, так как имеет место следующий отрицательный результат:

Предложение 1. *Линейных совершенных кодов над над неассоциативными квазителами с правой единицей не существует.*

Доказательство. Пусть F — неассоциативное квазитело с правой единицей и $C \subset F_0^I$ — совершенный линейный код. Рассмотрим любые три ненулевых элемента $a, b, c \in F$. Для двух различных индексов $i_1, i_2 \in I$ рассмотрим вектор $\mathbf{x} \in F_0^I$ с координатами $x_{i_1} = 1$, $x_{i_2} = c$, $x_i = 0$ для всех остальных индексов $i \in I$, $i \neq i_1, i_2$. Вес такого вектора равен двум, поэтому существует единственный вектор $\mathbf{y} \in C$ веса 3, для которого $\|\mathbf{x}-\mathbf{y}\| = 1$. Следовательно, $\mathbf{y} = \mathbf{e}_{i_1}+c\mathbf{e}_{i_2}+d\mathbf{e}_{i_3}$ для некоторых $d \in F^*$, $i_3 \in I$, $i_3 \neq i_1, i_2$. В силу предполагаемой линейности кода C, получаем $b\mathbf{e}_{i_1} + (bc)\mathbf{e}_{i_2} + (bd)\mathbf{e}_{i_3} \in C$, $(ab)\mathbf{e}_{i_1} + a(bc)\mathbf{e}_{i_2} + a(bd)\mathbf{e}_{i_3} \in C$, $(ab)\mathbf{e}_{i_1} + (ab)c\mathbf{e}_{i_2} + (ab)d\mathbf{e}_{i_3} \in C$. Поэтому $(ab)\mathbf{e}_{i_1} + a(bc)\mathbf{e}_{i_2} + a(bd)\mathbf{e}_{i_3} - ((ab)\mathbf{e}_{i_1} + (ab)c\mathbf{e}_{i_2} + (ab)d\mathbf{e}_{i_3}) = (a(bc) - (ab)c)\mathbf{e}_{i_2} - (a(bd) - (ab)d)\mathbf{e}_{i_3} \in C$. Вес полученного вектора из C не больше двух, поэтому, в частности $a(bc) - a(bc) = 0$ для любых $a, b, c \in F$, что противоречит предполагаемой неассоциативности квазитела F. Предложение доказано.

2. Конструкция совершенных групповых кодов над неассоциативными квазителами.

Рассмотрим множество J мощности $|J| \geqslant 2$. По аксиоме выбора (в случае $|J| \geqslant \aleph_0$) его можно вполне упорядочить наименьшим ординальным числом α,

т. е. можно считать, что $J = \{\beta : \beta < \alpha\}$. Для каждого $\beta < \alpha$ Фиксируем ненулевой элемент $b_\beta \in F^*$. Для любого ординала $\beta \in J$, в модуле F_0^J рассмотрим подмножество

$$L_\beta = \left\{ \mathbf{0}_\beta \oplus b_\beta \oplus \mathbf{x} : \mathbf{x} \in F_0^{\{\gamma:\beta<\gamma<\alpha\}} \right\},$$

где $\mathbf{0}_\beta$ — нулевой вектор в $F_0^{\{\gamma:0\leqslant\gamma<\beta\}}$. Неформально говоря, в L_β собраны все векторы $\mathbf{x} = (x_\gamma)_{\gamma\in J}$ из F_0^J, у которых все координаты $x_\gamma = 0$ при $\gamma < \beta$, $x_\beta = b_\beta$, x_γ произвольны при $\beta < \gamma$ и равны нулю за исключением некоторого конечного числа координат. Рассмотрим объединение

$$A_\alpha = \bigcup \{L_\beta : \beta \in J\} \subset L = F_0^J, \tag{5}$$

которое будем называть *множеством столбцов проверочной матрицы*. Для любого столбца $\mathbf{a} \in A_\alpha$ рассмотрим одномерный подмодуль $\ell_\mathbf{a} = F\mathbf{a}$. Функция выбора теперь определится однозначно

$$E(\ell_\mathbf{a}) = \mathbf{a} \quad (\mathbf{a} \in A_\alpha). \tag{6}$$

Лемма 3. *Для множества $\mathscr{P} = \{\ell_\mathbf{a} : \mathbf{a} \in A_\alpha\}$, одномерных подмодулей модуля $L = F_0^J$ выполнены аксиомы* (a),(b).

Доказательство. Пусть $\mathbf{a}_1, \mathbf{a}_2 \in A_\alpha$, $\mathbf{a}_1 \neq \mathbf{a}_2$ и $\delta_1\mathbf{a}_1 = \delta_2\mathbf{a}_2$ при некоторых $\delta_1, \delta_2 \in F^*$. Если $\mathbf{a}_1 \in L_{\beta_1}$, $\mathbf{a}_2 \in L_{\beta_2}$ и $\beta_1 < \beta_2$, то у вектора $\mathbf{a}_1$ все координаты с номерами $\gamma < \beta_2$ должны быть нулевыми, что противоречит тому, что у $\mathbf{a}_1$ координата с номером β_1 равна $b_{\beta_1} \neq 0$. По той же причине не может быть $\beta_1 > \beta_2$. При $\beta_1 = \beta_2 = \beta$ равенство координат $\delta_1\mathbf{a}_1 = \delta_2\mathbf{a}_2$ с этим номером дает соотношение $\delta_1 b_\beta = \delta_2 b_\beta$. Следовательно, $\delta_1 = \delta_2 = \delta$ (по закону правого сокращения). Равенство $\delta\mathbf{a}_1 = \delta\mathbf{a}_2$ в любой координате $\beta < \gamma$ дает соотношение $\delta a_1 = \delta a_2$. В силу закона левого сокращения в квазителе F получаем $a_1 = a_2$, что влечет равенство $\mathbf{a}_1 = \mathbf{a}_2$, вопреки нашему предположению. мы доказали, что $\ell_{\mathbf{a}_1} \cap \ell_{\mathbf{a}_2} = \{\mathbf{0}\}$ при $\mathbf{a}_1 \neq \mathbf{a}_2$. Для доказательства свойства (b) рассмотрим любой вектор $\mathbf{x} \in L$. Пусть его ненулевая координата с наименьшим номером β равна x_β. Ее можно записать в виде yb_β, при некотором $y \in F^*$. Для любого номера $\gamma > \beta$ уравнение $yz = x_\gamma$ имеет единственное решение $z = a_\gamma$. полагая $a_\beta = b_\beta$, $a_\gamma = 0$ для всех $\gamma < \beta$, получим вектор $\mathbf{a} \in L$, для которого $\mathbf{x} = y\mathbf{a}$. Значит свойство (b) тоже выполнено. Лемма доказана.

Теперь из леммы 2 и леммы 3 уже следует существование групповых совершенных кодов над произвольным квазителом F, без каких либо ограничений.

Предложение 2. *Если F — произольное квазитело, то код Хэмминга $\mathscr{H}_E = \mathscr{H}_E(A_\alpha)$, построенный с помощью леммы* 2, *проверочной матрицы A_α из* (5) *и функции выбора* (6) *является групповым совершенным кодом. Если квазитело F имеет правую единицу, то код $\mathscr{H}_E$ будет линейным тогда и только тогда, когда квазитело F удовлетворяет аксиоме ассоциативности.*

Замечание 1. Ординал α в определении проверочной матрицы A_α и совершенного кода $\mathscr{H}_E(A_\alpha)$ обладает тем свойством, что любой ординал $\beta < \alpha$ имеет меньшую мощность, $|\beta| < |\alpha|$. Такие ординалы называются в теории множеств *начальными*. Поэтому конструкция кода $\mathscr{H}_E(A_\alpha)$ зависит только от мощности начального ординала α (числа строк проверочной матрицы A_α). Функция выбора однозначно задается формулой (6). Поэтому, для конечных ординалов $\alpha = 2, 3, \ldots$, коды Хэмминга $\mathscr{H}_E(A_\alpha)$ будем далее обозначать символами $\mathscr{H}_F^{(2)}$, $\mathscr{H}_F^{(3)}$, $\ldots$, указывая в нижнем индексе квазитело F, а в верхнем индексе число строк проверочной матрицы A_α. Для первого бесконечного ординала ω_0, счетной мощности $\aleph_0$, проверочная матрица A_{ω_0} будет иметь счетное множество строк, а код Хэмминга над квазителом F будет обозначаться символом $\mathscr{H}_F^{(\omega_0)}$. Следующим будет первый несчетный ординал ω_1 (наименьшей несчетной мощности $\aleph_1 = |\omega_1|$). Проверочная матрица A_{ω_1} будет иметь $\aleph_1$ строк, а код Хэмминга, построенный по такой матрице, обозначаем символом $\mathscr{H}_F^{(\omega_1)}$, и т. д. Код Хэмминга $\mathscr{H}_F^{(\alpha)}$ (для любого начального ординала α) зависит еще от выбора ненулевых элементов $b_\beta \in F^*$, но при наличии в квазителе F правой единицы мы всегда будем считать, что все $b_\beta = 1$.

Рассмотрим теперь простую конструкцию, позволяющую получать из тела F неассоциативное квазитело F_1 с правой единицей. Элементы $n = \underbrace{1 + \cdots + 1}_{n}$ порождают минимальное подполе F_0, относительно которого можно считать F векторным пространством. Считаем, что $F_0 \neq F$. Рассмотрим любую F_0-линейную биекцию $V : F \to F$, для которой $V(1) = 1$ и $V(a) = a$ для некоторого элемента $a \in F \setminus F_0$ (можно взять в качестве V тождественное отображение). Также полагаем $U(1) = a$, $U(a) = 1$. Так как $1, a$ линейно независимы над F_0, то можно продолжить U до линейной биекции $U : F \to F$. Введем на F новую операцию умножения $x \circ y = U^{-1}((Ux)(Vy))$ (такое преобразование операции умножения называется *изотопией*). Из линейности операторов U и V следует, что для $\circ$ выполнены аксиомы дистрибутивности. Кроме этого, $x \circ 1 = U^{-1}((Ux)(V1)) = U^{-1}((Ux)1) = U^{-1}(Ux) = x$. Допустим, что $1 \circ x = x$ для всех $x \in F$. Тогда $U(1 \circ a) = Ua = 1 = (U1)(Va) = aa$. Или $0 = a^2 - 1 = (a-1)(a+1)$. Получили противоречие с $a \neq \pm 1$. Поэтому новое умножение $\circ$ неассоциативно (иначе его правая единица была бы одновременно и левой единицей). В случае конечных полей подобная конструкция рассматривалась в [6].

Из теоремы Альберта [7] следует, что любое квазитело изотопно телу, см. [8], стр. 71. Следовательно, любое квазитело (в частности, конечное поле), не изотопное простым полям $\mathbb{Q}$, F_p (p — простое), изотопно неассоциативному квазителу с правой (левой) единицей. Это дает возможность строить совершенные групповые коды конечной длины над конечными неассоциативными квазителами. К сожалению такие коды эквивалентны стандартным кодам Хэмминга над конечными полями. Для построения новых конечных групповых кодов есть воз-

можность рассматривать не квазитела, а так называемые конечные почти-поля Цассенхауза, [9] (см. также [10, 11]).

Отображение $A : F_0^{I_1} \to F_0^{I_2}$ называется *изометрией*, если A является взаимно однозначным и сохраняет расстояние Хэмминга между векторами, т. е. $\|A(\mathbf{x}) - A(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$. В [4] показано, что любая изометрия A имеет вид

$$A(\mathbf{x}) = A\left(\sum_{i\in I_1} x_i\mathbf{e}_i\right) = \sum_{i\in I_1} b_i(x_i)\mathbf{e}_{\pi(i)} \quad (\mathbf{x} = (x_i)_{i\in I_1} \in F_0^{I_1}), \tag{4}$$

где $\pi : I_1 \to I_2$ — биективное отображение I_1 на I_2, и для любого индекса $i \in I_1$ b_i — биективное отображение тела F, для которого $b_i(0) = 0$ для всех $i \in I_1$, кроме некоторого конечного подмножества индексов из I_1.

Определение 3. Два совершенных кода $C_1 \subset F_0^{I_1}$, $C_2 \subset F_0^{I_2}$ называются *эквивалентными*, если существует изометрия $A : F_0^{I_1} \to F_0^{I_2}$, такая что $A(C_1) = C_2$. Если, кроме этого, $A(\mathbf{0}) = \mathbf{0}$, то коды C_1 и C_2 называем *изоморфными*.

Так как групповые совершенные коды содержат нулевой вектор, то два групповых совершенных кода $C_1 \subset F_0^{I_1}$, $C_2 \subset F_0^{I_2}$ эквивалентны тогда и только тогда, когда они изоморфны. В этом случае существует изометрия $A : F_0^{I_1} \to F_0^{I_2}$, $A(C_1) = C_2$, для которой выполняется равенство (4), где $\pi : I_1 \to I_2$ — биективное отображение и для любого индекса $i \in I_1$ b_i — биективное отображение тела F, для которого $b_i(0) = 0$ для всех $i \in I_1$ без исключения.

Назовем тело F *конечномерным*, если в его центре $Z(F) = \{x \in F : \forall y \in F,\ xy = yx\}$ существует подтело F_0, являющееся полем, относительно которого F является конечномерным векторным пространством, в противном случае называем тело F *бесконечномерным*. В этом случае говорят, что F является *алгеброй* над полем F_0. Классическими примерами алгебр являются: 4-мерная алгебра кватернионов $\mathbb{H}$ и 8-мерная алгебра октав $\mathbb{O}$ над полем $\mathbb{R}$.

В заключение этого параграфа мы построим бесконечную серию попарно неэквивалентных кодов над телом F, являющимся конечномерной алгеброй над своим подполем $F_0 \subset Z(F)$. Так как $F_0 \subset Z(F)$, то код $\mathscr{H}_F^{(\alpha)}$ будет на самом деле F_0-линейным.

Теорема 2. *Если мощности ординалов α_1 и α_2 не равны ($|\alpha_1| \neq |\alpha_2|$), то коды Хэмминга $\mathscr{H}_F^{(\alpha_1)}$ и $\mathscr{H}_F^{(\alpha_2)}$ не эквивалентны.*

Доказательство. Рассмотрим сначала случай конечных ординалов. Пусть проверочная матрица A_{α_1} имеет m_1 строк, а матрица A_{α_2} имеет m_2 строк и $2 \leqslant m_1 < m_2$. Проверочная матрица A_{α_2} содержит единичную подматрицу. Обозначим столбцы этой поматрицы $\mathbf{a}_1, \ldots, \mathbf{a}_{m_2}$. В силу эквивалентности (1), для любого ненулевого вектора $\mathbf{x} \in \mathscr{H}_F^{(\alpha_2)}$ существует столбец $\mathbf{a} \in A_{\alpha_2}$, $\mathbf{a} \neq \mathbf{a}_n$ $(1 \leqslant n \leqslant m_2)$, для которого координата $x_{\mathbf{a}} \neq 0$ (носитель $[\mathbf{x}]$ не может входить

в $\{\mathbf{a}_1, \ldots, \mathbf{a}_{m_2}\}$). Покажем, что в коде $\mathscr{H}_F^{(\alpha_1)}$ это свойство не выполнено. Это означает, что любое множество столбцов $\{\mathbf{a}_1, \ldots, \mathbf{a}_{m_2}\}$ линейно зависимо над F, т. е. уравнение

$$x_1\mathbf{a_1} + \cdots + x_{m_2}\mathbf{a}_{m_2} = \mathbf{0} \tag{5}$$

имеет ненулевое решение. Пусть размерность F над F_0 равна s. Тогда каждый элемент $x \in F$ можно разложить по базису векторного пространства F, $x = x^{(1)}i_1 + \ldots x^{(s)}i_s$. Рассмотрим в наборе столбцов $\{\mathbf{a}_1, \ldots, \mathbf{a}_{m_2}\}$, составляющем фрагмент проверочной матрицы A_{α_1} какую нибудь l-ю строку $(a_{l,1}, \ldots a_{l,m_2})$. Произведение

$$x_n a_{l,n} = f_{(1)}(x_n^{(1)}, \ldots x_n^{(s)}, a_{l,n}^{(1)}, \ldots, a_{l,n}^{(s)})i_1 + \cdots + f_{(s)}(x_n^{(1)}, \ldots x_n^{(s)}, a_{l,n}^{(1)}, \ldots, a_{l,n}^{(s)})i_s,$$

где $f_{(r)}(x_n^{(1)}, \ldots x_n^{(s)}, a_{l,n}^{(1)}, \ldots, a_{l,n}^{(s)})$ $(1 \leqslant r \leqslant s)$ — какие-то билинейные выражение над F_0 от $(x_n^{(1)}, \ldots x_n^{(s)})$, $a_{l,n}^{(1)}, \ldots, a_{l,n}^{(s)}$, задаваемые таблицей умножения базисных элементов $i_p i_q = \sum\limits_{r=1}^{s} c_{p,q}^r i_r$ $(c_{p,q}^r \in F_0)$. Явный вид этих выражений нам не потребуется. Равенство нулю (5) теперь эквивалентно однородной линейной системе уравнений над полем F_0

$$\sum_{n=1}^{m_2} f_{(r)}(x_n^{(1)}, \ldots x_n^{(s)}, a_{l,n}^{(1)}, \ldots, a_{l,n}^{(s)}) = 0 \quad (1 \leqslant r \leqslant s, 1 \leqslant l \leqslant m_1),$$

состоящую из sm_1 уравнений и $sm_2 > sm_1$ неизвестных $x_n^{(r)}$ $(1 \leqslant r \leqslant s, 1 \leqslant n \leqslant m_2)$. Такая система имеет ненулевое решение. Поэтому уравнение (5) тоже имеет ненулевое решение $(x_1, \ldots, x_{m_2})$. Следовательно, ненулевой вектор $\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_{m_2}\mathbf{e}_{m_2}$ принадлежит коду $\mathscr{H}_F^{(\alpha_1)}$ и его носитель входит в множество индексов $\mathbf{a}_1, \ldots, \mathbf{a}_{m_2}$. Так как такое свойство ненулевых векторов кода $\mathscr{H}_F^{(\alpha_1)}$ невозможно изменить, перестановкой координат и перестановкой ненулевых элементов тела F, то код $\mathscr{H}_F^{(\alpha_1)}$ не может быть эквивалентен коду $\mathscr{H}_F^{(\alpha_2)}$.

Пусть теперь мощность ординала α бесконечна, а мощность ординала α_1 меньше, чем $|\alpha_2|$. Если α_1 — конечный ординал, то из предыдущего доказательства очевидно следует, что коды $\mathscr{H}_F^{(\alpha_1)}$ и $\mathscr{H}_F^{(\alpha_2)}$ неэквивалентны. Если мощность множества проверочной матрицы A_{α_1} меньше мощности множества столбцов матрицы A_{α_2}, то тоже можно сразу сказать, что коды $\mathscr{H}_F^{(\alpha_1)}$, $\mathscr{H}_F^{(\alpha_2)}$ неэквивалентны. Поэтому считаем, что ординал α_1 тоже бесконечен и мощности множества столбцов у матриц A_{α_1} и A_{α_2} одинаковые. Нам осталось доказать, что любое множество столбцов матрицы $\{\mathbf{a}_m\}_{m \in M}$ мощности $|\alpha_2|$ линейно зависимо над телом F. Для этого заменим каждый столбец $\mathbf{a}_m$ на "увеличенный" столбец $\mathbf{a}_m^{(s)}$ следующим образом. Каждый элемент $a_{l,m}$ столбца $\mathbf{a}_m^{(s)}$ заменяем на столбец

$$\begin{pmatrix} a_{l,m}^{(1)} \\ \vdots \\ a_{l,m}^{(s)} \end{pmatrix} \quad \text{где} \quad a_{l,m} = a_{l,m}^{(1)}i_1 + \cdots + a_{l,m}^{(s)}i_s$$

Так как все $a_{l,m}^{(r)}$ принадлежат полю F_0, то "увеличенные" столбцы $\mathbf{a}_m^{(s)}$ $(m \in M)$ принадлежат (над полем F_0) векторному пространству столбцов размерности $s|\alpha_1| = |\alpha_1|$. Поэтому множество столбцов $\{\mathbf{a}_m^{(s)}\}_{m\in M}$ (мощности $|\alpha_2| > |\alpha_1|$) линейно зависимо над полем F_0, т. е. для некоторого конечного набора $\mathbf{a}_{m_1}^{(s)}, \ldots, \mathbf{a}_{m_1}^{(s)}$ будет выполняться $c_1\mathbf{a}_{m_1}^{(s)} + \cdots + c_k\mathbf{a}_{m_k}^{(s)} = \mathbf{0}$ при некоторых $c_1, \ldots, c_k \in F_0^*$. Следовательно то же самое будет верно и для исходных столбцов $c_1\mathbf{a}_{m_1} + \cdots + c_k\mathbf{a}_{m_k} = \mathbf{0}$. Получили линейную зависимость множества столбцов $\{\mathbf{a}_m\}_{m\in M}$ даже не над всем телом F, а только над его частью F_0. Теорема доказана.

Следствие. *Для алгебры октав $\mathbb{O}$, для любых двух ординалов α_1, α_2, имеющих разную мощность, коды Хэмминга $H_{\mathbb{O}}^{(\alpha_1)}$ и $H_{\mathbb{O}}^{(\alpha_2)}$ не эквивалентны.*

Замечание 2. Если тело F неассоциативно, то классификация F_0-линейных кодов является неполной, так как неизвестно, любой ли F_0-линейный совершенный код эквивалентен одному из кодов $\mathscr{H}_F^{(\alpha)}$. Кроме этого, не проведена классификация F_0-линейных совершенных кодов над бесконечномерными телами и квазителами. С другой стороны, получена полная классификация совершенных линейных кодов над любыми ассоциативными телами.

3. Классификация совершенных линейных кодов над ассоциативными телами.

Определение 4. Два совершенных кода $C_1 \subset F_0^{I_1}$, $C_2 \subset F_0^{I_2}$ называются *линейно изоморфными*, если существует линейная изометрия $A : F_0^{I_1} \to F_0^{I_2}$, такая что $A(C_1) = C_2$, где

$$A(\mathbf{x}) = A\left(\sum_{i\in I_1} x_i\mathbf{e}_i\right) = \sum_{i\in I_1} x_i\alpha_i\mathbf{e}_{\pi(i)} \quad (\mathbf{x} = (x_i)_{i\in I_1} \in F_0^{I_1}),$$

где $\pi : I_1 \to I_2$ — биективное отображение и $\alpha_i \in F^*$ $(i \in I_1)$.

Очевидно, понятие линейного изоморфизма является частным случаем понятия просто изоморфизма. Переходим непосредственно к классификации линейных совершенных кодов над ассоциативным телом F. Рассмотрим два линейных совершенных кода $C_1 \subset F_0^{I_1}$, $C_2 \subset F_0^{I_2}$. По теореме 1 существуют два линейных пространства L_1, L_2 и два биективных отображения $\psi_1 : I_1 \to \mathscr{P}_1$, $\psi_2 : I_2 \to \mathscr{P}_2$, на множество всех одномерных подпространств $\mathscr{P}_1$, $\mathscr{P}_2$ пространств L_1, L_2, соответственно, что для некоторых функций выбора $E_1 : \mathscr{P}_1 \to L_1 \setminus \{\mathbf{0}\}$ $(E_1(\ell) = \mathbf{a}_\ell^{(1)}, \ell \in \mathscr{P}_1)$, $E_2 : \mathscr{P}_2 \to L_2 \setminus \{\mathbf{0}\}$ $(E_2(\ell) = \mathbf{a}_\ell^{(2)}, \ell \in \mathscr{P}_2)$ имеет место эквивалентность

$$\mathbf{x} = (x_i)_{i\in I_1} \in C_1 \iff \sum_{i\in I_1} x_i\mathbf{a}_{\psi_1(i)}^{(1)} = \mathbf{0},$$

$$\mathbf{x} = (x_i)_{i\in I_2} \in C_2 \iff \sum_{i\in I_2} x_i\mathbf{a}_{\psi_2(i)}^{(2)} = \mathbf{0}.$$

В предположении аксиомы выбора в пространствах L_1, L_2 существуют базисы Гамеля. Мощности всех базисов Гамеля одинаковы для данного пространства L (над ассоциативным телом), см. [8], стр. 240. Эту мощность принято называть *алгебраической размерностью* линейного пространства L и обозначать его через $\dim L$. Теперь в лемме 2 в качестве $\mathscr{P}$ следует взять все одномерные подпространства пространства L. Для них, очевидно, выполняются оба условия (a) и (b), причем функция выбора, в отличие от общего случая, произвольным образом выбирает из каждого одномерного подпространства ℓ ненулевой элемент $\mathbf{a}_\ell \in \ell$. Множество всех одномерных подпространств теперь образует некоммутативную (ассоциативную) *проективную геометрию* размерности $\dim L - 1$. Такая проективная геометрия плоскости рассматривалась еще Д. Гильбертом, см. [12]. § 26.

Так как мощность $|\mathscr{P}| = (\dim L)|F|$, то из леммы 2 (и предложения 2) следует, что для любого индексного множества I, мощности $|I| \geqslant |F|$, в пространстве F_0^I существуют линейные совершенные коды. Их полная классификация дается следующей теоремой:

Теорема 3. *В предположении аксиомы выбора, если* $\dim L_1 = \dim L_2$*, то совершенные линейные коды* $C_1 \subset F_0^{I_1}$, $C_2 \subset F_0^{I_2}$ *линейно эквивалентны. Если же* $\dim L_1 \neq \dim L_2$*, то коды* C_1 *и* C_2 *не эквивалентны.*

Доказательство. В наборе $\{\mathbf{a}^{(1)}_{\psi_1(i)}\}_{i\in I_1}$ собраны представители всех одномерных подпространств пространства L_1. Некоторая линейно независимая часть этого набора составляет базис Гамеля пространства L_1. Пусть для подмножества $J_1 \subset I_1$ поднабор $\{\mathbf{a}^{(1)}_{\psi_1(i)}\}_{i\in J_1}$ является базисом Гамеля в L_1 и для другого подмножества $J_2 \subset I_2$ поднабор $\{\mathbf{a}^{(2)}_{\psi_2(i)}\}_{i\in J_2}$ является базисом Гамеля в I_2. Из равенства размерностей $\dim L_1 = \dim L_2$ следует существование взаимно однозначного отображения $\varphi : J_1 \to J_2$. Полагаем $B(\mathbf{a}^{(1)}_{\psi_1(i)}) = \mathbf{a}^{(2)}_{\psi_2(\varphi(i))}$. По линейности отображение B однозначно продолжается до линейного (слева) изоморфизма L_1 и L_2, которое будем обозначать той же буквой B. Так как для любого $i \in I_1$ существует $\ell \in \mathscr{P}_2$, для которого $B(\mathbf{a}^{(1)}_{\psi_1(i)}) \in \ell$, т. е. $B(\mathbf{a}^{(1)}_{\psi_1(i)}) = \alpha_i \mathbf{a}^{(2)}_{\psi_2(\pi(i))}$ при некоторых $\pi(i) \in I_2$, $\alpha_i \in F^*$. Пусть теперь $\mathbf{x} = (x_i)_{i\in I_1} \in C_1$ и $\sum_{i\in I_1} x_i \mathbf{a}^{(1)}_{\psi_1(i)} = \mathbf{0}$. Тогда

$$B\left(\sum_{i\in I_1} x_i \mathbf{a}^{(1)}_{\psi_1(i)}\right) = \sum_{i\in I_1} x_i\alpha_i \mathbf{a}^{(2)}_{\psi_2(\pi(i))} = \sum_{k\in I_2} x_{\pi^{-1}(k)}\alpha_{\pi^{-1}(k)} \mathbf{a}^{(2)}_{\psi_2(k)} = \mathbf{0}.$$

Следовательно, $\mathbf{x} = (x_i)_{i\in I_1} \in C_1 \iff \mathbf{y} = (x_{\pi^{-1}(k)}\alpha_{\pi^{-1}(k)})_{k\in I_2} \in C_2$. Полагая $A(\mathbf{x}) = \sum\limits_{i\in I_1} x_i\alpha_i \mathbf{e}_{\pi(i)}$ для всех $\mathbf{x} = (x_i)_{i\in I_1} \in F_0^{I_1}$ получаем требуемый линейный изоморфизм кодов C_1 и C_2. Отсюда, в частности, следует равенство мощностей индексных множеств $|I_1| = |I_2|$.

Допусти $\dim L_1 \neq \dim L_2$. Можно считать, без ограничения общности, что $\dim L_1 > \dim L_2$. Если, при этом, $|I_1| \neq |I_2|$ то сразу можно сказать, что коды C_1 и C_2 не эквивалентны. Поэтому считаем, что $|I_1| = |I_2|$. Рассмотрим в теореме 1 для кода C_1 поднабор $\{\mathbf{a}^{(1)}_{\psi_1(i)}\}_{i\in J_1}$ ($J_1 \subset I_1$) являющийся базисом Гамеля в L_1. В частности, если носитель ненулевого вектора $\mathbf{x} = (x_i)_{i\in I_1} \in F_0^{I_1}$ лежит в J_1, то $\sum_{i\in I_1} x_i \mathbf{a}^{(1)}_{\psi_1(i)} \neq \mathbf{0}$. Это значит, что для кода C_1 существует подмножество индексов $J_1 \subset I_1$ мощности $|J_1| = \dim L_1$ такое, что носитель любого ненулевого вектора из C_1 не лежит в J_1. Для кода C_2 это свойство не выполнено. Для любого подмножества $J \subset I_2$ мощности $\dim L_1$ поднабор $\{\mathbf{a}^{(2)}_{\psi_2(i)}\}_{i\in J}$ линейно зависим. Поэтому для некоторого ненулевого финитного вектора $\mathbf{x} = (x_i)_{i\in I_2}$ выполняется $\sum_{i\in I_2} x_i \mathbf{a}^{(2)}_{\psi_2(i)} = \sum_{i\in J} x_i \mathbf{a}^{(2)}_{\psi_2(i)} = \mathbf{0}$. Мы нашли ненулевой вектор $\mathbf{x} \in C_2$ с носителем, лежащим в J. Это свойство показывает, что коды C_1 и C_2 не могут быть эквивалентными. Теорема полностью доказана.

Предложение 3. *Линейный (слева) совершенный код $\mathscr{H}^{(\alpha)}_F$ над ассоциативным телом F является одновременно линейным справа тогда и только тогда, когда тело F коммутативно, т. е когда F является полем.*

Доказательство этого предложения полностью аналогично доказательству предложения 1.

Возникает также вопрос об эквмвалентности (для данного ординала α) линейных слева кодов Хэмминга $\mathscr{H}^{(\alpha)}_F$ и линейных справа кодов Хэмминга ${}_F H^{(\alpha)}$. В общем виде этот вопрос не решен, но для совершенных кодов над телом кватернионов $\mathbb{H}$ можно дать полный ответ.

Предложение 4. *Для любого ординала α, линейный слева код Хэмминга $\mathscr{H}^{(\alpha)}_{\mathbb{H}}$ изоморфен (нелинейно) линейному справа коду Хэмминга ${}_{\mathbb{H}}\mathscr{H}^{(\alpha)}$.*

Доказательство. В теле кватернионов есть операция сопряжения со свойствами "антилинейности" $\overline{ab} = \overline{b}\,\overline{a}$, $\overline{a+b} = \overline{a} + \overline{b}$ ($a, b \in \mathbb{H}$). Поэтому сопряженный код Хэмминга $\overline{\mathscr{H}^{(\alpha)}_{\mathbb{H}}} = \{\overline{\mathbf{x}} : \mathbf{x} \in \mathscr{H}^{(\alpha)}_{\mathbb{H}}\}$ является линейным справа совершенным кодом, который, по теореме 3, эквивалентен (линейно справа) коду Хэмминга ${}_{\mathbb{H}}\mathscr{H}^{(\alpha)}$. Так как операция сопряжения является перестановкой ненулевых элементов тела $\mathbb{H}$, то коды $\mathscr{H}^{(\alpha)}_{\mathbb{H}}$ и $\overline{\mathscr{H}^{(\alpha)}_{\mathbb{H}}}$ изоморфны (в частности, эквивалентны). Поэтому коды $\mathscr{H}^{(\alpha)}_{\mathbb{H}}$ и ${}_{\mathbb{H}}\mathscr{H}^{(\alpha)}$ тоже изоморфны (и эквивалентны). Предложение доказано.

Список литературы

[1] Конвей Д. Х., Смит Д. А. *О кватернионах и октавах.* М: МЦНМО. 2019.

[2] Cohn. *Skew Field Constructions.* Lecture Note Series 27. Cambridge, 1977.

[3] Cohn. *Skew Fields.* Cambridge Univ. Press, 1995.

[4] Malyugin S. A. *Linear perfect codes of infinite length over infinite fields* // Сибирские электронные математические известия. 2020, Т.17, С. 1165–1182.

[5] Малюгин С. А. *Систематические и несистематические совершенные коды бесконечной длины над конечными полями* // Сибирские электронные математические известия. 2019, Т.16, С. 1732–1751.

[6] Ильиных А. П. *Квазитела, ассоциированные аддитивной группы конечного поля* // Труды ИММ УрО РАН, 2007, том 13, № 1, С. 99–101.

[7] Albert A. A. *Quasigroups I* // Trans. Amer. Math. Soc. 54 (1943). P. 507–519.

[8] Курош А. Г. *Лекции по общей алгебре.* М: Наука, 1973.

[9] Zassenhaus H. *Über endliche Fastkörper* // Abh. Math. Semin. Univ. Hambg. 1935. vol. 11, no. 1, 187–220.

[10] Levchuk V.M., Kravtsova O.V. *Problems on structure of finite quasifields and projective translation planes* // Lobachevskii J. Math. 2017. Vol. 38, No. 4, 688–698.

[11] Кравцова О.В., Левчук В.М. *Вопросы строения конечных почти-полей* // Труды Института математики и механики УрО РАН. 2019. Т. 25, № 4, 107–117.

[12] Гильберт Д. *Основания геометрии.* М: ГИТТЛ, 1948.