О.В. Маркова

Конспект спецкурса “Алгебраические основы теории кодов и линейных рекуррентных последовательностей”

Версия от *25 февраля 2026г.*

Содержание

Лекция 1. Основные параметры кодов: размерность, расстояние Хэмминга, исправление ошибок. Линейные коды. Граница Синглтона. МДР-коды, их свойства. Граница Хэмминга (граница сферической упаковки). Совершенные коды. Двоичный код Хэмминга. Граница Плоткина. Эквидистантные коды. Симплексный код.

Под *кольцом* в нашем курсе будет пониматься конечное ассоциативное, коммутативное кольцо с единицей, т.е. конечное множество $(\mathcal{R}, +, \cdot)$ с двумя бинарными операциями (для удобства их называют сложением и умножением), удовлетворяющими следующим аксиомам:
1) $(\mathcal{R}, +)$ — абелева группа с нейтральным элементом 0 (аддитивная группа кольца);
2) выполнены тождества *дистрибутивности*:

$$\forall a, b, c \in \mathcal{R}, \quad a(b+c) = ab + ac, \quad (a+b)c = ac + bc;$$

3) $(\mathcal{R}, \cdot)$ — полугруппа, т.е. операция $\cdot$ ассоциативна;
4) в $\mathcal{R}$ имеется нейтральный относительно умножения элемент 1 (или e, или 1_R, когда приходится говорить одновременно о разных кольцах);
5) $\forall a, b, c \in \mathcal{R}, \quad ab = ba$, т.е. операция $\cdot$ коммутативна.

Определение 1.1. *Правым модулем* над кольцом $\mathcal{R}$, или правым $\mathcal{R}$-модулем, называется абелева группа $(M, +)$ с определёнными на ней операциями умножения справа на элементы кольца $\mathcal{R}$, которые удовлетворяют тождествам

$$a(rs) = (ar)s, \ (a+b)r = ar + br, \ a(r+s) = ar + as, a \cdot 1 = a$$

для всех $a, b \in M, \ r, s \in \mathcal{R}$.

Аналогично можно определить левый $\mathcal{R}$-модуль.

Определение 1.2. *Подмодуль* произвольного модуля M — это его подмножество, содержащее 0 и замкнутое относительно операций сложения, взятия противоположного элемента и умножения на элементы кольца.

Определение 1.3. Внешняя *прямая сумма* $M_1 \oplus \ldots \oplus M_n$ $\mathcal{R}$-модулей $M_1, \ldots, M_n$ — множество всех строк $(m_1, \ldots, m_n)$, где $m_i \in$

M_i $\forall i \in \{1, \ldots, n\}$, с покомпонентными сложением и умножением на элементы кольца $\mathcal{R}$.
В частности, если $M_1 = \ldots = M_n = M$ мы будем рассматривать $\mathcal{R}$ модуль M^n строк длины n.

Определение 1.4. Отображение $f : M \to N$ правых модулей над кольцом $\mathcal{R}$ называется *гомоморфизмом*, если

$$\forall a, b \in M,\ r \in \mathcal{R},\ f(a+b) = f(a) + f(b),\ f(ar) = f(a)r.$$

Гомоморфизм модулей называется *изоморфизмом*, если он является биективным отбражением. Изоморфизм модуля в себя называется *автоморфзмом*.

1°. Основные параметры кодов: размерность, расстояние Хэмминга, исправление ошибок. Линейные коды.

Определение 1.5. Пусть Ω — некоторое конечное множество, $|\Omega| > 1$, — *алфавит*. Пусть n — натуральное число, Ω^n — декартова степень множества Ω. Элементы множества Ω^n будем называть *словами длины* n в алфавите Ω.

Определение 1.6. *Расстоянием Хэмминга* между словами $\mathbf{a} = (a_1, \ldots, a_n)$ и $\mathbf{b} = (b_1, \ldots, b_n)$ из Ω^n назовём число

$$d(\mathbf{a}, \mathbf{b}) = |\{i : 1 \le i \le n \ \&\ a_i \ne b_i\}|.$$

Нетрудно проверить, что (Ω^n, d) — метрическое пространство, которое и называется *пространством Хэмминга*.

Определение 1.7. Произвольное непустое подмножество $\mathcal{C}$ пространства Ω^n называется *кодом длины* n над алфавитом Ω.

Определение 1.8. *Размерностью* (более точно, *комбинаторной размерностью*) кода $\mathcal{C}$ называется действительное число $\dim(\mathcal{C}) = \log_q |\mathcal{C}|$, где $q = |\Omega|$.

Определение 1.9. *Расстоянием* (точнее, *минимальным расстоянием*) кода $\mathcal{C}$ при $|\mathcal{C}| > 1$ называется число

$$d(\mathcal{C}) = \min\{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathcal{C}\ \&\ \mathbf{a} \ne \mathbf{b}\},$$

расстояние кода из одного слова можно считать равным 0.

Если код $\mathcal{C}$ над алфавитом мощности q имеет длину n, размерность k и расстояние d, говорят, что $\mathcal{C}$ есть $[n,k,d]_q$-код. Некоторые из этих параметров можем опускать, если они неизвестны или несущественны.

Передачу информации по каналу связи можно описать следующим образом:

$$\text{слово } w \xrightarrow{\text{канал связи}} \text{слово } w' .$$

Если $w' \neq w$, говорят, что при передаче данных произошла ошибка. В простейшем случае можно считать, что искажения любых двух символов — равновероятные независимые события. Желательно, чтобы приёмник мог обнаруживать и, по возможности, исправлять слово w', получая исходное слово w.

Для этого применяют процесс кодирования/декодирования, который можно описать так.

Пусть M — известное множество входных слов (как правило, $M = \Omega^k$ для некоторого натурального числа k). Выбирается некоторое инъективное отображение (кодирование) $\varphi : M \to \Omega^n$, где $\mathcal{C} = \varphi(M)$ — некоторый известный код. Допустим, надо передать слово m. Вместо него по каналу связи передаётся слово $w = \varphi(m)$ и полученное слово w' проверяется на принадлежность коду $\mathcal{C}$. Если $w' \in \mathcal{C}$, считается, что передано (однозначно определённое) слово $\varphi^{-1}(w')$. Если же $w' \notin \mathcal{C}$, выбирается ближайшее (в смысле Хэмминга) к w' слово $w'' \in \mathcal{C}$. Если такое слово определено однозначно, предполагается, что передано слово $\varphi^{-1}(w'')$ (*принцип максимального правдоподобия*). Если же на минимальном расстоянии от слова w' находится несколько слов, принадлежащих коду $\mathcal{C}$, то фиксируется ошибка, которую невозможно исправить.

Теорема 1.10. Пусть d — расстояние Хэмминга кода $\mathcal{C}$, $2r < d$ и $s < d$. Тогда код $\mathcal{C}$ обнаруживает s ошибок и исправляет r ошибок.

◀ Очевидно, что если $m \in M$, $d(w', \varphi(m)) = s < d(\mathcal{C})$ и $w' \in \mathcal{C}$, то $w' = \varphi(m)$. Заметим, что для любого слова $a \in \Omega^n$ существует не более одного слова $c \in \mathcal{C}$, для которого выполнено неравенство $d(a,c) \leq r$. Действительно, пусть $c_1, c_2 \in C$, $d(a,c_1) \leq r$ и $d(a,c_2) \leq r$. Тогда $d(c_1,c_2) \leq d(c_1,a) + d(a,c_2) \leq 2r < d$, откуда $c_1 = c_2$. Поскольку, по предположению, $d(w', \varphi(m)) = r$ и $\varphi(m) \in \mathcal{C}$, получаем, что $w'' = \varphi(m)$ и $\varphi^{-1}(w'') = m$. ▶

Примеры.
1. Повторение слова. Если любое слово $w = (w_1, \ldots, w_k)$ кодировать словом $(w|w) = (w_1, \ldots, w_k, w_1, \ldots, w_k)$, то получается $[2k, k, 2]$-код. Видно, что он обнаруживает одну ошибку и ни одной не исправляет, а объём передаваемой информации увеличивается вдвое.
2. Код проверки на чётность. Пусть на множестве Ω задана групповая операция "+" (не обязательно коммутативная). Тогда слово $w = (w_1, \ldots, w_k)$ можно кодировать словом $(w_1, \ldots, w_k, -(w_k + \ldots + w_1))$. Тогда получится $[k+1, k, 2]$-код, но скорость передачи информации (т.е. отношение k/n) у кода проверки на чётность выше, чем у кода удвоения.

Определение 1.11. Пусть M — конечный правый или левый модуль над кольцом $\mathcal{R}$, $|M| \geq 2$. *Линейным кодом длины* n над модулем M называется произвольный подмодуль $\mathcal{R}$-модуля M^n.

Основные частные случаи:
$M = \mathcal{R}_{\mathcal{R}}$ или $M = {}_{\mathcal{R}}\mathcal{R}$ — говорят о коде над кольцом $\mathcal{R}$.
$M = \mathcal{R}$, где $\mathcal{R} = \mathbb{F}$, $\mathbb{F}$ — конечное поле. В этом случае говорят о линейных кодах над полем $\mathbb{F}$.

Примеры. Почти все коды, которые мы построим в данной лекции — линейные коды над полем (двоичный код Хэмминга, обобщённый код Рида–Соломона, симплексный код).

Определение 1.12. Пусть M — конечный модуль. Назовём *весом* слова $\mathbf{a} = (a_1, \ldots, a_n) \in M^n$ число

$$||\mathbf{a}|| = |\{i : 1 \leq i \leq n \ \&\ a_i \neq 0\}|.$$

Очевидны следующие соотношения:
1) $\forall \mathbf{a}, \mathbf{b} \in M^n : d(\mathbf{a}, \mathbf{b}) = ||\mathbf{a} - \mathbf{b}||$;
2) $\forall \mathcal{C} \leq M^n : d(\mathcal{C}) = \min\{||\mathbf{a}|| : \mathbf{a} \in \mathcal{C} \setminus \{0\}\}$.

2°. Граница Синглтона. МДР-коды, их свойства.

Теорема 1.13 (Граница Синглтона)**.** Если $\mathcal{C}$ есть $[n, k, d]$-код, то

$$d \leq n - k + 1. \tag{1.1}$$

◀ Пусть $m = |\mathcal{C}|$. Перенумеруем все слова кода $\mathcal{C}$: $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$, $1 \leq i \leq m$. Составим из них матрицу, в которой выделим первые $d-1$ столбцов:

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} = \left(\begin{array}{ccc|ccc} a_{11} & \ldots & a_{1,d-1} & a_{1d} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{m,d-1} & a_{md} & \ldots & a_{mn} \end{array}\right)$$

Поскольку $d(\mathcal{C}) = d$, то в выделенной группе последних $n - d + 1$ столбцов этой матрицы любые две строки различны. Следовательно, количество кодовых слов не превосходит количества различных строк длины $n - d + 1$ в алфавите Ω, т.е. $m \leq q^{n-d+1}$, где $q = |\Omega|$. Логарифмируя по основанию q, получаем требуемую оценку.►

Определение 1.14. Код $\mathcal{C}$ называется *кодом с максимально достижимым расстоянием*, или *МДР-кодом*, если $\mathcal{C}$ есть $[n, k, n - k + 1]$-код, т.е. неравенство (1.1) обращается в равенство.

Тривиальными примерами МДР-кодов являются:
— $[n, n, 1]$-код Ω^n;
— $[n, 1, n]$-код констант $\mathcal{C} = \{(a, \ldots, a) \in \Omega^n\}$;
— $[n, n - 1, 2]$-код проверки на чётность.

Пример. Пусть $\mathbb{F}$ — конечное поле, $q = |\mathbb{F}|$, $M = \mathbb{F}[x|k] = \{f(x) \in \mathbb{F}[x] : \deg f(x) < k\}$, $x_1, \ldots, x_n$ — различные элементы поля $\mathbb{F}$, где $n \geq k$. $u_1, \ldots, u_n$ — обратимые элементы $\mathbb{F}$, отображение $\varphi : \mathbb{F}[x|k] \to \mathbb{F}^n$ задано правилом

$$\varphi(f(x)) = (u_1 f(x_1), \ldots, u_n f(x_n)).$$

Образ $\varphi(\mathbb{F}[x|k])$ называется *обобщённым* $[n, k]$-*кодом Рида–Соломона* над полем $\mathbb{F}$ и даёт менее тривиальный пример МДР-кода.

Предложение 1.15. Обобщённый $[n, k]$-код Рида–Соломона является МДР-кодом.

◄ Если $f(x) \in \mathbb{F}[x|k]$ и $f(x) \neq 0$, то по теореме Безу число корней многочлена $f(x)$ среди $x_1, \ldots, x_n$, равное $n - d(\varphi(f(x)), 0)$, удовлетворяет также неравенству $n - d(\varphi(f(x)), 0) \leq \deg(f(x)) < k$, откуда $d(\varphi(f(x)), 0) > n - k$. Во-первых, отсюда видно, что $\ker \varphi = 0$, поэтому $\dim\ \varphi(\mathbb{F}[x|k]) = \dim\ \mathbb{F}[x|k] = k$. Во-вторых, беря в качестве $f(x)$ разность любых различных многочленов из $\mathbb{F}[x|k]$, убеждаемся, что расстояние d данного кода также удовлетворяет неравенству $d > n - k$, что, в силу границы Синглтона, возможно лишь при $d = n - k + 1$. ►

3°. Граница Хэмминга (граница сферической упаковки). Совершенные коды. Двоичный код Хэмминга.

Теорема 1.16 (Граница Хэмминга, или граница сферической упаковки)**.** Пусть $\mathcal{C}$ есть $[n,k,d]_q$-код над алфавитом Ω и $d > 2r$. Тогда

$$q^k \le \frac{q^n}{s_q(n,r)}, \text{ где } s_q(n,r) = \sum_{i=0}^{r} (q-1)^i \binom{n}{i}. \tag{1.2}$$

◀ Нетрудно видеть, что i-е слагаемое в $s_q(n,r)$ — число точек пространства Ω^n, лежащих на расстоянии i от произвольной фиксированной точки $\mathbf{a}$ этого пространства, поэтому $s_q(n,r) = |O_r(\mathbf{a})|$, где

$$O_r(\mathbf{a}) = \{\mathbf{b} \in \Omega^n : d(\mathbf{a},\mathbf{b}) \le r\}.$$

В силу неравенства треугольника $O_r(\mathbf{a}) \cap O_r(\mathbf{a}') = \varnothing$ при $\mathbf{a}, \mathbf{a}' \in \mathcal{C}$ и $\mathbf{a} \ne \mathbf{a}'$, следовательно,

$$q^k s_q(n,r) = |\mathcal{C}| s_q(n,r) = \left| \bigcup_{\mathbf{a}\in\mathcal{C}} O_r(\mathbf{a}) \right| \le |\Omega^n| = q^n.$$

▶

Определение 1.17. Код $\mathcal{C}$ называется *совершенным*, если неравенство в (1.2) обращается в равенство (при этом обязательно $d = 2r+1$).

Пример. Двоичный код Хэмминга $\mathcal{H}_2(l)$ длины $n = 2^l - 1$ — множество слов $a \in \mathbb{Z}_2^n$, удовлетворяющих условию $Ha^T = 0$, где H — матрица, столбцы которой — все ненулевые столбцы длины l над $\mathbb{Z}_2$.

Предложение 1.18. Двоичный код Хэмминга $\mathcal{H}_2(l)$ является линейным $[n, n-l, 3]_2$ совершенным кодом.

◀ Линейность очевидна по построению. Поскольку матрица H содержит все ненулевые столбцы высоты l, то $\mathrm{rk} H = l$, откуда $\dim \mathcal{H}_2(l) = n - l$.

Так как матрица H не содержит нулевого столбца и любые два её столбца различны, то никакое ненулевое слово веса ≤ 2 не удовлетворяет условию $Ha^T = 0$, значит, $d(\mathcal{H}_2(l)) \ge 3$. С другой стороны, матрица H содержит столбцы $\mathbf{e}_1^T$, $\mathbf{e}_2^T$, $\mathbf{e}_1^T + \mathbf{e}_2^T$ (здесь $\mathbf{e}_s^T = (0,\dots,0,1,0,\dots,0)^T$ — столбец с единицей на s-ом месте), поэтому код $\mathcal{H}_2(l)$ содержит слово веса 3 и $d(\mathcal{H}_2(l)) = 3$.

В равенстве (1.2) для $d = 3$ имеем $r = 1$, $k = n - l$, $s_2(n,1) = \sum\limits_{i=0}^{1} (2-1)^i \binom{n}{i} = 1 + n = 1 + (2^l - 1) = 2^l$, поэтому $2^{n-l} = \dfrac{2^n}{s_2(n,1)}$ и

код $\mathcal{H}_2(l)$ является совершенным. ►

4°. Граница Плоткина. Эквидистантные коды. Симплексный код.

Теорема 1.19 (Граница Плоткина)**.** Пусть $\mathcal{C}$ есть $[n,k,d]_q$-код. Тогда

$$d \le \frac{nq^{k-1}(q-1)}{q^k-1} = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n \tag{1.3}$$

◄ Пусть $\mathcal{C} \subseteq \Omega^n$, где $|\Omega| = \{\omega_1,\dots,\omega_q\}$, $M = |\mathcal{C}|$. Обозначим через π_i проекцию Ω^n на i-ю координату (т.е. $\pi_i((a_1,\dots,a_n)) = a_i$ при $i = 1,\dots,n$) и положим

$$m_{ij} = |\{\mathbf{a} \in \mathcal{C} : \pi_i(\mathbf{a}) = \omega_j\}| = \sum_{\mathbf{a}\in M} \delta_{\pi_i(a),\omega_j}.$$

По определению, для любой пары $\mathbf{a},\mathbf{b} \in \mathcal{C}$ при $\mathbf{a} \ne \mathbf{b}$ имеем $d \le d(\mathbf{a},\mathbf{b})$. Суммируя по всем парам, получим

$$M(M-1)d \le \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}} d(\mathbf{a},\mathbf{b}). \tag{1.4}$$

С другой стороны, $d(\mathbf{a},\mathbf{b}) = \sum_{i=1}^n \left(1 - \delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})}\right)$. Таким образом, правую часть неравенства (1.4) можно переписать в виде

$$\sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}}\sum_{i=1}^n (1-\delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})}) = nM^2 - \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}}\sum_{i=1}^n \delta_{\pi_i(\mathbf{a}),\pi_i(\mathbf{b})} =$$

$$= nM^2 - \sum_{i=1}^n \sum_{\mathbf{a},\mathbf{b}\in\mathcal{C}} \sum_{\omega\in\Omega} \delta_{\pi_i(\mathbf{a}),\omega}\delta_{\pi_i(\mathbf{b}),\omega} = nM^2 - \sum_{i=1}^n\sum_{j=1}^q m_{ij}^2.$$

Теперь применим неравенство Коши–Буняковского к векторам $(1,1,\dots,1)$ и $(m_{i1},m_{i2},\dots,m_{iq})$:

$$\left(\sum_{j=1}^q m_{ij}\right)^2 \le q\sum_{j=1}^q m_{ij}^2.$$

При каждом $i = 1,\dots,n$, $\sum_{j=1}^q m_{ij} = M$, поэтому

$$M(M-1)d \le nM^2 - n/qM^2 = nM^2\frac{q-1}{q}.$$

►
Если неравенство (1.3) обращается в равенство, говорят, что код лежит на границе Плоткина. Как видно из доказательства теоремы 1.19, необходимым (но не достаточным!) условием этого является эквидистантность кода в смысле следующего определения.

Определение 1.20. Код $\mathcal{C}$ называется *эквидистантным*, если все расстояния между различными словами кода $\mathcal{C}$ одинаковы.

Очевидным примером эквидистантного кода является уже упомянутый код констант. Более сложно устроен следующий

Пример. Пусть $\mathbb{F}$ — конечное поле, $|\mathbb{F}| = q$, V — линейное пространство над $\mathbb{F}$, $k = \dim_{\mathbb{F}} V$. Положим $n = q^k - 1$ и как-нибудь занумеруем ненулевые векторы пространства V:

$$V \setminus \{0\} = \{v_1, \ldots, v_n\}.$$

Рассмотрим далее сопряжённое пространство V^*, состоящее из линейных функций $V \to \mathbb{F}$ и составим код

$$\mathcal{C} = S_P(k) = \{(f(v_1), \ldots, f(v_n)) : f \in V^*\}.$$

Ясно, что $|\mathcal{C}| = |V^*| = |V| = q^k$, а $d(\mathcal{C}) = n - (q^{k-1} - 1) = q^k - q^{k-1}$, так как ядро любой ненулевой линейной функции — подпространство размерности $k-1$ пространства V. Таким образом, вычисляя правую часть (1.3), имеем

$$\frac{nq^{k-1}(q-1)}{q^k - 1} = q^{k-1}(q-1) = d(\mathcal{C}).$$

Задачи к лекции 1.

Задача 1. Пусть $\mathcal{C}$ есть $[n, k, d]$-код над алфавитом Ω и $d > 2r$, причём $q^k = \dfrac{q^n}{s_q(n, r)}$ (см. (1.2)). Покажите, что $d = 2r + 1$.

Задача 2. Опишите совершенные МДР-коды.

Задача 3. Опишите эквидистантные МДР-коды.

Задача 4. Приведите пример эквидистантного кода, для которого неравенство (1.3) является строгим.

Задача 5. Для кода $\mathcal{C} = \{(a, b, a+b) | a, b \in \mathbb{Z}_m\}$ найдите размерность k и минимальное расстояние d для общего m. При каких m код $\mathcal{C}$ является МДР-кодом?

Задача 6. Исследуйте существование линейных МДР-кодов длины $n = 4$, размерности $k = 2$ над кольцом $\mathbb{Z}_4$.

Лекция 2. Изометрические преобразования пространства Хэмминга. Теорема А.А. Маркова.

1°. Общий случай.

Определение 2.1. Пусть Ω — алфавит, $n \in \mathbb{N}$. Биективное отображение $\varphi : \Omega^n \to \Omega^n$ называется *изометрией*, если

$$d(\varphi(\mathbf{a}), \varphi(\mathbf{b})) = d(\mathbf{a}, \mathbf{b})$$

для любых слов $\mathbf{a}, \mathbf{b} \in \Omega^n$ (иначе говоря, если φ сохраняет расстояние Хэмминга).

Определение 2.2. Если $\Omega = M$ — модуль над кольцом $\mathcal{R}$, то изометрия $\varphi : \Omega^n \to \Omega^n$ называется *линейной изометрией*, если $\varphi : \Omega^n \to \Omega^n$ — гомоморфизм $\mathcal{R}$-модулей.

Заметим, что изометрии $\mathfrak{S}(\Omega^n)$ составляют подгруппу группы S_{Ω^n} всех биективных преобразований множества Ω^n в себя.

Изометрии пространства Хэмминга устроены очень просто, как показывает следующая

Теорема 2.3 (А.А. Марков, 1956 г.)**.** Биекция $\varphi : \Omega^n \to \Omega^n$ является изометрией тогда и только тогда, когда φ задаётся следующим правилом:

$$\forall \mathbf{a} = (a_1, \ldots, a_n) \in \Omega^n, \quad \varphi(\mathbf{a}) = (\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)})), \qquad (2.1)$$

где $\sigma \in S_n$, $\pi_i \in S_\Omega$, $i = 1, \ldots, n$, а S_Ω обозначает группу всех биективных отображений множества Ω в себя.

◀ Преобразования, заданные правилом (2.1), называются *мономиальными*. Очевидно, что мономиальное преобразование является изометрией.

1. Отметим, что мономиальные преобразования $\mathcal{M}(\Omega^n)$ образуют подгруппу группы $\mathfrak{S}(\Omega^n)$. Действительно, очевидно, что тождественное отображение мономиально. Если $\phi, \psi \in \mathcal{M}(\Omega^n)$ и $\phi(\mathbf{a}) = (\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)}))$, $\psi(\mathbf{a}) = (\rho_1(a_{\tau(1)}), \ldots, \rho_n(a_{\tau(n)}))$, то

$$\psi\phi(\mathbf{a}) = \psi(\pi_1(a_{\sigma(1)}), \ldots, \pi_n(a_{\sigma(n)})) = \\ = (\rho_1(\pi_{\tau(1)}(a_{\sigma\tau(1)})), \ldots, \rho_n(\pi_{\tau(n)}(a_{\sigma\tau(n)}))),$$

также является мономиальным преобразованием. Отсюда также следует мономиальность обратного к мономиальному отображению: $\phi^{-1}(\mathbf{a}) = (\pi^{-1}_{\sigma^{-1}(1)}(a_{\sigma^{-1}(1)}), \ldots, \pi^{-1}_{\sigma^{-1}(n)}(a_{\sigma^{-1}(n)}))$.

2. Пусть $\varphi \in \mathfrak{S}(\Omega^n)$ — произвольная изометрия. В силу сказанного выше для того, чтобы доказать мономиальность φ, достаточно доказать мономиальность преобразования вида $\eta_1\varphi\eta_2$, где $\eta_1, \eta_2 \in \mathcal{M}(\Omega^n)$. Это позволит нам далее, не ограничивая общности считать, что φ обладает каким-то требуемым свойством, добившись того, чтобы $\eta_1\varphi\eta_2$ им обладало.

3. Переобозначив буквы алфавита, будем считать, что $\Omega = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Положим $\mathbf{0} = (0, \ldots, 0)$.

Можно считать, что $\varphi(\mathbf{0}) = \mathbf{0}$. Действительно, если $\varphi(\mathbf{0}) = (c_1, \ldots, c_n)$ для тех $i = 1, \ldots, n$, что $c_i \neq 0$ возьмём в качестве $\nu_i \in S_\Omega$ транспозицию $(0, c_i)$, для оставшихся i положим $\nu_i = id$. Взяв мономиальное преобразование η_1, соответствующие подстановкам $\nu_i \in S_\Omega$ и тождественной $\sigma \in S_n$, получаем, что $\eta_1\varphi(\mathbf{0}) = \mathbf{0}$.

4. Как и в линейном случае, обозначим за $||\mathbf{a}||$ число ненулевых координат слова $\mathbf{a} \in \Omega^n$. Имеем

$$||\varphi(\mathbf{a})|| = d(\varphi(\mathbf{a}), \mathbf{0}) = d(\varphi(\mathbf{a}), \varphi(\mathbf{0})) = d(\mathbf{a}, \mathbf{0}) = ||\mathbf{a}||.$$

5. В частности, для $\mathbf{e}_s = (0, \ldots, 0, 1, 0, \ldots, 0)$ с единицей на s-ом месте, $s = 1, \ldots, n$, из $||\mathbf{e}_s|| = 1$ получаем, что $||\varphi(\mathbf{e}_s)|| = 1$, откуда

$$\varphi(\mathbf{e}_s) = u_s\mathbf{e}_{\omega(s)},$$

где $u\mathbf{e}_i$ обозначает слово с u на i-ом месте и нулями на остальных, $u_s \in \Omega \setminus \{0\}$, $\omega : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Покажем, что $\omega \in S_n$. Пусть $p, q \in \{1, \ldots, n\}, p \neq q$. Тогда $d(\mathbf{e}_p, \mathbf{e}_q) = 2$, откуда $d(u_p\mathbf{e}_{\omega(p)}, u_q\mathbf{e}_{\omega(q)}) = 2$. Следовательно, $\omega(p) \neq \omega(q)$, т.е. ω — инъективное отображение, поэтому $\omega \in S_n$. Для $u_s \neq 1$ взяв транспозиции $\tau_s = (1, u_s) \in S_\Omega$, для оставшихся s положив $\tau_s = id$ и определяя мономиальное преобразование η_2, соответствующее подстановкам $\tau_s \in S_\Omega$ и тождественной $\sigma \in S_n$, и домножив φ на η_2, получаем, что

$$\varphi(\mathbf{e}_s) = \mathbf{e}_{\omega(s)},\ \omega \in S_n.$$

6. Для любого $s \in \{1, \ldots, n\}$ и любого $u \in \Omega \setminus \{0\}$ имеем

$$||\varphi(u\mathbf{e}_s)|| = ||u\mathbf{e}_s|| = 1,$$

$$d(\varphi(u\mathbf{e}_s), \mathbf{e}_{\omega(s)}) = d(u\mathbf{e}_s, \mathbf{e}_s) = 1.$$

Отсюда получаем, что

$$\varphi(u\mathbf{e}_s) = \pi_s(u)\mathbf{e}_{\omega(s)},\ \pi_s : \Omega \to \Omega, \pi_s(0) = 0, \pi_s(1) = 1.$$

При этом $\pi_s \in S_\Omega$ для каждого $s \in \{1, \ldots, n\}$. Действительно, если $u, v \in \Omega, u \neq v$, то

$$d(u\mathbf{e}_s, v\mathbf{e}_s) = 1 = d(\varphi(u\mathbf{e}_s), \varphi(v\mathbf{e}_s)) = d(\pi_s(u)\mathbf{e}_{\omega(s)}, \pi_s(v)\mathbf{e}_{\omega(s)}),$$

значит, $\pi_s(u) \neq \pi_s(v)$, т.е. π_s — инъективное отображение, поэтому $\pi_s \in S_\Omega$.

Взяв мономиальное отображение η_3, с подстановками, обратными к $\pi_{\omega^{-1}(1)}, \ldots, \pi_{\omega^{-1}(n)}$ и ω, и умножив его на φ, будем считать, что

$$\varphi(u\mathbf{e}_s) = u\mathbf{e}_s,\ \forall u \in \Omega,\ s \in \{1, \ldots, n\}.$$

7. Докажем, что $\varphi = id$ — тождественное преобразование на Ω^n. Предположим противное: пусть $\varphi(\mathbf{a}) = \mathbf{b}$, $\mathbf{b} \neq \mathbf{a}$ для некоторых $\mathbf{a}, \mathbf{b} \in \Omega^n$. При этом по доказанному в пункте 4, $||\mathbf{b}|| = ||\mathbf{a}||$. По построению $a_i \neq b_i$ для некоторого $i \in \{1, \ldots, n\}$. Имеем две возможности.

Случай $a_i = 0$. Тогда $b_i \neq 0$, откуда

$$d(\mathbf{a}, b_i\mathbf{e}_i) = ||a|| + 1 = ||b|| + 1,$$

с другой стороны,

$$d(\varphi(\mathbf{a}), \varphi(b_i\mathbf{e}_i)) = d(\mathbf{b}, b_i\mathbf{e}_i) = ||b|| - 1.$$

Противоречие с тем, что φ — изометрия.

Случай $a_i \neq 0$. Тогда

$$d(\mathbf{a}, a_i\mathbf{e}_i) = ||a|| - 1 = ||b|| - 1,$$

с другой стороны,

$$d(\varphi(\mathbf{a}), \varphi(a_i\mathbf{e}_i)) = d(\mathbf{b}, a_i\mathbf{e}_i) \geq ||b||.$$

Противоречие с тем, что φ — изометрия.

Полученные противоречия доказывают, что $\varphi = id$, поэтому мономиально.▶

2°. Линейный случай. Пусть $\Omega = M$ — модуль над кольцом $\mathcal{R}$. Линейное мономиальное преобразование — преобразование вида (2.1), для которого $\pi_s \in \mathrm{Aut}(M),\ s \in \{1, \ldots, n\}$.

Докажем линейную версию теоремы А.А.Маркова.

Теорема 2.4 (А.А.Марков)**.** Биекция $\varphi : M^n \to M^n$, где M — модуль над кольцом $\mathcal{R}$, является линейной изометрией тогда и только тогда, когда она является линейным мономиальным преобразованием.

◀ Пусть φ — линейное мономиальное преобразование вида (2.1). Тогда

$$\varphi(\mathbf{a}+\mathbf{b}) = (\pi_1(a_{\sigma(1)}+b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)}+b_{\sigma(n)})) = \\ = (\pi_1(a_{\sigma(1)})+\pi_1(b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)})+\pi_n(b_{\sigma(n)})) = \varphi(\mathbf{a})+\varphi(\mathbf{b})$$

$$\varphi(\mathbf{a}r) = (\pi_1(a_{\sigma(1)}r),\dots,\pi_n(a_{\sigma(n)}r) = \\ = (\pi_1(a_{\sigma(1)})r,\dots,\pi_n(a_{\sigma(n)})r) = \varphi(\mathbf{a})r$$

для любых $r \in \mathcal{R}, \mathbf{a}, \mathbf{b} \in M^n$. Следовательно, φ является линейной изометрией.

Обратно, пусть φ — линейная изометрия. По теореме 2.3 φ является мономиальным преобразованием.

По линейности φ для любых $r \in \mathcal{R}, \mathbf{a}, \mathbf{b} \in M^n$ имеем

$$(\pi_1(a_{\sigma(1)}+b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)}+b_{\sigma(n)})) = \varphi(\mathbf{a}+\mathbf{b}) = \\ = \varphi(\mathbf{a})+\varphi(\mathbf{b}) = (\pi_1(a_{\sigma(1)})+\pi_1(b_{\sigma(1)}),\dots,\pi_n(a_{\sigma(n)})+\pi_n(b_{\sigma(n)}))$$

откуда получаем, что $\pi_i(a+b) = \pi_i(a)+\pi_i(b)$ для любых $a, b \in M$ и $i \in \{1,\dots,n\}$.

Аналогично,

$$(\pi_1(a_{\sigma(1)}r),\dots,\pi_n(a_{\sigma(n)}r)) = \varphi(\mathbf{a}r) = \\ = \varphi(\mathbf{a})r = (\pi_1(a_{\sigma(1)})r,\dots,\pi_n(a_{\sigma(n)})r),$$

откуда получаем, что $\pi_i(ar) = \pi_i(a)r$ для любых $a \in M$, $r \in \mathcal{R}$ и $i \in \{1,\dots,n\}$.

Следовательно, $\pi_i \in \mathrm{Aut}(M)$ для всех $i \in \{1,\dots,n\}$, поэтому φ является линейным мономиальным преобразованием. ▶

Рассмотрим важный частный случай, когда $M = \mathcal{R}$, т.е. линейные коды над кольцом $\mathcal{R}$. Любой эндоморфизм π (гомоморфизм в себя) кольца $\mathcal{R}$ определяется элементом $\pi(1)$, поскольку $\pi(r) = \pi(1)r$. При этом $\pi \in \mathrm{Aut}(\mathcal{R}_{\mathcal{R}})$ тогда и только тогда, когда $\pi(1) \in \mathcal{R}^*$ — обратимый элемент кольца $\mathcal{R}$.

Следовательно, для любой линейной изометрии φ модуля $\mathcal{R}^n$ существуют элементы $u_1, \ldots, u_n \in \mathcal{R}^*$ и $\sigma \in S_n$ такие, что φ задается правилом

$$\forall \mathbf{a} \in \mathcal{R}^n : \ \varphi(\mathbf{a}) = (u_1 a_{\sigma(1)}, \ldots, u_n a_{\sigma(n)}).$$

Определение 2.5. Два (линейных) кода $\mathcal{C}_1$ и $\mathcal{C}_2$ длины n над алфавитом Ω называются (*линейно*) *эквивалентными*, если существует (линейная) изометрия $\varphi : \Omega^n \to \Omega^n$, такая, что $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Сразу заметим, что все параметры эквивалентных кодов одинаковы.

Определение 2.6. Подгруппа $\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathfrak{S}(\Omega^n) : \sigma(\mathcal{C}) = \mathcal{C}\}$ называется *группой автоморфизмов* кода $\mathcal{C}$.

Определение 2.7. Подгруппа $\mathcal{L}\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}) \cap \mathrm{Aut}(M^n)$ называется *группой линейных автоморфизмов* линейного кода $\mathcal{C}$.

Используя теорему Лагранжа и связь орбит и стабилизаторов действия, можно получить

Теорема 2.8. Число кодов $\mathcal{C}' \in \Omega^n$, эквивалентных коду $\mathcal{C} \in \Omega^n$ равно индексу $[\mathfrak{S}(\Omega^n) : \mathrm{Aut}(\mathcal{C})]$ подгруппы $\mathrm{Aut}(\mathcal{C})$ в группе $\mathfrak{S}(\Omega^n)$. Если $\mathcal{C}' = \sigma(\mathcal{C})$, $\sigma \in \mathfrak{S}(\Omega^n)$, то $\mathrm{Aut}(\mathcal{C}') = \sigma^{-1}\mathrm{Aut}(\mathcal{C})\sigma$.

Задачи к лекции 2.

Задача 1. Покажите, что группа $\mathfrak{S}(\Omega^n)$ всех изометрий пространства Ω^n — это полупрямое произведение $(S_\Omega)^n \rtimes S_n$.

Задача 2. Покажите, что для двоичного алфавита ($\Omega = \mathbb{Z}_2$) группа линейных изометрий совпадает с группой всех преобразований вида $\mathbf{x}^T \to P\mathbf{x}^T + \mathbf{v}^T$, где P— матрица перестановки координат и $\mathbf{v}^T$— фиксированный вектор-столбец.

Задача 3. Заметим, что линейная изометрия σ над конечным полем $\mathbb{F}$ — это линейный оператор на пространстве $\mathbb{F}^n$. Укажите вид матрицы этого оператора в стандартном базисе.

Задача 4. Докажите, что группа линейных изометрий действует транзитивно на множестве слов фиксированного веса m (для любого $0 \leq m \leq n$), т.е. для любых слов $\mathbf{a}, \mathbf{b}$ одинакового веса m существует изометрия σ такая, что $\sigma(\mathbf{a}) = \mathbf{b}$.

Задача 5. Найдите группу автоморфизмов простого двоичного кода $\mathcal{C} = \{(0,0,0),(1,1,1)\}$ длины 3.

Задача 6. Найдите группу автоморфизмов кода констант $\mathcal{C} = \{(a,\ldots,a) \in \Omega^n\}$ для произвольных Ω и n.

Задача 7. Найдите группу автоморфизмов двоичного кода Хэмминга $\mathcal{H}_2(l)$.

Список литературы

[1] М.М. Глухов, В.П. Елизаров, А.А. Нечаев. Алгебра, т. 1,2. Изд. “Гелиос АРВ”, М., 2003.

[2] В.Л. Куракин, А.А. Нечаев. Линейные коды и полилинейные рекурренты.

[3] Р. Лидл, Г. Нидеррайтер. Конечные поля, т. 1,2. Изд. “Мир”, М., 1988.

[4] В.Т. Марков, Конспект спецкурса “Теория колец” 2016/2017 учебного года. Тема «Кольца и модули в теории кодирования». http://halgebra.math.msu.su/wiki/doku.php/specialcourses:ringtheory

[5] А.А. Нечаев. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам// Фундаментальная и прикладная математика, 1995, Т.1, № 1, 229-254.