О.В. Маркова

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

Версия от *19 марта 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 $\mathcal{H}_2(l)$.

Лекция 3. Реальная длина кода. Теорема Мак-Вилльямс о продолжении изометрий линейных кодов.

Определение 3.1. Пусть $\mathbb{F}$ — произвольное конечное поле. Линейные коды $\mathcal{C}, \mathcal{L} \leqslant {}_{\mathbb{F}}\mathbb{F}^n$ *линейно изометричны*, если существует изоморфизм линейных пространств

$$\tau : {}_{\mathbb{F}}\mathcal{C} \to {}_{\mathbb{F}}\mathcal{L} \tag{3.1}$$

такой, что

$$d(\mathbf{a}, \mathbf{b}) = d(\tau(\mathbf{a}), \tau(\mathbf{b})) \ \forall \ \mathbf{a}, \mathbf{b} \in \mathcal{C}. \tag{3.2}$$

Определение 3.2. *Реальной длиной кода* $\mathcal{C}$ называется число

$$l(\mathcal{C}) = |\{i \in \{1, \ldots, n\} : \ \exists \mathbf{a} = (a_1, \ldots, a_n) \in \mathcal{C} \ a_i \neq 0\}|.$$

Сначала докажем вспомогательную лемму.

Код $\mathcal{C}$ в этом случае можно рассматривать как код длины $l(\mathcal{C})$, при этом $l(\mathcal{C})$ минимальное такое число.

Реальная длина кода также связана и с другими кодовыми параметрами. Докажем два утверждения о её связи с весами кодовых слов в линейном случае.

Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный код над полем $\mathbb{F}$.

Очевидно, что $d(\mathcal{C}) \leq ||\mathbf{a}|| \leq l(\mathcal{C})$ для любого слова $\mathbf{a} \in \mathcal{C} \setminus \{0\}$, т.е. минимальное кодовое расстояние и реальная длина кода служат границами весов кодовых слов. По определению минимального расстояния слово веса $d(\mathcal{C})$ в коде $\mathcal{C}$ всегда содержится. Следующее предложение показывает, когда в коде $\mathcal{C}$ есть слово веса $l(\mathcal{C})$.

Предложение 3.3. Пусть $\mathbb{F}$ — конечное поле мощности q. Тогда
1.любой линейный код $\mathcal{C} \leq \mathbb{F}^n$, имеющий реальную длину $l(\mathcal{C}) \leq q$, содержит слово веса $l(\mathcal{C})$;
2. для любого такого l, что $n \geq l > q$, среди кодов длины n и реальной длины l существуют коды, не содержащие слов веса l.

◀ Положим $l = l(\mathcal{C})$. Для простоты обозначений пусть ненулевые координаты слов из $\mathcal{C}$ расположены в позициях $1, \ldots, l$.

1. Пусть $l \leq q$. Обозначим $\mathbf{a}(i) = (a(i)_1, \ldots, a(i)_n) \in \mathcal{C}$, так что $a(i)_i \neq 0$, $i = 1, \ldots, l$.

Доказательство проведем индукцией по l.

База индукции. При $l \leq 1$ утверждение верно.

Шаг индукции. Допустим, что $l > 1$ и для $l-1$ утверждение доказано.

Это означает, что существует слово $\mathbf{a} \in \langle \mathbf{a}(i) |\ i = 1, \ldots, l-1 \rangle$ такое, что $a_k \neq 0,\ k = 1, \ldots, l-1$. Действительно, предположение индукции применимо к коду $\mathcal{C}' = \langle \tilde{\mathbf{a}}(i) |\ i = 1, \ldots, l-1 \rangle$, где $\tilde{a}(i)_m = a(i)_m$, при $m \neq l$, и $\tilde{a}(i)_l = 0$. При этом в $\mathcal{C}'$ слово $\tilde{\mathbf{a}}$ веса $l-1$ выражается как линейная комбинация $\tilde{\mathbf{a}} = \sum\limits_{j=1}^{l-1} \alpha_j \tilde{\mathbf{a}}(j)$. Тогда можно взять $\mathbf{a} = \sum\limits_{j=1}^{l-1} \alpha_j \mathbf{a}(j)$ и $a_k = \tilde{a}_k \neq 0$ при $k = 1, \ldots, l-1$.

Добавляем к рассмотрению слово $\mathbf{b} = \mathbf{a}(l)$.

Если $a_l \neq 0$, то $||\mathbf{a}|| = l$ и это требуемое слово; если $b_i \neq 0$ для всех $i = 1, \ldots, l$, то $||\mathbf{b}|| = l$ и это требуемое слово. В противном случае рассмотрим слова $\mathbf{a} + \alpha\mathbf{b},\ \alpha \in \mathbb{F},\ \alpha \neq 0$. Пусть $y_i(x) = b_i x + a_i,\ i = 1, \ldots, l-1$. При каждом i по построению $a_i \neq 0$, значит уравнение $y_i(x) = 0$ имеет в $\mathbb{F}$ не более одного решения. При этом слово $\mathbf{b}$ имеет нулевую координату в позициях $[1, l]$, значит по крайней мере одно из уравнений $y_i(x) = 0$ несовместно. Следовательно, если $X = \{x \in \mathbb{F} |\ \exists i \in \{1, \ldots, l-1\}\ y_i(x) = 0\}$, то $|X| \leq l-2$. Из условия на число элементов поля следует, что найдётся $\alpha \in \mathbb{F},\ \alpha \neq 0$, что $\alpha \notin X$, т.е. $a_i + \alpha b_i \neq 0,\ i = 1, \ldots, l$. Слово $\mathbf{a} + \alpha\mathbf{b} \in \langle \mathbf{a}(i) |\ i = 1, \ldots, l \rangle$ и есть искомое.

2. Пусть $n \geq l > q$. Рассмотрим $\mathcal{C} = \langle \mathbf{a}, \mathbf{b} \rangle \leq \mathbb{F}^n$, где $a_2 = \ldots = a_l = 1$, $a_1 = a_{l+1} = \ldots = a_n = 0$, $b_1 = 1$, $b_2 = b_{q+2} = \ldots = b_n = 0$, $b_3, \ldots, b_{q+1}$ — все различные ненулевые элементы поля $\mathbb{F}$. Тогда для любого $\alpha \in \mathbb{F}^*$ имеем номер $t = 3, \ldots, q+1$, что $\alpha = -b_t$. Поэтому в слове $\mathbf{b} + \alpha\mathbf{a}$ на месте t стоит 0 и значит, его вес меньше l. Все слова в коде $\mathcal{C}$ кратны $\mathbf{a}, \mathbf{b}$, либо $\mathbf{b} + \alpha\mathbf{a}$, поэтому содержат 0 на позициях $[1, l]$. Таким образом, в коде $\mathcal{C}$ реальной длины l нет слов веса l. ►

Для доказательствва теоремы Мак-Вилльямс сначала докажем вспомогательную лемму.

Лемма 3.4. Пусть $\mathbb{F}$ — конечное поле мощности q. Тогда для любого линейного кода $\mathcal{C} \leq \mathbb{F}^n$ справедливо равенство

$$\sum_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = \frac{q-1}{q} |\mathcal{C}| l(\mathcal{C}).$$

◄ Для каждого $i \in \{1, \ldots, n\}$ рассмотрим проекцию

$$\pi_i : \mathbb{F}^n \to \mathbb{F},\ \pi_i(\mathbf{a}) = a_i.$$

Поскольку π_i — гомоморфизм пространств, то $\pi_i(\mathcal{C})$ является подпространством $\mathbb{F}$, соответственно, $\pi_i(\mathcal{C}) \in \{0, \mathbb{F}\}$ и

$$l(\mathcal{C}) = |\{i \in \{1, \ldots, n\} : \ \pi_i(\mathcal{C}) = \mathbb{F}\}|.$$

Кроме того, если рассмотреть ядро ограничения гомоморфизма π_i на пространство $\mathcal{C}$: $\mathcal{K}_i = \mathrm{Ker}(\pi_i|_{\mathcal{C}})$, то по теореме о гомоморфизме

$$|\mathcal{K}_i| = \frac{|\mathcal{C}|}{|\pi_i(\mathcal{C})|} = \begin{cases} \frac{|\mathcal{C}|}{q}, \text{ если } \pi_i(\mathcal{C}) = \mathbb{F}, \\ |\mathcal{C}| \text{ если } \pi_i(\mathcal{C}) = 0. \end{cases}$$

Справедливы равенства

$$\sum_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = \sum_{\mathbf{a} \in \mathcal{C}} \sum_{i=1}^{n} ||a_i|| = \sum_{i=1}^{n} \sum_{\mathbf{a} \in \mathcal{C}} ||a_i||.$$

При условии $\pi_i(\mathcal{C}) = \mathbb{F}$ прообраз в $\mathcal{C}$ каждого элемента $a \in \mathbb{F}$ при гомоморфизме $\pi_i|_{\mathcal{C}}$ имеет мощность $|\mathcal{K}_i|$, поэтому

$$\sum_{\mathbf{a} \in \mathcal{C}} ||a_i|| = \sum_{\mathbf{a} \in \mathcal{C}} ||\pi_i(\mathbf{a})|| = |\mathcal{K}_i| \sum_{a \in \mathbb{F}} ||a|| = |\mathcal{K}_i|(q-1) = \frac{q-1}{q}|\mathcal{C}|.$$

При условии $\pi_i(\mathcal{C}) = 0$ имеем $\sum\limits_{\mathbf{a} \in \mathcal{C}} ||a_i|| = 0$.

В итоге,

$$\sum_{i=1}^{n} \sum_{\mathbf{a} \in \mathcal{C}} ||a_i|| = \frac{q-1}{q}|\mathcal{C}|l(\mathcal{C}).$$

►

Следствие 3.5. Пусть $\mathbb{F}$ — конечное поле. Если эквидистантный линейный код $\mathcal{C} \leq \mathbb{F}^n$ лежит на границе Плоткина, то $l(\mathcal{C}) = n$.

◄ Вспомним, что код лежит на границе Плоткина, если $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n$.

Для эквидистантного линейного кода имеем $||\mathbf{a}|| = d$ для любого $\mathbf{a} \in \mathcal{C} \setminus \{0\}$, откуда по лемме о сумме весов получаем $\sum\limits_{\mathbf{a} \in \mathcal{C}} ||\mathbf{a}|| = (|\mathcal{C}| - 1)d = \frac{q-1}{q}|\mathcal{C}|l(\mathcal{C})$ и $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}l(\mathcal{C})$.

Приравнивая эти два выражения для d получаем требуемое равенство $l(\mathcal{C}) = n$.►

Перейдём к основной теореме данной лекции.

Теорема 3.6 (Теорема Ф. Мак-Вилльямс, 1962)**.** Пусть $\mathbb{F}$ — произвольное конечное поле. Тогда любая линейная изометрия (3.1) линейных кодов над $\mathbb{F}$ продолжается до линейного над $\mathbb{F}$ мономиального преобразования (2.1).

◀ Как было показано в теореме 2.3, мономиальные преобразования $\mathcal{M}(\mathbb{F}^n)$ образуют группу. Поэтому для доказательства существования продолжения τ, достаточно доказать результат для произведения τ и некоторых мономиальных преобразований.

Проведём доказательство индукцией по $l(\mathcal{C}) \geq 0$.

База индукции. Если $l(\mathcal{C}) = 0$, то $\mathcal{C} = 0$. В этом случае утверждение очевидно: в качестве продолжения τ можно взять произвольное мономиальное преобразование из $\mathcal{M}(\mathbb{F}^n)$.

Шаг индукции. Пусть теорема верна для всех кодов $\mathcal{C}, \mathcal{L} \leq \mathbb{F}^n$ произвольной длины $n \in \mathbb{N}$ таких, что $0 \leq l(\mathcal{C}) < l$ для некоторого $l \in \mathbb{N}$. Докажем её для $l(\mathcal{C}) = l$. Ввиду линейности отображения τ на пространстве $\mathcal{C}$ условие (3.2) эквивалентно

$$||\tau(\mathbf{a})|| = ||\mathbf{a}|| \ \forall \mathbf{a} \in \mathcal{C}.$$

По лемме 3.4 отсюда следует, что $l(\mathcal{L}) = l(\mathcal{C})$.

Поскольку $l(\mathcal{C}) = l > 0$, то $\pi_i(\mathcal{C}) = \mathbb{F}$ для некоторого $i \in \{1, \ldots, n\}$. Умножив при необходимости τ справа на мономиальное преобразование, меняющее местами i-ую и первую координаты, без ограничения общности можем считать, что $i = 1$. Тогда код $\mathcal{C}$ содержит слово $\mathbf{a}_1 = (1, *, \ldots, *)$. Вспомним, что для $\mathcal{K}_1 = \mathrm{Ker}(\pi_1|_{\mathcal{C}})$ справедливо $\dim \mathcal{K}_1 = \dim \mathcal{C} - 1$, $|\mathcal{K}_1| = \frac{|\mathcal{C}|}{q}$, $q = |\mathbb{F}|$. Более того,

$$\mathcal{C} = \mathbb{F}\mathbf{a}_1 \oplus \mathcal{K}_1,$$

т.к. $\mathbf{a}_1 \notin \mathcal{K}_1$ по построению. Поскольку по определению первые координаты всех слов в $\mathcal{K}_1$ равны нулю и $\mathcal{K}_1 \subset \mathcal{C}$, то

$$l(\mathcal{K}_1) \leq l - 1 < l.$$

Рассмотрим линейный код $\tau(\mathcal{K}_1) \subset \tau(\mathcal{C}) = \mathcal{L}$. По лемме 3.4 отсюда следует, что $l(\tau(\mathcal{K}_1)) = l(\mathcal{K}_1) < l$. Следовательно, существует индекс $j \in \{1, \ldots, n\}$ такой, что $\pi_j(\mathcal{L}) = \mathbb{F}$, но $\pi_j(\tau(\mathcal{K}_1)) = 0$. Умножив при необходимости τ слева на мономиальное преобразование, меняющее местами j-ую и первую координаты, без ограничения общности можем считать, что $j = 1$. Рассмотрим подпространство $\mathcal{L}_1 = \mathrm{Ker}(\pi_1) \cap \mathcal{L}$. Имеем $\tau(\mathcal{K}_1) \subseteq \mathcal{L}_1$. Поскольку $\pi_1(\mathcal{L}) = \mathbb{F}$, то $|\mathcal{L}_1| = \frac{|\mathcal{L}|}{q} = \frac{|\mathcal{C}|}{q} = |\mathcal{K}_1|$. Следовательно, $\tau(\mathcal{K}_1) = \mathcal{L}_1$.

Поскольку τ — биекция из $\mathcal{C}$ в $\mathcal{L}$, $\tau(\mathcal{K}_1) = \mathcal{L}_1$ и $\mathbf{a}_1 \notin \mathcal{K}_1$, то $\tau(\mathbf{a}_1) \notin \mathcal{L}_1$. Значит, $\tau(\mathbf{a}_1) = \mathbf{b}_1 = (\beta, *, \ldots, *)$, $\beta \in \mathbb{F}^*$. Откуда имеем разложение

$$\mathcal{L} = \mathbb{F}\mathbf{b}_1 \oplus \mathcal{L}_1.$$

Для произвольного числа $c \in \mathbb{F}$ из линейности τ следует, что

$$\tau(c\mathbf{a}_1) = c\tau(\mathbf{a}_1) = c\mathbf{b}_1 = (c\beta, *, \ldots, *).$$

Тогда для произвольного слова $\mathbf{a} \in \mathcal{C}$ получаем

$$\mathbf{a} = a_1\mathbf{a}_1 + (0, a'_2, \ldots, a'_n),\ \tau(\mathbf{a}) = a_1\tau(\mathbf{a}_1) + \tau((0, a'_2, \ldots, a'_n)),$$

причём $\tau((0, a'_2, \ldots, a'_n)) \in \mathcal{L}_1$, откуда

$$\tau(\mathbf{a}) = (a_1\beta, \tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a})),$$

где $\tau_i : \mathcal{C} \to \mathbb{F}$, $i \in \{2, \ldots, n\}$ — линейные функции.

Покажем, что линейные функции $\tau_2, \ldots, \tau_n$ не зависят от первой координаты вектора $\mathbf{a} \in \mathcal{C}$, т.е. для любых $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, если $a_2 = b_2, \ldots, a_n = b_n$, то $\tau_i(\mathbf{a}) = \tau_i(\mathbf{b})$, $i \in \{2, \ldots, n\}$. Если $a_1 \neq b_1$, то $||\mathbf{a}-\mathbf{b}|| = 1$. Поскольку τ — линейная изометрия, то $||\tau(\mathbf{a})-\tau(\mathbf{b})|| = 1$. При этом $(\tau(\mathbf{a}))_1 = a_1\beta \neq b_1\beta = (\tau(\mathbf{b}))_1$, следовательно, все остальные координаты этих векторов обязательно равны.

Введём обозначения

$$\mathcal{C}' = \left\{(a_2, \ldots, a_n) \in \mathbb{F}^{n-1} :\ \exists a_1 \in \mathbb{F}(a_1, a_2, \ldots, a_n) \in \mathcal{C}\right\},$$

$$\mathcal{L}' = \left\{(b_2, \ldots, b_n) \in \mathbb{F}^{n-1} :\ \exists b_1 \in \mathbb{F}(b_1, b_2, \ldots, b_n) \in \mathcal{L}\right\},$$

и зададим отображение $\tau' : \mathcal{C}' \to \mathbb{F}^{n-1}$ условием

$$\tau'((a_2, \ldots, a_n)) = (\tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a}))\ \forall (a_2, \ldots, a_n),$$

где $a_1 \in \mathbb{F}$ произвольная константа, для которой $(a_1, a_2, \ldots, a_n) \in \mathcal{C}$. По доказанному выше отображение τ' определено корректно (не зависит от выбора a_1). Поскольку $\tau : \mathcal{C} \to \mathcal{L}$ — биекция, то из равенства $\tau(\mathbf{a}) = (a_1\beta, \tau_2(\mathbf{a}), \ldots, \tau_n(\mathbf{a}))$ заключаем, что $\tau'(\mathcal{C}') = \mathcal{L}'$, т.е. τ' — изоморфизм линейных пространств $\mathcal{C}'$ и $\mathcal{L}'$. Поскольку

$$\forall \mathbf{a} \in \mathcal{C} :\ ||\tau(\mathbf{a})|| = ||\mathbf{a}|| = ||a_1|| + ||(a_2, \ldots, a_n)||$$

и

$$||\tau(\mathbf{a})|| = ||a_1\beta|| + ||\tau'(a_2, \ldots, a_n)||,$$

то

$$\forall \mathbf{a}' \in \mathcal{C}' : \ ||\tau'(\mathbf{a}')|| = ||\mathbf{a}'||.$$

Таким образом, $\tau' : \mathcal{C}' \to \mathcal{L}'$ — линейная изометрия. Из определения пространства $\mathcal{C}'$ также следует, что $l(\mathcal{C}') = l - 1 < l$. Соответственно, можно применить предположение индукции: линейная изометрия τ' продолжается до линейного мономиального преобразования $\sigma' : \mathbb{F}^{n-1} \to \mathbb{F}^{n-1}$, с подстановкой $\rho' \in S_{n-1}$ на множестве $\{2, \ldots, n\}$ и обратимыми константами $u_2, \ldots, u_n \in \mathbb{F}^*$. Тогда продолжением τ будет мономиальное преобразование $\sigma : \mathbb{F}^n \to \mathbb{F}^n$, с подстановкой $\rho \in S_n$, $\rho(1) = 1$, $\rho(j) = \rho'(j)$, $j \in \{2, \ldots, n\}$, и обратимыми константами $\beta, u_2, \ldots, u_n \in \mathbb{F}^*$. ▶

Задачи к лекции 3.

Задача 1. Пусть $\Omega = \mathbb{F}_2$, $n = 4$, $\mathcal{C} = \mathcal{L} \subset \mathbb{F}_2^4$ — код проверки на чётность и $\tau : \mathcal{C} \to \mathcal{L}$ линейное отображение, определённое на базисе $\tau((1,1,0,0)) = (0,0,1,1)$, $\tau((1,0,1,0)) = (1,0,1,0)$, $\tau((1,0,0,1)) = (0,1,1,0)$ и продолженное по линейности. а) Докажите, что $\tau : \mathcal{C} \to \mathcal{L}$ — изометрия; б) постройте линейную изометрию $\sigma \in \mathfrak{S}(\mathbb{F}_2^4)$, продолжающую τ; в) установите, сколько всего линейных изометрий $\mathfrak{S}(\mathbb{F}_2^4)$ являются продолжениями τ?

Задача 2. Приведите пример кодов и их изометрии, для которых не выполняется утверждение теоремы Мак-Вилльямс о продолжении.

Задача 3. (О замене условия линейности на мощность). Пусть $\Omega = \mathbb{F}_2$, $n = 3$. Найдите минимальное такое $m \in \mathbb{N}$, что любая изометрия $\tau : \mathcal{C} \to \mathcal{L}$ произвольных кодов из Ω^3 мощности не менее m продолжается до мономиального преобразования на Ω^3.

Задача 4. (О замене условия линейности на область определения). Пусть $\Omega = \mathbb{F}_2$, $n \in \mathbb{N}$. Пусть $\mathcal{C} = \{\mathbf{0}, \mathbf{e}_1, \ldots, \mathbf{e}_n\} \subset \Omega^n$, $\mathcal{L} \subset \Omega^n$. Покажите, что любая изометрия $\tau : \mathcal{C} \to \mathcal{L}$ продолжается до мономиального преобразования на Ω^n.

Лекция 4. Проверочная и порождающая матрицы, гарантируемый ранг и расстояние линейного кода над полем. Проверочная и порождающая матрицы в стандартной форме. Двойственный код, его проверочная и порождающая матрицы. Коды, двойственные к двоичному коду Хэмминга и к обобщённому коду Рида–Соломона.

1°. Проверочная и порождающая матрицы, гарантируемый ранг и расстояние линейного кода над полем. Проверочная и порождающая матрицы в стандартной форме.

Определение 4.1. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Наименьший (по включению) подмодуль $\langle S\rangle_{\mathcal{R}}$ модуля M, содержащий множество S, называется *подмодулем, порождённым множеством* S.

Если $N = \langle S\rangle_{\mathcal{R}}$, говорят также, что S — *система образующих подмодуля* N.

Предложение 4.2. Пусть S — произвольное множество элементов правого модуля M над кольцом $\mathcal{R}$. Тогда

$$\langle S\rangle_{\mathcal{R}} = S\mathcal{R} = \{x_1r_1 + \ldots + x_nr_n : x_i \in S, r_i \in \mathcal{R}, i = 1,\ldots,n,\ n \geq 0\}.$$

Определение 4.3. Если слова $g_i = (g_{i1},\ldots,g_{in})$, $i = 1,\ldots,m$ порождают код $\mathcal{C}$ длины n над модулем M, то матрица

$$G = \begin{pmatrix} g_{11} & \ldots & g_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ g_{m1} & \ldots & g_{mn} \end{pmatrix}$$

называется *порождающей матрицей* кода $\mathcal{C}$.

Определение 4.4. Пусть M — левый $\mathcal{R}$-модуль и $\mathcal{C}$ — код над M длины n. Матрица $H = (h_{ij})$ размера $r\times n$ над кольцом $\mathcal{R}$ называется *проверочной матрицей* кода $\mathcal{C}$ длины n над M, если

$$\mathcal{C} = \left\{\mathbf{a} \in M^n :\ H\mathbf{a}^T = 0\right\}. \tag{4.1}$$

Можно заметить, что для кодов над модулями и даже над кольцами проверочная матрица существует далеко не всегда. Однако, из курса линейной алгебры следует, что в случае линейных кодов над

полем $\mathbb{F}$ ($M = \mathcal{R} = \mathbb{F}$) любой код (т.е. подпространство в $\mathbb{F}^n$) задаётся некоторой однородной системой линейных уравнений вида (4.1), которой заведомо удовлетворяют строки порождающей матрицы кода и не удовлетворяют никакие другие векторы. Поэтому получаем следующий критерий.

Теорема 4.5. Пусть G и H — матрицы над полем $\mathbb{F}$ размеров $r \times n$ и $m \times n$, соответственно. Тогда следующие условия эквивалентны:

1. G и H — порождающая и проверочная матрицы некоторого кода $\mathcal{C}$ длины n над $\mathbb{F}$;
2. $HG^T = 0$ и $\mathrm{rk}(G) + \mathrm{rk}(H) = n$.

При этом размерность кода $\mathcal{C}$ равна $\mathrm{rk}(G)$.

Из (4.1) и теоремы 4.5 легко следует, что если умножить проверочную матрицу H (соответственно, порождающую матрицу G) кода $\mathcal{C}$ слева на обратимую матрицу A, (соответственно, B) допустимых размеров, то определяемый каждой из них код не изменится (т.к. $AH(BG)^T = AHG^TB = 0$). В частности, элементарные преобразования строк матриц H и G, т.е. прибавление к строке другой строки, умноженной на элемент поля, перестановка строк и умножение строки на ненулевой элемент поля, не меняют множества решений системы (4.1) (соответственно, линейной оболочки системы строк матрицы G), поэтому можно считать, что каждая из них содержит набор столбцов единичной матрицы порядков $n - \mathrm{rk}(\mathcal{C})$ и $\mathrm{rk}(\mathcal{C})$, соответственно, и число строк каждой из них равно её рангу.

Пример. Код проверки на чётность над полем задаётся матрицами

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix} \text{ и } G = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & 0 & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & & \dots & 1 & 0 & -1 \\ 0 & 0 & & \dots & 0 & 1 & -1 \end{pmatrix}.$$

Перестановка столбцов порождающей матрицы линейного кода соответствует переходу к некоторому линейно эквивалентному коду. При этом проверочную матрицу нового кода можно получить той же перестановкой столбцов. Следовательно, любой линейный код над полем линейно эквивалентен коду с проверочной матрицей *стандартного вида*: $H = (H'| - E)$, где E — единичная матрица порядка $n - k$, а H' — некоторая матрица размера $n - k \times k$.

Смысл этой записи в том, что первые k символов любого кодового слова $(a_1, \ldots, a_n)$ являются определяющими, а остальные вычисляются как $(a_{k+1}, \ldots, a_n) = (a_1, \ldots, a_k)(H')^T$.

Если код $\mathcal{C}$ имеет проверочную матрицу H в стандартной форме, то условиям $HG^T = 0$, $\mathrm{rk}H + \mathrm{rk}G = n$ удовлетворяет матрица $G = (E|(H')^T)$ размера $k \times n$, где E — единичная матрица порядка k. Она называется порождающей матрицей *стандартного вида*. Соответственно, любой линейный код над полем линейно эквивалентен коду с порождающей матрицей стандартного вида.

Определение 4.6. *Гарантируемым рангом* прямоугольной матрицы A над полем $\mathbb{F}$ называется число $\varkappa(A)$, равное максимальному числу s такому, что любые s столбцов матрицы линейно независимы (если A содержит нулевой столбец, считаем, что $\varkappa(A) = 0$).

Очевидно, что $\mathrm{rk}(A) \geq \varkappa(A)$.

Предложение 4.7. Если H — проверочная матрица ненулевого линейного кода $\mathcal{C}$ над полем, то $d(\mathcal{C}) = \varkappa(H) + 1$. Код $\mathcal{C}$ является МДР-кодом в точности тогда, когда $\varkappa(H) = \mathrm{rk}H$.

◀ Наличие в коде $\mathcal{C}$ слова веса d равносильно тому, что некоторые d столбцов матрицы H линейно зависимы, откуда $d(\mathcal{C}) > \varkappa(H)$. С другой стороны, по определению гарантируемого ранга, существует линейно зависимая система из $\varkappa(H)+1$ столбцов матрицы H, откуда $d \leq \varkappa(H) + 1$.

Действительно, $d(\mathcal{C}) = \varkappa(H) + 1$ и $n - k + 1 = \mathrm{rk}H + 1$. Поэтому $d(\mathcal{C}) = n - k + 1$ в точности при совпадении $\varkappa(H) = \mathrm{rk}H$. ▶

Предложение 4.8. Линейный код $\mathcal{C}$ над полем с проверочной матрицей $H = (H'|-E)$ стандартного вида является МДР-кодом тогда и только тогда, когда в матрице H' все квадратные подматрицы невырождены.

◀ Согласно предыдущему предложению, $\mathcal{C}$ есть МДР-код тогда и только тогда, когда любая система из $n-k$ столбцов матрицы H линейно независима. Пусть $H'[i_1, \ldots, i_s|j_1, \ldots, j_s]$ подматрица размера $s \times s$ матрицы H', составленная из элементов, стоящих на пересечении строк с номерами $i_1, \ldots, i_s$ и столбцов с номерами $j_1, \ldots, j_s$. Рассмотрим систему столбцов матрицы H с номерами $j_1, \ldots, j_s, k + i_{s+1}, \ldots, k + i_{n-k}$, где $i_{s+1}, \ldots, i_{n-k} \in \{1, \ldots, n-k\} \setminus \{i_1, \ldots, i_s\}$. Т.е.

это столбцы с номерами $j_1, \ldots, j_s$ из матрицы H' и столбцы с номерами $i_{s+1}, \ldots, i_{n-k}$ из матрицы $-E$. По формуле разложения определителя по столбцу определитель матрицы $(n-k)\times(n-k)$, построенный на этих столбцах, равен $\pm \det H'[i_1, \ldots, i_s | j_1, \ldots, j_s]$. Следовательно, линейная независимость этих столбцов равносильна невырожденности подматрицы $H'[i_1, \ldots, i_s | j_1, \ldots, j_s]$. ►

2°. Двойственный код, его проверочная и порождающая матрицы. Пусть $\mathbb{F}$ — конечное поле. Определим скалярное умножение векторов $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ правилом $\mathbf{ab} = a_1 b_1 + \cdots + a_n b_n \in \mathbb{F}$.

Определение 4.9. *Кодом, двойственным к линейному коду* $\mathcal{C} < \mathbb{F}^n$ называется код

$$\mathcal{C}^\circ = \{\mathbf{b} \in \mathbb{F}^n : \mathbf{b}\mathcal{C} = 0\},$$

(под $\mathbf{b}\mathcal{C} = 0$ понимается, что $\mathbf{ba} = 0$ для любого $\mathbf{a} \in \mathcal{C}$).

Теорема 4.10. Пусть $\mathcal{C}$ — линейный $[n, k]$-код над полем $\mathbb{F}$ с порождающей матрицей G и проверочной матрицей H. Тогда
1) $\mathcal{C}^\circ$ есть линейный $[n, n-k]$-код над $\mathbb{F}$ с порождающей матрицей H и проверочной матрицей G;
2) $\mathcal{C}^{\circ\circ} = \mathcal{C}$;
3) для любого линейного кода $\mathcal{L} \leq \mathbb{F}^n$ справедливы равенства

$$(\mathcal{C} + \mathcal{L})^\circ = \mathcal{C}^\circ \cap \mathcal{L}^\circ, \ (\mathcal{C} \cap \mathcal{L})^\circ = \mathcal{C}^\circ + \mathcal{L}^\circ.$$

◄ 1) Условие $\mathbf{b}\mathcal{C} = 0$ эквивалентно системе линейных уравнений $G\mathbf{b}^T = 0$. Поэтому матрица G будет проверочной для кода $\mathcal{C}^\circ$. Соответственно, из теоремы 4.5 получаем, что H — его порождающая матрица и $\dim \mathcal{C}^\circ = n - k$.

2) Получается из 1) повторным применением теоремы 4.5.

3)$(\mathcal{C} + \mathcal{L})^\circ = \{\mathbf{b} \in \mathbb{F}^n : \mathbf{b}(\mathcal{C} + \mathcal{L}) = 0\}$. В частности, $\mathcal{C}, \mathcal{L} \subseteq \mathcal{C} + \mathcal{L}$, $\mathbf{b}\mathcal{C} = 0$ и $\mathbf{b}\mathcal{L} = 0$, поэтому $(\mathcal{C}+\mathcal{L})^\circ \subseteq \mathcal{C}^\circ \cap \mathcal{L}^\circ$. Обратно, если $\mathbf{b} \in \mathcal{C}^\circ \cap \mathcal{L}^\circ$, то $\mathbf{b}\mathcal{C} = 0$ и $\mathbf{b}\mathcal{L} = 0$, значит, $\mathbf{b}(\mathcal{C} + \mathcal{L}) = 0$ и $(\mathcal{C} + \mathcal{L})^\circ \supseteq \mathcal{C}^\circ \cap \mathcal{L}^\circ$. Второе утверждение доказывается аналогично.►

Утверждение (1) теоремы 4.10 является эквивалентным определением двойственного кода.

Предложение 4.11. Пусть $\mathcal{C}$ — линейный $[n, k, n-k+1]$ МДР код над полем $\mathbb{F}$. Тогда $\mathcal{C}^\circ$ есть линейный $[n, n-k, k+1]$ МДР код над $\mathbb{F}$.

◄ Можно считать, что $\mathcal{C}$ имеет проверочную матрицу стандартного вида. Тогда по предложению 4.8 в матрице H' все квадратные подматрицы невырождены. По теореме 4.10 матрица $G = (E|(H')^T)$ является проверочной для кода $\mathcal{C}^\circ$. В матрице $(H')^T$ все квадратные подматрицы тоже невырождены, значит по предложению 4.8 код $\mathcal{C}^\circ$ также является МДР кодом.►

Определение 4.12. Линейный код $\mathcal{C} < \mathbb{F}^n$ называется *самоортогональным*, если $\mathcal{C} \subseteq \mathcal{C}^\circ$, и *самодвойственным*, если $\mathcal{C} = \mathcal{C}^\circ$.

Предложение 4.13. Пусть $\mathcal{C}$ — линейный $[n, k]$ самодвойственный код над полем $\mathbb{F}$. Тогда n обязательно чётное число и $k = \frac{n}{2}$.

◄ Имеем $\mathcal{C} = \mathcal{C}^\circ$, значит $k = \dim \mathcal{C} = \dim \mathcal{C}^\circ$. С другой стороны, по теореме 4.10 $\dim \mathcal{C}^\circ = n - k$. Откуда, $n - k = k$, или $n = 2k$.►

3°. Код, двойственный к обобщённому коду Рида–Соломона. 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

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

Напомним, что образ $\varphi(\mathbb{F}[x|k])$ называется *обобщённым* $[n, k]$*-кодом Рида–Соломона* над полем $\mathbb{F}$. Обозначим его $GRS_q(n, k)$. Его порождающая матрица имеет вид

$$G = \begin{pmatrix} u_1 & u_2 & \ldots & u_n \\ u_1 x_1 & u_2 x_2 & \ldots & u_n x_n \\ \vdots & \vdots & & \vdots \\ u_1 x_1^{k-1} & u_2 x_2^{k-1} & \ldots & u_n x_n^{k-1} \end{pmatrix}.$$

Предложение 4.14. $GRS_q(n, k)^\circ = GRS_q(n, n - k)$.

◄ Рассмотрим элементы

$$y_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} (x_i - x_j)^{-1}, \ v_i = y_i u_i^{-1} \in \mathbb{F}^*, \ i = 1, \ldots, n,$$

и матрицу

$$H = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1x_1 & v_2x_2 & \dots & v_nx_n \\ \vdots & \vdots & & \vdots \\ v_1x_1^{n-k-1} & v_2x_2^{n-k-1} & \dots & v_nx_n^{n-k-1} \end{pmatrix}.$$

Код с порождающей матрицей H является кодом $GRS_q(n, n-k)$. Достаточно показать, что H — проверочная для кода $GRS_q(n,k)$, поскольку по теореме 4.10 это доказывает, что она порождающая для двойственного кода. По построению очевидно, что $\mathrm{rk}H = n-k$, следовательно, достаточно доказать равенство $HG^T = 0$.

Элемент на позиции (s,t) матрицы HG^T равен

$$\sum_{i=1}^{n} v_i x_i^{s-1} u_i x_i^{t-1} = \sum_{i=1}^{n} y_i x_i^{s+t-2}.$$

Возьмём матрицу Вандермонда

$$V = V(x_1, \dots, x_n) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix}.$$

Имеем $|V| = \prod\limits_{1 \le s < t \le n} (x_t - x_s)$, алгебраические дополнения элементов последней строки этой матрицы имеют вид

$$V_{n,j} = (-1)^{n+j} \prod_{\substack{1 \le s < t \le n \\ s,t \ne j}} (x_t - x_s).$$

Отметим, что

$$\frac{V_{n,i}}{|V|} = \prod_{\substack{s=1 \\ s \ne i}}^{n} (x_i - x_s)^{-1} = y_i.$$

Откуда

$$\sum_{i=1}^{n} y_i x_i^{s+t-2} = |V|^{-1} \sum_{i=1}^{n} x_i^{s+t-2} V_{n,i} = 0 \ \ —$$

фальшивое разложение определителя Вандермонда (элементы взяты из строки с номером $s+t-1 \le n-1$, а алгебраические дополнения

для n-ой строки.) ►

4°. Код, двойственный к двоичному коду Хэмминга.

Определение 4.15. Код $\mathcal{M}_2(l)$, двойственный к двоичному коду Хэмминга $\mathcal{H}_2(l)$, называется *кодом Макдональда.*

Предложение 4.16. Код Макдональда $\mathcal{M}_2(l)$, двойственный к двоичному коду Хэмминга $\mathcal{H}_2(l)$, является линейным эквидистантным $[n, l, 2^{l-1}]_2$-кодом, лежащим на границе Плоткина.

◄ Линейность очевида по построению. Поскольку матрица H, проверочная для кода Хэмминга, содержит все ненулевые столбцы высоты l, то $\dim \mathcal{M}_2(l) = \mathrm{rk} H = l$.

Вычислим расстояние кода $\mathcal{M}_2(l)$ и докажем его эквидистантность. Поскольку матрица H содержит все столбцы высоты l, кроме нулевого, то любая её строка содержит в точности $\dfrac{2^l}{2} = 2^{l-1}$ единиц. Проведем дальнейшее доказательство индукцией по l.

База индукции. При $l = 1$ имеем $n = 1$, $H = (1)$ и слово (1) веса 1 является единственным ненулевым словом в коде $\mathcal{M}_2(1)$.

Шаг индукции. Пусть $l > 1$ и для всех $m < l$ утверждение верно. Пусть H' — порождающая матрица кода $\mathcal{M}_2(l-1)$, составленная из всех ненулевых столбцов высоты $l-1$. Обозначим $\mathbf{0} = (0, \ldots, 0)$, $\mathbf{1} = (1, \ldots, 1)$. Тогда $H = \begin{pmatrix} H' & \mathbf{0}^T & H' \\ \mathbf{0} & 1 & \mathbf{1} \end{pmatrix}$ (ненулевой столбец высоты l можно получить либо из ненулевого столбца высоты $l-1$ приписыванием 0 или 1, либо единицу можно также приписать к нулевому столбцу).

Любое ненулевое слово $\mathbf{a} \in \mathcal{M}_2(l)$ — сумма некоторых строк матрицы H. Если в сумме не участвует последняя строка, то $\mathbf{a} = (\mathbf{a}', 0, \mathbf{a}')$, где $\mathbf{a}' \in \mathcal{M}_2(l-1) \setminus \{0\}$. По предположению индукции $||\mathbf{a}'|| = 2^{l-2}$, соответственно, $||\mathbf{a}|| = 2||\mathbf{a}'|| = 2^{l-1}$. В противном случае, $\mathbf{a} = (\mathbf{a}', 0, \mathbf{a}') + (\mathbf{0}, 1, \mathbf{1})$. Заметим, что $||\mathbf{a}' + \mathbf{1}|| = 2^{l-1} - 1 - ||\mathbf{a}'||$. Откуда, $||\mathbf{a}|| = ||\mathbf{a}'|| + 1 + 2^{l-1} - 1 - ||\mathbf{a}'|| = 2^{l-1}$. Следовательно, веса всех ненулевых слов линейного кода $\mathcal{M}_2(l)$ одинаковы, поэтому он является эквидистантным кодом с минимальным расстоянием $d = 2^{l-1}$.

Вспомним, что код лежит на границе Плоткина, если $d = \frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n$. В данном случае $q = 2$, $n = 2^l - 1$, $|\mathcal{M}_2(l)| = 2^l$, отку-

да

$$\frac{q-1}{q}\frac{|\mathcal{C}|}{|\mathcal{C}|-1}n = \frac{2^l}{2(2^l-1)}\cdot(2^1-1) = 2^{l-1} = d(\mathcal{M}_2(l)).$$

►

Заметим, что $|\mathcal{M}_2(l)| = 2^l = n+1$. Оказывается, что мощность кода Макдональда является максимально возможной среди любых эквидистантных линейных n-кодов.

Теорема 4.17. Пусть $\mathcal{C}$ — эквидистантный линейный код в $\mathbb{F}_2^n$, тогда $|\mathcal{C}| \leq n+1$.

◄ Пусть $\mathcal{C} = \{\mathbf{c_1}, \ldots, \mathbf{c_s}\}$, и при этом $d(\mathbf{c_i}, \mathbf{c_j}) = d$, для всех $i \neq j$. Для любых различных $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ имеем

$$d(\mathbf{a},\mathbf{b}) = \sum_{i=1}^{n}|a_i - b_i| = \sum_{i=1}^{n}(a_i-b_i)^2 = ||\mathbf{a}|| + ||\mathbf{b}|| - 2\mathbf{ab}$$

(все вычисления, в частности, модуля и скалярного произведения выполняются над $\mathbb{R}$). Откуда для $\mathbf{a}, \mathbf{b} \in \mathcal{C} \setminus \{0\}$ получаем, что $d = 2d - 2\mathbf{ab}$ и $\mathbf{ab} = \frac{d}{2}$. Без ограничения общности можно считать, что $\mathbf{c_1} = 0$.

Вычислим определитель Грама для векторов $\mathbf{c_2}, \ldots, \mathbf{c_s}$ как векторов в $\mathbb{R}^n$ (для $(0,1)$-векторов вес Хэмминга совпадает со скалярным квадратом):

$$\begin{vmatrix} d & \frac{d}{2} & \ldots & \frac{d}{2} \\ \frac{d}{2} & d & \ldots & \frac{d}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d}{2} & \frac{d}{2} & \ldots & d \end{vmatrix} = \frac{d^{s-1}}{2^{s-1}} \begin{vmatrix} 2 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 2 \end{vmatrix} = \frac{d^{s-1}}{2^{s-1}} s \neq 0,$$

т.е. $c_2, \ldots, \mathbf{c_s}$ линейно независимы над $\mathbb{R}$.

Итак, имеем $s-1$ линейно независимых векторов. В пространстве $\mathbb{R}^n$ может быть не более n линейно независимых векторов, значит, $s-1 \leq n$ и $s \leq n+1$. ►

Задачи к лекции 4.

Задача 1. Приведите примеры матриц A, B без нулевых столбцов, для которых $\varkappa A = \mathrm{rk}A$, $\varkappa B < \mathrm{rk}B$.

Задача 2. (Критерий миноров над кольцом, обобщение предложения 4.8) Докажите, что если G — $k \times n$ матрица над кольцом $\mathcal{R}$ и все миноры порядка k матрицы G обратимы в $\mathcal{R}$, то код с порождающей матрицей G является МДР-кодом.

Задача 3. Покажите, что в предыдущей задаче условие "миноры порядка k не равны нулю" не достаточно: приведите пример $[n, k]$ не МДР-кода над $\mathbb{Z}_6$, так что все миноры порядка k его порождающей матрицы G ненулевые.

Задача 4. Приведите пример самодвойственного кода.

Задача 5. Приведите пример самоортогонального кода, не являющегося самодвойственным.

Задача 6. Возможно ли подобрать параметры $q, n, k,\ x_1, \ldots, x_n$, $u_1, \ldots, u_n$ так, чтобы код $GRS_q(n, k)$ был самодвойственным?

Лекция 5. Построение новых кодов из заданных. Граница Грайсмера.

1°. Добавление констант

Определение 5.1. Код $\mathcal{C} \subseteq \mathbb{F}^n$ *содержит константы*, если он содержит все слова вида $(a, \ldots, a)$, $a \in \mathbb{F}$. Для линейного кода это условие равносильно включению $\mathbf{1} = (1, \ldots, 1) \in \mathcal{C}$.

Определение 5.2. Для произвольных $\alpha \in \mathbb{F}$ и $\mathbf{a} \in \mathbb{F}^n$ обозначим через $s_\alpha(\mathbf{a})$ количество координат в слове $\mathbf{a}$, равных α. Также положим $s_{\max} = \max\{s_\alpha(\mathbf{a}) : \ \mathbf{a} \in \mathcal{C} \setminus \{0\}, \ \alpha \in \mathbb{F}\}$.

Определение 5.3. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный код, не содержащий констант. Тогда говорят, что код $\mathcal{C}^c = \mathcal{C} + \mathbb{F}\mathbf{1}$ *получен из кода* $\mathcal{C}$ *добавлением констант.* Заметим, что добавление констант к коду равносильно приписыванию строки $\mathbf{1}$ к его порождающей матрице.

Предложение 5.4. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n, k, d]_q$-код, не содержащий констант. Тогда код $\mathcal{C}^c = \mathcal{C} + \mathbb{F}\mathbf{1}$ есть линейный $[n, k+1, d']_q$-код с расстоянием $d' = n - s_{\max} \leq d$.

◀ По построению код $\mathcal{C}^c$ есть линейный $[n, k+1]_q$-код. Вычислим его расстояние.

Произвольное слово $\mathbf{b} \in \mathcal{C}^c$ представляется в виде $\mathbf{b} = \mathbf{a} - \alpha\mathbf{1}$, где $\mathbf{a} \in \mathcal{C}, \alpha \in \mathbb{F}$. По построению $||b|| = n - s_\alpha(\mathbf{a}) \geq n - s_{\max}$. Выражение $n - s_{\max} \geq 1$ в силу того, что код $\mathcal{C}$ не содержит констант. Откуда видно, что $d' \geq n - s_{\max}$. Выбирая такие $\mathbf{a} \in \mathcal{C} \setminus \{0\}$ и $\alpha \in \mathbb{F}$, что $s_{\max} = s_\alpha(\mathbf{a})$, получаем, что $||b|| = n - s_{\max}$ и $d' = n - s_{\max}$.

Неравенство $d' \leq d$ следует из включения $\mathcal{C} \leq \mathcal{C}^c$. ▶

2°. Добавление проверки на чётность

Определение 5.5. Код $\mathcal{C} \subseteq \mathbb{F}^n$ *содержит проверку на чётность*, если его двойственный код $\mathcal{C}^\circ$ содержит слово $\mathbf{1}$.

Определение 5.6. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n, k, d]_q$-код с проверочной матрицей H размера $l \times n$. Тогда говорят, что код $\widehat{\mathcal{C}} \leq \mathbb{F}^{n+1}$ с проверочной матрицей

$$\widehat{H} = \begin{pmatrix} \mathbf{1} & 1 \\ H & \mathbf{0}^T \end{pmatrix}$$

получен из кода $\mathcal{C}$ добавлением проверки на чётность.

Предложение 5.7. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код с проверочной матрицей H размера $l \times n$. Тогда линейный код $\widehat{\mathcal{C}} \leq \mathbb{F}^{n+1}$, полученный из кода $\mathcal{C}$ добавлением проверки на чётность, есть линейный $[n+1,k,\widehat{d}]_q$-код с расстоянием $\widehat{d} \in \{d, d+1\}$. Если код $\mathcal{C}$ содержит проверку на чётность, то $\widehat{d} = d$.

◀ По построению $\mathrm{rk}\widehat{H} = \mathrm{rk}H + 1$, поэтому $\dim\widehat{\mathcal{C}} = n + 1 - \mathrm{rk}\widehat{H} = n - \mathrm{rk}H = k$.

Вычислим расстояние кода $\widehat{\mathcal{C}}$. Вспомним, что $d(\widehat{\mathcal{C}}) = \varkappa(\widehat{H})+1$. Заметим, что любые $\varkappa(H)$ столбцов матрицы $\widehat{H}$ линейно независимы, поскольку любые $\widehat{H}$ из первых n столбцов получены приписыванием 1 к линейно независимым столбцам матрицы H, а последний столбец не выражается через остальные, если они также линйено независимы.

С другой стороны, если мы возьмём в матрице $\widehat{H}$ $\varkappa(H)+1$ столбцов из первых n так, что сооответсвующие столбцы линейно зависимы в H, то их линейная комбинация с теми же коэффициентами даст столбец, пропорциональный последнему. Следовательно, в матрице $\widehat{H}$ есть $\varkappa(H)+2$ линейно зависимых столбца, и $\varkappa(\widehat{H}) \leq \varkappa(H)+1$. Таким образом, $d \leq \widehat{d} \leq d+1$. ▶

Следствие 5.8. Если $q = 2$ и d нечётно, то $\widehat{d} = d + 1$.

◀ Если $q = 2$, то все слова кода $\widehat{\mathcal{C}}$ имеют чётный вес, поэтому $\widehat{d}$ чётно, значит не равно d в данном случае.▶

3°. Расширение кода

Определение 5.9. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код. Тогда про код $\mathcal{C}^{ext}$, полученный из кода $\mathcal{C}$ добавлением констант и проверки на чётность, говорят, что он есть *расширение кода* $\mathcal{C}$ или *расширенный код* $\mathcal{C}$.

Следствие 5.10. Пусть $\mathcal{C} \leq \mathbb{F}^n$ — линейный $[n,k,d]_q$-код, не содержащий констант. Тогда код $\mathcal{C}^{ext}$ есть линейный $[n+1,k+1,d^{ext}]_q$-код, где $d^{ext} = n - s_{\max} + \delta$, $\delta \in \{0,1\}$.

4°. Декартово произведение кодов

Определение 5.11. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, \ldots, m$. Тогда о коде

$$\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_m \leq \mathbb{F}^{n_1 + \cdots + m_m},$$

состоящем из всех слов вида $(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, $\mathbf{a}_i \in \mathcal{C}_i$, $i = 1, \ldots, m$, говорят как о *декартовом произведении кодов* $\mathcal{C}_1, \ldots, \mathcal{C}_m$. При этом коды $\mathcal{C}_i$ называют *компонентами* кода $\mathcal{C}$.

Предложение 5.12. Код $\mathcal{C}$ есть $[n_1 + \cdots + n_m, k_1 + \cdots + k_m, d]_q$-код для $d = \min\{d_1, \ldots, d_m\}$. $\mathcal{C}$ — линейный код тогда и только тогда, когда все его компоненты линейны. При этом проверочная матрица кода $\mathcal{C}$ задаётся равенством

$$H = \begin{pmatrix} H_1 & 0 & \ldots & 0 \\ 0 & H_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & H_m \end{pmatrix},$$

где H_i — проверочная матрица кода $\mathcal{C}_i$, $i = 1, \ldots, m$.

5°. Тензорное произведение кодов

Определение 5.13. *Тензорным произведением матриц* $A \in M_{m,n}(\mathbb{F})$ *и* $B \in M_{k,l}(\mathbb{F})$ называется матрица

$$A \otimes B = \begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \ldots & a_{mn}B \end{pmatrix} \in M_{mk,nl}(\mathbb{F}).$$

Определение 5.14. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. *Тензорным произведением кодов* $\mathcal{C}_1$ *и* $\mathcal{C}_2$ называется код $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2 \in \mathbb{F}^{n_1 n_2}$, порождённый всеми словами вида

$$\mathbf{a} \otimes \mathbf{b},\ \mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$$

(под тензорным произведением кодовых слов понимается их произведение как $1 \times n_i$ матриц).

Предложение 5.15. Пусть $\mathcal{C}_i$ — линейные $[n_i, k_i, d_i]_q$-коды над полем $\mathbb{F}$, с порождающими матрицами $G^{(i)} \in M_{k_i, n_i}$ и проверочными матрицами $H^{(i)} \in M_{n_i - k_i, n_i}$, $i = 1, 2$. Тогда код $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2$

есть линейный $[n_1n_2, k_1k_2, d_1d_2]_q$-код с порождающей матрицей $G = G^{(1)} \otimes G^{(2)}$ и проверочной матрицей $H = \begin{pmatrix} H^{(1)} \otimes E_{n_2} \\ E_{n_1} \otimes H^{(2)} \end{pmatrix}$.

◀ Пусть $G^{(i)} = \begin{pmatrix} \mathbf{a}_1^{(i)} \\ \vdots \\ \mathbf{a}_{k_i}^{(i)} \end{pmatrix}$, $i = 1, 2$. Любое слово кода $\mathcal{C}$ линейно выражается через множество слов $\mathbf{a}_r^{(1)} \otimes \mathbf{a}_s^{(2)}$, $r = 1, \ldots, k_1$, $s = 1, \ldots, k_2$. Эти слова составлют множество строк матрицы G, следовательно она является порождающей матрицей кода $\mathcal{C}$.▶

По свойству тензорного произведения $\dim \mathcal{C} = \mathrm{rk}G = \mathrm{rk}G^{(1)} \cdot \mathrm{rk}G^{(2)} = k_1k_2$.

Вычислим расстояние кода $\mathcal{C}$. Для этого рассмотрим изоморфизм $\varphi : \mathbb{F}^{n_1n_2} \to M_{n_1,n_2}(\mathbb{F})$ линейных пространств, сопоставляющий любому слову $\mathbf{c} = (c_1, \ldots, c_{n_1n_2})$ матрицу

$$\varphi(\mathbf{c}) = \begin{pmatrix} c_1 & \ldots & c_{n_2} \\ \vdots & & \vdots \\ c_{(n_1-1)n_2+1} & \ldots & c_{n_1n_2} \end{pmatrix}.$$

Тогда для любых $\mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$ слову

$$\mathbf{a} \otimes \mathbf{b} = (a_1b_1, \ldots, a_1b_{n_2}, a_2b_1, \ldots, a_2b_{n_2}, \ldots, a_{n_1}b_1, \ldots, a_{n_1}b_{n_2}) \in \mathcal{C}$$

соответствует матрица

$$\varphi(\mathbf{a} \otimes \mathbf{b}) = \begin{pmatrix} a_1b_1 & a_1b_2 & \ldots & a_1b_{n_2} \\ a_2b_1 & a_2b_2 & \ldots & a_2b_{n_2} \\ \vdots & \vdots & & \vdots \\ a_{n_1}b_1 & a_{n_1}b_2 & \ldots & a_{n_1}b_{n_2} \end{pmatrix},$$

столбцы которой принадлежат коду $\mathcal{C}_1$, а строки — $\mathcal{C}_2$. По линейности это верно для любой матрицы из пространства $\varphi(\mathcal{C})$. Следовательно, если $M \in \varphi(\mathcal{C}) \setminus \{0\}$, то в M есть столбец с весом не менее d_1, а значит есть не менее d_1 ненулевой строки. Вес каждой из этих строк не менее d_2, поэтому в матрице M не менее d_1d_2 ненулевых элементов. Значит, столько же ненулевых элементов содержит кодовое слово $\mathbf{c} = \varphi^{-1}(M) \in \mathcal{C} \setminus \{0\}$ и $||\mathbf{c}|| \geq d_1d_2$. Таким образом, $d(\mathcal{C}) \geq d_1d_2$. Выбирая $\mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2$ так, что $||\mathbf{a}|| = d_1$, $||\mathbf{b}|| = d_2$ получаем, что $||\mathbf{a} \otimes \mathbf{b}|| = d_1d_2$. Следовательно, $d(\mathcal{C}) = d_1d_2$. Осталось найти проверочную матрицу кода $\mathcal{C}$.

Условие $HG^T = 0$ выполнено по определению матриц G и H. Пусть для слова $\mathbf{c} \in \mathbb{F}^{n_1 n_2}$ выполнено равенство $H\mathbf{c}^T = 0$. Тогда для матрицы $M = \varphi(\mathbf{c})$ это означает, что выполнены равенства $H^{(1)}M = 0, H^{(2)}M^T = 0$. Из условия $H^{(2)}M^T = 0$ следует, что строки матрицы M являются линейными комбинациями строк матрицы $G^{(2)}$, поэтому $M = UG^{(2)}$ для некоторой матрицы $U \in M_{n_1,k_2}(\mathbb{F})$. Тогда $H^{(1)}M = H^{(1)}UG^{(2)} = 0$. Поскольку строки матрицы $G^{(2)}$ линейно независимы отсюда следует, что $H^{(1)}U = 0$. Это означает, что столбцы матрицы U принадлежат коду $\mathcal{C}_1$ и линейно выражаются через столбцы матрицы $G^{(1)}$. Тогда из равенства $M = UG^{(2)}$ заключаем, что матрица M является линейной комбинацией матриц $(\mathbf{a}_r^{(1)})^T \cdot \mathbf{a}_s^{(2)}$, а её прообраз слово $\mathbf{c}$ — линейной комбинацией слов $\mathbf{a}_r^{(1)} \otimes \mathbf{a}_s^{(2)}$, $r = 1, \ldots, k_1$, $s = 1, \ldots, k_2$, базисных для кода $\mathcal{C}$. Таким образом, $\mathbf{c} \in \mathcal{C}$. Значит, однородной системе с матрицей H удовлетворяют слова кода $\mathcal{C}$ и только они, поэтому H — проверочная матрица этого кода.

6°. Гибридный код

Определение 5.16. Пусть $\mathcal{C}_i$ — линейные $[n, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. *Гибридом кодов кодов* $\mathcal{C}_1$ *и* $\mathcal{C}_2$ называется код $\mathcal{C} = \mathcal{C}_1 \dashv \mathcal{C}_2 \in \mathbb{F}^{2n}$, состоящий из всех слов вида

$$(\mathbf{a}, \mathbf{a} + \mathbf{b}),\ \mathbf{a} \in \mathcal{C}_1, \mathbf{b} \in \mathcal{C}_2.$$

Предложение 5.17. Пусть $\mathcal{C}_i$ — линейные $[n, k_i, d_i]_q$-коды над полем $\mathbb{F}$, $i = 1, 2$. Тогда код $\mathcal{C} = \mathcal{C}_1 \dashv \mathcal{C}_2$ есть линейный $[2n, k_1 + k_2, d]_q$-код с $d = \min\{2d_1, d_2\}$.

◀ По построению очевидно, что $\mathcal{C}$ есть линейный $[2n, k_1 + k_2]_q$-код. Вычислим его расстояние. Сразу видно, что $d \leq \min\{2d_1, d_2\}$, поскольку в $\mathcal{C}$ есть слова $(\mathbf{a}, \mathbf{a})$ и $(0, \mathbf{b})$ с $||\mathbf{a}|| = d_1$ и $||\mathbf{b}|| = d_2$.

С другой стороны по неравенству треугольника получаем, что

$$||(\mathbf{a}, \mathbf{a} + \mathbf{b})|| = ||\mathbf{a}|| + ||\mathbf{a} + \mathbf{b}|| \geq ||\mathbf{a}|| + |||\mathbf{a}|| - ||\mathbf{b}|||\,.$$

Если $\mathbf{a} = 0$, то вес такого слова не меньше d_2.

Пусть $\mathbf{a} \neq 0$. Если $||\mathbf{b}|| \geq ||\mathbf{a}|| (> 0)$, то $||\mathbf{a}|| + |||\mathbf{a}|| - ||\mathbf{b}||| = ||\mathbf{b}|| \geq d_2$. Пусть $0 < ||\mathbf{b}|| < ||\mathbf{a}||$. Имеем $||(\mathbf{a}, \mathbf{a} + \mathbf{b})|| \geq ||\mathbf{a}|| > ||\mathbf{b}|| \geq d_2$, иначе $\mathbf{b} = 0$ и $||(\mathbf{a}, \mathbf{a})|| \geq 2d_1$. ▶

7°. Увеличение размерности с сохранением расстояния

Предложение 5.18. Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$ и $\mathbf{b} \in \mathbb{F}^n \setminus \mathcal{C}$ – слово, расстояние от которого до любого слова из кода $\mathcal{C}$ не меньше, чем $d-1$. Тогда код $\mathcal{C}'$, состоящий из всех слов вида

$$(\mathbf{a} + \alpha\mathbf{b}, \alpha),\ \mathbf{a} \in \mathcal{C}, \alpha \in \mathbb{F},$$

есть линейный $[n+1, k+1, d]$-код. Если G — порождающая матрица кода $\mathcal{C}$, то порождающей для $\mathcal{C}'$ будет, например, матрица $G' = \begin{pmatrix} G & \mathbf{0}^T \\ \mathbf{b} & 1 \end{pmatrix}$.

8°. Граница Грайсмера.

Далее будем использовать обозначение $\lceil x \rceil = \min\{i \in \mathbb{Z} : i \geq x\}$. Легко проверить, что если $a, b \in \mathbb{R}$ и $c \in \mathbb{N}$, то

$$\left\lceil \frac{a}{bc} \right\rceil = \left\lceil \frac{\left\lceil \frac{a}{b} \right\rceil}{c} \right\rceil. \tag{5.1}$$

Действительно, для любого $i \in \mathbb{Z}$ имеем

$$i \geq \frac{a}{bc} \Leftrightarrow ic \geq \frac{a}{b} \Leftrightarrow ic \geq \left\lceil \frac{a}{b} \right\rceil \Leftrightarrow i \geq \frac{\left\lceil \frac{a}{b} \right\rceil}{c}.$$

Теорема 5.19 (Граница Грайсмера)**.** Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$. Тогда

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil. \tag{5.2}$$

◀ 1. Обозначим через $N_q(k,d)$ наименьшее число N, для которого существует линейный код над $\mathbb{F}$ длины N размерности k, расстояние которого не меньше d. Заметим, что это определение корректно: достаточно рассмотреть код длины kd, состоящий из всех слов вида

$$(\underbrace{\alpha_1, \ldots, \alpha_1}_{d \text{ раз}}, \underbrace{\alpha_2, \ldots, \alpha_2}_{d \text{ раз}}, \ldots, \underbrace{\alpha_k, \ldots, \alpha_k}_{d \text{ раз}}), \quad \alpha_1, \ldots, \alpha_k \in \mathbb{F}.$$

Еще заметим, что функция $N_q(k,d)$ монотонна по второму аргументу: $N_q(k,d) \leq N_q(k,\tilde{d})$ при $d \leq \tilde{d}$.

2. Докажем следующее неравенство:

$$N_q(k,d) \geq d + N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right). \tag{5.3}$$

Пусть некоторый $[n, k, \tilde{d}]_q$-код с $n = N_q(n, d)$ и $\tilde{d} \geq d$ задаётся порождающей матрицей G ранга k, первая строка которой имеет вес $\tilde{d}$. Переходя к линейно эквивалентному коду, можем считать, что матрица G состоит из k строк и имеет вид

$$\left(\begin{array}{c|c} \overbrace{0\ldots0}^{n-\tilde{d}} & \overbrace{1\ldots1}^{\tilde{d}} \\ \hline G' & G'' \end{array}\right).$$

Заметим, что $\mathrm{rk}G' = k - 1$. Действительно, запишем строки матрицы G в виде $a_i = (a_i'|a_i'')$, $i = 1, \ldots, k$, где a_i' и a_i'' — строки матриц G' и G'', причём $a_1' = 0$. Допустим, что $\sum_{i=2}^{k} \lambda_i a_i' = 0$ для некоторых $\lambda_2, \ldots, \lambda_k \in P$. Положим $b = \sum_{i=2}^{k} \lambda_i a_i''$. Ясно, что для некоторого $\lambda \in \mathbb{F}$ имеем $||b - \lambda a_1''|| < \tilde{d}$. Следовательно,

$$||-\lambda a_1 + \sum_{i=2}^{k} \lambda_i a_i|| = ||-\lambda(a_1'|a_1'') + \sum_{i=2}^{k} \lambda_i (a_i'|a_i'')|| = ||(0|b - \lambda a_1'')|| < \tilde{d},$$

откуда $-\lambda a_1 + \sum_{i=2}^{k} \lambda_i a_i = 0$ и $\lambda_2 = \ldots = \lambda_k = 0$.

Пусть теперь d' — минимальное расстояние кода $\mathcal{C}'$, порождённого строками матрицы G'. Тогда в коде $\mathcal{C}$ содержится слово вида $(a|b)$, где $||a|| = d'$. Но в слове b длины $\tilde{d}$ над $\mathbb{F}$ хотя бы один символ, скажем, λ, встречается не менее чем $\left\lceil \frac{\tilde{d}}{q} \right\rceil$ раз (иначе число вхождений каждого символа меньше $\tilde{d}/q$, а сумма этих q чисел равна $\tilde{d}$). Значит, $||b - \lambda a_1''|| \leq \tilde{d} - \left\lceil \frac{\tilde{d}}{q} \right\rceil$. Имеем $\tilde{d} \leq ||(a|b) - \lambda a_1|| = d' + ||b - \lambda a_1''|| \leq d' + \tilde{d} - \left\lceil \frac{\tilde{d}}{q} \right\rceil$. Таким образом, $d' \geq \left\lceil \frac{\tilde{d}}{q} \right\rceil \geq \left\lceil \frac{d}{q} \right\rceil$, поэтому $n - d \geq n - \tilde{d} \geq N_q(k-1, d') \geq N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right)$, откуда сразу следует (5.3).

3. Теперь применим доказанное неравенство к $[n, k, d]_q$-коду

несколько раз. Имеем

$$n \geq N_q(k,d) \geq d + N_q\left(k-1, \left\lceil \frac{d}{q} \right\rceil\right) \geq$$
$$\geq d + \left\lceil \frac{d}{q} \right\rceil + N_q\left(k-2, \left\lceil \frac{\left\lceil \frac{d}{q} \right\rceil}{q} \right\rceil\right) \overset{(5.1)}{=}$$
$$= d + \left\lceil \frac{d}{q} \right\rceil + N_q\left(k-2, \left\lceil \frac{d}{q^2} \right\rceil\right) \geq \ldots \geq$$
$$\geq d + \left\lceil \frac{d}{q} \right\rceil + \ldots + \left\lceil \frac{d}{q^{k-2}} \right\rceil + N_q\left(1, \left\lceil \frac{d}{q^{k-1}} \right\rceil\right),$$

откуда
следует утверждение теоремы, поскольку, очевидно, $N_q(1,m) = m$ для любого натурального числа m.►

9°. Уменьшение длины кода

Предложение 5.20. Пусть $\mathcal{C}$ — линейный $[n,k,d]_q$-код над полем $\mathbb{F}$ и $\in \mathcal{C}$ – слово веса d с ненулевыми координатами в позициях $i_1,\ldots,i_d$. Тогда код $\overline{\mathcal{C}}$, получающийся из кода $\mathcal{C}$ вычеркиванием всех слов, пропорциональных $\mathbf{c}$, и вычёркиванием в остальных словах координат с номерами $i_1,\ldots,i_d$ есть линейный $[n-d,k-1,d_1]$-код, где $d_1 \geq \left\lceil \frac{d}{q} \right\rceil$. Если $\mathcal{C}$ — не МДР-код (т.е. $d \leq n-k$), то двойственный к коду $\overline{\mathcal{C}}$ код $\overline{\mathcal{C}}^\circ$ есть $[n-d, n-d-(k-1), d_0]$-код, где $d_0 \geq d(\mathcal{C}^\circ)$.

◄ Первое утверждение сразу следует из доказательства пункта 2 теоремы о границе Грайсмера.

Введённая в этом утверждении матрица G' будет проверочной для кода $\overline{\mathcal{C}}^\circ$, поэтому это линейный код длины $n-d$ и размерности $(n-d) - \mathrm{rk}G' = (n-d)-(k-1) \geq 1$, т.к. $d \leq n-k$.

Пусть G — порождающая матрица кода $\mathcal{C}$, она же будет проверочной матрицей для кода $\mathcal{C}^\circ$. Тогда по предложению о связи расстояния кода и гарантируемого ранга имеем $\varkappa(G) = d(\mathcal{C}^\circ) - 1$. И поскольку код и двойственный к нему являются МДР-кодами одновременно, то $\varkappa(G) < \mathrm{rk}G = k$. Таким образом, число $\varkappa(G)$ не превосходит числа $k-1$ столбцов матрицы G'. С учётом этого, из строения матрицы G видно, что в матрице G' любые $\varkappa(G)$ столбцов линейно независимы. Следовательно, $\varkappa(G') \geq \varkappa(G)$. В итоге получаем, что $d_0 \geq d(\mathcal{C}^\circ)$. ►

Следствие 5.21. Пусть $\mathcal{C}$ — линейный МДР-код $[n,k,d]_q$-код над полем $\mathbb{F}$ мощности q размерности $k \geq 2$. Тогда $d \leq q$ и $n \leq q+k-1$.

◀ Поскольку $\mathcal{C}$ — МДР-код, то $d = n-(k-1)$ и $n = d+k-1$. Поэтому в обозначениях предыдущего доказательства имеем, что матрица G' размера $(k-1)\times(k-1)$ имеет $\mathrm{rk}G' = k-1$. Следовательно, $\overline{\mathcal{C}} = \mathbb{F}^{k-1}$ и $d_1 = 1$. Откуда $\left\lceil \frac{d}{q} \right\rceil \leq 1$, $d \leq q$ и $n \leq q+k-1$. ▶

Задачи к лекции 5.

Задача 1. Определите кодовые параметры расширенного симплексного кода $S_P(k)^{ext}$ (см. последний пример Лекции 1). Будет ли он лежать на границе Плоткина?

Задача 2. Определите кодовые параметры расширенного двоичного кода Хэмминга $\mathcal{H}_2(l)^{ext}$. Будет ли он совершенным кодом?

Задача 3. Докажите, что для любых матриц $A \in M_{m,n}(\mathbb{F})$ и $B \in M_{k,l}(\mathbb{F})$ выполнено $\mathrm{rk}(A \otimes B) = \mathrm{rk}A \cdot \mathrm{rk}B$.

Задача 4. Приведите пример, когда тензорное произведение двух $[n,k]$ МДР-кодов тоже является МДР-кодом?

Задача 5. Прмените конструкцию из раздела 7 "Увеличение размерности с сохранением расстояния" к $[n,k]$ коду Рида–Соломона $\mathcal{C}$ с параметрами $x_1 = 0$, $x_2, \ldots, x_n$ — различные ненулевые элементы поля $\mathbb{F}$, $u_1 = \ldots = u_n = 1$ и слову $\mathbf{b} = (0, x_1^k, \ldots, x_n^k)$.

Задача 6. При каких значениях k код $\mathcal{C}'$ из предыдущей задачи является МДР-кодом?

Задача 7. Приведите пример кода, лежащего на границе Грайсмера.

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.