Дубна, 20-24.07.2016 Курс "Линейные коды"
"Современная м-ка"

Лекция №1

1 Основные задачи теории кодирования

$$\{\text{слова длины } k\} \xrightarrow[\text{(инъективно)}]{\text{кодирование}} \{\text{слова длины } n,\ n \geq k\}$$

(сообщения) (кодовые слова)

$\downarrow$ передача с шумами

$\{$слова длины $n\}$

$\downarrow$ исправление ошибок (декодирование)

$$\{\text{сообщение}\} \xleftarrow[\text{сообщения}]{\text{восстановл.}} \{\text{кодовые слова}\}$$

Простейший код: Кратное повторение: $\underbrace{abc}_{k} \to \underbrace{abcabcabc}_{n}$

отображение $\varphi_{k,m}$

$\downarrow$ abcabcacc

$\downarrow$ abc $\leftarrow$ abcabcabc

$\varphi_{k,m}(a_1 \dots a_k) = \underbrace{a_1 \dots a_k \dots a_1 \dots a_k}_{m \text{ раз}}$, $n = mk$

abc $\to$ abcabcabcabcabc – исправляет 2 ошибки, но не 3:

$\underbrace{\text{abcabcaccaccacc}}_{3\text{ искажения}} \xrightarrow{\text{декод}}$ accaccaccaccacc, что неправильно.

Пусть A – некот. алфавит и A^n – мн-во слов длины n над A.

Опр Расстояние Хэмминга на A^n: $v = (v_1, .., v_n)$, $w = (w_1, .., w_n)$, $v_i, w_j \in A$

$d(v,w) = \#\{i \mid v_i \neq w_i\}$

Опр Метрика на мн-ве X это отображ. $\mu: X \times X \to \mathbb{R}_{\geq 0}$:

1) $\mu(x,y) = 0 \Leftrightarrow x = y$; 2) $\mu(x,y) = \mu(y,x)$ $\forall x, y \in X$;

3) $\mu(x,y) \leq \mu(x,z) + \mu(z,y)$ $\forall x,y,z \in X$ [нер-во треугольника].

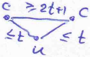
Утв $d(\cdot,\cdot)$ определяет метрику на A^n.

$\square$ 1), 2) очевидно; 3) упражн.

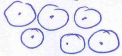
Опр Пусть $C \subseteq A^n$ – подмн-во, которое мы считаем мн-вом кодовых слов, или просто кодом. Говорят, что код C исправляет t ошибок, если $\forall c, c' \in C$, $c \neq c'$ шары $B_t(c) = \{v \in A^n \mid d(c,v) \leq t\}$ и $B_t(c')$ не пересекаются. Другими словами, от $\forall u \in A^n$ на расст. $\leq t$ лежит не более одной точки из C.

Опр Пусть $d(C) = \min\limits_{\substack{c,c'\in C \\ c\ne c'}} d(c,c')$.

Тв Если $d(C)\ge 2t+1$, то код C исправляет t ошибок.

□ От против. Пусть $u \in B_t(c)\cap B_t(c')$. Тогда  — противоречие с нер-вом треуг. ■

Опр Код $C\in A^n$ назыв. совершенным, если $\exists\, t\in\mathbb{N}: A^n = \bigsqcup\limits_{c\in C} B_t(c)$



Ограничение: A — конечное поле

(2) Конечные поля Опр Поле $(F,+,\cdot)$ — мн-во с двумя бинар. операциями

сложение: ассоц. $a+(b+c)=(a+b)+c$; коммут $a+b=b+a$); нейтр эл-т 0: $0+a=a$

обрат. эл-т $\forall a\ \exists -a:\ a+(-a)=0$ [абелева группа по сложению]

умнож.: ассоц. $a(bc)=(ab)c$; коммут $ab=ba$; нейтр эл-т 1: $a\cdot 1=a$

обрат. эл-т $\forall a\ne 0\ \exists a^{-1}:\ a\cdot a^{-1}=1$ [т.е. $F\setminus\{0\}$ — абел. группа по умнож.]

связь: дистрибут: $a(b+c)=ab+ac$

Конечное поле — поле из конеч. числа эл-ов

Пример $\mathbb{Z}_p=\{\bar0,\bar1,\dots,\overline{p-1}\}=\mathbb{Z}/(p)$, p — простое

$\forall \bar a\in\mathbb{Z}_p\setminus\{0\}$ $\bar a\cdot\bar1,\ \bar a\cdot\bar2,\ \dots,\ \bar a\cdot\overline{p-1}$ — попарно разные $\Rightarrow \exists\,\bar b:\ \bar a\bar b=\bar1$

В $\mathbb{Z}_n$, n непростое $n=rs \Rightarrow \bar r\bar s=\bar0$ (делит. нуля), $\underbrace{\bar r^{-1}\bar r\cdot\bar s}_{\bar s}=\bar r^{-1}\bar0=\bar0$ — противор.

Есть ли другие поля?

Пусть $\mathbb{F}_q$ — поле из q эл-ов $\Rightarrow 0,\ 1,\ 1+1,\ 1+1+1,\ \dots\in\mathbb{F}_q$

Тогда $\underbrace{1+\ldots+1}_{m} = \underbrace{1+\ldots+1}_{r} \Rightarrow \underbrace{1+\ldots+1}_{m-r} = 0$ Пусть p – наименьшее

число: $\underbrace{1+\ldots+1}_{p} = 0$ (характеристика поля). ~~char~~ $\mathbb{F}_q$

Лемма p – простое

$\square$ Если $p = p_1 \cdot p_2$, то $\underbrace{1+\ldots+1}_{p} = 0 = \underbrace{(1+\ldots+1)}_{p_1}\underbrace{(1+\ldots+1)}_{p_2}$ – делит. нуля противор $\blacksquare$

Итак, $\{\overline{0}, 1, 1+1, \ldots, \underbrace{1+1+\ldots+1}_{p-1}\} = \mathbb{Z}_p \subseteq \mathbb{F}_q$

Теорема $q = p^n$ для некот. натур. n

$\square$ Выберем в $\mathbb{F}_q$ базис как в вект. пр-ве над $\mathbb{Z}_p$: $e_1, \ldots, e_n$ Тогда

$\forall a \in \mathbb{F}_q \ \exists! \ \alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p : a = \alpha_1 e_1 + \ldots + \alpha_n e_n \Rightarrow |\mathbb{F}_q| = q = p^n$ $\blacksquare$

Как построить поле из p^n эл-ов?

Пусть $h(x)$ – ~~неприв~~ мн-н степени n над $\mathbb{Z}_p$. Рассмотрим многочлены $\mathbb{Z}_p[x]$ по модулю $h(x)$: эл-ты это остатки по модулю $h(x)$, которые складываются как обычно, а умнож. по модулю $h(x)$.

Обозн. $\mathbb{Z}_p[x]/(h(x))$ – здесь p^n эл-ов: $\alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1}$.

Опр $h(x)$ неприводим, если $h(x) = h_1(x) h_2(x) \Rightarrow h_1(x) = const$ или $h_2(x) = const$

Теорема $\mathbb{Z}_p[x]/(h(x))$ – поле $\Leftrightarrow$ $h(x)$ неприв.

$\square$ $(\Rightarrow)$ иначе делит. нуля $(\Leftarrow)$ если $a(x)$ – ненулевой остаток, то $\text{НОД}(a(x), h(x)) = 1 \Rightarrow \exists u(x), v(x) : a(x)u(x) + h(x)v(x) = 1$ – обратный ход в алг. Евкл. $\Rightarrow \overline{a(x)}\ \overline{u(x)} = \overline{1} \Rightarrow \overline{a(x)}^{-1} = \overline{u(x)}$ $\blacksquare$

Пример x^2+x+1 неприв. над $\mathbb{Z}_2 \Rightarrow \mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$

Эл-ты: $\{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$

	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Теорема $\forall$ простого p и $\forall$ натур. n $\exists!$ поле $\mathbb{F}_q$ из $q = p^n$ эл-ов.

Схема док-ва: 1) В группе $(\mathbb{F}_q \setminus \{0\}, \times)$ $q-1$ элемент $\Rightarrow a^{q-1} = 1$ $\forall a \in \mathbb{F}_q \setminus \{0\}$ $\Rightarrow$ все эл-ты поля явл. корнями мн-на $x^q - x$ над $\mathbb{Z}_p$ $\Rightarrow$ $\mathbb{F}_q$ совпадает с полем разл. этого мн-на $\Rightarrow$ $\mathbb{F}_q$ единств.

2) Рассм. $q=p^n$ и мн-н x^q-x над $\mathbb{Z}_p$. Существует поле F, большее $\mathbb{Z}_p$, в котором x^q-x имеет ровно q корней. Сумма и произв. корней вновь корень $\Rightarrow$ ~~также~~ все эти корни образуют в F подполе $\mathbb{F}_q$ из q элементов ■ 4

Полезный факт В конечном поле $\mathbb{F}_q$ $\exists$ эл-та: $\mathbb{F}_q=\{0,1,a,a^2,\dots,a^{q-2}\}$

Примеры $\mathbb{Z}_5=\{0,1,2,\underset{4}{2^2},\underset{3}{2^3}\}$. Элемент a называется примитивным

$\mathbb{F}_4=\{\bar{0},\bar{1},\bar{x},\underset{x+1}{\bar{x}^2}\}$

Теорема $\forall$ простого p и $\forall$ натур. n $\exists$ неприв. мн-н степени n над $\mathbb{Z}_p$.

□ Дост. взять миним. мн-н $\mu_a(x)$ для примитив. эл-та $a\in\mathbb{F}_q$ ■

Следствие $\mathbb{F}_q \cong \mathbb{Z}_p[x]/(h(x))$, где $h(x)$ - неприв. мн-н степени n над $\mathbb{Z}_p$.

Пример Мн-ны x^3+x^2+1 и x^3+x+1 неприв. над $\mathbb{Z}_2$

Тогда $\mathbb{Z}_2[x]/(x^3+x^2+1)$ и $\mathbb{Z}_2[x]/(x^3+x+1)$ - две реализации поля $\mathbb{F}_8$.

Лекция №2

3) Линейная алгебра над $\mathbb{F}_q$:

Арифм. вект. пр-во $\mathbb{F}_q^n = \{(x_1, .., x_n) \mid x_i \in \mathbb{F}_q\}$

~~1) Сложение~~
$u = (u_1, .., u_n)$
$v = (v_1, .., v_n)$
$u + v = (u_1 + v_1, .., u_n + v_n)$
2) умнож. на скаляр
$\lambda \in \mathbb{F}_q$ $\lambda u = (\lambda u_1, .., \lambda u_n)$

Базис — набор $\{u_1, .., u_n\}$ такой что $\forall u \in \mathbb{F}_q^n$
$\exists!\ \alpha_1, .., \alpha_n \in \mathbb{F}_q : u = \alpha_1 u_1 + .. + \alpha_n u_n$

Пример Станд. базис $e_1 = (1, 0, .., 0), .., e_n = (0, .., 0, 1)$

Посчитаем: $\# \mathbb{F}_q^n = q^n$, число базисов $= (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$

Подпр-во: подмн-во $U \subseteq \mathbb{F}_q^n$: 1) $\forall u, u' \in U$ $u + u' \in U$
2) $\forall \lambda \in \mathbb{F}_q, u \in U$ $\lambda u \in U$.

Пример Мн-во решений одн. СЛУ $\begin{cases} a_{11}x_1 + .. + a_{1n}x_n = 0 \\ - - - - - \\ a_{s1}x_1 + .. + a_{sn}x_n = 0 \end{cases} \subseteq \mathbb{F}_q^n$ — подпр-во

Базис подпр-ва: $u_1, .., u_k \in U$, $\dim U = k$.

Число подпр-в размерности k в $\mathbb{F}_q^n$: $\dfrac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}$

4) Линейный код (ограничение 2)

Мн-во сообщений $= \mathbb{F}_q^k$

Код = подпр-во $C \subseteq \mathbb{F}_q^n$, $\dim C = k$

Кодирование — линейное отображ. $\varphi: \mathbb{F}_q^k \to \mathbb{F}_q^n$, $\mathrm{Im}\,\varphi = C$
$\varphi(\lambda_1 u_1 + .. + \lambda_k u_k) = \lambda_1 \varphi(u_1) + .. + \lambda_k \varphi(u_k)$

$\varphi: \mathbb{F}_q^k \to C$ — биекция

Пример Кратное повторение
$\varphi_{k,m}: \mathbb{F}_q^k \to \mathbb{F}_q^n$, $n = m \cdot k$
$\varphi_{k,m}(a_1, .., a_k) = \underbrace{(a_1, .., a_k, .., a_1, .. a_k)}_{m \text{ раз}}$ ← C — подпр-во таких векторов, задается очевидной ОСЛУ

Опр Пусть $u \in \mathbb{F}_q^n$. Вес Хэмминга вектора $u \in \mathbb{F}_q^n$:
$$wt(u) = \#\{i \mid u_i \neq 0\}$$

Утв Пусть $C \subseteq \mathbb{F}_q^n$ — подпр-во. Тогда $d(C) = \min\limits_{u \in C \setminus \{0\}} wt(u)$.

□ С одной стороны, $wt(u) = d(0, u)$. С другой, $d(u, v) = wt(u - v)$
Поэтому $\min\limits_{u \neq v} d(u, v) = \min\limits_{u \neq 0} wt(u)$ ■ | Выигрыш от этого: не надо перебирать все пары!

Пример Для кода $\varphi_{k,m}$ имеем $d(C) = m = \frac{n}{k}$ => исправл. $\left[\frac{m-1}{2}\right]$ ошибок.

Характеристики кода: $[n, k, d]_q$ — код

длина, размерн, наим. расстояния, порядок поля

Цель: фиксируем q, k, n. Найти k-мерное подпр-во $C \subseteq \mathbb{F}_q^n$ для которого $d(C)$ максимально.

Другими словами, пусть $d(n,k,q) = \max\limits_{\substack{C \subseteq \mathbb{F}_q^n \\ \dim C = k}} d(C)$ → чему равно? → на каких подпр-вах реализуется?

Пример $n=4, k=2, q=2$ $C = \{(0,0,0,0), (1,1,0,0), (0,0,1,1), (1,1,1,1)\} \subseteq \mathbb{F}_2^4$

Можно показать, что $d(4,2,2) = 2$

Кодирование — как находить $\varphi(v) \in \mathbb{F}_q^n$, где $v \in \mathbb{F}_q^k$?

Лин. отображ. задаются матрицей: $\varphi(v) = (v_1, .., v_k) \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} = vG$

Опр Матрица G назыв. порождающей матрицей кода C, её строки — координаты образов $e_1, .., e_k \in \mathbb{F}_q^k$ в $\mathbb{F}_q^n$ — базис в Ив

Опр Проверочная матрица кода C — это матрица H размера $(n-k) \times n$ т.ч. $\forall v \in \mathbb{F}_q^n$ $Hv = 0 \Leftrightarrow v \in C$.

Как её построить? Составим СЛУ $xG = 0$. Пр-во решений системы имеет размерность $n - \operatorname{rk} G = n-k$. Пусть $\omega_1, .., \omega_{n-k}$ базис пр-ва решений. Тогда $H = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_{n-k} \end{pmatrix}$ — строки.

Замеч $d(C) = s+1$, где ~~s — max число л/н столбцов в H~~. $\forall s$ столбцов в H л/н и s — max с этим св-вом.

Опр Синдромом вектора $u \in \mathbb{F}_q^n$ от-но кода $C \subseteq \mathbb{F}_q^n$ назыв. вектор $Hu \in \mathbb{F}_q^{n-k}$. Ясно, что $u \in C \Leftrightarrow$ синдром$(u) = 0$.

5 Идеальный пример: Код Хэмминга $[7,4,3]_2$: $\mathbb{F}_2^4 \to \mathbb{F}_2^7$

$$G = \begin{pmatrix} 1&0&0&0&1&0&1 \\ 0&1&0&0&1&1&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{pmatrix} \quad (x_1,x_2,x_3,x_4) \to (x_1,x_2,x_3,x_4,x_1+x_2+x_3,x_2+x_3+x_4,x_1+x_2+x_4)$$

$$H = \begin{pmatrix} 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{pmatrix}$$ Синдром $$S(v) = \begin{pmatrix} x_1+x_2+x_3+x_5 \\ x_2+x_3+x_4+x_6 \\ x_1+x_2+x_4+x_7 \end{pmatrix}$$

Ясно, что $d \le 3$. Если сложить ≥ 3 строк в G, то уже из первых 4-х коор. получим 3 единицы $\Rightarrow d=3 \Rightarrow t=1$.

Декодирование: 8 значений синдрома

Это совершенный код: 2^7 точек распались на 2^4 шаров по 8 точек в каждом ($1+7$ позиций для замены)

000	OK
100	x_5
010	x_6
001	x_7
110	x_3
101	x_1
011	x_4
111	x_5

какую переменную изменить.

Общий код Хэмминга: на каждой прямой в $\mathbb{F}_q^m$ возьмем по одному ненулевому вектору и составим из них матрицу H:

$$H = m\underbrace{\Big(\,|\,|\,|\,|\,|\,|\,|\,|\,\Big)}_{n=\frac{q^m-1}{q-1}}$$ $\mathrm{rk}\, H = m \Rightarrow \dim C = k = n-m$

– получаем $[n, n-m]_q$-код.

Столбцы попарно независимы $\Rightarrow d=3 \Rightarrow t=1$.

Утв Код Хемминга $[n, n-m, 3]_q$ совершенен.

□ Всего точек q^n, имеем q^{n-m} шаров по $(q-1)n+1 = q^m$ точек в каждом ■

В исходном примере: $m=3$, $q=2$, $n=\frac{2^3-1}{2-1}=7$, $k=7-3=4$.

6 Автоморфизмы и изометрии кодов

: $GL_n(q)$ – группа невырожд. матриц.

$P_n(q)$ – группа перестановок координат, $|P_n(q)| = n!$

$D_n(q)$ – подгруппа диагональных матриц в $GL_n(q)$, $|D_n(q)| = (q-1)^n$

$Iso_n(q) = P_n(q) \ltimes D_n(q)$ – перест. коорд. и их умнож. на ненул. скаляры

Предл Пусть $\varphi: \mathbb{F}_q^n \to \mathbb{F}_q^n$ – лин. отображ. Тогда

$d(u,v) = d(\varphi(u), \varphi(v))\ \forall u,v \in \mathbb{F}_q^n \Leftrightarrow \varphi \in Iso_n(q)$.

□ Ясно, что $Iso_n(q)$ сохр. расст. Хэмминга. Обратно, возьмем $u=0$, $v=e_i \Rightarrow \varphi(e_i) = \lambda e_j \Rightarrow \varphi \in Iso_n(q)$ ■

С точки зрения порожд. матрицы G

$P_n(q)$ – перестановки столбцов, $D_n(q)$ – умнож. столбцов на число

Опр Код $C \subseteq \mathbb{F}_q^n$ эквивал. (соот. изометричен) коду $C' \subseteq \mathbb{F}_q^n$ (8)
если $C' = \varphi(C)$ для некот. $\varphi \in P_n(q)$ (соот. $\varphi \in \mathrm{Iso}_n(q)$).

Опр $\mathrm{Aut}(C) = \{\varphi \in P_n(q) \mid \varphi(C) = C\}$

$\mathrm{Iso}(C) = \{\varphi \in \mathrm{Iso}_n(q) \mid \varphi(C) = C\}$

7) **Дуальный код** Пусть $u, v \in \mathbb{F}_q^n$. Определим $\langle u,v \rangle = u_1v_1 + \ldots + u_nv_n$

Для подпр-ва $C \subseteq \mathbb{F}_q^n$ положим $C^\perp = \{u \in \mathbb{F}_q^n \mid \langle u,v\rangle = 0 \ \forall v \in C\}$

Порожд. матрица для $C \Leftrightarrow$ провер. матрица для $C^\perp$. $(C^\perp)^\perp = C$

Если C – это $[n,k]_q$-код, то $C^\perp$ это $[n, n-k]_q$-код. Чему равно $d(C^\perp)$?

Для этого полезно знать полное распред. C по весам:

$wt_i(C) = \#\{u \in C \mid wt(u) = i\}$, $F_C(x,y) = \sum_{i=0}^{m} wt_i(C)\, x^i y^{m-i}$

> весовая ф-я кода

Тождество Мак-Вильямса Если C – это $[n,k]_q$-код, то

$F_{C^\perp}(x,y) = q^{-k} F_C(y-x, y+(q-1)x)$.

Пример Бинарный $(q=2)$ код Хэмминга C_m длины $n = 2^m - 1$
и размерности $n-m$. Проверочная матрица для C_m: столбцы –
– все 2^m-1 ненул. векторов в $\mathbb{F}_2^m$ – она же порожд. для $C_m^\perp$

$\Rightarrow$ код $C_m^\perp$ состоит из нулевого вектора и 2^m-1 векторов веса 2^{m-1}

$$\Rightarrow F_{C_m^\perp}(x,y) = y^{2^m-1} + (2^m-1)\, x^{2^{m-1}} y^{2^{m-1}-1}$$

Отсюда по тождеству Мак-Вильямса можно вычислить F_{C_m}

Например, $F_{C_3}(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7$

– по 1 точке весов 0 и 7 и по 7 точек весов 3 и 4.

Лекция №3

8) Пять способов найти $d(C)$

Способ №1 Полный перебор q^k-1 ненул. векторов – поиск наим. веса

Упрощ. 1) не надо рассм. пропорц. вектора – делим на $q-1$;

2) если знаем автоморф. кода, перебор меньше;

3) из C и $C^\perp$ выбираем тот, у кого размер. меньше, и используем тождество Мак-Вильямса.

Способ №2 Линейная алгебра: $d(C) = \min$ число л/з столбцов пров. матр. H

М.сл. $G = (E_k \mid \underset{k\times(n-k)}{G'}) \Rightarrow H = ((-G')^T \mid E_{n-k})$ (＊просто из уст. $G\cdot H^T=0$＊)

⇓

кодирование в дописывании + мин. комбин. r строк G имеет вес $\geq r$.

Способ №3 Проективные системы

Опр Код невырожден если в G нет нулевых столбцов

Тогда столбцы $G \to$ точки в $\mathbb{P}^{k-1} \to$ "проективная система" (мультимн-во)

Система невырождена, если все её точки не лежат в гиперпл-ти в $\mathbb{P}^{k-1}$.

Два кода ~~эквивалентны~~ изометричны $\Leftrightarrow$ один получается из другого перестан. координат и умнож. на ненул. числа.

Две проект. сист. эквивалентны $\Leftrightarrow$ одна переводится в другую действием $PGL_k(q)$

Тогда $\left\{\begin{matrix}\text{классы ~~эквивал.~~ изометрии} \\ \text{невырожд. } [n,k]_q\text{-кодов}\end{matrix}\right\} = \left\{\begin{matrix}\text{классы эквивал. невырожденных проективных} \\ \text{систем и точек в } \mathbb{P}^{k-1}\end{matrix}\right\}$

Теорема $d(C_X) = n - \max\limits_H \{\#(X\cap H) : H \subseteq \mathbb{P}^{k-1} \text{ – гиперпл-ть}\}$

□ число нулей в строке с учетом действия $PGL_k = \#(X\cap H)$ ■

$\uparrow$ коор$=0$

~~Упр~~ Упр $d_r(C_X) = n - \max\limits_H \{\#(X\cap H) : H \subseteq \mathbb{P}^{k-1} \text{ – пл-ть коразмер. } r\}$

Способ 4 Конфигурация гиперплоскостей

С каждым столбцом g_i порожд. матрицы G невырожд. кода C свяжем гиперпл-ть $H_i \subseteq \mathbb{F}_q^k : \langle g_i, x\rangle = 0$.

Если $c = xG$ – кодовое слово, то $wt(c) = n - \#\{i \mid x \in H_i\}$

Найти $d(C)$ = найти точку $x \in \mathbb{F}_q^k \setminus \{0\}$, которая лежит в max числе H_i.

(H_i могут повторяться)

Способ 5: Алгебра: базисы Гребнера.

Пусть $L_i(x) = \langle g_i, x\rangle = 0$ – ур-е гиперпл-ти H_i. Тогда кодирование

$\mathbb{F}_q^k \ni x \mapsto xG = (L_1(x), \ldots, L_n(x)) = c$.

Рассмот. кольцо мн-в $\mathbb{F}_q[x_1, \ldots, x_k]$ и идеал J_s, порожд. всеми однород. мн-ми степени s. Пусть $I_s = \left(\prod_{e=1}^{s} L_{i_e}(x) \mid 1 \le i_1 < \ldots < i_e \le n\right)$.

Ясно, что $I_s \subseteq J_s$.

Утв Мн-во нулей $Z(I_s) = \{x \in \mathbb{F}_q^k \mid wt(c) < s,\ c = xG\}$

□ $x \in Z(I_s) \Leftrightarrow$ нельзя найти s лин. форм из $L_1, \ldots, L_n$, которые в точке x не равны 0 $\Leftrightarrow$ у c менее s ненул. коорд. ■

Следств $d(C) = \min\{s \in \mathbb{N} \mid Z(I_{s+1}) \neq \{0\}\}$

Для проверки этого условия можно использ. алгоритм Бухбергера из теории базисов Гребнера

Замечание Иногда ясно, что $I_s = J_s$, и тогда $Z(I_s) = \{0\}$.

9 Циклические коды

Опр Код $C \subseteq \mathbb{F}_q^n$ циклический, если $(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

$\mathbb{F}_q^n \ni (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$

Тогда $x \cdot (c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}) = c_{n-1} + c_0 x + \ldots + c_{n-2}x^{n-1}$

$\Rightarrow$ циклические коды в $\mathbb{F}_q^n \Leftrightarrow$ идеалы в $\mathbb{F}_q[x]/(x^n-1)$

Все такие идеалы главные и соотв. делителям мн-на $x^n - 1$ над $\mathbb{F}_q$

Пусть $g(x)$ делит $x^n - 1$. Тогда $C = \{c(x) \mid c(x) = r(x)g(x),\ r(x) \in \mathbb{F}_q[x]\}$

Пусть ~~мн~~ $x^n - 1 = g(x)h(x) \Rightarrow$ можно заменить $r(x)$ на остаток от деления на $h(x)$ (все равно $g(x)h(x) = 0 \pmod{x^n - 1}$) $\Rightarrow \deg r(x) < \deg h(x)$

$\Rightarrow \boxed{k = n - \deg g(x)}$

Мн-н $g(x)$ назыв. порождающим, а $h(x)$ – проверочным:

$c(x) \in C \Leftrightarrow c(x)h(x) = 0 \pmod{x^n - 1}$

(10) **Алгоритм декодирования** Пусть $C \subseteq \mathbb{F}_q^n$ это k-мерный код, исправ. t ошибок. Для любой точки $u \in \mathbb{F}_q^n$ нам надо либо найти (единств.) точку у C на расст. $\le t$ от u, либо указать, что такой точки нет.

Опр Смежный класс элемента $u \in \mathbb{F}_q^n$ по C это подмн-во

$u + C = \{u+c \mid c \in C\} \subseteq \mathbb{F}_q^n$

Замеч $u' \in u+C \Leftrightarrow Hu = Hu' \Leftrightarrow S(u)=S(u')$

Опр Лидер смеж. класса $u+C$ это такой $u_0 \in u+C$, что $wt(u_0) \le wt(u')$ $\forall u' \in u+C$

Пример Лидер C это 0.

$\forall u' \in u+C$ расст. от u' до C равно $wt(u_0)$ и ближайший эл-т к u' это $u'-u_0$

Если код исправляет t ошибок и $wt(u_0) \le t$, то лидер сн. класса единств.

Алгоритм Шаг 1 В каждом смеж. классе $u+C$ находим лидер

Шаг 2 Для данного $u \in \mathbb{F}_q^n$ если $wt(u_0) > t$, то произошло больше t ошибок, а если $wt(u_0) \le 0$, то $v = u - u_0$ — результат декодирования.

Пример Для $[7,4,3]_2$-кода Хэмминга лидеры сн. классов это $(0,..,0), (1,..,0), \ldots (0,..,0,1)$.

Пример $[50,20]_2$-код имеет $2^{30} \sim 10^9$ смеж. классов — нужны другие алгоритмы.

(11) **Коды Голея** **Теорема** Пусть q — степень простого числа и $[n,k,d]_q$-код C (линейный или нет) является совершенным $\Leftrightarrow$ либо $k=0$, либо $k=n$, либо $q=2$, $k=1$, $n=d$ нечетно, либо параметры совпадают с параметрами кодов Хэмминга $\left[n=\frac{q^m-1}{q-1}, n-m, 3\right]_q$, либо кодов Голея $[23,12,7]_2$ или $[11,6,5]_3$.

Тернарный код Голея C_{11} : $[11,6,5]_3$ — циклич. код с порождающим многочленом $x^5+x^4-x^3+x^2-1$ (делит $x^{11}-1$ над $\mathbb{F}_3$)

Вес 5 уже у порождающего мн-на. Группа автоморфизмов — ~~гр~~ группа Матье M_{11}, простая группа порядка $11\cdot 10\cdot 9\cdot 8$, действует 4-транзитивно.

Опр Система Штейнера $S(a,b,c)$ – набор b-элементных подмн-в (блоков) в c-элементном мн-ве X, такой что $\forall a$-элемент. подмн-во в X содержится ровно в одном блоке.

Пример Точки на прямых в $\mathbb{P}^2(\mathbb{F}_q)$ образуют $S(2, q+1, q^2+q+1)$

Утв Слова веса 5 образуют $S(4,5,11)$

Код совершенен: шары радиуса $\frac{d-1}{2} = 2$ с центрами в C_{11} покрывают все $\mathbb{F}_3^{11}$.

поскольку у слов min веса $\Sigma x_i \neq 0$

Его расширение C_{12} (добавляет 12-ю коор $= x_1 + \ldots + x_{11}$) – это $[12,6,6]_3$-код

Она самодвойств., $Aut(C_{12}) = M_{12}$, $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, 5-транзит.,

слова веса 6 образуют $S(5,6,12)$.

Бинарный код Голея C_{23} : $[23,12,7]_2$, циклич. с многочленом

$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$, $Aut(C_{23}) = M_{23}$, $|M_{23}| = 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$

4-транзит., слова веса 7 образуют $S(4,7,23)$, соверш: шары радиуса 3 покрывают $\mathbb{F}_2^{23}$.

Расширение C_{24} : $[24,12,8]_2$-самодвойст. код, $Aut(C_{24}) = M_{24}$,

(добавляем 24й бит четности) $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$, слова веса 8

образуют $S(5,8,24)$, группа 5-транзитивна.

12 Алгеброгеометрические коды

Рассмотрим систему однород. ур-й $\begin{cases} u_1(z_1,..,z_k)=0 \\ \vdots \\ u_m(z_1,.., z_k)=0 \end{cases}$ в $\mathbb{P}_q^{k-1}$. Мн-во её

решений образует проектив. систему. Если эта система невырождена,

получаем $[n,k]_q$-код $\begin{pmatrix} \vdots & | & | & | & | & | & | \\ \vdots & | & | & | & | & | & | \end{pmatrix}$, где n – число решений

Идея: использовать геометрию мн-я на нахожд. характеристик кода и декодирования.

Классический случай: кривые

Мы рассмотрим грассманиан $Gr(s,m)$: мн-во s-мерных подпр-в в $\mathbb{F}_q^m$.

$U = \langle v_1,..,v_s \rangle \subseteq \mathbb{F}_q^m \rightsquigarrow \langle v_1 \wedge \ldots \wedge v_s \rangle \in \mathbb{P}(\Lambda^s \mathbb{F}_q^m) = \mathbb{P}^{C_m^s - 1}$

Пусть $e_1,..,e_m$ – станд. базис в $\mathbb{F}_q^m$. Тогда коорд. точки $v_1 \wedge \ldots \wedge v_s$ в базисе

$\{e_{i_1} \wedge \ldots \wedge e_{i_s}\}$ в $\Lambda^s \mathbb{F}_q^m$ – это миноры $s \times s$ матрицы $s\begin{pmatrix} \overset{v_1}{\text{—}} \\ \overset{v_2}{\text{—}} \\ \underset{m}{\cdots} \end{pmatrix}$

Эти координаты удовлетвор. квадратич. соотнош. Плюккера.

Примеры $Gr(1,m) = Gr(m-1,m) = \mathbb{P}^{m-1}$

$Gr(2,4) \subseteq \mathbb{P}^5$ задан ур-ем $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0$ (квадрика Плюккера)

Число Плюккеровых координат: $C_m^s =: k$.

Число точек на $Gr(s,m)$: $\dfrac{(q^m-1)(q^m-q)\dots(q^m-q^{s-1})}{(q^s-1)(q^s-q)\dots(q^s-q^{s-1})} =: n$

Пример Для $Gr(2,4)$ над $\mathbb{F}_2$: $k = \frac{4!}{2!2!} = 6$, $n = \frac{(2^4-1)(2^4-2)}{(2^2-1)(2^2-2)} = \frac{15\cdot 14}{3\cdot 2} = 35$

Теорема (Ryan - Ноган) $\underset{(q=2)}{}$ $\underset{q\text{ любое}}{}$ $\boxed{d(C) = q^{(m-s)\cdot s}}$

(q=2) q любое

В случае $Gr(2,4)$ над $\mathbb{F}_2$ $d(C) = 2^{2\cdot 2} = 16 \rightsquigarrow t=7$: код переводит сообщ. длины 6 в слово длины 35 и исправляет 7 ошибок

(очень близко к границе Плоткина)

Замечание Методом крат. повтор. для исправления 7 ошибок сообщение длины 6 нужно повторить 15 раз, т.е. длина будет не 35, а 90!

Ryan - Ryan (1990): описание векторов в C мин. веса $d(C) = 2^{(m-s)\cdot s}$

(q=2)

Таких векторов ровно $n = |Gr(s,m)| = |Gr(m-s,m)|$, и они находятся в биекции с подпр-ми $U \in Gr(m-s,m)$. А именно, рассм. отображе.

$$\varphi_U : Gr(s,m) \to \mathbb{F}_2, \quad V \to \begin{cases} 1, & \text{если } V \cap U = \{0\} \\ 0, & \text{иначе} \end{cases}$$

Тогда $U \rightsquigarrow (\varphi_U(V_1), \dots, \varphi_U(V_n))$, где $V_1, \dots, V_n$ — все s-мерн. подпр-ва в $\mathbb{F}_2^m$. Нужно понять, что (1) вес вектора равен $2^{(m-s)s}$; (2) вектор лежит в C; (3) других векторов min веса нет.

Поймем (1): н.сч. $U = \langle e_{s+1}, \dots, e_m \rangle$, $V = \left(\begin{array}{ccc|ccc} 1 & & 0 & * & \dots & * \\ & \ddots & & \dots & & \dots \\ 0 & & 1 & * & \dots & * \end{array}\right)$, $\underbrace{\;}_{E_s}$ $\underbrace{* \dots *}_{m-s \text{ любые}}$

$\Rightarrow 2^{(m-s)\cdot s}$ таких подпр-в V что $V \cap U = \{0\}$

$\Rightarrow$ ровно $2^{(m-s)\cdot s}$ ненул. коор. у вектора $(\varphi_U(V_1), \dots, \varphi_U(V_n))$.