Подгруппа автоморфизмов и (1)

веса $d(C_{QR}(p))$. 29.11.2021

$p=7$ $C_{QR}(p)$ = код Хэмминга $H_4^{(7)}$

$p=23$ $C_{QR}(p)$ = код Голея G_{23} типа $[23, 12; 7]$

ТЕОРЕМА. $p \equiv 7 \bmod 8$

1) $d = \min w(m)$ – наименьший вес $0 \neq m \in C_{QR}(p)$ → алгебра $P^1(\mathbb{F}_p)$.

2) $d^2 - d + 1 \geq p$, → игра с многогранниками в конечном пространстве

Примеры 1) $p=7$, $d=3$ $9-3+1=7$

2) $p=23$ $5^2-5+1=21<23$! $\Rightarrow$ $d \geq 7$

3) $p=47$ $7^2-7+1=43<p=47$ $\Rightarrow$

$d(C_{QR}(47)) \geq 9$.

Д-во: 2) Пусть d — нечётное.

Тогда $d^2 - d + 1 \not\equiv p$.

$C_{QR}(p)$ идеал в $\mathbb{F}_2[x]/(x^p - 1)$

Пусть $a(x)$ — элемент минимального веса d.

$a(x) = \sum_{i=0}^{p-1} a_i x^i$ — имеет ровно d "1" среди коэффициентов

$a(x) \in C_{QR}(p) = C_{f_+(x)}$, где

$f_+(x) = \prod_{(\frac{k}{p})=1} (x - \alpha^k)$, $\alpha^p = 1$,

$\deg f_+(x) = \frac{p-1}{2}$

$a(x) = b(x) \cdot f_+(x) \mod (x^p - 1)$

Идея доказательства: Вычислить $a(x)\,\widetilde{a(x)} \mod (x^p - 1)$ двумя способами

1) $\widetilde{a(x)} := x^{p-1} a\left(\frac{1}{x}\right) = \sum a_i x^{p-1-i} \in \mathbb{F}_2[x]$

(3)

$$a(x)\cdot\widetilde{a(x)} = \sum_{0\le i,j\le p-1} (a_i\cdot a_j)x^{p-1-i+j} =$$

$d \bmod 2 = 1 \bmod 2$

$$= \sum_{i\neq j} a_i a_j x^{p-1-i+j} + \Big(\sum_{i=j} a_i^2\Big)x^{p-1}$$

$\to$ приведем d единиц к одной

Всего данный многочлен содержит не более, чем d^2-d+1 единичных коэф.

$a(x)\cdot\widetilde{a(x)} \bmod (x^p-1)$ $\to$ число единиц не увеличивается.

2) Другой метод

$$a(x) = b(x) f_+(x) \bmod x^p-1$$

$$\widetilde{a(x)} = x^{\frac{p-1}{2}} b\left(\frac{1}{x}\right) x^{\frac{p-1}{2}} f_+\left(\frac{1}{x}\right) \bmod x^p-1$$

$$f_-(x) = \prod (x-\alpha^\ell)$$

$$\left(\frac{\ell}{p}\right) = -1$$

$$\widetilde{a(x)} = \widetilde{b(x)}\cdot f_-(x) \bmod (x^p-1)$$

$$f_+(x) f_-(x) = \frac{x^p-1}{x-1} \Leftrightarrow (x-1) f_+(x) f_-(x) \equiv 0 \bmod (x^p-1)$$

$\forall k$: $1 \cdot x^k f_+(x) f_-(x) \equiv 1 \cdot f_+(x) f_-(x) \mod (x^p - 1)$ (4)

$\forall h(x) \in \mathbb{F}_2[x]$

$$h(x) \cdot f_+(x) f_-(x) \equiv h(1) f_+(x) f_-(x) \mod (x^p - 1)$$

$$a(x) \cdot \widetilde{a}(x) \equiv b(x) \cdot \widetilde{b}(x) f_+(x) f_-(x) \mod x^p - 1$$

$x = 1$

$p \equiv 1 \mod 2$

$$a(1)\widetilde{a}(1) \equiv b(1)\widetilde{b}(1) \left(1 + x + \dots + x^{p-1}\right)_{x=1} \equiv b(1)\widetilde{b}(1) \mod 2$$

$d \bmod 2 \cdot d \bmod 2 \equiv 1 \mod 2$

$(d \equiv 1 \mod 2)$

$$1 \equiv b(1)\widetilde{b}(1) \mod 2.$$

$$a(x)\widetilde{a}(x) \equiv b(x)\widetilde{b}(x) f_+(x) f_-(x) \equiv$$

$$\equiv b(1)\widetilde{b}(1)(1 + \dots + x^{p-1}) \mod (x^p - 1)$$

$$\equiv (1 + x + \dots + x^{p-1}) \mod (x^p - 1)$$

Следовательно,

$$w(a(x)\widetilde{a}(x)) = p$$

Итог: $w(a(x)\hat{a}(x)) \le d^2 - d + 1$, $w(a(x)\hat{a}(x)) = p$ $\Rightarrow$ (5)

$$\boxed{p \le d^2 - d + 1}$$

Группа автоморфизмов $\mathbb{P}^1(\mathbb{F}_p)$.

Новая модель $C_{QR}(p)$.

1-я модель: $C_{QR}(p) < \mathbb{F}_2^p$

линейное подпространство

2-я модель: циклический код

$C_{QR}(p) = C_{f_+(x)} = C_{e_+(x)}$ –

идеал в $\mathbb{F}_2[x]/(x^p - 1) \cong \mathbb{F}_2^p$

3-я модель: подмножества в $\mathbb{F}_p$

Пример: эл. $\overline{C_{QR}(p)}$ под. вв в $\mathbb{P}^1(\mathbb{F}_p)$

$u = (1\,0\,1\,1\,0\,0\,0) \in H_u^{(7)} < \mathbb{F}_2^7$

$\{0\,1\,2\,3\,4\,5\,6\} = \mathbb{F}_7$

вектор $\vec{u}$ — характеристическая ф-ция

$A_u = \{0, 2, 3\} \subset \mathbb{F}_7.$

$u, v \in \mathbb{F}_2^p \quad u \mapsto A_u \subset \mathbb{F}_p \quad u+v = A_u \oplus A_v$

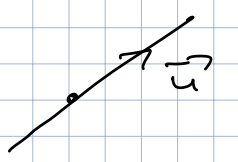
↓ симметрическая разность

$v \mapsto A_v$

Как записать $\overline{C_{QR}(p)}$?

Каждый вектор представим как под-во в $\mathbb{P}^1(\mathbb{F}_p)$.

Проективная прямая $\mathbb{P}^1(\mathbb{K})$ — это множество прямых через $\vec{0}$ в $\mathbb{K}^2$.



$\vec{u} = \begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} c \\ d \end{pmatrix} \quad \exists \lambda : \begin{pmatrix} a \\ b \end{pmatrix} = \lambda \begin{pmatrix} c \\ d \end{pmatrix}$

$\begin{pmatrix} a \\ b \end{pmatrix} \overset{b \neq 0}{\sim} \begin{pmatrix} x \\ 1 \end{pmatrix}$ или $\begin{pmatrix} a \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$\mathbb{P}^1(\mathbb{F}_p) = \left\{ \begin{pmatrix} x \\ 1 \end{pmatrix} = \frac{x}{1} = x \in \mathbb{F}_p \right\} \cup \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{0} = \infty \right\}$

$= \mathbb{F}_p \cup \{\infty\}$

Группа $PSL_2(\mathbb{F}_p) = SL_2(\mathbb{F}_p)/\{\pm E_2\}$ (центр.)

действует на $\mathbb{P}^1(\mathbb{F}_p)$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax+b \\ cx+d \end{pmatrix} \sim \begin{pmatrix} \frac{ax+b}{cx+d} \\ 1 \end{pmatrix} \sim \frac{ax+b}{cx+d}.$$

$\begin{pmatrix} x \\ 1 \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \langle x \rangle = \frac{ax+b}{cx+d} \in \mathbb{F}_p \cup \{\infty\}$$

$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \langle x \rangle = \langle x \rangle \Leftrightarrow$ центр действует тривиально.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \mapsto \frac{a}{c}$$

$$St\{\infty\} = \{\infty\} \Leftrightarrow c = 0$$

$$\begin{pmatrix} \lambda & \beta \\ 0 & \lambda^{-1} \end{pmatrix} \{\infty\} = \{\infty\}$$

$$\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} = \left\{\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}\right\} \cdot \left\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \lambda \neq 0\right\}$$

$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \langle x \rangle = x + \beta$ — трансляция

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \langle x \rangle = \frac{\lambda x}{\lambda^{-1}} = \lambda^2 x \text{ - гомотетия.}$$

Упражнение.

$$PSL_2(\mathbb{K}) = \left\langle \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

$$T^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

$$\infty \longrightarrow 0$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} -1 \\ 0 \end{pmatrix} = 1\infty$$

$PSL_2(\mathbb{K})$ действует транзитивно на $\mathbb{P}^1(\mathbb{K})$:

$$x \xrightarrow{\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}} 0 \xrightarrow{T} \infty$$

Упражнение

$$|GL_2(\mathbb{F}_p)| = \left|\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = M, \det M \neq 0 \right\}\right| =$$

→ второй столбец

$$= (p^2-1)\cdot(p^2-p)$$

первый столбец

$GL_2(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^\times$ – сюръективно

$\det \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} = d.$

$SL_2(\mathbb{F}_p) = \operatorname{Ker} \det = \dfrac{|GL_2(\mathbb{F}_p)|}{p-1} = p(p^2-1)$

$|PSL_2(\mathbb{F}_p)| = \dfrac{|SL_2(\mathbb{F}_p)|}{|\pm E_2|} = \dfrac{1}{2} p(p^2-1)$

Частный случай $|PSL_2(\mathbb{F}_7)| = \frac{1}{2} \cdot 7 \cdot 48 = 7 \cdot 24 = 168 =$

$|GL_3(\mathbb{F}_2)| = 168.$

Факт: $GL_3(\mathbb{F}_2) \cong PSL_2(\mathbb{F}_7)$

ТЕОРЕМА. $PSL_2(\mathbb{F}_p) < Aut(C_{QR}(p))$

Следствие: $d(C_{QR(p)})$ – нечётное.

Что надо доказать

$PSL_2(\mathbb{F}_p)$: слово кода $\longmapsto$ слово кода.