Кодирование 03.12.2021

Тема: $PSL_2(\mathbb{F}_p)$ как подгруппа группы автоморфизмов чётного расширения квадратично-вычетного кода $\overline{C_{QR}(p)} < \mathbb{F}_2^{p+1}$

Напоминание: Мы доказали, что минимальная дистанция d кода $C_{QR}(p) < \mathbb{F}_2^p$ удовлетворяет неравенству

$$d^2 - d + 1 \geq p$$

при предположении, что d нечётное.

Сегодня: Мы докажем, что d нечётная, изучив некоторую подгруппу

$$Aut\left(\overline{C_{QR}(p)}\right).$$

Этой подгруппой будет

$$PSL_2(\mathbb{F}_p) < Aut\left(\overline{C_{QR}(p)}\right)$$

Для этого мы рассмотрим новую, третью модель $C_{QR}(p)$

$$SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{F}_p) \quad \det = 1 \right\} \qquad (2)$$

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

Доказали: $|PSL_2(\mathbb{F}_p)| = \frac{1}{2} p(p^2-1)$.

Действие $SL_2(\mathbb{F}_p)$ на проективной прямой $\mathbb{P}^1(\mathbb{F}_p)$.

$$\mathbb{P}^1(\mathbb{F}_p) = \{ \text{одномерные подпр-ва в } \mathbb{F}_p^2 \} =$$

$$= \left\{ \overline{v \neq \begin{pmatrix} \lambda \\ \mu \end{pmatrix}} \Big/ \text{коллинеарность} \right\}.$$

$SL_2(\mathbb{F}_p)$ задаёт обратимое линейное преобразование на $\mathbb{F}_p^2$

$M \in SL_2(\mathbb{F}_p)$ задаёт тривиальное действие на прямых $\Leftrightarrow M = \pm E_2$.

$$M \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} a\lambda + b\mu \\ c\lambda + d\mu \end{pmatrix} -$$

согласовано с отношением "коллинеарн.

M - тождественно $\Leftrightarrow M = \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \Leftrightarrow \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$

Вывод: $\forall M \in PSL_2(\mathbb{F}_p)$ задаёт перестановку одномерных лин. подпр. в $\mathbb{F}_p^2$.

Другое описание $\mathbb{P}^1(\mathbb{F}_p)$

$$\begin{pmatrix}0\\0\end{pmatrix} \neq \begin{pmatrix}\lambda\\ \mu\end{pmatrix} \overset{\mu\neq 0}{\sim} \begin{pmatrix}\lambda\mu^{-1}\\ 1\end{pmatrix} = \begin{pmatrix}x\\1\end{pmatrix} \mapsto \frac{x}{1} = x \in \mathbb{F}_p$$

$$\overset{\mu=0}{\sim} \begin{pmatrix}1\\0\end{pmatrix} \mapsto \frac{1}{0} = \infty$$

$$\mathbb{P}^1(\mathbb{F}_p) \overset{\text{новые коор.}}{=} \mathbb{F}_p \sqcup \{\infty\}$$

$$\begin{pmatrix}x\\1\end{pmatrix} \leftarrow x \qquad \begin{pmatrix}1\\0\end{pmatrix} \mapsto \infty$$

Действие $SL_2(\mathbb{F}_p)$ в этих координатах

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} \cdot \begin{pmatrix}x\\1\end{pmatrix} = \begin{pmatrix}ax+b\\ cx+d\end{pmatrix} \mapsto \frac{ax+b}{cx+d} \in \mathbb{F}_p \sqcup \{\infty\}$$

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

$$= \frac{a+b/\infty}{c+d/\infty} = \frac{a}{c}.$$

Следствие $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ сохраняет $\infty \iff c = 0$

$$St(\infty) = \left\{ \begin{pmatrix} a & b \\ \boxed{0} & a^{-1} \end{pmatrix}, a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}$$

$c = 0$

$$\cong \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\} \cdot \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{F}_p \right\}.$$

Линейное действие $PSL_2(\mathbb{F}_p)$ в координате $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p^2 / \mathbb{F}_p^*$ превращается в дробно-линейное действие в модели $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$.

Следствие. Каждый элемент $M \in PSL_2(\mathbb{F}_p)$ определяет перестановку $p+1$ элетов в $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$.

$$PSL_2(\mathbb{F}_p) \hookrightarrow S_{p+1}.$$

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

$$T^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ в } PSL_2(\mathbb{F}_2)$$

$$T \cdot \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle x \rangle = \frac{-1}{x}$$

$T\langle 0\rangle = \infty \qquad T(\infty) = 0,$ (5)

$PSL_2(\mathbb{F}_p)$ действует транзитивно на $\mathbb{P}^1(\mathbb{F}_p)$

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

$x \longmapsto 0 \longmapsto \{\infty\}$

$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\langle x\rangle = x - x = 0$

общая формула

$$\frac{ax+b}{cx+d} \overset{c\neq 0}{=} \frac{a}{c} + \frac{-1}{c(cx+d)} = \frac{a}{c} + \frac{1}{c^2}\cdot\frac{-1}{x+\frac{d}{c}} =$$

$$= \frac{a}{c} + \frac{1}{c^2}\, T\left(x+\frac{d}{c}\right)$$

$$\begin{pmatrix} 1 & \frac{a}{c} \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix} \qquad \begin{pmatrix} 1 & d/c \\ 0 & 1 \end{pmatrix}$$

$$\begin{array}{r|l} ax+b & cx+d \\ \hline ax+\frac{ad}{c} & \frac{a}{c} \end{array}$$

$$b - \frac{ad}{c} = \frac{cb-ad}{c} = \frac{-1}{c}$$

Вывод Группа $PSL_2(\mathbb{F}_p)$ порождена элементами $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $x \in \mathbb{F}_p$, $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $\lambda \in \mathbb{F}_p^*$

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

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\langle x\rangle = x+b \qquad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\langle x\rangle = \frac{\lambda x}{\lambda^{-1}} = \lambda^2 x$$

$T\langle x\rangle = -\frac{1}{x}$.

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

$C_{QR}(p) < \mathbb{F}_2^p \qquad \overline{C_{QR}(p)} < \mathbb{F}_2^{p+1}$

Вектор $u \in \mathbb{F}_2^p$ представим как хар. функцию подмножества $\mathbb{F}_p$.

Пример. $u = (1011000) \in \mathbb{F}_2^7$

$\{0123456\} = \mathbb{F}_7$

$u \mapsto A_u = (0,2,3) \subset \mathbb{F}_7$.

$u+v \mapsto A_u \oplus A_v$ симметрическая разность

Каждый вектор $C_{QR}(p)$ есть под-во $\mathbb{F}_p$.

$\overline{C_{QR}(p)} = \{ (u_n ; \text{сумма коор в } \mathbb{F}_2)$

$C_{QR}(p)$ характ. символ $\infty\}$.

$\overline{u} \in \overline{C_{QR}(p)} \mapsto A_{\overline{u}} \subset \mathbb{F}_p \cup \{\infty\}$.

$\emptyset \longrightarrow (0,0,\dots,0) \in \vec{0}$

$\underline{1} = (\underbrace{1,\dots,1}_{p}) \in \mathbb{F}_2^p \longmapsto \mathbb{F}_p$

$\overline{\underline{1}} = (\underbrace{1,\dots,1}_{p};1) \longmapsto \mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}.$

В этой модели: $PSL_2(\mathbb{F}_p)$ действует на $\mathbb{P}^1(\mathbb{F}_p)$ и на любом его подмножестве. Более того, $PSL_2(\mathbb{F}_p)$ задаёт перестановку координат. Следовательно, $PSL_2(\mathbb{F}_p)$ сохраняет вес любого вектора.

Мы должны доказать, что слова кода $\overline{C_{QR}(p)}$ переходят в слова кода.

Рассмотрим базис кода $C_{QR}(p)$.

$C_{QR}(p) = C_{f_+(x)} = C_{\ell_+(x)}$

$$e_+(x) = \sum_{\left(\frac{k}{p}\right)=1} x^k \longmapsto \boxed{R_+ \subset \mathbb{F}_p}$$ (8)

циклический сдвиг: сдвиг на право $(0,1,2,\dots,p-1)$

$$R_+ \overset{\mathbb{F}_p}{\longmapsto} R_+ + 1$$

Обозначим

$$m_0 = R_+, \quad m_s = m_0 \overset{\mathbb{F}_p}{+} s = R_+ \overset{\mathbb{F}_p}{+} s, \quad s \in \mathbb{F}_p$$

$$\dim C_{f_+} = p - \frac{p-1}{2} = \frac{p+1}{2}$$

Вывод: 1) слова $m_s \in C_{QR}(p)$ и содержат базис данного кода.

$\overline{m_0} = (m_0; 1) \in \overline{C_{QR}(p)}$ $\overline{m_0} \subset \mathbb{F}_p \cup \{\infty\}$

$w(m_0) = \# R_+ = \frac{p-1}{2} = \frac{8k+7-1}{2} = 4k+3$

$\overline{m_s} = m_s \cup \{\infty\} \subset \mathbb{P}^1(\mathbb{F}_p)$.

$\{\overline{m_s}, s \in \mathbb{F}_p\}$ порождает $\overline{C_{QR}(p)}$.

Действие $PSL_2(\mathbb{F}_p)$ на словах кода $\overline{C_{QR}(p)}$

1) $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \langle \bar{m}_s \rangle = \bar{m}_{s+b} \in \overline{C_{QR}(p)}$

$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \langle \{R_+ + s, \infty\} \rangle = \{R_+ + s + b, \infty\} =$

2) $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \langle R_+ + s, \infty \rangle = \{ \lambda^2 (r+s), \infty \} =$

$r + s$

$\lambda^2 r \in R_+$

$= \{R_+ + \lambda^2 s, \infty\} = \bar{m}_{\lambda^2 s} \in \overline{C_{QR}(p)}$

Лемма $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in PSL_2(\mathbb{F}_p)$

1) $T \langle \bar{m}_0 \rangle = \bar{m}_0 \oplus \bar{1} \in \overline{C_{QR}(p)}$

2) $\forall\, s \in R_+ \quad T \langle \bar{m}_s \rangle = \bar{m}_0 \oplus \bar{m}_{T\langle s \rangle}$

3) $\forall\, s \in R_- \quad T \langle \bar{m}_s \rangle = \bar{m}_0 \oplus \bar{m}_{T(s)} \oplus \bar{1}$

$\in \overline{C_{QR}(p)}$

Д-во 1). $T = \begin{pmatrix} 0 & r \\ 1 & 0 \end{pmatrix}$ $T(r) = -\frac{1}{r}$ $T(\infty) = 0$

$$T(R_+ \cup \{\infty\}) = \left\{-\frac{1}{r}, r \in R_+\right\} \cup \{0\} =$$

$\frac{1}{r} \in R_+$ $-\frac{1}{r} \in R_-$: $\left(\frac{-1}{p}\right) = -1$

$$= R_- \cup \{0\} \overset{\circ}{=}$$

$$= (R_+ \cup \{\infty\}) \oplus (F_p \cup \{\infty\}) =$$

$$= (\cancel{R_+} \cup \{\infty\}) \oplus (\cancel{R_+} \cup R_- \cup \{0\} \cup \cancel{\{\infty\}}) =$$

$$\overset{\circ}{=} R_- \cup \{0\}$$

Мы доказали, что $T\langle \bar{u}_0 \rangle = \bar{u}_0 \oplus \bar{1}$