Завершение док-ва теоремы:

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

Напоминание.

1) p - простое, $p \equiv 7 \bmod 8 \Leftrightarrow \left(\frac{-1}{p}\right) = -1$, $\left(\frac{2}{p}\right) = 1$.

2) $C_{QR(p)} = C_{e_+(4)} \subset \mathbb{F}_2[x]/(x^p - 1) \overset{\text{лин.пр-во}}{\cong} \mathbb{F}_2^p$

3) $\mathbb{F}_2^p \cong$ множество подмножеств $\mathbb{F}_p$.

$u + v \mapsto A_u \oplus A_v$ (сим. разность)

4) $\overline{C}_{QR(p)} < \mathbb{F}_2^{p+1} = \{(x_1, \dots, x_p; x_{p+1})\}$ $\Rightarrow$

подм-во в $\mathbb{F}_p$ $\rightarrow$ индикатор ∞

$\overline{C}_{Qp}(p) \cong$ множество подмножеств в $\mathbb{F}_p \cup \{\infty\} =$

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

5) Мы установили, что группа $PSL_2(\mathbb{F}_p) = SL_2(\mathbb{F}_p)/\pm E_2$ действует на $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$ дробно-линейными преобразованиями:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \langle x \rangle = \frac{ax+b}{cx+d}$$

$x \in \mathbb{F}_p \cup \{\infty\}$

6) Мы доказали, что $PSL_2(\mathbb{F}_p)$ переставляет элементы $\mathbb{P}^1(\mathbb{F}_p)$ и это действие транзитивно.

7) $PSL_2(\mathbb{F}_p)$ действует как перестановка координат пр-ва $\mathbb{F}_2^{p+1} = 2^{\mathbb{P}^1(\mathbb{F}_p)}$

8) Мы завершим д-во того, что

$$PSL_2(\mathbb{F}_p) \leq Aut(\overline{C}_{QR}(p))$$

надо доказать, что $\forall M \in PSL_2(\mathbb{F}_p)$ перевод слово кода в другое слово кода.

9) Обрезочный $C_{QR}(p)$ и $\overline{C}_{QR}(p)$ в новой модели кода.

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

$$e_+(x) = \sum_{(\frac{k}{p})=1} x^k \mapsto R_+ = \text{множество ненулевых вычетов в } \mathbb{F}_p.$$

Циклический сдвиг: $R_+ + 1$ в $\mathbb{F}_p$

$m_0 = R_+ \subset \mathbb{F}_p$.

$\{ m_s = R_+ + s \subset \mathbb{F}_p \quad \forall s \in \mathbb{F}_p \} \subset C_{QR}(p)$

оно содержит будис кода $C_{QR}(p)$

$\overline{m}_0 = R_+ \cup \{\infty\}$ $\quad |R_+| = \frac{p-1}{2} = \frac{8k+7-1}{2} = 4k+3$

$\overline{m}_s = (R_+ + s) \cup \{\infty\} \in \overline{C}_{QR}(p) \quad \forall s \in \mathbb{F}_p$

М-но содержит будис $\overline{C}_{QR}(p)$

---

10) Надо доказать, что $\forall M \in PSL_2(\mathbb{F}_p)$

$M \langle \overline{m}_s \rangle \in \overline{C}_{QR}(p)$

11) Мы доказали, что $PSL_2(\mathbb{F}_p)$ порождена элементами вида:

$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \langle x \rangle = x + b \quad \forall b \in \mathbb{F}_p$

$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \langle x \rangle = a^2 x \quad \forall a \in \mathbb{F}_p^*$

$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle x \rangle = -\frac{1}{x}$ $\quad T\langle 0 \rangle = \infty, \; T(\infty) = 0.$

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \overline{m}_S = \{R_+ + S\} \cup \{\infty\} = \{R_+ + S + b\} \cup \{\infty\}$$

$$= \overline{m}_{S+b} \in \overline{C}_{QR}(p)$$

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \overline{m}_S = \{a^2(R_+ + S)\} \cup \{\infty\} = \{R_+ + a^2 S\} \cup \{\infty\} =$$

$$= \overline{m}_{a^2 S} \in \overline{C}_{QR}(p)$$

$$T^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \{\pm E_2\}$$

$T^2 = E_2$ в $PSL_2(\mathbb{F}_p)$

$\overline{T}$ – элемент порядка 4 в $PSL_2(\mathbb{F}_p)$.

$\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{F}_p\right\}$ = цикл. группа порядка p

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

кв. вычеты ↑ кв. невычеты ↗

$$\mathbb{F}_p = \{0\} \cup \underset{\downarrow}{R_+} \cup R_-, \quad \overline{1} = (\overbrace{1, \dots, 1}^{p+1 \text{ единица}}) = \mathbb{P}^1(\mathbb{F}_p)$$

(5)

Лемма. 1) $T(\overline{m}_0) = \overline{m}_0 \oplus \overline{\Pi} \in \overline{C}_{QR}(p)$

2) $\forall\, s \in R_+$: $T(\overline{m}_s) = \overline{m}_{T(s)} \oplus \overline{m}_0$

3) $\forall\, s \in R_-$: $T(\overline{m}_s) = \overline{m}_{T(s)} \oplus \overline{m}_0 \oplus \overline{\Pi}$

→ упражнение

Д-во: 0) $\overline{\Pi} = \mathbb{P}^1(\mathbb{F}_p) \mapsto (f_+(x) f_-(x), \infty)$

$= (\underbrace{1 + x + \ldots + x^{p-1}}_{p\text{-элементов}}, \infty) \in \overline{C}_{QR}(p)$

1) $T(\overline{m}_0) = T(R_+ \cup \{\infty\}) = \{-\frac{1}{r},\ r \in R_+\} \cup \{0\} =$

$\frac{1}{r} \in R_+ \Rightarrow -\frac{1}{r} \in R_-$, т.к. $\left(\frac{-1}{p}\right) = -1$.

$= R_- \cup \{0\} = \overline{m}_0 \oplus \mathbb{P}^1(\mathbb{F}_p) =$

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

2) $\forall\, s \in R_+$: $T(\overline{m}_s) = ?$ $\quad \{0\} \cup \{\infty\}$

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

R_+

a) $r + s = 0 \Leftrightarrow r = -s \in -R_+ = R_-$?!

$\{ t = -\frac{1}{r+s},\ r \in R_+ \}$ $\quad t \in F_p^\times = R_+ \sqcup R_-$

$t \neq 0, \infty$

$-\frac{1}{t} = r+s \iff -\frac{1}{t} - s \in R_+ \iff$

$-1 - ts \in tR_+ \iff \boxed{1+ts \in t \cdot R_-}$

$\{ -\frac{1}{r+s}, r \in R_+ \} = \{ t \in R_+ : 1+ts \in R_- \} \sqcup$

$\{ t \in R_- : 1+ts \in R_+ \}$

Вычислим $\overline{m}_{T(s)} = ?$ $\quad s \in R_+$, $T(s) \in F_p^\times$

$\overline{m}_{T(s)} = \{ \infty \} \sqcup \{ R_+ - \frac{1}{s} \}$

$t \in F_p$

$\infty \neq t = r - \frac{1}{s} \iff t + \frac{1}{s} \in R_+ \iff ts+1 \in R_+$

$\{ R_+ - \frac{1}{s} \} = \{ 0 \} \sqcup \{ t \in R_+ : ts+1 \in R_+ \} \sqcup$

$\sqcup \{ t \in R_- : ts+1 \in R_+ \}$

$T(\overline{m}_s) \oplus \overline{m}_{T(s)} = \overline{m}_0 \implies$

$$\left(\{0\} \cup \{t \in R_+ : 1+ts \in R_-\} \cup \{b \in R_- : 1+ts \in R_+\}\right) \quad (7)$$

$$(1) \quad \left(\{\infty\} \cup \{0\} \cup \{t \in R_+ : ts+1 \in R_+\} \cup \{t \in R_- : ts+1 \in R_+\}\right) =$$

$$= \{\infty\} \cup \{t \in R_+ : 1+ts \in R_\pm\} =$$

$1+ts = 0 \Leftrightarrow ts = -1 \in R_-$, а $ts \in R_+$ ($t \in R_+$, $s \in R_+$)!

$$= \{\infty\} \cup R_+ = \overline{\mathbb{m}_0}$$

$$\Rightarrow \boxed{\overline{\Gamma(\mathbb{m}_s)} = \overline{\mathbb{m}_{\Gamma(s)}} + \overline{\mathbb{m}_0}}$$

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

Следствие. Минимальный длина слов кода $C_{QR}(p)$ нечётна.

<u>Д-во:</u> Предположим, что

$$d = \min_{\bar{0} \neq u \in C_{QR}(p)} w(u) \text{ — чётно.}$$

$\exists\ u :\ w(u) = d$ и

$$\bar{u} = (u; 0) \in \overline{C}_{QR}(p).$$

$\forall\ M \in PSL_2(\mathbb{F}_p) \quad M\langle \bar{u} \rangle \in \overline{C}_{QR}(p)$

↓ действует транзитивно на координатах, т.е. на $\mathbb{P}^1(\mathbb{F}_p)$.

Пусть $\underset{\mathbb{F}_p}{i \in}$ — ненулевая координата u

Возьмём $M\langle i \rangle = \infty$. Тогда

$$M(\bar{u}) = (u'; \overset{\infty}{1}) \in \overline{C}_{QR}(p)$$

$$d = w(\bar{u}) = w(M(\bar{u})) \Rightarrow w(u') = d - 1$$

$\overline{u'} = (u', 1) \in \overline{C}_{QR}(p)$ и $u' \in C_{QR}(p)$

$$\boxed{w(u') = d - 1 < d \ ?!}$$

Используя этот факт, мы уже доказали, что d удовл условию

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

Замечание. Можно доказать, что

$$\begin{array}{ccc} PSL_2(\mathbb{F}_7) & \cong & GL_3(\mathbb{F}_2). \\ \wedge & & \wr\!\wr \\ Aut(\overline{H}_4^{(7)}) & & Aut(H_4^{(7)}) \end{array}$$

Две простые группы порядка 168.

Чтобы это получить из нашей теории, нужно найти $Aut(\overline{H}_4^{(7)})$ и использовать простоту $PSL_2(\mathbb{F}_7)$ и $GL_3(\mathbb{F}_2)$.