Кодирование 22.11.2021

Квадратично-вычетный код $C_{QR}(p)$ и самодвойственность его тёплого расширения.

$$\overline{C_{QR}(p)}^{\perp} = \overline{C_{QR}(p)}$$

p - простое, $p \equiv 7 \bmod 8$.

ТЕОРЕМА (Критерий самодвойственности нечётного линейного кода).

Пусть C – нечётный линейный код, $\overline{C}$ – его тёплое расширение. Тогда

$\overline{C}^{\perp} = \overline{C}$ $\Leftrightarrow$ $C^{\perp} = C_0$ - чётный подкод.

Пусть C - бинарный линейный код в $\mathbb{F}_2^n$.

$C_0 = \{(x_1,\dots,x_n) \in C : x_1+\dots+x_n = 0\} \subset C$.

$C_0 = C \Leftrightarrow \forall\, m \in C \quad W(m) \equiv 0 \bmod 2$.

C называем чётным кодом.

Если $\exists\, m \in C : w(m) \equiv 1 \mod 2$,
C называется *нечётным*:

$$C_0 \subsetneq C$$

$$C/C_0 \cong \mathbb{F}_2$$

$\forall\, m_1, m_2 \in C \quad w(m_1) = w(m_2) \equiv 1 \mod 2$

$w(m_1 - m_2) = w(m_1) + w(m_2) - 2|m_1 \cap m_2| \equiv 0 \pmod 2$

$m_1 - m_2 \in C_0$

$$C/C_0 = C_0 + (\varepsilon + C_0) \qquad w(\varepsilon) \equiv 1 \mod 2$$

$w(m) \bmod 2 \overset{def}{=} \overline{w(m)} \in \mathbb{F}_2$

$\overline{w} : \mathbb{F}_2^n \to \mathbb{F}_2$

$$\overline{w} : C \to \mathbb{F}_2 \qquad \ker \overline{w} = C_0$$

$C \neq C_0 \Rightarrow \overline{w}$ — сюръективно, $C/C_0 \cong \mathbb{F}_2$.

Замечания. 1) $C_0 \subsetneq C \Rightarrow C_0^{\perp} \supsetneq C^{\perp}$

2) $C \subset \mathbb{F}_2^n \Rightarrow \overline{C} \subset \mathbb{F}_2^{n+1}$

$\overline{C} = \{ (m, \overline{w}(m)),\ \forall\, m \in C \} \subset \mathbb{F}_2^{n+1}$

Ясно, что $\overline{C}$ – лин. подпространство

$$\dim C = \dim \overline{C}$$

$$C = C_0 \Rightarrow \overline{C} = (C, 0) \subset \mathbb{F}_2^{n+1}$$

Предложение. Пусть $C \subset \mathbb{F}_2^n$ нетривиальный код. Тогда

$$\overline{C}^{\frac{1}{\mathbb{F}_2^{n+1}}} = \left(C^{\frac{1}{\mathbb{F}_2^n}}, 0\right) \sqcup \left(C_0^{\frac{1}{}} \setminus C^{\frac{1}{}}, 1\right).$$

$\overline{\qquad}$ → $(n+1)$ – координата

Д-во. 1) Пусть $(a; 0) \in \overline{C}^{\frac{1}{\mathbb{F}_2^{n+1}}}$

$\forall \ (u, \overline{w}(u)) \in \overline{C}$

$$0 = (a,0) \cdot (u, \overline{w}(u)) = (a,u) + 0 \cdot \overline{w}(u) = (a,u)$$

$$\Leftrightarrow \quad a \perp C \Leftrightarrow \quad a \in C^{\frac{1}{}}$$

2) Рассмотрим $(a, 1) \in \overline{C}^{\frac{1}{}}$

→ доп. линейность

$$\overline{C} = (C_0, 0) \sqcup (C \setminus C_0, 1)$$

$\varepsilon + C_0$, где $\overline{w}(\varepsilon) = 1$

2-а) $\left((a,1), (b_0, 0)\right) = (a, b_0) + 0 = (a, b_0) = 0 \Rightarrow$

$b_0 \in C_0$

$\Rightarrow a \perp C_0 \Rightarrow \boxed{a \in C_0^{\perp}}$ (4)

2-б) $(a,1) \perp (C \setminus C_0, 1) \Rightarrow$

$((a,1),(\varepsilon,1)) = (a,\varepsilon) + 1 = 0 \Rightarrow$

$\boxed{(a,\varepsilon) = 1} \Leftrightarrow (a, \varepsilon + C_0) = (a,\varepsilon) = 1$

$a \in C_0^{\perp}$

$\Rightarrow a \in C_0^{\perp} \setminus C^{\perp}$

2-с) $\supset$

$(a,1) \in (C_0^{\perp} \setminus C^{\perp}, 1) \Rightarrow (a,1) \in \overline{C}^{\perp}$

Д-во Теоремы 1

Имеем

$\overline{C} = (C_0, 0) \sqcup (C \setminus C_0, 1)$ (def)

$\Leftrightarrow$

$\overline{C}^{\perp} = (C^{\perp}, 0) \sqcup (C_0^{\perp} \setminus C^{\perp}, 1)$ (Предложение)

$C_0 = C^{\perp} \Leftrightarrow C_0^{\perp} = C \Rightarrow C \setminus C_0 = C_0^{\perp} \setminus C^{\perp}$

(5)

$C_{QR}(p) = ?$ — квадратично-вычетный код длины p.

$C_{QR}(p) \subset \mathbb{F}_2^p$, p — простое, $p \equiv 7 \pmod 8$

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

$C_{QR}(p) = C_{\ell_+(x)} \subset \mathbb{F}_2[x]/(x^p - 1)$

$\ell_+(x) = \sum_{\left(\frac{k}{p}\right)=1} x^k$, $\ell_+(x)^2 \equiv \ell_+(x) \bmod (x^p - 1)$

$w(\ell_+(x)) = \#\{\text{квадратичные вычеты}\} = \frac{p-1}{2} = \frac{8k+7-1}{2} = (4k+3)$

$C_{QR}(p)$ — порождается циклическим и перестановочным многочленом $\ell_+(x)$

В частности $C_{QR}(p)$ — нечётный.

$\overline{C_{QR}(p)}$ — порождается словами веса $\equiv 0 \bmod 4$.

$$f_+(x) = \text{НОД}\left(x^p - 1,\ e_+(x)\right)$$

$$= \prod_{\left(\frac{k}{p}\right)=1} (x - \alpha^k) \qquad \deg f_+(x) = \frac{p-1}{2}$$

$$f_-(x) = \text{НОД}\left(x^p - 1,\ e_-(x)\right)$$

$$e_-(x) = \sum_{\left(\frac{\ell}{p}\right)=1} x^\ell \equiv \sum_{\left(\frac{-1}{p}\right)=1} x^{(-k \bmod p)} \bmod (x^p - 1)$$

$$\left(\frac{k}{p}\right)$$

$$x^p - 1 = (x-1)\, f_+(x)\, f_-(x)$$

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

$$\dim C_{QR}(p) = p - \left(\frac{p-1}{2}\right) = \frac{p+1}{2}.$$

Напоминание: было доказано, что

$$\boxed{C_f^{\perp} = C_{\tilde{g}}}, \text{ где } x^n - 1 = f(x) \cdot g(x)$$

$$\tilde{g}(x) = x^{\deg g}\, g\left(\frac{1}{x}\right)$$

Лемма. Пусть C_f – нетривиальный циклический код

Тогда $(C_f)_0 = C_{(x-1)f(x)}$.

Д-во: $C_f = \{ h(x) f(x) \bmod x^n - 1 \}$.

$\overline{w}(h(x)f(x)) = h(1) f(1)$.

Если C_f - неприводимый, то $\exists\, h(x)$:

$h(1) f(1) \overset{\mathbb{F}_2}{=} 1 \Rightarrow f(1) \overset{\mathbb{F}_2}{=} 1$.

$$(C_f)_0 = \{ h(x) f(x) \bmod x^n - 1 \mid \underbrace{h(1) f(1) \overset{*}{=} 0}_{\Updownarrow} \} =$$

$h(x) = (x-1) h'(x) \quad \Leftrightarrow h(1) = 0$

$$= \{ (x-1) h'(x) f(x) \bmod x^n - 1 \} = C_{(x-1)f(x)}.$$

ТЕОРЕМА. $\boxed{C_{QR(p)}^{\frac{1}{}} = C_{QR(p)}}$

Д-во: Надо доказать, что

2) $C_{QR(p)}^{\frac{1}{}} = (C_{QR(p)})_0$

1) $C_{QR}(p)$ — неприводимый.

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

$$x^p - 1 = (x-1) f_+(x) f_-(x)$$

$$\left(C_{f_+(x)}\right)^{\perp} = C_{\widetilde{(x-1)}\,\widetilde{f_-(x)}} = C_{(x-1) f_+(x)} =$$

$$\widetilde{f_-(x)} = f_+(x) \text{ !}$$

$$\left(C_{f_+(x)}\right)_0 \Rightarrow \overline{C_{f_+}}^{\perp} = \overline{C_{f_+}}$$

Следствие. 1) $G_{24} = \overline{G_{23}}$

2) $G_{24}^{\perp} = G_{24}$

3) $\forall\, m \in G_{24} \quad w(m) \equiv 0 \mod 4.$

4) G_{23} — бинарный совершенный код типа $[23, 12; 7]$

Д-60. 1) $G_{23} = G_{QR}(23)$ $23 \equiv 7 \bmod 8$

$\Rightarrow G_{24}^{\perp} = G_{24}.$

3) G_{23} — порождён смежн. сдвигами многочлена $e_+(x)$ или цикл. сдвигами многочлена $f_+(x)$

$w(e_+(x)) = 11$, $w(f_+(x)) = 7$ (имеет образующий)

Следовательно G_{24} порождено словами длины 8.

$$w(m_1+m_2) = 8+8-2\underbrace{|m_1 \wedge m_2|}_{\text{чётное}} \equiv 0 \pmod 4$$

Но $m_1 \perp m_2$

4) $d(G_{23}) \geq 5$

$w(m) = 5 \Rightarrow w((m,1)) = 6 \not\equiv 0 \pmod 4$

6   $w((m,0)) = 6 \not\equiv 0 \pmod 4$

$\exists\ w(f_+(x)) = 7 \Rightarrow$

$$\boxed{d(G_{23}) = 7.}$$

G_{23} – совершенный код.

$L \mid B_3(u)$

$u \in G_{23}$

$$|B_3(u)| = |B_3(0)| = 1 + C_{23}^1 + C_{23}^2 + C_{23}^3 =$$

$$= 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

$$2^{11} \cdot |G_{23}| = 2^{11} \cdot 2^{12} = 2^{23}.$$

$$H_4^{(7)} = C_{QR}(7)$$

$$G_{23} = C_{QR}(23)$$

$p = 7, 15, 23, 31, 39, 47$

Следующая лекция: 1) Структура кодов G_{23} и G_{24}.

2) Группа автоморфизмов $C_{QR}(p)$