Кодирование 15.11.2021

Бинарный код Голея

$$G_{23} = [23, 12; 7].$$

Мы показали, что циклический код можно задавать идеалом, т.е. $e(x) \in \mathbb{F}_p[x]$:

$$e(x)^2 \equiv e(x) \mod x^n - 1$$

Разберём задачу о разложении многочлена $x^{23} - 1 \in \mathbb{F}_2[x]$ на неприводимые множители.

$\operatorname{ord}^{\times}_{\mod 23} 2 =$ см. лекцию 11.11 $= 11 \Rightarrow$

имеются две циклотомические орбиты:

$$R_+ = \{ 2^n \mod 23 \quad 1 \le n \le 11 \} =$$

$$= \{ 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1 \mod 23 \}$$

$$R_- = -R_+ = \{ 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \mod 23 \}$$

$$2 R_{\pm} \equiv R_{\mp} \mod 23$$

Каждая орбита даёт неприводимый многочлен над полем $\mathbb{F}_2$.

$$f_{\pm}(x) = \prod_{k \in R_{\pm}} (x - \alpha^k) \in \mathbb{F}_2[x]$$

где α – примитивный корень степени 23 из единицы (над $\mathbb{F}_2$).

$d = \operatorname{ord}^{\times}_{\bmod 23} 2 = 11 \Rightarrow \alpha \in \mathbb{F}_{2^{11}}$

$(2^{11} - 1 \equiv 0 \bmod 23)$

$C_{f_{\pm}} = [23, 12, d]$, $d \geq 5$.

23 – $\deg f_{\pm}$

Как найти многочлен $f_{\pm}(x)$?

Построим два идемпотента:

$$e_{\pm}(x) = \sum_{k \in R_{\pm}} x^k \in \mathbb{F}_2[x]$$

$$\ell_-(x) = x^5 + x^7 + x^{10} + x^{11} + x^{14} + x^{15} + x^{17} + x^{19} + \quad (3)$$
$$x^{20} + x^{21} + x^{22} \in \mathbb{F}_2[x]$$

$$\ell_+(x) = x^1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} +$$
$$x^{16} + x^{18}$$

---

c-ba: $\quad \ell_\pm(x)^2 = \sum_{k \in R_\pm} x^{2k} \overset{\mod(x^{23}-1)}{\equiv} \sum_{x \in R_{\pm 1}} x^k$

$$2R_\pm \equiv R_\pm \mod 23$$

1) $\ell_\pm(x)^2 \equiv \ell_\pm(x) \mod (x^{23}-1)$

2) $1 + \ell_+(x) + \ell_-(x) = \dfrac{x^{23}-1}{x-1}$

$\alpha \in \mathbb{F}_{2^{11}}$, $\alpha^{23} - 1 = 0$

1) $\Rightarrow \quad \ell_\pm(\alpha)^2 = \ell_\pm(\alpha) \quad \left((\alpha^{23}-1)=0\right)$

$\ell_\pm(\alpha) \in \mathbb{F}_2$

$\ell_\pm(\alpha) \in \mathbb{F}_{2^{11}} \qquad a^2 = a \iff a = 0 \vee 1.$

2) $\Rightarrow$ $1 + \ell_+(\alpha) + \ell_-(\alpha) = 0$ $\Longrightarrow$

Имеем две различные следующие

$$\begin{cases} \ell_+(\alpha) = 1 \quad \text{и} \quad \ell_-(\alpha) = 0 \\ \ell_+(\alpha) = 0 \quad \text{и} \quad \ell_-(\alpha) = 1. \end{cases} \quad \left(\text{это верно } \forall\, \alpha^k\right)$$

$$x^{23} - 1 = (x-1)\, f_+(x)\, f_-(x)$$

Как связаны идемпотенты и образующие циклического кода?

1) $\ell(x)^2 \equiv \ell(x) \mod x^n - 1$

2) $f(x) = \text{НОД}\left(\ell(x), x^n - 1\right)$.

Итог: имеем $\text{НОД}\left(x^{23} - 1, \ell_\pm(x)\right)$

$$\text{НОД}\left(x^{23} - 1, \ell_+(x)\right) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} = f_+(x)$$

$$\text{НОД}\left(x^{23} - 1, \ell_-(x)\right) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} = f_-(x)$$

$$\frac{x^{23}-1}{x-1} = \left[(1+x+x^5+x^6+x^7+x^9+x^{11})\right] \cdot (1+x^2+x^4+x^5+x^6+x^{10}+x^{11}).$$

(5)

Выводы

1) Циклические коды C_{f_+} и C_{f_-} – это бинарные линейные коды типа $[23, 12; d]$, где $d \geq 5$.

2) Мы нашли порождающие матрицы данных кодов:

$$G_+ = \left[\begin{pmatrix} 1&1&0&0&0&1&1&1&0&1&0&1&\underbrace{0\,0\,0\,\ldots\,0}_{11} \\ 0&1&1&0&0&0&1&1&1&0&1&0&1&0\,\ldots\,0 \\ \vdots & & & & & & & & & & & & & \end{pmatrix}\right] \quad (12 \text{ строк})$$

$$G_+ \in M_{12\times 23}(\mathbb{F}_2)$$

Теорема C_{f_+} и C_{f_-} — это совершенные бинарные коды типа $[23, 12; 7]$, т.е.

$$F_2^{23} = \bigsqcup_{u \in C_{f_\pm}} B_u \quad (3).$$

Это совершенный бинарный код Голея $G_{23} = [23, 12; 7]$. $d = 5$

1) $C_{f_+} \cong C_{f_-}$ (упражнение)

2) Пусть $f = f_\pm$. Обозначим через $\overline{C}_f$ — тёмное расширение. Тогда $\overline{C}_f$ есть самодвойственный код типа $[24, 12; 8]$.

Это тёмный код Голея G_{24}.

$$\left(\overline{C}_f\right)^\perp = \overline{C}_f.$$

Аналогия:

совершенный бинарный код Хэмминга

$$H_7^{(4)} = [7; 4; 3]$$

$$\left(\overline{H_7^{(4)}}\right) = H_8^{(4)} = [8, 4; 4]:$$

$$\left(H_8^{(4)}\right)^{\perp} = H_8^{(4)}$$

Определения

1) Чётное расширение бинарного кода $C \subset \mathbb{F}_2^n$:

$$\overline{C} = \{((\underbrace{a_1, \dots, a_n}_{\in C}), \underbrace{a_1 + \dots + a_n}_{\in \mathbb{F}_2}) \} \subset \mathbb{F}_2^{n+1}$$

$$\overline{C} = \{(m, w(m) \bmod 2), m \in C\} \subset \mathbb{F}_2^{n+1}$$

Если C – линейный код, то

$\overline{C}$ — линейный код.

2) Пусть C – нечётный код в $\mathbb{F}_2^n$,

т.е. $\exists\, u \in C \quad w(u) \equiv 1 \bmod 2$.

Чётный подкод C_0:

$$C_0 = \{ u \in C : w(u) \equiv 0 \bmod 2 \} \subset C$$

$\neq$

если C – нечётный

Упражнение 1. Пусть $C_f \subset \mathbb{F}_2^n$ – циклический код длины n. Докажите

$$\overline{C}_f = \{ (h(x) f(x) \bmod x^n - 1,\ h(1) f(1)) \} \subset \mathbb{F}_2^{n+1}$$

$\overline{C}_f$ – линейный код.

Упражнение 2. Чётный подкод кода нечётного циклического кода C_f:

$$(C_f)_0 = C_{(x-1) f(x)}$$

$$x^{23} - 1 = (x-1) f_{11}(x) g_{11}(x)$$

Упражнение 3 Пусть $C < \mathbb{F}_2^n$ — бинарный нелинейный код.

$\overline{C} = \{(m, w(m) \bmod 2)\} \subset \mathbb{F}_2^{n+1}$ — его чётное расширение.

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