28.10.2021 Циклические коды (1)

Лекция 15 (продолжение).

Мы рассмотрели $x^{15}-1$ над $\mathbb{F}_2$ (+).

Исследуем $x^{15}-1$ над $\mathbb{F}_7$.

1) $\operatorname{ord}^{\times}_{\bmod 15} 7 = \operatorname{ord}_{(\mathbb{Z}/15\mathbb{Z})^{\times}} 7$

$\Phi_n(x)$ над $\mathbb{F}_q$ $\quad d = \operatorname{ord}^{\times}_{\bmod n} q$

$7^1, \; 7^2 \equiv 4 \bmod 15, \; 7^3 \equiv -2 \equiv 13 \bmod 15, \; 7^4 \equiv 1 \; (15)$

$\operatorname{ord}^{\times}_{\bmod 15} 7 = 4$

$\deg \Phi_{15}(x) = \varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$

$\Phi_{15}(x)$ раскладывается в произв. двух неприв. многочленов степени 4 над $\mathbb{F}_7$.

Пусть α – неприводимый корень кор. 15 из 1 над $\mathbb{F}_7$.

$\{\alpha, \alpha^7, \alpha^4, \alpha^{13}\} \to (x-\alpha)(x-\alpha^7)(x-\alpha^4)(x-\alpha^{13})$

$2 \to 14 \to 8 \to 11 \bmod 15$

-1

$\{\alpha^2, \alpha^{14}, \alpha^8, \alpha^{11}\} \mapsto (x-\alpha^2)(x-\alpha^{14})(x-\alpha^8)(x-\alpha^{11})$ (2)

примитивные корни ст. 15 из 1

$\alpha^3 \mapsto (\alpha^3)^7 = \alpha^6 \mapsto \alpha^{42} = \alpha^{12} \mapsto \alpha^{84} = \alpha^9 \mapsto \alpha^{63} = \alpha^3$

$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$

корни степени 5 из 1 $\Rightarrow$

$\phi_5(x) \overset{\mathbb{F}_7}{=} (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$ –

неприводимый над $\mathbb{F}_7$.

$\alpha^5 \mapsto \alpha^{35} = \alpha^5$ $\quad \{\alpha^5\}$

$\alpha^{10} \mapsto \alpha^{70} = \alpha^{10}$ $\quad \{\alpha^{10}\}$ $\mapsto$ корни степени 3 из 1 над $\mathbb{F}_7$.

$\phi_3(x) = x^2+x+1$ – раскладывается на лин. множители над $\mathbb{F}_7$.

$x^2+x+1 = \boxed{(x-\alpha^5)} \cdot \boxed{(x-\alpha^{10})} = (x-2)(x-4)$

$\phi_3(2) \equiv 0 \pmod 7 \Rightarrow \phi_3(4) \equiv 0 \pmod 7$

Вывод. Разложение $x^{15}-1$ над $\mathbb{F}_7$.

$x^{15}-1 = \phi_{15}(x)\,\phi_5(x)\,\phi_3(x)\,(x-1) =$

$f_1(x) \cdot f_2(x)$ (неприводимый) $(x-2)(x-4)\cdot(x-1)$ (3)

Всего 6 неприводимых многочленов:

3 многочлена степени 4 и 3 линейных.

линейных цикл. кодов $= 2^6 = 64$.

---

(2) Оценка минимального расстояния циклических кодов.

Циклотомические орбиты:

* $\alpha^1, \alpha^2, \alpha^4, \alpha^{13} \mapsto f_1(x)$ $\dim C_{f_1} = 15-4 = 11$

2 14 8 11

3 6 12 9

* 5

10

0

Теорема (25.10.21) Пусть среди корней $f(x) \in \mathbb{F}_p[x]$ $(f(x) \mid x^n - 1,\ (n,p)=1)$ имеется последовательность степеней $\alpha^t, \alpha^{t+1}, \dots, \alpha^{t+(r-1)}$. Тогда $d(C_f) \geq r+1$.

$g = f_1(x)(x-\alpha^5) \mapsto \alpha^4, \alpha^5 \overset{\text{Теорема}}{\Longrightarrow}$

$d(C_g) \geq 3 \quad \deg g = 5 \quad \dim C_g = 10$

$\{1, 7, 4, 13; 3, 6, 12, 9; 5\} \mapsto (3,4,5,6,7)$

$h = f_1(x)\,\Phi_5(x)(x-\alpha^5) = f_1(x)(x^4+x^3+x^2+x+1)(x-2)$

$\deg h = 9 \quad \dim C_h = 15-9 = 6, \quad |C_h| = 7^6$

$d(C_h) \geq 6$

$C_h^{\perp} = C_{\tilde{g}}, \quad g = \dfrac{x^{15}-1}{f_1(x)\,\Phi_5(x)(x-\alpha^5)}$

$d(C_{\tilde{g}}) \geq ?$

Вопрос $x^{15}-1$ над полем $\mathbb{F}_4$?

Теорема о разложении (и её док-во)
верны над полем $\mathbb{F}_q$, $(q, n) = 1$

$\operatorname{Ord}^{\times}_{\bmod 15} 4 = ?$

Вопрос: Как строить чётное расширение циклического кода ?

Вес слова чётен ?

$w(m) \equiv 0 \pmod 2$, поле $\mathbb{F}_2$

$m \mapsto m(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

$w(m) \equiv a_0 + a_1 + \dots + a_{n-1} \pmod 2$

↓ чётен ↓ $\mathbb{F}_2$ ↓ ‖ $m(1)$

$\mathbb{F}_2$:

$C_f = \{ h(x) \cdot f(x) \bmod x^n - 1 \} =$

$= \{ h(x) \cdot f(x),\ h(x) \bmod g(x) \}$

$f \cdot g = x^n - 1$

Чётное расширение C_f :

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

$x^{15} - 1 \overset{\mathbb{F}_2}{=} f_1^{(4)} f_2^{(4)} \phi_5^{(4)} \cdot \phi_3^{(2)} (x-1)$

Задача. $\overline{C}_f < \mathbb{F}_2^{n+1}$ $(\overline{C}_f)^{\perp} = ?$ (6)

Назад к $x^{15}-1$ над $\mathbb{F}_2$.

1) У нас получился код Хэмминга типа $(15, 11; 3)$.

Обобщения. Серия кодов Хэмминга как циклические коды.

$$x^{15}-1 = x^{2^4-1}$$

Рассмотрим общий случай

$$x^{2^m-1}-1 \quad \text{над} \quad \mathbb{F}_2$$

$$\operatorname{ord}_{\mathrm{mod}\, 2^m-1} 2 = m \Rightarrow$$

$\Phi_{2^m-1}(x)$ = произведению неприводимых многочленов степени m.

Пусть α – примитивный корень степени 2^m-1, или образующая

мультипл. группа $\mathbb{F}_{2^m}^{\times} = \langle \alpha \rangle$.

Орбита: $\underbrace{(\alpha, \alpha^2}_{d \geq 3}, \alpha^4, \ldots, \alpha^{2^{m-1}})$ $\quad \alpha^{2^m} = \alpha$.

$f(x) = (x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{2^{m-1}}) \in \mathbb{F}_2[x]$

$\dim C_f = (2^m - 1) - m \quad d(C_f) \geq 3$

$(2^m - 1,\ 2^m - 1 - m,\ \begin{pmatrix} d \\ VI \\ 3 \end{pmatrix}) \Rightarrow d = 3$

↓

разбиение на циклы

Проверка, что получился совершенный код Хэмминга

$[2^m - 1,\ 2^m - 1 - m,\ 3] \quad \forall\ m \geq 2$

$m = 3 \quad [7, 4, 3]$

Вопрос (25.10.21) ③

$x^{15}-1$ содержит в разложении все неприводимые многочлены степени 4. Объяснить этот факт!

Теорема Рассмотрим многочлен

$$x^{p^n}-x \in \mathbb{F}_p[x],\ p\text{-простое}.$$

Тогда

$$x^{p^n}-x \overset{\mathbb{F}_p}{=} \prod \text{все неприводимые над } \mathbb{F}_p \text{ многочлены степени } m,$$

где $m \mid n$.

Пример $x^{16}-x \in \mathbb{F}_2[x] \Rightarrow$

$$x^{16}-x = \underbrace{x}_{\deg 1}\underbrace{(x-1)}_{1}\underbrace{(x^2+x+1)}_{2}\underbrace{f_1 f_2 f_3}_{\deg 4}.$$

$x^{2^4}-x$

Наблюдение (пример лекции 25.10.21)

Многочлен $x^{15}-1 \in \mathbb{F}_2[x]$ содержит в разложении все неприводимые над $\mathbb{F}_2$ многочлены степеней 2 и 4.

Как объяснить этот факт?

ТЕОРЕМА Рассмотрим многочлен

$$x^{p^n}-x \in \mathbb{F}_p[x].$$ Тогда он имеет следующее разложение на неприводимые над полем $\mathbb{F}_p$:

$$x^{p^n}-x = \prod \underline{\text{все}} \text{ неприводимые многочлены степени } \underline{m}, \text{ где } \underline{m \mid n}$$

Пример (25.10)

$$x^{16}-x \overset{\mathbb{F}_2}{=} x\cdot(x-1)\,(x^2+x+1)\,(\text{Три неприводимых степени } 4)$$

Доказательство.

1) Рассмотрим циклотомический мнг.

$$\Phi_{p^n-1}(x) \in \mathbb{F}_p[x].$$

$$\operatorname{ord}^{\times}_{\bmod (p^n-1)} p = n.$$ (9)

Следовательно (см. основная теорема из лекции от 25.10), $\Phi_{p^n-1}(x)$ раскладывается в произведение неприводимых над $\mathbb{F}_p$ многочленов степени n.

2) Пусть $f(x) \in \mathbb{F}_p[x]$ — неприводимый многочлен степени n такой, что $f(x)$ делит $x^{p^n-1} - 1$.

Поле $\mathbb{F}_p^{(f)} = \mathbb{F}_p[x]/(f)$ содержит $p^{\deg f} = p^n$ элементов. Рассмотрим корень $\beta = x + (f) \in \mathbb{F}_p^{(f)}$ многочлена $f(x)$.

$\beta^{p^n-1} = 1$, т.к. $\left|\left(\mathbb{F}_p^{(f)}\right)^{\times}\right| = p^n - 1$.

Следовательно, $\operatorname{НОД}_{\mathbb{F}_p^{(f)}}(f(x), x^{p^n-1} - 1) \neq 1$.

Согласно алгоритму Евклида коэффициенты $\operatorname{НОД}_{\mathbb{F}_p^{(f)}}(f(x), x^{p^n-1} - 1)$ лежат в $\mathbb{F}_p$,

т.е. $\text{нод}_{\mathbb{F}_p}(f(x), x^{p^n-1}-1) \neq 1$, (10)

и $f(x)$ делит $x^{p^n-1}-1$, т.к. f - неприводим.

Мы доказали, что любой неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$ степени n делит $x^{p^n-1}-1$.

Следовательно, $x^{p^n-1}-1$ делится на их произведение!

3) Рассмотрим произвольный неприводимый делитель $g(x) \in \mathbb{F}_p[x]$ многочлена $x^{p^n}-x = x\prod_{0<k<p^n}(x-\alpha^k)$, где α образующая $\mathbb{F}_{p^n}^{\times}$. Положим $\deg g(x) = n$!

$\beta = x+(g) \in \mathbb{F}_p^{(g)} = \mathbb{F}_p[x]/(g)$ - корень многочлена $g(x)$, который порождает поле $\mathbb{F}_p^{(g)}$ над полем $\mathbb{F}_p$.

$g(x)$ делит $x^{p^n}-x$. Следовательно, можно вложить поле $\mathbb{F}_p^{(g)}$ в

поле $\mathbb{F}_{p^n}$, отождествим β с одним из корней α^k многочлена $x^{p^n} - x$. Получаем, что

$$\mathbb{F}_{p^{(g)}} \subset \mathbb{F}_{p^n}.$$

Рассмотрим $\mathbb{F}_{p^n}$ как векторное пр-во над $\mathbb{F}_{p^{(g)}}$. Пусть

$$\ell = \dim_{\mathbb{F}_{p^{(g)}}} \mathbb{F}_{p^n}.$$

Тогда $p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^{(g)}}|^\ell = (p^m)^\ell$.

Следовательно, $p^n = p^{m\ell}$ и

$$\boxed{m \text{ делит } n}$$

Мы доказали, что если $g(x) \mid x^{p^n} - x$, то $\deg g$ делит n.

4) Пусть $m \mid n$.

Докажем, что любой неприводимый многочлен степени m над F_p делит $x^{p^n} - x$.

Лемма 1) $x^M - 1$ делит $x^N - 1 \iff M \mid N$.

Д-во.

$$x^N - 1 = x^{N-M}(x^M - 1) + x^{N-M} - 1.$$

Вывод: евклидово деление для многочленов даёт в этом случае деление N на M.

2) $p^m - 1$ делит $p^n - 1 \iff m \mid n$

Д-во: аналогично.

Вывод: Для $m \mid n$ $x^{p^m-1} - 1$ делит $x^{p^n-1} - 1$, а выше мы доказали утверждение о $x^{p^m-1} - 1$.