Лекция-Семинар 27.11.2020

Циклические коды и многочлены.

Первая половина (стр. 1–10) – задачи на тему последней лекции; вторая половина (стр 11–20) – новый материал.

Напоминание: Циклический линейный код длины n над полем $\mathbb{F}_q$ задаётся произвольным делителем $f(x) \in \mathbb{F}_q[x]$ многочлена $x^n - 1 \in \mathbb{F}_q[x]$.

Линейное пр-во $\mathbb{F}_q^n \cong$ фактор кольцо $\mathbb{F}_q[x]/(x^n-1)$

$(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n \mapsto a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \bmod x^n - 1$

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

$$\deg f = k \Rightarrow \dim C_f = (n-k).$$

Если код $C \subset \mathbb{F}_q^n$ циклический, то порождающий его унитарный многочлен задаётся словом кода с самым длинным "нулевым хвостом" –

$$(b_0, b_1, \dots, \overset{0 \neq}{b_{k-1}}, \underbrace{0, \dots, 0}_{\text{макс. число нулей}}) \in C \Rightarrow$$

$$(a_0, a_1, \dots, a_{k-2}, 1, 0, \dots, 0) = \left(\frac{b_0}{b_{k-1}}, \frac{b_1}{b_{k-1}}, \dots \frac{b_{k-2}}{b_{k-1}}, 1\right)$$

$$f(x) = a_0 + a_1 x + \dots + a_{k-2} x^{k-1} + x^{k-1} \quad -$$

порождающий унитарный многочлен.

Задача 1 Найти число бинарных линейных циклических кодов длины 7.

Решение. Коды длины 7 отвечают делителям $x^7 - 1$ над полем $\mathbb{F}_2$. $\Phi_7(x) \in \mathbb{F}_2[x]$

$$x^7 - 1 \overset{\mathbb{F}_2}{=} (x+1)(x^3+x+1)(x^3+x^2+1).$$

Второй и третий многочлен неприводимые (почему?), так как у них нет корней над $\mathbb{F}_2$.

Произвольный делитель $f(x)$ многочлена $x-1$ имеет вид

$$(x+1)^a (x^3+x+1)^b (x^3+x^2+1)^c, \quad a,b,c = 0,1.$$

Следовательно, имеется ровно 8 делителей и ровно 8 кодов.

Упражнение 2. Описать циклические коды

C_1 и C_{x^7+1}; C_{x+1} и $C_{\Phi_7(x)}$;

C_{x^3+x+1} и $C_{(x+1)(x^3+x+1)}$.

Являются ли они двойственными (взаимно ортогональными)?

Проблема I. Как описать все делители многочлена $x^n - 1$ над конечным полем $\mathbb{F}_q$, где $q = p^m$?

- Рассмотрим разложение над $\mathbb{Z}$:

$$x^n - 1 \overset{\mathbb{Z}}{=} \prod_{m \mid n} \Phi_m(x)$$ (см. курс алгебры)

Рассматривая это тождество по mod p, получаем тождество над $\mathbb{F}_p$.

$\mathbb{F}_p$ является простым подполем поля $\mathbb{F}_{p^m}$ для любого m. Следовательно,

$$x^n - 1 \overset{\mathbb{F}_{p^m}}{=} \prod_{m \mid n} \left(\Phi_m(x) \bmod p\right)$$

есть тождество над $\mathbb{F}_{p^m}$.

Если $(n, p) = 1$, то $x^n - 1$ не имеет кратных корней в $\mathbb{F}_{p^m}$. В этом случае мы изучили на прошлой лекции поведение **кругового многочлена** $\Phi_m(x)$ **над полем** $\mathbb{F}_q$.

Напомним этот результат.

ТЕОРЕМА (См. прошлую лекцию). (4)

Пусть $q = p^k$ и $(n, q) = 1$. Положим

$$d = \operatorname{ord}_n q = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} q.$$

Тогда круговой многочлен $\Phi_n(x)$ раскладывается в произведение $\frac{\varphi(n)}{d}$ неприводимых многочленов степени d.

Разберёмся в этом результате!

Задача 3 Исследовать поведение кругового многочлена $\Phi_{11}(x)$ над полями $\mathbb{F}_p$ для всех простых p.

Решение. Исследуем мультипликативную группу $(\mathbb{Z}/11\mathbb{Z})^\times$.

1) Эта группа циклическая, т.к. 11 простое.

2) Найдём образующую этой группы.

$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10 \mod 11$

$2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1 \mod 11$

Следовательно

$\operatorname{ord}_{11} 2, 8, 7, 6 = 10$

$\operatorname{ord}_{11} 4, 5, 9, 3 = 5$

$\operatorname{ord}_{11} 10 = 2 \qquad \operatorname{ord}_{11} 1 = 1$

} 4 случая по числу делителей порядка 10

Напомню: если $\operatorname{ord}_G a = n$, то

$$\operatorname{ord}_G a^k = \frac{n}{(k, n)}$$

(повторите тему "Цикл. группы")

Вывод: 1) Если простое $p \equiv 2, 6, 7, 8 \mod 11$, (т.е. $p = 13, 17, 29, 19, \ldots$) то $\Phi_{11}(x)$ неприводим над $\mathbb{F}_p$.

2) Если $p \equiv 3, 4, 5, 9 \mod 11$, то $\Phi_{11}(x)$ разлагается в произведение двух неприводимых множителей степени 5 над $\mathbb{F}_p$.

Например, для $p = 47, 37, 39, 31, \ldots$

3) Если $p \equiv 10 \mod 11$, то $\Phi_{11}(x)$ разлагается в произведение 5 неприводимых квадр. многочленов над $\mathbb{F}_p$

Например, для $p = 43$.

4) Если $p \equiv 1 \bmod 11$ (например, $p=23$), то $\Phi_{11}(x)$ раскладывается на линейные множители над $\mathbb{F}_p$!

Задача 4 Исследовать поведение многочлена $\Phi_{15}(x)$ над $\mathbb{F}_p$.

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

2) Вычислить $\Phi_{15}(x)$ над $\mathbb{Z}$.
(Этого не требуется для изучения поведения $\Phi_{15}(x)$ над $\mathbb{F}_p$.)

3) $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times = \left(\mathbb{Z}/3\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/5\mathbb{Z}\right)^\times =$

$\cong C_2 \times C_4$ (произведение двух циклических групп порядка 2 и 4).

4) Любой элемент $a \in C_2 \times C_4$ имеет порядок 1, 2 или 4. Следовательно, $C_2 \times C_4$ не является циклической, т.к. в ней нет элемента порядка 8.

5) **Вывод.** Для любого $(p, 15) = 1$ $\operatorname{ord}_{(\mathbb{Z}/15\mathbb{Z})^\times} p = 1, 2$ или 4, поэтому

Для любого $p \neq 3, 5$ многочлен $\Phi_{15}(x)$ является приводимым над $\mathbb{F}_p$

б) $\operatorname{ord}_{(\mathbb{Z}/15\mathbb{Z})^\times} p = 1 \Leftrightarrow p \equiv 1 \bmod 15$. $p = 31, \dots$

Тогда $\Phi_{15}(x)$ раскладывается на линейные множители над $\mathbb{F}_p$.

ЗАДАЧА 5 В каком расширении $\mathbb{F}_{p^m}$ поля $\mathbb{F}_p$ лежит примитивные корни степени 11 из 1?

Решение. 1) Мы показали выше, что многочлен Φ_{11} раскладывается на линейные множители над $\mathbb{F}_p$, если $p \equiv 1 \bmod 11$. Следовательно, поле $\mathbb{F}_{23}$ содержит примитивный корень степени 11 из 1.

2) Что можно сказать про поле $\mathbb{F}_2$? Где лежит его корень степени 11 над $\mathbb{F}_2$?

$\varphi(11) = \left|(\mathbb{Z}/11\mathbb{Z})^\times\right| = 10 \Rightarrow 2^{10} \equiv 1 \bmod 11$

$\Rightarrow \mathbb{F}_{2^{10}}^\times$ – циклическая группа порядка $2^{10}-1$, которая содержит элемент

порядка 11, т.е. корень степени 11 из 1.

Это соответствует Достаточной ТЕОРЕМЕ:

$q = 2^{10}$, $\operatorname{ord}_{11} q = 1 \Rightarrow \Phi_{11}(x)$

раскладется на линейные множители над полем $\mathbb{F}_{2^{10}}$, т.е. имеет в нём корни.

3) Обобщение. Пусть p - простое.

$p^{10} \equiv 1 \bmod 11 \Rightarrow \operatorname{ord}_{(\mathbb{Z}/11\mathbb{Z})^\times} p^{10} = 1 \Rightarrow$

$\mathbb{F}_{p^{10}}$ содержит примитивный корень степени 11 из 1 для $\forall p$.

4) Окончательное решение Задачи 5.

Пусть n произвольное и $(p, n) = 1$.

$q = p^{\varphi(n)} \equiv 1 \bmod n \Rightarrow$

$\operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} p^{\varphi(n)} = 1 \Rightarrow$

$\Phi_n(x)$ всегда раскладывается на линейные множители над полем $\mathbb{F}_{p^{\varphi(n)}}$.

Мы установили важный ФАКТ:

Поле $\mathbb{F}_{p^{\varphi(n)}}$ содержит примитивный корень степени n из 1 для любого p, если $(p,n)=1$. Конечно, это же верно для любого d такого, что $p^d \equiv 1 \bmod n$. Наименьшее такое d даст нам расширение наименьшей степени $\mathbb{F}_{p^d}$, содержащее примитивный корень степени n из 1 над $\mathbb{F}_p$.

ПРИЛОЖЕНИЕ. Существование неприводимых многочленов произвольной степени m над полем $\mathbb{F}_p$.

Задача 6 Круговой многочлен $\Phi_{p^m-1}(x)$ раскладывается в произведение неприводимых многочленов степени m.

Решение. $n = p^m - 1$, $(n,p)=1$.

$p^m \equiv 1 \bmod (p^m-1)$ и m наименьшая положительная степень с таким с-вом.

Следовательно, $\operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} p = m$.

Утверждение Задачи 6 следует из Теоремы. Мы доказали, что m делит $\varphi(p^m-1)$ и что существуют по крайней мере $\frac{1}{m}\varphi(p^m-1)$ неприводимых многочленов степени m над полем $\mathbb{F}_p$.

Теперь вы можете ответить на вопрос о всех делителях многочлена x^n-1 над полем $\mathbb{F}_q$ $((n,q)=1)$.

$$x^n-1 = \prod_{m \mid n} \Phi_m(x).$$

Поведение каждого множителя Φ_m над полем $\mathbb{F}_q$ описывается Теоремой о круговом многочлене. Это даст нам все неприводимые делители x^n-1.

Упражнение 7. Найти число циклических кодов длины 16 над любым полем $\mathbb{F}_p$, где $p \neq 2$.

ПРОБЛЕМА II.

Как оценить минимальную длину $d(C_f) = \min_{0 \neq m \in C_f} w(m)$ циклического кода, порождённого многочленом f?

В общем виде трудно найти $d(C_f)$ для делителя f многочлена $x^n - 1$. Однако, мы докажем теорему, которая даёт хорошую оценку снизу на $d(C_f)$. Задачи, которые мы решали выше, подготовили вас к этому результату.

Пусть $f(x)$ — произвольный делитель $x^n - 1$ над полем $\mathbb{F}_p$. Мы установили выше, что $x^n - 1$ (и, следовательно, $f(x)$) разлагается на линейные множители в поле $\mathbb{F}_{p^{\varphi(n)}}$.

Напомним, что если $f(x) \in \mathbb{F}_p[x]$, то $(f(x))^p = f(x^p)$, поэтому $f(\alpha) = 0 \Rightarrow f(\alpha^p) = 0$.

Пусть $f(x) \in \mathbb{F}_p[x]$, $f(x) \mid (x^n - 1)$ над $\mathbb{F}_p$ и $(n, p) = 1$, $f(x)$ — унитарный.

Пусть α — примитивный корень степени n из 1. Например, можно взять $\alpha \in \mathbb{F}_{p^{\varphi(n)}}$. Тогда

$$f(x) = \prod_{j=1}^{s} (x - \alpha^{k_j}) \in \mathbb{F}_p[x].$$

Обозначим через $S_f = \{k_1, \dots, k_s\}$ множество показателей степеней корня α.

Отметим, что $1 \le k_j \le n$ и $pS \equiv S \bmod p$, так как α^{pk_j} тоже корень $f(x)$.

В множестве S_f могут быть последовательности степеней типа $k, k+1, k+2, \dots$

Теорема Пусть $\exists\, t, r \in \mathbb{N}$ такие, что $t, t+1, \ldots, t+r-1 \in S_f$. Тогда верно следующая оценка на минимальную длину $d(C_f)$ линейного циклического кода над полем $\mathbb{F}_p$:

$$d(C_f) \geq r+1$$

Доказательство. От противного. Пусть код C_f содержит слово m веса $\leq r$. $m = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_p$ заменим на многочлен $m(x) = \sum_{i=0}^{n-1} a_i x^i$, в котором имеется не больше r коэффициентов отличных от 0!

Следовательно, $m(x) \equiv h(x) f(x) \bmod x^n - 1$,

и $m(\alpha^k) = h(\alpha^k) f(\alpha^k) + g(\alpha^k)(\alpha^n - 1)$, т.е.

$m(\alpha^{i \cdot j}) = 0$ для любого $1 \leq j \leq s$.

В частности $m(\alpha^{t+k}) = 0$ для $0 \leq k \leq r-1$.

Перепишем все эти r условий на многочлен

$$m(x) = \sum_{i=1}^{r} a_i x^{m_i}, \quad a_i \in \mathbb{F}_p, \quad 0 \leq m_i \leq n-1$$

$$m(\alpha^{t+k}) = \sum_{i=1}^{r} a_i (\alpha^{t+k})^{m_i} = \sum_{i=1}^{r} (a_i \alpha^{t m_i})(\alpha^{m_i})^k = 0.$$

Это равенство выполняется для всех $0 \le k \le r-1$.

Рассмотрим $r \times r$ – матрицу:

$$A = \begin{pmatrix} 1 & \alpha^{m_1} & \alpha^{2m_1} & \dots & \alpha^{m_1(r-1)} \\ 1 & \alpha^{m_2} & \alpha^{2m_2} & \dots & \alpha^{m_2(r-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{m_r} & & & \alpha^{m_r(r-1)} \end{pmatrix}$$

Её определитель (определитель Вандермонда!) не равен нулю, так как

$\alpha^{m_i} \neq \alpha^{m_j}$, $0 \le m_i, m_j \le n-1$ и α примитивный корень степени n.

Следовательно, система линейных уравнений с матрицей A имеет только нулевое решение. Поэтому

$$\forall i \quad a_i \alpha^{t m_i} = 0 \iff \forall i \quad a_i = 0$$

Следовательно, m – нулевое слово!

Теорема доказана.

Пример Новая конструкция кода Хэмминга $H_4^{(7)}$.

Рассмотрим циклические бинарные коды длины 7 над $\mathbb{F}_2$.

$$x^7-1 = x^7+1 \overset{\mathbb{F}_2}{=} (x+1)(x^3+x+1)(x^3+x^2+1)$$

Исследуем циклический код $C_f = C_{1+x+x^3}$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ – поле из 8 элементов.

Пусть $\alpha = x \bmod x^3+x+1$ – корень многочлена $1+x+x^3$ в поле $\mathbb{F}_8$.

α будет образующей циклической группы $\mathbb{F}_8^\times$ простого порядка 7. Отметим, что

α, α^2 и α^4 – корни $1+x+x^3$, а

α^3, α^5 и α^6 – корни $1+x^2+x^3$.

Доказанная выше теорема даёт оценки

$$d(C_{1+x+x^3}) \geq 3 \text{ и } d(C_{1+x^2+x^3}) \geq 3.$$

$(1+x+x^3) \in C_{1+x+x^3} \Rightarrow \boxed{d(C_{1+x+x^3}) = 3}$

и $\boxed{\dim C_{1+x^2+x^3} = 3.}$

Мы получили новую конструкцию бинарного кода Хэмминга $[7, 4; 3]$.

Порождающая матрица кода C_{1+x+x^3} (см. первую лекцию про циклические коды) равна бинарной 4×7 – матрице

$$G_f = \begin{pmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{pmatrix}.$$

Она не совпадает с порождающей матрицей $H_4^{(7)}$!

Упражнение 8. Найти проверочную матрицу кода C_{1+x+x^3}, т.е. порождающую матрицу двойственного (ортогонального) кода.

Важное замечание. Свойство цикличности **не сохраняется** при изоморфизме кодов.

Мы определили код $H_4^{(7)}$ матрицей

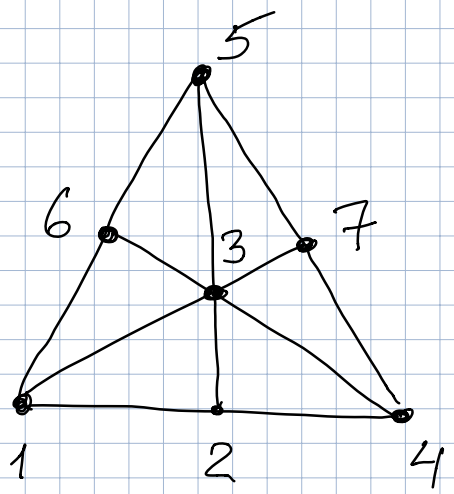
$$G_H = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

Четвёртый вектор кода $H_4^{(7)}$ веса 3 равен (0101010) $((2)+(4))$

17)

В этой реализации код Хэмминга $H_4^{(7)}$ не является циклическим. (убедитесь!)

Дадим реализацию, совпадающую с циклическим кодом C_{1+x+x^3}.



Образующие

Прямые: (1 2 4)
(2 3 5)
(4 3 6)
(4 7 5)

Порождающая матрица

$$G_{1+x+x^3} = G_f = \begin{pmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{pmatrix}.$$

Упражнение 9. Доказать изоморфность кодов $C_{1+x+x^3} \cong C_{1+x^2+x^3}$.

Естественные арифметические условия на разбиение $\mathbb{F}_2^n = \bigsqcup_{m \in C} B_m(t)$ чр-ва на шары радиуса t показывают, что кроме серии кодов Хэмминга может существовать совершенный код $[23, 12; 7]$.

Пример Циклический бинарный код длины 23.

$$x^{23}-1 = (x-1)\,\Phi_{23}(x).$$

Исследуем $\Phi_{23}(x)$ над полем $\mathbb{F}_2$.

Группа $\left(\mathbb{Z}/23\mathbb{Z}\right)^{\times}$ циклическая.

$$2^{11} = 1024\cdot 2 = 2048 = 1 + 89\cdot 23 \equiv 1 \bmod 23,$$

т.е. $\operatorname{ord}_{(\mathbb{Z}/23\mathbb{Z})^{\times}} 2 = 11$ (Почему?)

По теореме о круговом многочлене $\Phi_{23}(x)$ раскладывается (над $\mathbb{F}_2$) в произведение двух неприводимых многочленов степени 11:

$$\Phi_{23}(x) = f(x)\cdot g(x) \quad \text{в } \mathbb{F}_2[x]$$

$$\deg f = \deg g = 11.$$

Исследуем структуру корней $f(x)$ и $g(x)$.

Пусть α – первообразный корень степени 23 из 1 над полем $\mathbb{F}_2$.

Как мы установили выше, такой корень имеется в поле $F_{2^{11}}$, так как $2^{11} - 1 \equiv 0 \mod 23$.

Рассмотрим 2-циклотомические орбиты первообразного корня α:

$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^9, \alpha^{18},$
$\alpha^{36} = \alpha^{13}, \alpha^{26} = \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha$

Орбита 1: $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

Вторая орбита получится, если начать с α^5

$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40} = \alpha^{17}, \alpha^{34} = \alpha^{11}, \alpha^{22} = \alpha^{-1},$
$\alpha^{-2} = \alpha^{21}, \alpha^{-4} = \alpha^{19}, \alpha^{-8} = \alpha^{15}, \alpha^{30} = \alpha^7,$
$\alpha^{14}, \alpha^{28} = \alpha^5$

Орбита 2: $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$

Первая и вторая орбиты дают корни многочленов f и g (см. доказательство теоремы о поведении кругового многоугольника). Какой из многочленов

получится, зависит от выбора корня α. В любом случае мы получаем, что

$$\dim C_f = \dim C_g = 23 - 11 = 12$$

$$d(C_f) \geq 5 \quad \text{и} \quad d(C_g) \geq 5.$$

Отметим, что мы пока не нашли сами многочлены f и g. На самом деле можно доказать, что

$$\boxed{d(C_f) = d(C_g) = 7} \quad !$$

и

$$C_f \cong C_g \cong \underline{\text{код Голея}}\ [23, 12; 7]$$

исключительный (нет серии) совершенный код.

Упражнение 10. Найти разложение $\Phi_{23}(x)$ над полем $\mathbb{F}_2$.