Теория кодирования. Листок 2.
Циклические коды и многочлен $X^n - 1$ на конечным полем

В. А. Гриценко, 14 октября 2021

Задача 1. 1) **Бинарный код "повторение"** – это код типа $(2; n, 1, n)$. Он состоит из двух слов длины n в $\mathbb{F}_2^n$: $(0, 0, \ldots, 0)$ и $(1, 1, \ldots, 1)$. Сколько ошибок он исправляет? Доказать, что он циклический. Каким многочленом он порождается?

2) **Код "четности"** – это ядро линейной формы $x_1 + \ldots + x_n$ в $\mathbb{F}_2^n$. Определить его тип. Доказать, что он циклический. Каким многочленом он порождается?

3) Пусть $C < \mathbb{F}_q^n$ циклический код, порожденный многочленом $g(X) \in F_q[X]$. Как построить его **четное расширение** в $\mathbb{F}_q^{n+1}$?

Задача 2. 1) Каким многочленом порождается бинарный код Хэмминга $H_4^{(7)}$? Наити порождающий многочлен его двойственного кода (ортогонального дополнения).

2) Найти разложение многочлена $X^7+1 \in \mathbb{F}_2[X]$ на неприводимые. Описать все бинарные линейные циклические коды длины 7 (т.е. коды в $\mathbb{F}_2^7$).

Задача 3. **Автоморфизм Фробениуса** (повторение). Пусть $\mathbb{K}$ – конечное поле характеристики $p \neq 0$.

1) Описать свойства отображения $a \mapsto a^p$.

2) Доказать, что $a^p = a$ тогда и только тогда, когда a принадлежит простому подполю $\mathbb{F}_p$ поля $\mathbb{K}$.

3) Пусть $Q(X) \in \mathbb{K}[X]$. $Q(X)^p = Q(X^p)$ тогда и только тогда, когда $Q(X) \in \mathbb{F}_p[X]$. В частности, если $Q(X) \in \mathbb{F}_p[X]$, $a \in \mathbb{K}$ и $Q(a) = 0$, то $Q(a^p) = 0$, $Q(a^{p^2}) = 0$, $Q(a^{p^3}) = 0$, ...

4) $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ тогда и только тогда, когда m делит n.

5) Описать подполе $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, используя автоморфизм Фробениуса.

Задача 4. **Круговой многочлен** $\Phi_n(x) \in \mathbb{C}[x]$ (повторение).

$$X^n - 1 = \prod_{d|n} \Phi_d(X), \qquad \Phi_d(X) = \prod_{(k,n)=1} (X - e^{2\pi i \frac{k}{n}}) \in \mathbb{Z}[X]$$

1) $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)} \in \mathbb{Z}[X]$, где $\mu(m)$ – функция Мебиуса.

2) Вычислить Φ_8, Φ_{12}, Φ_{15}.

3) $\Phi_n(X)$ неприводимый многочлен степени $\varphi(n)$ над $\mathbb{Z}$. (См. любой учебник по алгебре.)

Задача 5. **Круговой многочлен над конечным полем.**

1) $\Phi_n(X)$ можно рассматривать (по модулю простого p) как многочлен над $\mathbb{F}_p$. Следовательно, многочлен $\Phi_n(X)$ можно рассматривать над $\mathbb{F}_{p^m}$. Пусть $n = p^k m$, где $(p, m) = 1$. Доказать, что в поле $\mathbb{F}_p$

$$X^n - 1 = (X^m - 1)^{p^k}.$$

В частности, над $\mathbb{F}_p$ не существует примитивного корня степени $p^k m$ $(k > 1)$ из единицы.

2) Исследовать разложение на множители многочленов $\Phi_{p-1}(X)$, $\Phi_p(X)$ и $\Phi_{p+1}(X)$ над полем $\mathbb{F}_p$.

3) Многочлен $\Phi_n(X)$ распадается в произведение линейных множителей над $\mathbb{F}_p$ тогда и только тогда, когда $p \equiv 1 \mod n$.

4) Что вы можете сказать о разложении $\Phi_n(X)$ над $\mathbb{F}_p$, если $n \equiv -1 \mod n$?

5) Если $p \equiv 1 \mod 4$, то X^2+1 имеет два корня в $\mathbb{F}_p$. Если $p \equiv -1 \mod 4$, то X^2+1 неприводим в $\mathbb{F}_p$.

6) Многочлен $\Phi_n(X)$ неприводим над $\mathbb{F}_p$ тогда и только тогда, когда $p \mod n$ порождает мультипликативную группу $(\mathbb{Z}/n\mathbb{Z})^\times$. Что вы можете сказать в этом случае про число n?

7) Доказать, что многочлены Φ_8, Φ_{12}, Φ_{15} приводимы над любым полем $\mathbb{F}_p$.

Указание. В этой задаче нужно использовать следующую теорему, доказанную в лекциях. Рассмотрим круговой многочлен $\Phi_n(X) \in \mathbb{F}_p[X]$, где $(n,p)=1$. Обозначим через d порядок p в мультипликативной группе вычетов $(\mathbb{Z}/n\mathbb{Z})^\times$, т.е. $d = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} p$. Доказать, что

$$\Phi_n(X) = f_1(X) \cdot \ldots \cdot f_l(X),$$

где $\deg(f_1) = \ldots = \deg(f_l) = d$, все многочлены неприводимы и попарно различны.

8) Доказать аналог этой теоремы, заменив p на $q = p^m$.

Задача 6. $\Phi_{p^m-1}(X)$.

1) Полином $\Phi_{p^m-1}(X)$ раскладывается над полем $\mathbb{F}_p$ в произведение унитарных неприводимых попарно различных многочленов степени m. В частности, m делит $\varphi(p^m-1)$ и **для любого m имеется неприводимый многочлен степени m над полем $\mathbb{F}_p$.**

2) Опишите разложение на множители в $\mathbb{F}_{p^m}$ каждого из этих неприводимых делителей $\Phi_{p^m-1}(X)$ степени m?

Задача 7*. 1) Исследовать разложение многочлена $X^{15}-1$ над простыми полями $\mathbb{F}_p$.

2) Аналогичный вопрос всех конечными полями $\mathbb{F}_{p^m}$ для $p \neq 3, 5$.

Задача 7*.

1) Многочлен $X^{p^n} - X \in \mathbb{F}_p$ разлагается в произведение всех неприводимых многочленов степени d, где d делитель n.

2) Для числа неприводимых $M_n(p)$ многочленов степени n над полем $\mathbb{F}_p$ получаем

$$\frac{p^n - p^{[n/2]+1}}{n} \leq M_n(p) \leq \frac{p^n}{n}.$$

Задача 8*. **"Мультипликативная" конструкция** поля $\mathbb{F}_{16}$

1) Наити разложение многочлена $X^{16}-X$ над полем $\mathbb{F}_2$.

2) Наити в поле $\mathbb{F}_{16}$ примитивный элемент a порядка 15 и построить таблицу сложения для степеней a^k.