Лекция 10

Ilya Yaroshevskiy

9 ноября

Содержание

1 Минимальные многочлены **1**

2 Циклические коды **3**
2.1 Порождающий и проверочный многочлены 3
2.2 Кодирование циклических кодов 4
2.3 Свойства порождающего многочлена 4
2.4 Проверочная матрица над расширенным полем 4
2.5 Коды Боуза-Чоудхури-Хоквингема 5
2.6 Граница БЧХ 5
2.7 Коды БЧХ 6

1 Минимальные многочлены

Определение. Минимальными многочленом элемента $\beta \in GF(p^m)$ над $GF(p)$ называется нормированный многочлен $M_\beta(x) \in GF(p)[x]$ наименьшей сетепени, т.ч. $M_\beta(\beta) = 0$

Теорема 1.1. $M_\beta(x)$ неприводим над $GF(p)$

Доказательство. Если $M_\beta(x) = M_1(x)M_2(x), \deg M_i(x) < \deg M(x), M_i(x) \in GF(p)[x]$ и $M_\beta(\beta) = 0$, то $M_1(\beta) = 0$ или $M_2(\beta) = 0 \implies$ степень $M_\beta(x)$ не минимальна □

Теорема 1.2. Если $f(x) \in GF(p)[x]$ и $f(\beta) = 0$, то $M_\beta(x) | f(x)$ ($f(x)$ делится на этот минимальный многочлен)

Доказательство.

$$f(x) = q(x)M_\beta(x) + r(x), 0 = f(\beta) = q(\beta)0 + r(\beta)$$

Теорема 1.3. $M_\beta(x) | (x^{p^m} - x)$ для $\beta \in GF(p^m)$

Доказательство. Утверждение непосредственно вытекает из предыдущей теоремы □

Теорема 1.4.

Доказательство. $GF(p^m)$ образует m-мерное линейное пространство над $GF(p) \implies$ любые $m+1$ элементов $GF(p^m)$ линейно зависимы над $GF(p)$. В частности $\forall \beta : \exists a_0, a_1, \ldots, a_m \in GF(p) : \sum_{i=0}^{m} a_i \beta^i = 0 \implies M(x) = \sum_{i=0}^{m} a_i x^i \in GF(p)[x]$ имеет корень β. Возможно, $M(x)$ можно разложить на сомножители меньшей степени. $M_\beta(x) | M(x)$, т.е. $\deg M_\beta(x) \le \deg M(x) \le m$ □

Теорема 1.5. Если α – примитивный элемент $GF(p^m)$, то степень его минимального многочлена равна m

Доказательство.

- Пусть $M_\alpha(x) = \pi(x) = \sum_{i=0}^{d} \pi_i x^i, \pi_i \in GF(p)$, причем $\alpha^d = -\sum_{i=0}^{d-1} \pi_i \alpha^i, d \le m$
- $\alpha^{d+1} = -\sum_{i=0}^{d-1} \pi_i \alpha^{i+1} = -\sum_{i=0}^{d-2} \pi_i \alpha^{i+1} + \pi_{d-1} \sum_{i=0}^{d-1} \pi_i \alpha^i = \sum_{i=0}^{d-1} a_{d+1,i} \alpha^i$
- Всякий $\beta \in GF(p^m) \setminus \{0\}$ может быть представлен как $\beta = \alpha^j = \sum_{i=0}^{d-1} a_{j,i} \alpha^i, a_{j,i} \in GF(p)$

- $GF(p^m)$ – m-мерное линейное пространство над $GF(p) \implies d \geq m$

□

Минимальные многочлен примитивного элемента поля называется примитивным. Не все неприводимые многочлены являются примитивными. Элементы $\beta \in GF(p^m)$ представимы как $\beta = \sum_{i=0}^{m-1} b_{\beta,i}\alpha^i, b_{\beta,i} \in GF(p)$

Теорема 1.6. Все конечные поля $GF(p^m)$ изоморфны

Доказательство.
- Пусть F и G – поля, содержащие p^m элементов
- Пусть α – примитивный элемент поля F с минимальным многочленом $\pi(x)$
- $\pi(x)|(x^{p^m} - x) \implies \exists\beta \in G : \pi(\beta) = 0$. Теперь F можно рассматривать как множество многочленов от α степени не более $m-1$, а G – как множество многочленов от β степени не боее $m-1$. Тогда соответсвие $\alpha \leftrightarrow \beta$ задает изоморфизм полей F и G

□

Пример. Рассмотрим два способа задания поля $GF(2^3)$

Через многочлен x^3+x+1	Через многочлен x^3+x^2+1
$(000) = 0$	$(000) = 0$
$(001) = 1 = \alpha^0$	$(001) = 1 = \gamma^0$
$(010) = \alpha$	$(010) = \gamma$
$(100) = \alpha^2$	$(100) = \gamma^2$
$(011) = \alpha^3 = \alpha + 1$	$(101) = \gamma^3 = \gamma^2 + 1$
$(110) = \alpha^4 = \alpha^2 + \alpha$	$(111) = \gamma^4 = \gamma^2 + \gamma + 1$
$(111) = \alpha^5 = \alpha^2 + \alpha + 1$	$(011) = \gamma^5 = \gamma + 1$
$(101) = \alpha^6 = \alpha^2 + 1$	$(110) = \gamma^6 = \gamma^2 + \gamma$

$\alpha^3 + \alpha + 1 = 0$. $(\gamma^3)^3 + \gamma^3 + 1 = \gamma^2 + \gamma^3 + 1 = 0$, т.е. $\pi(\alpha) = \pi(\gamma^3) = 0$, где $\pi(x) = x^3 + x + 1$. Таким образом, соответствие $\alpha \leftrightarrow \gamma^3$ задает изоморфизм между этими двумя полями

Теорема 1.7. $\forall\beta \in GF(p^m) : M_\beta(x) = M_{\beta^p}(x)$

Доказательство.

$$\mathbb{0} = M_\beta(\beta) = \sum_{i=0}^{d} M_{\beta,i}\beta^i, M_{\beta,i} \in GF(p)$$

$$\mathbb{0} = (M_\beta(\beta))^p = \sum_{i=0}^{d} M_{\beta,i}^p\beta^{pi} = \sum_{i=0}^{d} M_{\beta,i}\beta^{pi} = M_(\beta^p) \implies M_{\beta^p}(x)|M_\beta(x)$$

Т.к. минимальные многочлены неприводимы, $M_{\beta^p}(x) = M_\beta(x)$. $\beta, \beta^p, \ldots, \beta^{p^{m_\beta-1}}$ – сопряженные многочлены □

Теорема 1.8. $M_\beta(x) = \prod_{i=0}^{m_\beta-1}(x-\beta^{p^i})$, где m_β – наименьшее положительное число, т.ч. $\beta^{p^{m_\beta-1}} = \beta$

Доказательство. $M_(\beta) = 0$ – очевидно. $\prod_{i=0}^{m_\beta-1}(x - \beta^{p^i}) = \sum_{i=0}^{m_\beta} a_i x^i$.

$$\sum_{i=0}^{m_\beta} a_i^p x^{pi} = \left(\prod_{i=0}^{m_\beta-1}(x - \beta^{p^i})\right)^p = \prod_{i=0}^{m_\beta-1}(x^p - \beta^{p^{i+1}}) = \prod_{i+0}^{m_\beta-1}(x^p - \beta^{p^i}) = \sum_{i=0}^{m_\beta} a_i x^{pi} \implies a_i \in GF(p)$$

$M_\beta(x)$ имеет корни $\beta, \beta^p, \ldots, \beta^{p^{m_\beta-1}} \implies$ предлагаемый многочлен имеет наименьшую возможную степень □

2 Циклические коды

Определение. Линейный блоковый код $\mathcal{C}$ длины n над полем $\mathbb{F}$ называется циклическим, если любой циклический сдвиг его кодового слова также является кодовым словом, т.е. $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \implies (c_{n-1}, c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$

Замечание. Многочленное представление вектора $(c_0, c_1, \ldots, c_{n-1}) : c(x) = \sum_{i=0}^{n-1} c_i x^i$. Циклический свдиг вектора на одну позицию эквивалентен

$$xc(x) = xc_0 + x^2 c_1 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n \equiv c_{n-1} + xc_0 + x^2 c_1 + \cdots + c_{n-2}x^{n-1} \mod x^n - 1$$

В дальнейшем вектор $(c_0, c_1, \ldots, c_{n-1})$ и соответствующей многочлен $c(x)$ будут считаться равнозначными

Теорема 2.1. Подмножество $\mathcal{C} \subset \mathbb{F}[x] \setminus (x^n - 1)$ образует циклический код ттогда, когда:

1. $\mathcal{C}$ образует группу по сложению
2. Если $c(x) \in \mathcal{C}$ и $a(x) \in \mathbb{F}[x] \setminus (x^n - 1)$, то $[a(x)c(x) \mod (x^n - 1)] \in \mathcal{C}$

Доказательство.

- Пусть $\mathcal{C}$ обладает указанными свойствами $\implies$
  - $\mathcal{C}$ замкнуто относительно операции умножения на скаляр $\implies$ образует линейное пространство
  - Умножение на x^i не выводит за пределы $\mathcal{C} \implies$ циклический код
- Пусть $\mathcal{C}$ – циклический код
  - линейный код по определению образует группу по сложению
  - Умножение на произвольный многочлен можно представить как взвешенную сумму циклических сдвигов

□

2.1 Порождающий и проверочный многочлены

Замечание.

- Порождающий многочлен циклическоо кода – ненулевой кодовый многочлен $g(x) \in \mathcal{C}$ нименьшей степени с коэффициентов при старшем члене 1
- Все кодовые слова $c(x)$ в ЦК делятся на $g(x)$

  Предположим противное $\implies c(x) = a(x)g(x) + r(x), r(x) \in \mathcal{C}$. $\deg r(x) < \deg g(x)$, что противоречит предположению о минимальности степени $g(x)$
- Порождающий многочлен циклического кода единственен
- ЦК длины n с ПМ $g(x)$ сущесвует ттогда, когда $g(x) | (x^n - 1)$
  - Существует код $\mathcal{C}$ с ПМ $g(x) \implies$
    - $x^n - 1 = a(x)g(x) + r(x), \deg r(x) < \deg g(x)$
    - $b(x) \equiv a(x)g(x) \mod (x^n - 1), b(x) \in \mathcal{C}$
    - $r(x) = (x^n - 1 - a(x)g(x)) \equiv -a(x)g(x) \mod (x^n - 1), r(x) \in \mathcal{C} \implies r(x) = 0$
  - $\Leftarrow$: в качестве порождающего многочлена можно выбрать любой делитель $x^n - 1$
- $(x^n - 1) = h(x)g(x), h(x)$ – проверочный многочлен кода
- Для любого $c(x) \in \mathcal{C} : c(x)h(x) = a(x)g(x)h(x) \equiv 0 \mod x^n - 1$
- Размерность циклического кода равна $kd \deg h(x)$

2.2 Кодирование циклических кодов

Замечание. Несистематическое кодирование $c(x) = a(x)g(x)$

$$(c_0, \dots, c_{n-1}) = (a_0, \dots, a_{k-1}) \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_{n-k} & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & \dots & g_{n-k} \end{pmatrix}$$

Замечание. Систематическое кодирование (информационные символы $a_0, \dots, a_{k-1}$ в $c_{n-k}, \dots, c_{n-1}$)

$$c(x) = x^{n-k}a(x) - r(x)$$

$$r(x) \equiv x^{n-k}a(x) \mod g(x), \deg r(x) < \deg g(x)$$

Каждому методу кодирования соответствует своя порождающая матрица. Все порождающие матрицы выражаются друг через друга как $G' = QG$, где Q – обратимая матрица. Используемый метод кодирования не влияет на корректирующую способность кода

2.3 Свойства порождающего многочлена

- $x^n - 1 = \prod_{i=0}^{l-1} f_i(x)$, где $f_i(x)$ – неприводимые над $GF(q)$ многочлены. Разложение однозначно с точностью до порядка записи сомножителей и их домножения на обратимые элементы
- $g(x)|(x^n - 1) \implies g(x) = \prod_{i \in J} f_i(x), J \subset \{0, \dots, l-1\}$. Если все $f_i(x)$ различны , есть $2^l - 2$ нетривиальных циклических кода
- Циклические коды над $GF(q)$ длины $n = q^m - 1$ называются примитивными

Теорема 2.2. Пусть $\beta_1, \beta_2, \dots, \beta_r \in GF(q^m)$ – корни порождающего многочлена $g(x)$ примитивного циклического кода $\mathcal{C}$ над полем $GF(q)$. Многочлен $c(x) \in GF(q)[x]$ является кодовым тогда и только тогда, когда $c(\beta_1) = c(\beta_2) = \dots = c(\beta_r) = 0$

Доказательство. $c(x) = a(x)g(x) \implies$ все корни $g(x)$ являются корнями $c(x)$. $c(\beta_1) = 0 \implies M_i(x)|c(x)$, где $M_i(x)$ – минимальный многочлен β_i. Если $M_i(x)|c(x), i = 1, \dots, r \implies g(x)|c(x) \implies c(x) \in \mathcal{C}$ □

2.4 Проверочная матрица над расширенным полем

Замечание. Пусть порождающий многочлен циклического кода $\mathcal{C}$ над $GF(q)$ имеет корни $\beta_1, \dots, \beta_r \in GF(q^m) \implies \forall c(x) \in \mathcal{C} : c(\beta_i) = 0, 1 \le i \le r \implies \sum_{j=0}^{n-1} c_j \beta_i^j = 0 \implies Gc^T = 0$

$$\begin{pmatrix} \beta_1^0 & \beta_1^1 & \dots & \beta_1^{n-1} \\ \beta_2^0 & \beta_2^1 & \dots & \beta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_r^0 & \beta_r^1 & \dots u\beta_r^{n-1} & \end{pmatrix}$$

Проверочная матрица H' над $GF(q)$: заменить $\beta_i^j \in GF(q^m)$ на вектора-столбцы длины m из $GF(q)$, соответствующие их разложению по некоторому базису $GF(q^m)$

Пример. код Хемминга: $q = 2, n = 7, g(x) = x^3 + x + 1, \beta_1 = \alpha, \beta_2 = \alpha^2, \beta_3 = \alpha^4$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha+1 \\ 1 & \alpha^2 & \alpha^2+\alpha & \alpha^2+1 & \alpha & \alpha+1 & \alpha^2+\alpha+1 \\ 1 & \alpha^2+\alpha & \alpha & \alpha^2+\alpha+1 & \alpha^2 & \alpha^2+1 & \alpha+1 \end{pmatrix}$$

$$\text{H'} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \sim H'' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

2.5 Коды Боуза-Чоудхури-Хоквингема

Определение. Кодом БЧХ над $GF(q)$ длины n с конструктивным расстоянием δ называтеся циклический код наибольшей возможной размерности, порождающий многочлен которого имеет корни $\alpha^b, \dots, \alpha^{b+\delta-2}$, где $\alpha \in GF(q^m)$ – примитивный корень степени n из 1

Замечание. В силу теоремы Лагранжа $n|(q^m - 1)$. Если невозможно подобрать такое m соответствующего кода БЧХ не существует

Замечание.

- $n = q^m - 1$ – примитивный код БЧХ
- $b = 1$ – код БЧХ в узком смысле
- $m = 1$ – код Рида-Соломона

2.6 Граница БЧХ

Теорема 2.3. Если порождающий многочлен циклического кода длины n над $GF(q)$ имеет корни $\alpha^b, \dots, \alpha^{b+\delta-1}$, где $\alpha \in GF(q^m)$ – примитивный корень степени n из 1, то минимальное расстояние этого кода $d \geq \delta$

Доказательство.

- Линейный блоковый код имеет минимальное расстояние d ттогда, когда любые $1, \dots, d-1$ столбцов его проверочной матрицы линейно независимы, но существует d линейно независимых столбцов
- Рассмотрим t $le\delta - 1$ столбцов $j_1, \dots, j_t$ проверочной матрицы над $GF(q^m)$. Первые t ее строк равны

$$\mathcal{H} = \begin{pmatrix} \alpha^{bj_1} & \alpha^{bj_2} & \dots & \alpha^{bj_t} \\ \alpha^{(b+1)j_1} & \alpha^{(b+1)j_2} & \dots & \alpha^{(b+1)j_t} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(b+t-1)j_1} & \alpha^{(b+t-1)j_2} & \dots & \alpha^{(b+t-1)j_t} \end{pmatrix} =$$

$$= \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_t} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(t-1)j_1} & \alpha^{(t-1)j_2} & \dots & \alpha^{(t-1)j_t} \end{pmatrix}}_{W} \operatorname{diag}(a^{bj_1}, \dots, a^{bj_t})$$

- W – матрица Вандермонда, α – примитивный корень степени n из 1 $\implies$ $\alpha^{j_1}, \dots, \alpha^{j_t}$ различны и отличны от 0 $\implies$ W обратима, $\mathcal{H}$ – обратима $\implies$ Любые $le\delta - 1$ столбцов H ЛНЗ над $GF(q^m)$ и $GF(q)$

□

2.7 Коды БЧХ

Порождающий многочлен $g(x) = \text{LCM}(M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \ldots, M_{\alpha^{b+\delta-2}}(x))$. Т.к. минимальные многочлены или взаимно просты, или совпадают, порождающий многочлен равен произведению всех различных минимальных многочленов элементов $\alpha^b, \ldots, \alpha^{b+\delta-2}$

Замечание. Размерность кода БЧХ $k \geq n - m(\delta - 1)$

- Проверочная матрица над $GF(q^m)$ содержит $\delta - 1$ строк
- Проверочная матрица над $GF(q)$ содержит $m(\delta - 1)$ строк. Некоторые их них могут быть линейно зависимы

Замечание. Двоичные коды БЧХ в узком смысле $(b = 1) : k \geq n - m\lfloor (d-1)/2 \rfloor$

- $M_\beta(x) = M_{\beta^2}(x)$
- $g(x) = \text{LCM}(M_{\alpha^1}(x), M_{\alpha^3}(x), \ldots, M_{\alpha^{\delta-2}}(x))$
- В проверочную матрицу над $GF(2^m)$ достаточно включить $\lfloor \frac{d-2}{2} \rfloor$ строк, соответствующих α^{2i+1}

Пример. $(15, 7, 5)$ примитивный код БЧХ в узком смысле над $GF(2)$

- α – примитивный элемент $GF(2^4)$, т.ч. $\alpha^4 + \alpha + 1 = 0$
- $M_\alpha(x) = M_{\alpha^2}(x) = M_{\alpha^4}(x) = x^4 + x + 1$
- $M_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$
- $g(x) = \text{LCM}(M_\alpha(x), M_{\alpha^2}(x), M_{\alpha^3}(x), M_{\alpha^4}(x)) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$