НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Модуль 1. Математические основы помехоустойчивого кодирования

Структура конечных полей. Основные свойства и теоремы о конечных полях.

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

12 июня 2020 г.

Свойства бинома Ньютона в конечном поле

Как известно, $(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, однако в конечном поле характеристики p справедлива:

Теорема

$(a+b)^{p^s} = a^{p^s} + b^{p^s}, \forall s \in \mathbb{N}$

Данное равенство доказывается индукцией по s: $s = 1$:

$$(a+b)^p = a^p + b^p + pab^{p-1} + \binom{p}{2} a^2 p^{p-2} + ... + pa^{p-1}b =$$

$$= a^p + b^p + p * T \equiv a^p + b^p \mod p$$

для $s > 1$:

$$(a+b)^{p^s} = ((a+b)^{p^{s-1}})^p = (a^{p^{s-1}})^p + (b^{p^{s-1}})^p = a^{p^s} + b^{p^s}.$$

Минимальные функции

Определение

Минимальной функцией (минимальным многочленом) для элемента $\beta \in GF(q^m)$ *называется такой нормированный многочлен* $m(x)$ *над* $GF(q)$ *минимальной степени, что* $m(\beta) = 0$.

Важные особенности минимальных функций:

- Это многочлены над $GF(q)$
- Но их корни лежат в расширении $GF(q^m)$
- Минимальные функции - важнейший класс многочленов над конечными полями
- Все основные алгебраические коды основаны на минимальных функциях

Важнейшие свойства минимальных функций

Теорема

- *Минимальная функция для* β *— неприводимый многочлен над* $GF(q)$.
- *Если многочлен* $f(x)$ *таков, что* $f(\beta) = 0$, *то* $m(x) | f(x)$, *где* $m(x)$ *— минимальная функция для* β.
- *Минимальная функция для* β *единственна (обратное вообще говоря неверно!)*
- *Для каждого элемента* $\beta \in GF(q^m)$ *существует минимальная функция.*
- *Степень минимальной функции элемента* $\beta \in GF(q^m)$ *— делитель* m.

Теорема о корнях многочленов в $GF(q)$

Теорема

Если $f(x)$ многочлен над $GF(q)$, $\beta \in GF(q^m)$ и $f(\beta) = 0$, то $f(\beta^q) = 0$.

Доказательство

Пусть $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ Согласно теореме о биноме Ньютона над конечным полем:

$$(f(x))^q = (a_0)^q + (a_1)^q x^q + \ldots + (a_n)^q x^{nq} = a_0 + a_1 x^q + \ldots + a_n x^{nq} = f(x^q),$$

так как $a_i \in GF(q)$, а потому $a_i^{q-1} = 1$, и $a_i^q = a_i$.

Делители $x^{q^m} - x$

Теорема

Неприводимые над $GF(q)$ многочлены $p(x)$, степени n которых делят m, и только они, являются делителями многочлена $x^{q^m} - x$. Т. е. многочлен $x^{q^m} - x$ распадается на произведение минимальных функций всех элементов поля $GF(q^m)$.

Пример

Пусть $m = 3$. $x^{2^3} - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$. Мы перечислили 2 неприводимых многочлена степени 1, которые являются минимальными функциями 0 и 1, а также все 2 неприводимых многочлена 3 степени, которые являются минимальными функциями для $\{\alpha,\alpha^2,\alpha^4\}$ и $\{\alpha^3,\alpha^5,\alpha^6\}$ (для поля из примера 1).

Пример для $x^{16} - x$

При $m = 4$

$$x^{2^4} - x = x(x+1)m_5(x)m_1(x)m_7(x)m_3(x),$$

где

$$m_5(x) = x^2 + x + 1$$

$$m_1(x) = x^4 + x + 1$$

$$m_7(x) = x^4 + x^3 + 1$$

$$m_3(x) = x^4 + x^3 + x^2 + x + 1.$$

Корнями минимальных функций $m_5(x), m_1(x), m_7(x), m_3(x)$ будут соответственно
В примере 1:

$$(\alpha^5, \alpha^{10}); (\alpha, \alpha^2, \alpha^4, \alpha^8); (\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}); (\alpha^3, \alpha^6, \alpha^{12}, \alpha^9)$$

В примере 2:

$$(\beta^5, \beta^{10}); (\beta^7, \beta^{14}, \beta^{13}, \beta^{11}); (\beta, \beta^2, \beta^4, \beta^8); (\beta^3, \beta^6, \beta^{12}, \beta^9)$$

Сопряженные элементы поля

Определение

Элементы поля, являющиеся корнями одного и того же неприводимого многочлена, называются сопряженными элементами поля.

Теорема

Все корни одного и того же неприводимого многочлена имеют одинаковый порядок.

Как строить минимальные функции?

Требуемые результаты:

Теорема

Все корни $\beta, \beta^q, \ldots, \beta^{q^{m1}} \in GF(q^m)$ *неприводимого над* $GF(q)$ *многочлена* $p(x)$ *степени* m *различны.*

Теорема

Если $f(x)$ *многочлен над* $GF(q)$, $\beta \in GF(q^m)$ *и* $f(\beta) = 0$, *то* $f(\beta^q) = 0$.

Теорема

Степень минимальной функции элемента $\beta \in GF(q^m)$ *— делитель* m.

Алгоритм построения минимальной функции

1. Фиксируем $\beta \in GF(q^m)$ для которого строится минимальная функция
2. Вычисляем последовательность: β, β^q, β^{q^2}, ... β^{q^i}, ... до тех пор, пока не найдем такой j : $\beta^{q^j} = \beta$. Такой номер всегда найдется (почему?)
3. Всего получим n различных β, β^q, ..., β^{q^n}, где n - некоторый делитель m (почему?)
4. Тогда $m_\beta(x) = (x - \beta)(x - \beta^q)...(x - \beta^{q^n})$

Проверка: после раскрытия скобок многочлен $m_\beta(x)$ должен быть над $GF(q)$!

Пример построения минимальной функции - начало

Построим минимальный многочлен $m_7(x)$ для элемента $\gamma = \alpha^7 \in GF(2^4)$ (Пример 1)
Вначале найдем все корни минимального многочлена. Имеем последовательно:

$$\gamma = \alpha^7,$$

$$\gamma^{2^1} = (\alpha^7)^2 = \alpha^{14},$$

$$\gamma^{2^2} = (\alpha^7)^4 = \alpha^{28} = \alpha^{15} * \alpha^{13} = \alpha^{13},$$

$$\gamma^{2^3} = (\alpha^7)^8 = \alpha^{56} = (\alpha^{15})^3 \alpha^{11},$$

а уже

$$\gamma^{2^4} = (\alpha^7)^{16} = \alpha^{112} = (\alpha^{15})^7 \alpha^7 = \alpha^7,$$

то есть мы зациклились. Это значит, что вместе с корнем α^7 корнями минимальной функции $m_7(x)$ будут также $\alpha^{14}, \alpha^{13}, \alpha^{11}$.

Пример построения минимальной функции - продолжение

Теперь нам необходимо вычислить:

$$m_7(x) = (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14})$$

Умножим скобки попарно и сгруппируем:

$$m_7(x) = (x^2+(\alpha^7+\alpha^{11})x+\alpha^7\alpha^{11})(x^2+(\alpha^{13}+\alpha^{14})x+\alpha^{13}\alpha^{14}),$$

применим таблицу сложения: $\alpha^7+\alpha^{11}=\alpha^8$, $\alpha^{13}+\alpha^{14}=\alpha^2$, тогда

$$m_7(x) = (x^2+\alpha^8x+\alpha^3)(x^2+\alpha^2x+\alpha^{12}),$$

$$m_7(x) = x^4+(\alpha^2+\alpha^8)x^3+(\alpha^{12}+\alpha^3+\alpha^{10})x^2+(\alpha^5+\alpha^5)x+1,$$

далее $\alpha^5+\alpha^5=0$, $\alpha^2+\alpha^8=1$, $\alpha^{12}+\alpha^3+\alpha^{10}=\alpha^{10}+\alpha^{10}=0$
Таким образом,

$$m_7(x) = x^4+x^3+1$$

Примитивные многочлены и примитивные элементы поля

Определение

Порядок корней неприводимого многочлена называется показателем, которому этот многочлен принадлежит. Если корни неприводимого многочлена являются порождающими (образующими) элементами мультипликативной группы поля, то корни называются примитивными, а сам неприводимый многочлен — примитивным.

Пример

Два неприводимых многочлена $x^4 + x + 1, x^4 + x^3 + 1$ *— примитивные. Неприводимый многочлен* $x^4 + x^3 + x^2 + x + 1$ *не является неприводимым. Его корни порождают подгруппу* 5 *порядка:*

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$$

отсюда

$$\xi^5 = \xi^4 + \xi^3 + \xi^2 + \xi = 1,$$

а значит $\xi^5 = 1$. *порождает подгруппу* 5 *порядка мультипликативной группы* $GF^*(2^4)$.

Циклотомические классы

Определение

Комплект показателей степеней в комплекте сопряженных элементов называется циклотомическим классом. Если i *минимальный показатель в этом комплекте, то циклотомическим классом будет* $i, i^q, i^{q^2}, \ldots, i^{q^{t-1}}$, *где* t *— степень неприводимого многочлена, корнями которого являются упомянутые сопряженные элементы. В случае поля* $GF(q^m)$ *указанные показатели степеней приводятся по модулю* $q^m - 1$.