НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Модуль 1. Математические основы помехоустойчивого кодирования

Конечные поля. Представление конечных полей. Арифметика конечных полей.

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

12 июня 2020 г.

Классы вычетов по модулю m

Пусть $m \in \mathbb{N}$, $m > 1$.

Определение

Два числа $a,b \in \mathbb{Z}$ *называются сравнимыми по модулю* m*, если при делении на* m *дают одинаковые остатки, т. е.*
$a = mt_1 + r$, $b = mt_2 + r$*. Запись:* $a \equiv b \mod m$*.*

Числа, сравнимые по модулю m, образуют класс чисел по модулю m. Всего имеется m классов; любое число можно представить в виде

$$mq + r, r = 0,1,...,m-1.$$

Взяв от каждого класса по одному вычету, получим полную систему вычетов по модулю m. В качестве полной системы вычетов употребляют наименьшие неотрицательные вычеты: $0, 1, ..., m-1$
Если p — простое, то полная система вычетов по модулю p образует поле $GF(p)$

Неприводимый многочлен

Пусть $F[x]$ — множество всех многочленов $f(x)$ всевозможных неотрицательных степеней с коэффициентами из поля $GF(p)$:

$$F[x] = \{f(x) : f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n + ..., f_i \in GF(p)\}.$$

Введем определение:

Определение

Многочлен $p(x) = a_0 + a_1 x + ... + a_m x^m$ называется неприводимым над полем $GF(p)$, если он не распадается на множители над этим полем.

Пример

Следующие многочлены неприводимы над $GF(2)$:

$$p(x) = x^2 + x + 1, p(x) = x^4 + x + 1, p(x) = x^4 + x^3 + x^2 + x + 1$$

Классы вычетов по модулю неприводимого многочлена

Разобъем множество $F[x]$ на p^m классов вычетов по модулю неприводимого многочлена $p(x)$. Для этого рассмотрим все остатки от деления многочленов из $F[x]$ на $p(x)$.Они имеют вид $b(x) = b_0 + b_1 x + ... + b_{m-1} x^{m-1}, b_i \in GF(p)$.
Два многочлена из множества $F[x]$ называются сравнимыми по модулю многочлена $p(x)$, если при делении на $p(x)$ они дают одинаковый остаток.
Таким образом, множество $F[x]$ распадается на непересекающиеся классы многочленов, сравнимых по модулю $p(x)$. Обозначим множество этих классов символом

$$F[x]/(p(x))$$

Структура $F[x]/(p(x))$

Теорема

$F[x]/(p(x))$ - поле. То есть множество ненулевых остатков $F^*[x]/(p(x))$ образуют мультипликативную группу.

Пример

Рассмотрим неприводимые над $GF(2)$ многочлены $p(x) = x^3 + x + 1$ и $p(x) = x^3 + x^2 + 1$. Тогда:

$$F[x]/p(x) = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

$$F^*[x]/p(x) = \{1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

Вычислим $(x^2 + 1) * (x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1$
Если $p(x) = x^3 + x + 1$, *тогда:*

$$x^4 + x^3 + x + 1 = (x + 1)(x^3 + x + 1) + (x^2 + x),$$

а значит:

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

Продолжение примера

Вычислим $(x^2+1)+(x^2+x+1)=x$. Очевидно, что суммирование не зависит от $p(x)$, а зависит только от p.
Для $p(x)=x^3+x+1$ найдем разбиение множества элементов $F^*[x]/p(x)$ на взаимнообратные элементы:

$$x^2+1=x^{-1}, x^2+x+1=(x^2)^{-1}, x^2+x=(x+1)^{-1},$$

например: $(x^2+x+1)x^2=x^4+x^3+x^2=(x^3+x+1)(x+1)+1$, а значит $(x^2+x+1)x^2\equiv 1 \mod x^3+x+1$.
Пусть $p(x)=x^3+x^2+1$, тогда

$$(x^2+1)*(x^2+x+1)=x^4+x^3+x+1=x(x^3+x^2+1)+x\equiv x \mod p(x)$$

Для $p(x)=x^3+x^2+1$ найдем разбиение множества элементов $F^*[x]/p(x)$ на взаимнообратные элементы:

$$x^2+x=x^{-1}, x^2=(x+1)^{-1}, x^2+x+1=(x^2+1)^{-1},$$

например: $(x^2+x)x=x^3+x^2=(x^3+x^2+1)+1$, а значит

$$(x^2+x)x\equiv 1 \mod x^3+x^2+1.$$

Несколько выводов по примеру

- Элементы поля $F[x]/p(x)$ и мультипликативной группы $F^*[x]/p(x)$ не зависят от $p(x)$, а зависят только от его степени m и поля $GF(p)$. Поэтому поле вычетов по модулю $p(x)$ будем обозначать $GF(p^m)$.
- Сложение/вычитание в $GF(p^m)$ зависит только от p.
- Умножение/разбиение на обратные элементы в $GF(p^m)$ зависит от $p(x)$
- Сложение в $GF(p^m)$ задается обычным поразрядным сложением векторов/многочленов
- Умножение в $GF(p^m)$ сводится к умножению соответствующих многочленов по правилам поля $GF(p)$ и поиску остатка по модулю $p(x)$

Поле разложения двучлена $x^{p^m} - x$

Группа $GF^*(p^m)$ называется мультипликативной группой поля $GF(p^m)$, и ее порядок равен $p^m - 1$.
Это значит, что для любого $\alpha \in GF^*(p^m)$:

$$\alpha^{p^m - 1} = 1,$$

или $\alpha \in GF^*(p^m)$ является корнем уравнения:

$$x^{p^m - 1} - 1 = 0$$

Если добавить $\alpha = 0$, то все элементы поля $GF(p^m)$ являются корнями уравнения:

$$x^{p^m} - x = 0,$$

то есть

$$x^{p^m} - x = \prod_{\alpha_i \in GF(p^m)} (x - \alpha_i)$$

Цикличность группы $GF^*(p^m)$

Теорема

Группа $GF^*(p^m)$ циклична.

Пример

Пусть поле $GF(2^3)$ построено по модулю многочлена $p(x) = x^3 + x + 1$. Возведем элемент $x \in GF(2^3)$ в последовательные степени, помня, что каждую степень x^i следует разделить на $p(x)$ и взять остаток от деления:

$$
\begin{aligned}
x^0 &= 1, \\
x^1 &= x, \\
x^2 &= x^2, \\
x^3 &= 1 + x, \\
x^4 &= x + x^2, \\
x^5 &= 1 + x + x^2, \\
x^6 &= 1 + x^2, \\
x^7 &= x + x^3 = x + 1 + x = 1.
\end{aligned}
$$

В итоге все ненулевые элементы группы $GF^*(2^3)$ можно представить как степени одного элемента x.

Задание поля посредством корня неприводимого многочлена

Рассмотрим уравнение, заданное в поле действительных чисел $\mathbb{R}$:

$$x^2 + 1 = 0$$

Известно, что оно не имеет корней в $\mathbb{R}$, но назначив его корнем число $i = \sqrt{-1}$: $i^2 + 1 = 0$ мы получим его решение в некотором другом поле $\mathbb{C}$ - поле комплексных чисел.
По сути, мы построили $\mathbb{C} = \{x + iy, x, y \in \mathbb{R}, i^2 = -1\}$ благодаря присоединению числа $i \notin \mathbb{R}$ к исходному полю $\mathbb{R}$.
Аналогично, неприводимый многочлен $p(x)$ не имеет корней в $GF(p)$, но допустим, что он имеет корень $\alpha \in GF(p^m)$. Тогда $p(\alpha) = 0$. И $GF(p^m)$ есть расширение $GF(p)$ при помощи α.

Пример 1

Пусть $p = 2, m = 4$. Построим $GF^*(2^4)$ по модулю многочлена $p(x) = x^4 + x + 1$, при условии $p(\alpha) = 0$, или, что то же $\alpha^4 = \alpha + 1$. Напомним, что в поле характеристики $p = 2$ выполняется равенство $y = y$.

$$
\begin{array}{llllll}
\alpha^0 = & 1 & & & & = (1000) \\
\alpha^1 = & & \alpha & & & = (0100) \\
\alpha^2 = & & & \alpha^2 & & = (0010) \\
\alpha^3 = & & & & \alpha^3 & = (0001) \\
\alpha^4 = & 1 & +\alpha & & & = (1100) \\
\alpha^5 = & & \alpha & +\alpha^2 & & = (0110) \\
\alpha^6 = & & & \alpha^2 & +\alpha^3 & = (0011) \\
\alpha^7 = & 1 & +\alpha & & +\alpha^3 & = (1101) \\
\alpha^8 = & 1 & & \alpha^2 & & = (1010) \\
\alpha^9 = & & \alpha & & +\alpha^3 & = (0101) \\
\alpha^{10} = & 1 & +\alpha & +\alpha^2 & & = (1110) \\
\alpha^{11} = & & \alpha & +\alpha^2 & +\alpha^3 & = (0111) \\
\alpha^{12} = & 1 & +\alpha & +\alpha^2 & +\alpha^3 & = (1111) \\
\alpha^{13} = & 1 & & +\alpha^2 & +\alpha^3 & = (1011) \\
\alpha^{14} = & 1 & & & +\alpha^3 & = (1001) \\
\alpha^{15} = & 1 & & & & = (1000).
\end{array}
$$

Пример 2

Пусть $p = 2, m = 4$. Построим $GF^*(2^4)$ по модулю многочлена $p(x) = x^4 + x^3 + 1$, при условии $p(\beta) = 0$, или, что то же $\beta^4 = \beta^3 + 1$. Напомним, что в поле характеристики $p = 2$ выполняется равенство $y = y$.

$$
\begin{array}{llllll}
\beta^0 = & 1 & & & & = (1000) \\
\beta^1 = & & \beta & & & = (0100) \\
\beta^2 = & & & \beta^2 & & = (0010) \\
\beta^3 = & & & & \beta^3 & = (0001) \\
\beta^4 = & 1 & & & +\beta^3 & = (1001) \\
\beta^5 = & 1 & +\beta & & +\beta^3 & = (1101) \\
\beta^6 = & 1 & +\beta & +\beta^2 & +\beta^3 & = (1111) \\
\beta^7 = & 1 & \beta & +\beta^2 & & = (1110) \\
\beta^8 = & & \beta & +\beta^2 & +\beta^3 & = (0111) \\
\beta^9 = & 1 & & +\beta^2 & & = (1010) \\
\beta^{10} = & & \beta & & +\beta^3 & = (0101) \\
\beta^{11} = & 1 & & \beta^2 & +\beta^3 & = (1011) \\
\beta^{12} = & 1 & +\beta & & & = (1100) \\
\beta^{13} = & & \beta & +\beta^2 & & = (0110) \\
\beta^{14} = & & & \beta^2 & +\beta^3 & = (0011) \\
\beta^{15} = & 1 & & & & = (1000).
\end{array}
$$

Умножение в полях из примеров 1 и 2

Допустим, для поля из примера 1 требуется умножить (1110) и (0011), и получить результат также в векторной форме. Алгоритм умножения следующий:

- Найти экспоненциальное представление: $(1110) = \alpha^{10}$, $(0011) = \alpha^{6}$
- Умножить экспоненциальные представления и учесть порядок группы: $\alpha^{10}\alpha^{6} = \alpha^{16} = \alpha^{15}\alpha = \alpha$
- Найти векторное представление $\alpha = (0100)$.
- Таким образом, $(1110) * (0011) = (0100)$.

На самом деле, при данном представлении поля удобнее пользоваться не векторной, а именно экспоненциальной записью его элементов. В этом случае умножение тривиально!

Обращение элементов из примеров 1 и 2

Допустим, для поля из примера 2 требуется найти элемент, обратный к (1011), и получить результат также в векторной форме. Алгоритм обращения следующий:

- Найти экспоненциальное представление: $(1011) = \beta^{11}$,
- Обратить экспоненциальные представления и учесть порядок группы:
  $(1011)^{-1} = \left(\beta^{11}\right)^{-1} = \beta^{-11} = \beta^{-11}\beta^{15} = \beta^4$
- Найти векторное представление $\beta^4 = (1001)$
- Таким образом, $(1011)^{-1} = (1001)$.

Сложение элементов из примеров 1 и 2

Допустим, для поля из примера 1 требуется найти сумму $\alpha^5 + \alpha^{11}$ и записать результат в экспоненциальной форме. Алгоритм суммирования следующий:

- Найти векторно представление: $\alpha^5 = (0110)$, $\alpha^{11} = (0111)$
- Найти поэлементную сумммy векторов по модулю 2: $(0110) + (0111) = (0001)$
- Найти экспоненциальное представление $(0001) = \alpha^3$
- Таким образом, $\alpha^5 + \alpha^{11} = \alpha^3$.

Вместо того, чтобы применять такой алгоритм суммирования, удобно хранить таблицы сложения экспонент элементов.

Таблица сложения для примера 1

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Таблица сложения для примера 2

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0