Теория конечного поля

Теория конечных полей является центральной математической теорией, лежащей в основе помехоустойчивого кодирования и криптологии. Конечные поля используются при кодировании, в современных блоковых шифрах, в поточных шифрах, а также в открытых криптосистемах.

Поле — это множество F с двумя бинарными операциями: аддитивная операция (сложение) и мультипликативная операция (умножение), если оно (вместе с этими операциями) образует коммутативное ассоциативное кольцо с единицей, все ненулевые элементы которого обратимы.

Связанные определения

Характеристика поля:

В поле всегда есть единица, не равная нулю. В аддитивной группе поля единица порождает циклическую подгруппу ⟨1⟩ = {1, 1 + 1, 1 + 1 + 1, . . .}. Если данная группа конечна и содержит n элементов, то говорят, что характеристика поля равна n. Если циклическая группа ⟨1⟩ бесконечна, то говорят, что характеристика поля - нулевая. Если n НЕ 0, то n – простое число.

----------Дополнительная информация----------

Кольцо — это множество R, на котором заданы две бинарные операции: + и ×, со следующими свойствами:

1. $\forall a, b \in R\,(a + b = b + a)$ – коммутативность сложения;
2. $\forall a, b, c \in R\,(a + (b + c) = (a + b) + c)$ – ассоциативность сложения;
3. $\exists 0 \in R\,\forall a \in R\,(a + 0 = 0 + a = a)$ – существование нейтрального элемента относительно сложения;
4. $\forall a \in R\,\exists b \in R\,(a + b = b + a = 0)$ – существование обратного элемента относительно сложения;
5. $\forall a, b, c \in R \begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}$ – дистрибутивность.

Кольца могут обладать следующими свойствами:

- ассоциативность умножения: $\forall a, b, c \in R\,(a \times (b \times c) = (a \times b) \times c)$ (*ассоциативное кольцо*);
- наличие единицы: $\exists e \in R\,\forall a \in R\,(a \times e = e \times a = a)$ (*кольцо с единицей*);
- коммутативность умножения: $\forall a, b \in R\,(a \times b = b \times a)$ (*коммутативное кольцо*);
- отсутствие *делителей нуля*: $\forall a, b \in R\,(a \times b = 0 \Rightarrow a = 0 \vee b = 0)$.

Обычно под кольцом понимают ассоциативное кольцо с единицей. Кольца, для которых выполнены все вышеперечисленные условия, называются целостными.

Конечное поле (поле Галуа)

Конечное поле или поле Галуа (названо в честь Эвариста Галуа) — поле, состоящее из конечного числа элементов.

Свойства конечных полей

- Характеристика конечного поля является простым числом p.
- Число элементов в конечном поле F является степенью его характеристики: $|F| = p^q$.
- Для любого простого числа p и натурального числа q существует единственное с точностью до изоморфизма поле из элементов p^q. Это поле обозначается GF (p^q).
- Мультипликативная группа конечного поля является циклической (В теории групп группа называется циклической, если она порождена одним элементом **a**, то есть все её элементы являются степенями **a**).

Поля и арифметические операции в конечных множествах

В современных ЭВМ для хранения чисел обычно используется фиксированное число бит. Нетрудно посчитать, что всего существует 2^n различных n-битовых чисел. Другими словами, мы имеем некоторое конечное множество чисел. На этом множестве необходимо выполнять операции умножения, деления, сложения и вычитания, причем так, чтобы результат любой операции также был n-битовым числом! В этом случае говорят, что множество замкнуто относительно введенных операций.

Для операций вычитания и деления ключевыми являются понятия нулевого, единичного и обратного элементов (см. доп. информация):

- Если мы хотим из x вычесть y, мы находим противоположный элемент -y и складываем его с x.
- если мы хотим x разделить на ненулевой y, мы должны найти обратный элемент $\frac{1}{y}$ и умножить его на x.

Построение полей Галуа GF(p)

Для построения полей Галуа типа GF(p) необходимо использовать модульную арифметику.

Тогда:

- Сложение: (a + b) mod p;
- Умножение: (a * b) mod p;
- Противоположные элементы: g = (p – a);
- Обратные элементы: (a * b) mod p = 1.

Построение полей Галуа GF(p^n)

Если множество содержит p^n элементов, то модульной арифметикой пользоваться нельзя.

Для арифметических операций в поле типа GF(p^n) определены несколько другие правила.

Стоит сказать, что в рамках изучаемого предмета (а именно, основы криптографии) для нас в больше степени имеют значение арифметические операции в поле GF(2^n). О таких полях и будет идти речь ниже.

Сложение в поле GF(p^n)

Любое число можно представить в виде: $a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1}$, где $a \in \{0, \dots, p-1\}$.

По сути дела, это обычное представление числа в степени счисления с основанием p. Таким образом, любое число из нашего множества мы можем также рассматривать как вектор длины n: $a = [a_0, a_1, a_2, ..., a_{n-1}]$

Операция сложения двух чисел осуществляется через сложение соответствующих векторов p-ого разложения. Причем сложение компонентов векторов мы будем вести по модулю p.

На примере поля GF(2^n):

$$a = [a_0, a_1, a_2, ..., a_{n-1}], a_i \in \{0, 1\}$$

$$b = [b_0, b_1, b_2, ..., b_{n-1}], b_i \in \{0, 1\}$$

$$c = a + b = [(a_0 + b_0) mod 2, ..., (a_{n-1} + b_{n-1}) mod 2]$$

Несложно заметить, что операция сложения в поле GF(2^n) эквивалентна битовой операции «исключающее ИЛИ» (XOR). Что очень хорошо, поскольку современные процессоры могут выполнять данную операцию чрезвычайно быстро.

Умножение в поле GF(2^n)

По аналогии со сложением, необходимо представить множители в полиномиальной форме и перемножить соответствующие векторы. Причем операцию сложения следует заменить операцией XOR.

Однако, при перемножении двух многочленов, может получиться многочлен более высокой степени, который не будет соответствовать ни одному из чисел нашего множества. Это решается следующим образом. Выбирается неприводимый многочлен степени n (грубо говоря, это такой многочлен, который нельзя представить в виде произведения других многочленов). После это, используя алгоритм деления многочленов столбиком, мы делим результат произведения на неприводимый многочлен. При делении столбиком также используется операция XOR. Остаток от деления и будет произведением полиномов.

Пример:

$$5 \cdot 7 = x^4 + x^3 + x + 1 = \left| \begin{array}{c} \text{Добавим некоторые слагаемые} \\ \text{но так, чтобы ничего не изменилось} \\ \text{(еще раз напомню, что под сложением} \\ \text{понимаю сложение по модулю 2)} \end{array} \right| =$$

$$(x^4 + x^2 + x) + (x^3 + x + 1) + x^2 + x = x \cdot (x^3 + x + 1) + (x^3 + x + 1) + x^2 + x =$$

$$= \left| \begin{array}{c} \text{Так как } x^3 + x + 1 = 0, \text{то} \\ \text{полученное выражение} \\ \text{можно упростить} \end{array} \right| = x^2 + x = 110 = 6$$

Такой же результат можно получить как остаток от деления полинома, полученного при умножении на порождающий полином:

$$\begin{array}{rll} + & x^4 + x^3 + x + 1 & \mid x^3 + x + 1 \\ & \underline{x^4 + x^2 + x} & \mid \overline{x+1} \\ & x^3 + x^2 + 1 & \\ + & \underline{x^3 + x + 1} & \\ & x^2 + x & - \text{ Остаток от деления} \end{array}$$