Поля Галуа

Для работы с информацией при кодировании и декодировании данных все арифметические операции выполняются в полях Галуа. Применяется так называемая полиномиальная арифметика или арифметика полей Галуа. Таким образом, результат любой операции также является элементом данного поля. Конкретное поле Галуа состоит из фиксированного диапазона чисел. Характеристикой поля называют некоторое простое число p. Порядок поля, т.е. количество его элементов, является некоторой натуральной степенью характеристики pm, где m∈N. При m=1 поле называется простым. В случаях, когда m>1, для образования поля необходим еще порождающий полином степени m, такое поле называется расширенным. GF(p^m) – обозначение поля Галуа.

Для работы с цифровыми данными естественно использовать p=2 в качестве характеристики поля. При m=1 элементом кодовой последовательности будет бит, при m=8 – 8 бит, то есть байт. Собственно, коды Рида-Соломона работающие с байтами и являются наиболее распространенными.

Перед тем как переходить к операциям кодирования и декодирования разберемся с арифметикой полей Галуа на примере GF(2^3). Данное поле состоит из чисел от 0 до 7.

Операция сложения

Самой простой является операция сложения, которая является простым побитовым сложение по модулю 2 (XOP).

Пример: 5+3=110=6

$$\begin{array}{r} 1\,0\,1 \\ \oplus\ 0\,1\,1 \\ \hline 1\,1\,0 \end{array}$$

Операция умножения

К сожалению, операция умножения гораздо сложнее, чтобы ее осуществить, необходимо преобразовать числа в полиномиальную форму.

Пример: 5=101=1·x^2+0·x^1+1·x^0=x^2+1

Как можно заметить число в полиномиальной форме представляет собой многочлен, коэффициентами которого являются значения разрядов в двоичном представлении числа.

Перемножим два числа в полиномиальной форме:
5·7=(x^2+1)·(x^2+x+1)=x^4+x^3+x^2+x^2+x+1=x^4+x^3+x+1=11011=27

Итак, во-первых, следует заметить, что даже в полиномиальной форме осуществляется сложение по модулю 2, поэтому x^2+x^2=0. Во-вторых, результат умножения 27 не входит в используемое поле GF(23) (оно же состоит из чисел от 0 до 7, как было сказано выше). Чтобы бороться с этой проблемой, необходимо использовать порождающий полином. Порождающий полином является неприводимым, то есть простым (по аналогии с простыми числами делится без остатка на 1 и на самого себя). В арифметике полей Галуа неприводимым полиномом является аналог простых чисел. Используем для примера порождающий полином f(x)=x^3+x+1.

Также предполагается, что x удовлетворяет уравнению f(x)=x^3+x+1=0

Вернемся к примеру с умножением:

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

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

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

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

$$\begin{array}{rl} & x^4 + x^3 + x + 1 \\ + & x^4 + x^2 + x \\ \hline & x^3 + x^2 + 1 \\ + & x^3 + x + 1 \\ \hline & x^2 + x \end{array} \quad \left| \begin{array}{l} x^3 + x + 1 \\ \hline x+1 \end{array} \right.$$

\- Остаток от деления

Составим таблицу умножения:

Полиномиальное представление		**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	**1**	1	2	3	4	5	6	7
x	**2**	2	4	6	3	1	7	5
x+1	**3**	3	6	5	7	4	1	2
x^2	**4**	4	3	7	6	2	5	1
x^2+1	**5**	5	1	4	2	7	3	6
x^2+x	**6**	6	7	1	5	3	2	4
x^2+x+1	**7**	7	5	2	1	6	4	3

Операция деления

Операцию деления в полиномиальной форме понять, возможно, но достаточно тяжело. Поэтому гораздо лучше осуществлять его по таблице умножения.

Пример:6÷5=7

Большое значение имеет таблица степеней элементов поля Галуа. Возведение в степень также осуществляется в полиномиальной форме, аналогично умножению.

Пример:5^2=⟦(x^2+1)⟧^2=x^4+x^2+x^2+1=x^4+x^2+x+x^2+x+1=x·(x^3+x+1)=x^2+x+1=111=7

Таким образом, составим таблицу степеней:

			Степени							
			0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Полиномиальное представление	1	**1**	1	1	1	1	1	1	1	1
	x	**2**	1	2	4	3	6	7	5	1
	x+1	**3**	1	3	5	4	7	2	6	1
	x^2	**4**	1	4	6	5	2	3	7	1
	x^2+1	**5**	1	5	7	6	3	4	2	1
	x^2+x	**6**	1	6	2	7	4	5	3	1
	x^2+x+1	**7**	1	7	3	2	5	6	4	1

Таблица степеней обладает цикличностью: седьмая степень соответствует нулевой, значит восьмая соответствует первой и т.д. При желании можно это проверить.

В полях Галуа существует понятие примитивного члена – элемент поля, чьи степени содержать все ненулевые элементы поля. Просмотрев таблицу степеней видно, что этому условию соответствуют все элементы (ну кроме 1 естественно). Однако это выполняется не всегда, для примера приведу таблицу степеней для GF(16).

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

Для полей, которые мы рассматриваем, то есть с характеристикой 2, в качестве примитивного члена всегда выбирают 2. Учитывая его свойство, любой элемент поля можно выразить через степень примитивного члена.
Пример: 5=26, 7=25

Воспользовавшись этим свойством, и учитывая цикличность таблицы степеней, попробуем снова перемножить числа:
5·7=2^6·2^5=2^(6+5)=2^11=2^(11 mod 7)=2^4=6
Результат совпал с тем, что мы вычислили раньше.

А теперь выполним деление:
6÷5=2^4÷2^6=2^(4-6)=2^(-2)=2^((-2)mod 7)=2^5=7
Полученный результат тоже соответствует действительности.

Ну и для полноты картины посмотрим на возведение в степень:
$5^2=([\![2^6)]\!]^2=2^{(6\cdot 2)}=2^{12}=2^{(12 \bmod 7)}=2^5=7$
Опять неожиданно получился такой же результат.

Такой подход к умножению и делению гораздо проще, чем реальные операции с использование полиномов, и для них нет необходимости хранить большую таблицу умножения, а достаточно лишь строки степеней примитивного члена поля.