Computation in Finite Fields

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

August, 2016

Multiplication in GF

Multiplication of two polynomials is simple:

$$\alpha^m \cdot \alpha^n = \alpha^{m+n}$$

For example,

$$\begin{aligned} x^4 \cdot x^6 &= x^{10} \\ &= x^3 \end{aligned}$$

We can verify this equation,

$$\begin{aligned} x^4 \cdot x^6 &= (x + x^2)(1 + x^2) \\ &= x + x^2 + x^3 + x^4 \\ &= x + x^2 + (1 + x) + (x + x^2) \\ &= 1 + x \text{ which is equal to } x^3 \end{aligned}$$

Multiplication in the form of powers of x is easy to calculate. On the contrary, multiplying two polynomials is more complicated (complexity is $O(n^2)$).

Addition in GF

Addition is the opposite – it is not simple to calculate addition of two powers of x without knowing their polynomial forms.
We can use Zech's logarithm to quickly solve the addition of two polynomials:

$$\begin{aligned}\alpha^m + \alpha^n &= \alpha^m \cdot (1 + \alpha^{n-m}) \\ &= \alpha^m \cdot \alpha^{Z(n-m)} \\ &= \alpha^{m+Z(n-m)}\end{aligned}$$

The values of $Z(n)$ are typically precomputed and stored in a look-up table.

n	x^n	x^n as poly	$1+x^n$	$Z(n)$
0	1	1	0	$-\infty$
1	x	x	$1+x$	3
2	x^2	x^2	$1+x^2$	6
3	x^3	$1+x$	x	1
4	x^4	$x+x^2$	$1+x+x^2$	5
5	x^5	$1+x+x^2$	$x+x^2$	4
6	x^6	$1+x^2$	x^2	2
7	x^7	1	0	$-\infty$

Table: Zech's logarithm for GF(2^3).

For example, suppose we would like to add x^4 to x^6 in GF(2^3):

$$\begin{aligned} x^4 + x^6 &= x^4 \cdot (1 + x^2) \\ &= x^4 \cdot x^6 \\ &= x^{10} = x^3 \end{aligned}$$

Or, with the help of a look-up table:

$$\begin{aligned} x^4 + x^6 &= x^{4+Z(2)} \\ &= x^{4+6} \\ &= x^{10} = x^3 \end{aligned}$$