Introduction to Galois Field $GF(2^8)$

Ren-Shiou Liu
Dept. of Industrial and Information Management
National Cheng Kung University

What is a Galois Field?

- A field is a finite set in which we can do addition, subtraction, multiplication, and division without leaving the set
  - If the order of a finite field is p^n, where p is a prime number, we usually denote the field as $GF(p^n)$
  - GF stands for Galois field (加洛亞場、高氏場), in honor of the mathematician who first studied finite field

Galois Field $GF(2^8)$

- All the elements in this field represent polynomials in the range of $[0, x^8)$
- The coefficients of all the polynomials in this field are either 0 or 1
- For example: $x^7 + x + 1$
- Arithmetic on the coefficients is performed modulo 2
- If multiplication results in a polynomial of degree greater than 7, then the polynomial is reduced module some irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$
- Division a/b is defined as $a \times b^{-1}$

Addition

$$
\begin{array}{lll}
x^7 & +x^5+x^4+x^3 & +x+1 \\
 & +(x^3 & +x+1) \\
\hline
x^7 & +x^5+x^4 &
\end{array}
$$

(a) Addition

$$
\begin{array}{lll}
x^7 & +x^5+x^4+x^3 & +x+1 \\
 & -(x^3 & +x+1) \\
\hline
x^7 & +x^5+x^4 &
\end{array}
$$

(b) Subtraction

Multiplication

- With irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

- Consider two elements $A = (a_7 a_6 \dots a_0)$ and $B = (b_7 b_6 \dots b_0)$ in $GF(2^8)$
  - $A + B = (c_7 c_6 \dots c_0)$, where $c_i = a_i \oplus b_i$
  - $A \times 2 = \begin{cases} (a_6 a_5 \dots a_0 0) & \text{If } a_7 = 0 \\ (a_6 a_5 \dots a_0 0) \oplus (00011011) & \text{Otherwise} \end{cases}$

This technique is based on the observation that

$$x^8 \bmod m(x) = x^4 + x^3 + x + 1$$

- Consider

$$f(x) = x^6 + x^4 + x^2 + x + 1$$
$$g(x) = x^7 + x + 1$$
$$m(x) = x^8 + x^4 + x^3 + x + 1$$

- What is the result of $f(x) \times g(x)\ mod\ m(x)$?

$$(01010111) \times (00000010) = (10101110)$$
$$(01010111) \times (00000100) = (01011100) \oplus (00011011) = (01000111)$$
$$(01010111) \times (00001000) = (10001110)$$
$$(01010111) \times (00010000) = (00011100) \oplus (00011011) = (00000111)$$
$$(01010111) \times (00100000) = (00001110)$$
$$(01010111) \times (01000000) = (00011100)$$
$$(01010111) \times (10000000) = (00111000)$$

Solution:

$$
\begin{aligned}
&(01010111) \times (10000011) \\
&= (01010111) \\
&\times [(00000001) \oplus (00000010) \oplus (10000000)] \\
&= (01010111) \oplus (10101110) \oplus (00111000) \\
&= (11000001)
\end{aligned}
$$

Multiplicative Inverse

- The multiplicative inverse of $x^6 + x^3 + 1$ in $\mathrm{GF}(2^8)$ defined over the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ can be obtained using the extended Euclidean algorithm

i	r_i	q_i	y_i
-1	$x^8 + x^4 + x^3 + x + 1$		0
0	$x^6 + x^3 + 1$		1
1	$x^5 + x^4 + x^3 + x^2 + x + 1$	x^2	x^2
2	x^3	$x + 1$	$x^3 + x^2 + 1$
3	$x^2 + x + 1$	$x^2 + x + 1$	$x^5 + x^2 + x + 1$
4	1	$x + 1$	$x^6 + x^5 + x^2$

$$\boldsymbol{y_i = y_{i-2} - q_i y_{i-1}}$$