MEMO NAME: GFAU URCAD Handout

SUBJECT: Analytical Approach to Generating Elements in the Galois Field

DATE: April 25, 2018

---

1 Elements

Once a polynomial is determined irreducible and primitive, its elements may be generated. The number of elements grow exponentially, $2^n - 1$, where n is the highest degree of the polynomial. This document will prove the generation of the elements in the polynomial

$$GF[x](2^3) = x^3 + x^2 + x^0$$

as well as demonstrate sample operations between them.

Proof. Let $\beta \in GF(2^3)$ be a root of $x^3 + x^2 + x^0$. That is, $\beta^3 + \beta^2 + \beta^0 = 0$
$\therefore$ The coefficients are in $GF(2) \implies \beta^3 = \beta^2 + \beta^0$
Since a field contains the additive and multiplicative identities,

$$\{0, 1 = \beta^0\} \in GF(2^3)$$

Also, because of closure of multiplication in a field,

$$\{\beta^1, \beta^2, \beta^3\} \in GF(2^3)$$

But,

$$\beta^3 = \beta^2 + \beta^0$$

$$\begin{aligned}\because \beta^4 &= \beta^1 \times \beta^3 \\ &= \beta^1 \times (\beta^2 + \beta^0) \\ &= \beta^3 + \beta^1 \\ &= \beta^2 + \beta^1 + \beta^0\end{aligned}$$

$$\begin{aligned}\because \beta^5 &= \beta^1 \times \beta^4 \\ &= \beta^1 \times (\beta^2 + \beta^1 + \beta^0) \\ &= \beta^3 + \beta^2 + \beta^1 \\ &= \beta^2 + \beta^0 + \beta^2 + \beta^1 \\ &= \beta^1 + \beta^0\end{aligned}$$

$$\begin{aligned}\because \beta^6 &= \beta^1 \times \beta^5 \\ &= \beta^1 \times (\beta^1 + \beta^0) \\ &= \beta^2 + \beta^1\end{aligned}$$

$$\begin{aligned}\because \beta^7 &= \beta^1 \times \beta^6 \\ &= \beta^1 \times (\beta^2 + \beta^1) \\ &= \beta^3 + \beta^2 \\ &= \beta^2 + \beta^0 + \beta^2 \\ &= \beta^0 = 1\end{aligned}$$

In conclusion, $\{0, \beta^0, \beta^1, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\} \in GF(2^3)$ □

2 Operations

The operations supported by the Galois Field Arithmetic Unit are

(a) Addition / Subtraction (bitwise exclusive disjunction): $\beta^i \pm \beta^j = \beta^i \oplus \beta^j$

(b) Multiplication: $\beta^i \times \beta^j = \beta^{i+j \pmod{2^n-1}}$

(c) Division: $\beta^i \div \beta^j = \beta^{i-j \pmod{2^n-1}}$

(d) Logarithm: $\log \beta^i = i$