L10

Tuesday, August 9, 2022 9:45 AM

* Recall that GF(p) is represented in two ways.

Representation # 1:

$$GF(p) = \{0, 1, 2, \cdots, p-1\}.$$

Representation # 2:

$$GF(p) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{p-2}\}$$

where α is a primitive element.

For $GF(p^m)$, each element is "associated" with a polynomial with degree $m-1$. Because each element is a remainder of $g(x)$, which is of degree m.

E.g. $g(x) = x^2 + 1 \in F_2[x]$.

then $GF(3^2) \leftrightarrow \{0, 1, 2, x, x+1$

then $GF(3^2) \Leftrightarrow \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$

We can then interpret them as

$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

This representation is closely related to Representation #1.

Question: How do we represent $GF(p^m)$ by Representation #2?

Ans: We need to find a primitive element $\alpha \in GF(p^m)$.

* Recall that order$(\alpha) = l$ if l is the smallest integer such that $\alpha^l = 1$ in $GF(p^m)$

* $\alpha \in GF(p^m)$ is primitive if $\text{ord}(\alpha) = p^m - 1$

That is $1, \alpha, \alpha^2, \cdots, \alpha^{p^m-2}$ cover the entire $GF(p^m) \setminus \{0\}$.

* α can be found by exhaustively compute $\text{ord}(\alpha)$ for all $\alpha \in GF(p^m) \setminus \{0\}$

---

* There is a relationship between the primitive element $\alpha \in GF(p^m)$ and the irreducible polynomial that generates $GF(p^m)$ $g(x) \in F_p[x]$

* Theorem: Any irreducible $g(x) \in F_p[x]$ of degree m must be a divisor of $x^{p^m-1} - 1 \in F_p[x]$

proof: The set $\{x^l \bmod g(x) : l \geq 0\}$ is a finite, subgroup of $GF(p^m) \setminus \{0\}$ under operation $\cdot$

$\Rightarrow$ The number of elements in the subgroup $= lo$ then ① $x^{lo} \bmod g(x) = 1$ ② and lo is a factor of $p^m - 1$

$\Rightarrow x^{p^m-1} \bmod g(x) = \left(x^{lo}\right)^{\frac{p^m-1}{lo}} \bmod g(x)$

$= 1 \iff x^{p^m-1} = 1 + d(x)g(x)$

$\iff g(x)$ is a divisor of $x^{p^m-1} - 1$

* An irreducible polynomial of d primitive if $g(x)$ is not a divisor of $x^n - 1$ for all $n < p^m - 1$

That is, the smallest n such that $g(x)$ is a divisor of $x^n - 1$ is when $n = p^m - 1$.

---

* This part is tricky.