Minimal Polynomials

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

October 9, 2014

Factoring $x^q - x$ over a Field F_q and F_p

Example

$F = \{0, 1, y, y+1\} \subset \mathbb{F}_2[y]$ under $+$ and $*$ modulo $y^2 + y + 1$

$$\begin{aligned} x^4 - x &= x(x-1)(x-y)(x-y-1) \\ &= x(x+1)[x^2 - x(y+y+1) + y^2 + y] \\ &= x(x+1)(x^2+x+1) \end{aligned}$$

The prime subfield of F is $\mathbb{F}_2$. $x, x+1, x^2+x+1 \in \mathbb{F}_2[x]$ are called the minimal polynomials of F

Example

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

$$x^5 - x = x(x-1)(x-2)(x-3)(x-4)$$

The prime subfield of $\mathbb{F}_5$ is $\mathbb{F}_5$.
$x, x-1, x-2, x-3, x-4 \in \mathbb{F}_5[x]$ are called the minimal polynomials of $\mathbb{F}_5$

Factoring $x^q - x$ over a Field F_q and F_p

- Let F_q be a finite field with characteristic p
- F_q has a subfield isomorphic to $\mathbb{F}_p$
- Consider the polynomial $x^q - x \in F_q[x]$
- Since the prime subfield contains ± 1, $x^q - x \in \mathbb{F}_p[x]$
- $x^q - x$ factors into a product of prime polynomials $g_i(x) \in \mathbb{F}_p[x]$

  $$x^q - x = \prod_i g_i(x)$$

  The $g_i(x)$'s are called the minimal polynomials of F_q
- There are two factorizations of $x^q - x$

$$x^q - x = \prod_{\beta \in F_q} (x - \beta) = \prod_i g_i(x) \implies g_i(x) = \prod_{j=1}^{\deg g_i(x)} (x - \beta_{ij})$$

- Each $\beta \in F_q$ is a root of exactly one minimal polynomial of F_q, called the minimal polynomial of β

Properties of Minimal Polynomials (1)

Let F_q be a finite field with characteristic p. Let $g(x)$ be the minimal polynomial of $\beta \in F_q$.
$g(x)$ is the monic polynomial of least degree in $\mathbb{F}_p[x]$ such that $g(\beta) = 0$

Proof.

- Let $h(x) \in \mathbb{F}_p[x]$ be a monic polynomial of least degree such that $h(\beta) = 0$
- Dividing $g(x)$ by $h(x)$, we get $g(x) = q(x)h(x) + r(x)$ where $\deg r(x) < \deg h(x)$
- Since $r(x) \in \mathbb{F}_p[x]$ and $r(\beta) = 0$, by the least degree property of $h(x)$ we have $r(x) = 0 \implies h(x)$ divides $g(x)$
- Since $g(x)$ is irreducible and $\deg h(x) = \deg g(x)$
- Since both $h(x)$ and $g(x)$ are monic, $h(x) = g(x)$

□

Properties of Minimal Polynomials (2)

Let F_q be a finite field with characteristic p. Let $g(x)$ be the minimal polynomial of $\beta \in F_q$.
For any $f(x) \in \mathbb{F}_p[x]$, $f(\beta) = 0 \iff g(x)$ divides $f(x)$

Proof.

- ($\Longleftarrow$) If $g(x)$ divides $f(x)$, then $f(x) = a(x)g(x)$
  $\implies f(\beta) = a(\beta)g(\beta) = 0$
- ($\Longrightarrow$) Suppose $f(x) \in \mathbb{F}_p[x]$ and $f(\beta) = 0$
- Dividing $f(x)$ by $g(x)$, we get $f(x) = q(x)g(x) + r(x)$ where $\deg r(x) < \deg g(x)$
- Since $r(x) \in \mathbb{F}_p[x]$ and $r(\beta) = 0$, by the least degree property of $g(x)$ we have $r(x) = 0 \implies g(x)$ divides $f(x)$

$\square$

Linearity of Taking pth Power

Let F_q be a finite field with characteristic p.

- For any $\alpha, \beta \in F$

$$(\alpha+\beta)^p = \sum_{j=0}^{p} \binom{p}{j} \alpha^j \beta^{p-j} = \alpha^p + \beta^p$$

- For any integer $n \geq 1$,

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

- For any $g(x) = \sum_{i=0}^{m} g_i x^i \in F[x]$,

$$\begin{aligned} [g(x)]^{p^n} &= \left(g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m\right)^{p^n} \\ &= g_0^{p^n} + g_1^{p^n} x^{p^n} + g_2^{p^n} x^{2p^n} + \cdots + g_m^{p^n} x^{mp^n} \end{aligned}$$

Test for Membership in $\mathbb{F}_p[x]$

Let F_q be a finite field with characteristic p. F has a subfield isomorphic to $\mathbb{F}_p$. For any $g(x) \in F[x]$

$$g^p(x) = g(x^p) \iff g(x) \in \mathbb{F}_p[x]$$

Note that $g(x) \in \mathbb{F}_p[x] \iff$ all its coefficients g_i belong to $\mathbb{F}_p$

Proof.

$$\begin{aligned} g^p(x) &= \left(g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m\right)^p \\ &= g_0^p + g_1^p x^p + g_2^p x^{2p} + \cdots + g_m^p x^{mp} \\ g(x^p) &= g_0 + g_1 x^p + g_2 x^{2p} + \cdots + g_m x^{mp} \end{aligned}$$

$$g^p(x) = g(x^p) \iff g_i^p = g_i \iff g_i \in \mathbb{F}_p$$

$\square$

Roots of Minimal Polynomials

Theorem

Let F_q be a finite field with characteristic p. Let $g(x)$ be the minimal polynomial of $\beta \in F_q$.
If $q = p^m$, then the roots of $g(x)$ are of the form

$$\left\{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\right\}$$

where n is a divisor of m

Proof.

We need to show that

- There is an integer n such that β^{p^i} is a root of $g(x)$ for $1 \leq i < n$
- n divides m
- All the roots of $g(x)$ are of this form

Roots of Minimal Polynomials

Proof continued.

- Since $g(x) \in \mathbb{F}_p[x]$, $g^p(x) = g(x^p)$
- If β is a root of $g(x)$, then β^p is also a root
- $\beta^{p^2}, \beta^{p^3}, \beta^{p^4}, \ldots,$ are all roots of $g(x)$
- Let n be the smallest integer such that $\beta^{p^n} = \beta$
- All elements in the set $\beta, \beta^p, \beta^{p^2}, \beta^{p^3}, \ldots, \beta^{p^{n-1}}$ are distinct
- If $\beta^{p^a} = \beta^{p^b}$ for some $0 \leq a < b \leq n-1$, then

$$\left(\beta^{p^a}\right)^{p^{n-b}} = \left(\beta^{p^b}\right)^{p^{n-b}} \implies \beta^{p^{n+a-b}} = \beta^{p^n} = \beta$$

- If n does not divide m, then $m = qn + r$ where $0 < r < n$

$$\beta^{p^m} = \beta \implies \beta^{p^r} = \beta$$

which is a contradiction

Roots of Minimal Polynomials

Proof continued.

- It remains to be shown that $\left\{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\right\}$ are the only roots of $g(x)$
- Let $h(x) = \prod_{i=0}^{n-1}(x - \beta^{p^i})$
- $h(x) \in \mathbb{F}_p[x]$ since

$$h^p(x) = \prod_{i=0}^{n-1}(x - \beta^{p^i})^p = \prod_{i=0}^{n-1}(x^p - \beta^{p^{i+1}}) = \prod_{i=0}^{n-1}(x^p - \beta^{p^i}) = h(x^p)$$

- Since $g(x)$ is the least degree monic polynomial in $\mathbb{F}_p[x]$ with β as a root, $g(x) = h(x)$

$\square$

Note: The roots of a minimal polynomial are said to form a cyclotomic coset

Minimal Polynomials of F_{16}

The prime subfield of F_{16} is $\mathbb{F}_2$.

$$x^{16}+x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

Let $F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ where α is a root of $x^4 + x + 1$

- x has root 0 and $x + 1$ has root 1
- The roots of $x^2 + x + 1$ are $\{\alpha^5, \alpha^{10}\}$
- The roots of $x^4 + x + 1$ are $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$
- The roots of $x^4 + x^3 + 1$ are $\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$
- The roots of $x^4 + x^3 + x^2 + x + 1$ are $\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$

Questions? Takeaways?