10/2/2021   Lecture 10 (Construction of Finite fields)

Announcement

→ Quiz 2 will be on Feb 21

→ Please fill forms w.r.t term paper.

Prime Fields → Finite fields whose size is a prime number

$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. addition & multiplication are (mod p) operations

0 → additive identity

1 → multiplicative identity

Existence of multiplicative inverse was guaranteed using Extended Euclidean division algorithm.

Size of a finite field can be either a prime number or power of a prime number.

Polynomial Arithmetic

$\mathbb{F}_p[x] \triangleq$ set of all polynomials over $\mathbb{F}_p$.

$$= \left\{ \sum_{i=0}^{d} a_i x^i \;\middle|\; a_i \in \mathbb{F}_p,\ d \geq 0 \right\}$$

d is the largest integer s.t. $a_d \neq 0$
d is known as $\deg(f)$.

$(\mathbb{F}_p[x], +, \mathbb{F}_p, \cdot)$.

Example:- $f(x) = 1 + 2x + 3x^2$
$g(x) = (1+4x)$

$\mathbb{F}_5$.

$$f(x) \cdot g(x) = (1+2x+3x^2)(1+4x)$$
$$= 1 + x + x^2 + 2x^3$$

for every coeff, you are doing a (mod 5) operation.

Euclidean Division algorithm & Extended EDA algorithm for polynomials.

$f(x)$ with $\deg(f) = t$
$g(x)$ with $\deg(g) = s$.
$t \geq s$.

$$f(x) = q(x)\,g(x) + \underline{r(x)} \leftarrow \text{Unique representation}$$

$$\deg(r(x)) < \deg(g(x))$$

GCD of two polynomials (f, g)

Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{F}_p[x]$. gcd of $f(x)$ and $g(x)$ is a polynomial $h(x)$ satisfying the following properties

1. $h(x) \mid f(x)$ and $h(x) \mid g(x)$
2. If any other polynomial $p(x)$
   $p(x) \mid f(x)$ and $p(x) \mid g(x)$,
   then $p(x) \mid h(x)$.

$h(x)$ is required to be a monic polynomial for it to be called a gcd.

If $d = \deg(h)$; $a_d \neq 0$

For monic polynomials, $a_d = 1$.

Using EDA; we want to compute the gcd of $x^6+x^3+x^2+1$ and x^3+1. over $\mathbb{F}_2$

$$x^3$$

$$x^3+1 \overline{\big)\, x^6+x^3+x^2+1}$$

$$x^6+x^3$$

$$x$$

$$x^2+1 \overline{\big)\, x^3+1}$$

$$x^3+x$$

$$x+1$$

$$\underline{\underline{x+1}} \overline{\big)\, x^2+1}$$

$$x^2+1$$

$$0.$$

$$(x+1)^2 = x^2+2x+1$$

$$= x^2+1$$

$$\gcd\left(x^6+x^3+x^2+1,\ x^3+1 \right)$$

$=$ Last nonzero remainder

$(x+1)$

gcd can be expressed as linear combination of the polynomials $f(x)$ & $g(x)$.

Remainders	$x^6+x^3+x^2+1$	x^3+1	Quotients
$x^6+x^3+x^2+1$	1	0	
$\to x^3+1$	0	1	x^3
$\to x^2+1$	$1-0\cdot x^3=1$	$0-1\cdot x^3=x^3$	x
$x+1$	$0-1\cdot x=x$	$1-x^3\cdot x=1+x^4$	$x+1$
0			

$$\gcd\left(x^6+x^3+x^2+1,\ x^3+1\right)=x+1$$

$$h(x)=\underline{r(x)}f(x)+\underline{s(x)}g(x)$$

Extended EDA allows you to Compute $r(x)$ & $s(x)$ as well.

$$\Rightarrow r(x)=x$$
$$s(x)=1+x^4.$$

$$x\left(x^6+x^3+x^2+1\right)$$
$$+\left(1+x^4\right)\left(1+x^3\right)$$
$$=x^7+x^4+x^3+x$$
$$+x^7+x^4+x^3+1$$
$$=1+x.$$

Suppose we are operating on $\mathbb{F}_3$.
and suppose if gcd turned out to be
$2x+1$

$$2^{-1}(2x+1) = \underline{\underline{x+2}}$$

$2x+1$ & $x+2$ both very well qualify to be called gcd.

To resolve the ambiguity, we include that gcd by definition has to be a monic polynomials.

Irreducible Polynomials.

$f(x) \in \mathbb{F}_p[x]$.

$f(x)$ is said to be irreducible if.

$f(x) = g(x)\,h(x)$ is not possible

where $\deg(g(x)) < \deg(f(x))$

$\deg(h(x)) < \deg(f(x))$

$$\underline{\underline{2x+1}} = 2(\underline{\underline{x+2}})$$

Irreducible polynomials are analogs of prime numbers.

Irreducible polynomials over $\mathbb{F}_2$

$0, 1$

deg 1 $\quad x, \quad x+1$

deg 2 $\quad x^2+x+1$

deg 3 $\quad x^3+x+1, \quad x^3+x^2+1$

deg 4 $\quad x^4+x+1 \qquad x^4+x^3+x^2+x+1$
$\quad x^4+x^3+1$

First identify all reducible polynomials of a certain degree.

Reducible polynomials of deg 2 over $\mathbb{F}_2$

$$x \cdot x \qquad x\cdot(x+1) \qquad (x+1)^2.$$
$$\downarrow \qquad \downarrow \qquad \downarrow$$
$$x^2 \qquad x^2+x \qquad x^2+1.$$

These 3 polynomials are reducible

$$x^3+1 = (x+1)(x^2+x+1)$$

To construct prime fields, we were looking at $\mathbb{F}_p$ and doing (mod p) operations.

To construct fields of prime power, we will look at $\mathbb{F}_p[x]$ and do (mod $f(x)$) operations, where $f(x)$ is an irreducible polynomial over $\mathbb{F}_p$.

$\left\{ \mathbb{F}_p[x] \middle\backslash f(x) \right\}$ = finite field with no. of elements which is a power of prime "p"

Has p^d elements where $d = \deg(f)$.

Elements of this finite field will be equivalence classes of a certain relation.

Define a relation on $\mathbb{F}_p[x]$ w.r.t $f(x)$ as
$$g(x) \sim h(x) \text{ iff } f(x) \mid (g(x) - h(x)).$$

<u>Claim</u>:- The above relation is an equivalence relation.

(i) Reflexive: $g \sim g$; $f(x) \mid 0$.

(ii) Symmetry: $f \mid (g-h)$ then it also divides $f \mid (h-g)$.

(iii) Transitive $f \mid (g-h)$ and $f \mid (h-p)$; then $f \mid (g-p)$.

$\Rightarrow$ Equivalence relation partitions $\mathbb{F}_p[x]$ into equivalence classes.

Notation used for equivalence class is

$[a(x)] \to$ denotes equivalence class corresponding to element $a(x)$.

We will construct a finite field of $16 = 2^4$ elements $\to$ Need an irreducible polynomial of deg 4. $\Rightarrow f(x) = x^4 + x + 1$.

$\mathbb{F}_2[x] \mid (x^4+x+1)$. $\leftarrow$ Equivalence classes w.r.t polynomial $f(x) = x^4 + x + 1$.

$[1]$ $[x]$ $[x^2]$ $[x^3]$

$[1+x]$ $[1+x^2]$ $[1+x^3]$ $[x+x^2]$

$[x+x^3]$ $[x^2+x^3]$ $[1+x+x^2]$ $[1+x+x^3]$.

$[1+x^2+x^3]$ $[x+x^2+x^3]$ $[1+x+x^2+x^3]$ $[0]$.

x & x^2 cannot be in the same equivalence class w.r.t $f(x) = x^4+x+1$.

$f \mid (g-h)$.

$(x^4+x+1) \mid \underbrace{(x+x^2)}$

Any $g(x)$ which has a deg < 4; has to belong to a distinct equivalence class.

List all possible polynomials of deg ≤ 3. & they all constitute distinct equivalence classes. $a_3 x^3 + a_2 x^2 + a_1 x + a_0$. $\Rightarrow$ No. of polynomials $= 2^4 = 16$.

How do you add and multiply equivalence classes?

$$[x] + [x^2] = [x + x^2]$$

well defined operation which does not depend on which representative you choose for the equivalence class

$$[x^2] \cdot [x^3] = [x^2 \cdot x^3]$$
$$= [x^5]$$
$$= [x^2 + x]$$

$$x^5 \bmod (x^4 + x + 1)$$
$$= x^2 + x$$