Finite Fields

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

September 25, 2014

Fields

Definition

A set F together with two binary operations $+$ and $*$ is a field if

- F is an abelian group under $+$ whose identity is called 0
- $F^* = F \setminus \{0\}$ is an abelian group under $*$ whose identity is called 1
- For any $a, b, c \in F$

$$a * (b + c) = a * b + a * c$$

Definition

A finite field is a field with a finite cardinality.

Example

$\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$ with mod p addition and multiplication where p is a prime. Such fields are called prime fields.

Some Observations

Example

- $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$
- $2^5 = 2 \bmod 5$, $3^5 = 3 \bmod 5$, $4^5 = 4 \bmod 5$
- All elements of $\mathbb{F}_5$ are roots of $X^5 - X = 0$
- $2^2 = 4 \bmod 5$, $2^3 = 3 \bmod 5$, $2^4 = 1 \bmod 5$
- $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ is cyclic

Example

- $F = \{0, 1, X, X + 1\}$ under $+$ and $*$ modulo $X^2 + X + 1$
- $X^4 = X \bmod (X^2 + X + 1)$, $(X + 1)^4 = X + 1 \bmod (X^2 + X + 1)$
- All elements of F are roots of $Y^4 - Y = 0$
- $(X + 1)^2 = X \bmod (X^2 + X + 1)$, $(X + 1)^3 = 1 \bmod (X^2 + X + 1)$
- $F^* = \{1, X, X + 1\}$ is cyclic

Field Isomorphism

Definition

Fields F and G are isomorphic if there exists a bijection $\phi : F \to G$ such that

$$\begin{aligned} \phi(\alpha + \beta) &= \phi(\alpha) \oplus \phi(\beta) \\ \phi(\alpha \star \beta) &= \phi(\alpha) \otimes \phi(\beta) \end{aligned}$$

for all $\alpha, \beta \in F$.

Example

- $F = \left\{ a_0 + a_1 X + a_2 X^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $X^3 + X + 1$
- $G = \left\{ a_0 + a_1 X + a_2 X^2 \middle| a_i \in \mathbb{F}_2 \right\}$ under $+$ and $*$ modulo $X^3 + X^2 + 1$

Uniqueness of a Prime Field

Theorem

Every field F with a prime cardinality p is isomorphic to $\mathbb{F}_p$

Proof.

- Let F be any field with p elements where p is prime
- F has a multiplicative identity 1
- Consider the additive subgroup $S(1) = \langle 1 \rangle = \{1, 1+1, \ldots\}$
- By Lagrange's theorem, $|S(1)|$ divides p
- Since $1 \neq 0$, $|S(1)| \geq 2 \implies |S(1)| = p \implies S(1) = F$
- F is isomorphic to the group $\mathbb{Z}_p$ under addition
- Elements in F can be labelled as $\{0, 1, 2, \ldots, p-1\}$
- $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is a field under $*$ modulo p
- F is isomorphic to $\mathbb{F}_p$

$\square$

Subfields

Definition

A nonempty subset S of a field F is called a subfield of F if

- $\alpha + \beta \in S$ for all $\alpha, \beta \in S$
- $-\alpha \in S$ for all $\alpha \in S$
- $\alpha * \beta \in S$ for all nonzero $\alpha, \beta \in S$
- $\alpha^{-1} \in S$ for all nonzero $\alpha \in S$

Example

$F = \{0, 1, X, X + 1\}$ under $+$ and $*$ modulo $X^2 + X + 1$
$\mathbb{F}_2$ is a subfield of F

Characteristic of a Field

Definition

Let F be a field with multiplicative identity 1. The characteristic of F is the smallest integer p such that

$$\underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ times}} = 0$$

Examples

- $\mathbb{F}_2$ has characteristic 2
- $\mathbb{F}_5$ has characteristic 5
- $\mathbb{R}$ has characteristic 0

Theorem

The characteristic of a finite field is prime

Prime Subfield of a Finite Field

Theorem

Every finite field has a prime subfield.

Examples

- $\mathbb{F}_2$ has prime subfield $\mathbb{F}_2$
- $F = \{0, 1, X, X + 1\}$ under $+$ and $*$ modulo $X^2 + X + 1$ has prime subfield $\mathbb{F}_2$

Proof.

- Let F be any field with q elements
- F has a multiplicative identity 1
- Consider the additive subgroup $S(1) = \langle 1 \rangle = \{1, 1 + 1, \dots\}$
- $|S(1)| = p$ where p is the characteristic of F
- $S(1)$ is a subfield of F and is isomorphic to $\mathbb{F}_p$

□

Questions? Takeaways?