Finite Fields

Dr. E.SURESH BABU

Assistant Professor

Computer Science and Engineering Department

National Institute of Technology, Warangal

Warangal

Fields

Fields:

- A **Field, denoted {F,+,×},** is an **integral domain** whose elements satisfy the following additional property:
  - ✓ For every element **a in F**, except the **element designated 0** (which is the identity element for the ’+’ operator), there must also exist in **F its multiplicative inverse.**

Fields:

- ✓ In Other Words, if **a ∈ F and a ≠ 0**, then there must exist an **element b ∈ F** such that

$$\mathbf{ab = ba = 1}$$

- ✓ where **'1' symbolically** denotes the element which serves as the **identity element** for the multiplication operation.
- ✓ For a given **a**, such a **b** is often designated $\mathbf{a^{-1}}$.

Fields

- A field is a non-empty set F with **two binary operators** which are usually denoted by + and *, that satisfy the usual arithmetic properties:
  - ✓ **(F, +) is an Abelian group with (additive) identity denoted by 0.**
  - ✓ **(F, *) is an Abelian group with (multiplicative) identity denoted by 1.**
  - ✓ **The distributive law holds: $(a+b)*c = a*c+b*c$ for all a, b, c $\in$ F.**

Summary

Algebraic Structure	*Supported Typical Operations*	*Supported Typical Sets of Integers*
Group	$(+\ \ -)$ or $(\times\ \ \div)$	$\mathbf{Z}_n$ or $\mathbf{Z}_n{}^*$
Ring	$(+\ \ -)$ and $(\times)$	$\mathbf{Z}$
Field	$(+\ \ -)$ and $(\times\ \ \div)$	$\mathbf{Z}_p$

Finite Fields

Finite Fields

- If the set F is finite, then the field is said to be a **finite field.**
- The order of a finite field is the **number of elements** in the finite field.

Finite Fields

- By definition, **(Z, +, *)** does not form a field because (Z, *) is **not** a **multiplicative group.**
  - ✓ $\mathbf{Z_n}$ is not a finite field is because not every element in Z_n is guaranteed to have a **multiplicative inverse**
  - ✓ (Z_n, +, *) in general is **not** a finite field
- In particular, An element ‘a; of $\mathbf{Z_n}$ **does not** have a **multiplicative inverse** if ‘a’ is **not relatively prime** to the modulus n.

Prime Finite Fields

- For prime n, every element $a \in Z_n$ will be **relatively prime** to n
  - ✓ There will **exist a multiplicative inverse** for every $a \in Z_n$ for prime n
- If Z_p is a **finite field**,
  - ✓ when we assume p denotes a **prime number.**
  - ✓ Z_p is referred as a **prime finite field.**

Prime Finite Fields

- A **Prime Finite Field** is also called a **Galois Field,** which is named in honour of Évariste Galois

Galois Field

❖ A Galois field, **GF(p^n), is a finite field** with **p^n elements.**

❖When **n = 1,** we have GF(p) field.

✓ This field can be the set **Z_p= {0, 1, …, p − 1},** with two arithmetic operations

Example

❖ A very common field of Galois field is **GF(2)** with the **set {0, 1}** and two operations- **addition and multiplication,**

GF(2)

{0, 1} $+$ $\times$

$+$	0	1
0	0	1
1	1	0

Addition

$\times$	0	1
0	0	0
1	0	1

Multiplication

a	0	1
$-a$	1	0

a	0	1
a^{-1}	—	1

Inverses

XOR **AND**

Example

- GF(5) on the set **Z_5 (5 is a prime)** with **addition and multiplication operators**

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

GF(2^n) FIELDS

Why GF(2^n) Fields is used

- Using Modulo Arithmetic will **not construct** a finite field with order of **p^m for m > 1.**
- For Example,
  - ✓ **$2^3 = 8$,** and we've already known (Z_8, +, *) is **not a field.**

Why GF(2^n) Fields is used

- We need to work in GF(2^n) that uses a **set of 2^n elements.**
  - ✓ The elements in this set are **n-bit words.**
- Let us define a **GF(2^2) field** in which the set has **four 2-bit words: {00, 01, 10, 11}.**

GF(2^2) Fields

Addition

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

$\otimes$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

$GF(2^n)$ Fields is used

- One way to work with **$GF(2^n)$** is by using the **polynomial basis.**

Thank U