

## Ch. 4 Finite Fields

### □ Topics in the Chapter

- Definition and Construction of Finite Field
- Classification of Polynomials
- Zech Algorithm (Add-One Table)
- Additions and Multiplication
- Structure of Finite Fields

### □ Example of Fields

○ Field: set of objects such that  $+, -, \times, \div$  are defined

(a)  $F = Z =$  set of integers:

$+, -, \times$  are possible, but  $\div$  is not possible.  $\Rightarrow$  not a field

(b)  $F = Q =$  set of rational numbers:

$+, -, \times, \div$  are possible  $\Rightarrow$  a field

(c)  $F = R =$  set of real numbers:

$+, -, \times, \div$  are possible  $\Rightarrow$  a field

(d)  $F = C =$  set of complex numbers:

$+, -, \times, \div$  are possible  $\Rightarrow$  a field

(e)  $F = F_3 = \{0, 1, 2\}$  under addition and multiplication modulo 3:

$+$	$0$	$1$	$2$
$0$	$0$	$1$	$2$
$1$	$1$	$2$	$0$
$2$	$2$	$0$	$1$

$\cdot$	$0$	$1$	$2$
$0$	$0$	$0$	$0$
$1$	$0$	$1$	$2$
$2$	$0$	$2$	$1$

Note: Finite or infinite

## □ Definition and Construction of Finite Fields

### ○ Field $F$

set of objects under addition and multiplication satisfying the following axioms

(a) closure:

$$a + b \in F, \quad \forall a, b \in F$$

(b) associativity:

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

$$\forall a, b, c \in F$$

(c) identity:  $\exists 0 \in F$  such that

$$0 + a = a + 0 = a, \quad \forall a \in F$$

(d) inverse: For any  $a \in F$ ,  
there exists  $-a \in F$  such that

$$a + (-a) = (-a) + a = 0.$$

(e) commutativity:

$$a + b = b + a, \quad \forall a, b \in F$$

(a) closure:

$$a \cdot b \in F, \quad \forall a, b \in F$$

(b) associativity

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

$$\forall a, b, c \in F$$

(c) identity:  $\exists 1 \in F$  such that

$$1 \cdot a = a \cdot 1 = a, \quad \forall a \in F$$

(d) inverse: For any  $a (\neq 0) \in F$ ,

$$\exists a^{-1} \in F \text{ such that}$$

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

(e) commutativity:

$$a \cdot b = b \cdot a, \quad \forall a, b \in F$$

(f) distributivity:  $a(b + c) = ab + ac, \quad \forall a, b, c \in F$

○ Field size = Number of field elements =  $|F|$

Example:

$Q, R, C$ : infinite

$F_3$ : finite

○ Finite field: a field with finite number of elements

(a) Notation:  $F = \text{GF}(q)$  or  $F_q$  if  $|F| = q$ .

(b) Galois field = finite field

Note:

(a)  $F$  is a finite field

$$\Leftrightarrow |F| = p^m \text{ for some prime } p \text{ and integer } m$$

(b)  $F = \text{GF}(p^m) = F_{p^m}$

= finite field with  $p^m$  elements

"Galois field"

○ Prime field  $F_p$

(a)  $F_p = \{0, 1, 2, \dots, p-1\}$ , for a prime  $p$

(b) Addition:  $a + b \pmod{p}$

Multiplication:  $a \cdot b \pmod{p}$

Example:  $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$3 + 5 = 1 \quad 3 \cdot 5 = 1$$

$$2 + 3 = 5 \quad 2 \cdot 3 = 6$$

Note: There is at least one element whose powers constitute all nonzero elements of the finite field.  $\Rightarrow$  *Primitive* element

Example:  $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$$

$\Rightarrow$  3 is a primitive element of  $F_7$ .

Note that 5 is also a primitive element of  $F_7$ .

Note: For any nonzero element  $a \in F_p$ ,

$$a^{p-1} = 1.$$

Example:  $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$1^{p-1} = 1^6 = 1; \quad 2^{p-1} = 2^6 = 64 = 1; \quad 3^{p-1} = 3^6 = 1$$

$$4^{p-1} = 4^6 = 1; \quad 5^{p-1} = 5^6 = 1; \quad 6^{p-1} = 6^6 = 1$$

### □ Extensions to the Finite Field $F_{p^m}$

- Complex numbers  $C$  from real numbers  $R$

$$C = \{a_0 + a_1 i \mid a_0, a_1 \in R, i^2 + 1 = 0\}$$

$$\mid \Leftarrow x^2 + 1 \quad (i = \sqrt{-1})$$

$R$

$$(a) \text{ Addition: } (a_0 + a_1 i) + (b_0 + b_1 i) = (a_0 + b_0) + (a_1 + b_1) i$$

(b) Multiplication:

$$(a_0 + a_1 i)(b_0 + b_1 i) = a_0 b_0 + (a_0 b_1 + a_1 b_0) i + a_1 b_1 \overbrace{i^2}^{i^2 = -1}$$

$$\boxed{i^2 = -1} \quad \swarrow$$

$$= (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0) i$$

Note: This extension method can be applied to the finite field  $F_p$  to get

its extension field  $F_{p^m}$ .

○ Extension of the finite field  $F_p$ : ( $p = 2$ )

(a)  $F_4$  from  $F_2 = \{0, 1\}$

$$F_4 = \{a_0 + a_1\alpha \mid a_i \in F_2, \alpha^2 + \alpha + 1 = 0\}$$

$$\mid \Leftarrow x^2 + x + 1$$

$$F_2$$

$$\text{Addition: } (a_0 + a_1\alpha) + (b_0 + b_1\alpha) = (a_0 + b_0) + (a_1 + b_1)\alpha$$

Multiplication:

$$(a_0 + a_1\alpha)(b_0 + b_1\alpha) = a_0b_0 + (a_0b_1 + a_1b_0)\alpha + a_1b_1\alpha^2$$

$$\boxed{\alpha^2 = \alpha + 1} \quad \overline{\quad} \quad \swarrow$$

$$= (a_0b_0 + a_1b_1) + (a_0b_1 + a_1b_0 + a_1b_1)\alpha$$

(b)  $F_8$  from  $F_2 = \{0, 1\}$

$$F_8 = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in F_2, \alpha^3 + \alpha + 1 = 0\}$$

$$\mid \Leftarrow x^3 + x + 1$$

$$F_2$$

(c)  $F_{16}$  from  $F_2 = \{0, 1\}$

$$F_{16} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in F_2, \alpha^4 + \alpha + 1 = 0\}$$

$$\mid \Leftarrow x^4 + x + 1$$

$$F_2$$

○ Example of the finite field  $F_8$

(a)  $F_8 = F_{2^3}$  defined by  $p(x) = x^3 + x + 1$ .

$\alpha$ : an element of  $F_8$  satisfying  $\alpha^3 + \alpha + 1 = 0$ .

(b) Structure:

$$F_8 = \{ a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in F_2, \alpha^3 + \alpha + 1 = 0 \}$$

$$\mid \Leftarrow x^3 + x + 1$$

$$F_2$$

multiplicative representation	additive representation	vector representation ( $\alpha^0 \alpha^1 \alpha^2$ )
0	0	(0 0 0)
$\alpha^0$	1	(1 0 0)
$\alpha^1$	$\alpha$	(0 1 0)
$\alpha^2$	$\alpha^2$	(0 0 1)
$\alpha^3$	$1 + \alpha$	(1 1 0)
$\alpha^4$	$\alpha + \alpha^2$	(0 1 1)
$\alpha^5$	$1 + \alpha + \alpha^2$	(1 1 1)
$\alpha^6$	$1 + \alpha^2$	(1 0 1)
$\alpha^7 = 1$		

Addition:  $\alpha^3 + \alpha^4 = (1 + \alpha) + (\alpha + \alpha^2) = 1 + \alpha^2 = \alpha^6.$

$$(1 + \alpha^2) + (1 + \alpha + \alpha^2) = \alpha. \text{ (easy)}$$

Multiplication:  $\alpha^3 \cdot \alpha^4 = \alpha^7 = 1, \text{ (easy)}$

$$(1 + \alpha^2) \cdot (1 + \alpha + \alpha^2) = \alpha^6 \cdot \alpha^5 = \alpha^{11} = \alpha^4.$$

○ Properties of the finite field  $F_{p^m}$

- (a)  $F_{p^m}$  = set of roots of  $x^{p^m} - x$  over  $F_p$
- (b) For any  $\beta (\neq 0) \in F_{p^m}$ ,  $\beta^{p^m-1} = 1$ . (Fermat's theorem)
- (c) There exists an element  $\alpha \in F_{p^m}$  such that

$$\alpha^s \neq 1 \quad \text{for any nonnegative integer } s < p^m - 1.$$

Then the element  $\alpha$  is called a *primitive* element of  $F_{p^m}$ .

Note that any nonzero element in  $F_{p^m}$  can be expressed as a power of  $\alpha$ , that is,

$$F_{p^m} = \{0, \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{p^m-2}\}.$$

○ Example of the finite field  $F_{16}$

- (a)  $F_{16} = F_{2^4}$  defined by  $p(x) = x^4 + x + 1$ .

$\alpha$ : an element of  $F_{16}$  satisfying  $\alpha^4 + \alpha + 1 = 0$ .

- (b) Structure:

$$F_{16} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in F_2, \alpha^4 + \alpha + 1 = 0\}$$

$$\mid \Leftrightarrow x^4 + x + 1$$

$$F_2$$

multiplicative representation	additive representation	vector ( $\alpha^0, \alpha^1, \alpha^2, \alpha^3$ )
$\alpha^0$	1	(1 0 0 0)
$\alpha^1$	$\alpha$	(0 1 0 0)
$\alpha^2$	$\alpha^2$	(0 0 1 0)
$\alpha^3$	$\alpha^3$	(0 0 0 1)
$\alpha^4$	$1 + \alpha$	(1 1 0 0)
$\alpha^5$	$\alpha + \alpha^2$	(0 1 1 0)
$\alpha^6$	$\alpha^2 + \alpha^3$	(0 0 1 1)
$\alpha^7$	$1 + \alpha + \alpha^3$	(1 1 0 1)
$\alpha^8$	$1 + \alpha^2$	(1 0 1 0)
$\alpha^9$	$\alpha + \alpha^3$	(0 1 0 1)
$\alpha^{10}$	$1 + \alpha + \alpha^2$	(1 1 1 0)
$\alpha^{11}$	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
$\alpha^{12}$	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
$\alpha^{13}$	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
$\alpha^{14}$	$1 + \alpha^3$	(1 0 0 1)
$\alpha^{15}$	1	(1 0 0 0)

Note: To find an additive representation of  $\alpha^i$ :

(a) Compute

$$x^i = (x^4 + x + 1)Q_i(x) + R_i(x)$$

$$\Rightarrow x^i = R_i(x) \pmod{x^4 + x + 1}$$

$$\alpha^i = R_i(\alpha)$$

(b)  $F_{2^m} = \{0, R_0(\alpha), R_1(\alpha), \dots, R_{2^m-2}(\alpha)\}$ .



Note: Primitive elements in  $F_{16}$

(a)  $\alpha^i$  runs through the set of all nonzero elements of  $F_{16}$ , as  $i$  runs from 0 to 14.  $\Rightarrow \alpha$  is a primitive element of  $F_{16}$ .

(b) All nonzero elements in  $F_{16}$  can be also expressed by  $\alpha^{2i}$ , but not by  $\alpha^{3i}$ .

$\Rightarrow \alpha^2$  is primitive, but  $\alpha^3$  is not primitive.

(c) If  $\gcd(2^m - 1, s) = 1$ , then  $\alpha^s$  is primitive in  $F_{2^m}$

(Any nonzero element in  $F_{16}$  can be expressed as  $\alpha^{si}$  for an integer  $i$ ).

$\Rightarrow$  There are 8 primitive elements in  $F_{16}$ .

## □ Properties of Polynomials and Their Roots

### ○ Polynomial over $F_q$

(a)  $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_mx^m$  is called a *polynomial of degree  $m$*  over  $F_q$  if  $f_i \in F_q$  for any  $i$  and  $f_m \neq 0$ .

(b)  $F_q[x] =$  set of all polynomials over  $F_q$

Note that  $F_q[x]$  is called the *polynomial ring* over  $F_q$ .

### ○ Irreducible polynomial over $F_q$

Polynomial which can not be factored into a product of polynomials of lower degree over  $F_q$ .

Example: Irreducible polynomials over  $F_2$

degree one:  $x, x+1$

degree two:  $x^2+x+1$

degree three:  $x^3+x+1, x^3+x^2+1$

degree four:

$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$

Note that  $x^2+1$  is not irreducible over  $F_2$  since

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

○ Primitive polynomial

- (a) A polynomial  $f(x) = f_0 + f_1x + \cdots + f_mx^m$  of degree  $m$  over  $F_2$  is primitive if  $f(x) \mid x^{2^m-1} - 1$ , but  $f(x) \nmid x^s - 1$  for any integer  $s < 2^m - 1$ .

(b) Example: Primitive polynomials over  $F_2$

$m = 2:$   $x^2+x+1$

$m = 3:$   $x^3+x+1, x^3+x^2+1$

$m = 4:$   $x^4+x+1, x^4+x^3+1$

$\vdots$

○ Roots of a polynomial

- (a) If  $f(\beta) = 0$ , then  $\beta$  is called a root of a polynomial  $f(x)$ .

Example:  $f(x) = x^3 + x + 1$  has three roots in  $F_8$ , since

$$x^3+x+1 = (x+\alpha)(x+\alpha^2)(x+\alpha^4).$$

- (b) If  $f(x)$  is an irreducible polynomial over  $F_q$ , then it will have roots in some extension field  $F_{q^m}$ , i.e. the polynomial can be expressed as the product of linear terms  $x - \beta_i$ , where

$$\beta_i \in F_{q^m}.$$

- (c) If  $f(x)$  is an irreducible polynomial over  $F_q$  and  $f(\beta) = 0$ ,  $f(\beta^q) = f(\beta^{q^2}) = f(\beta^{q^3}) = \dots = 0$ , that is,  $\beta^q, \beta^{q^2}, \beta^{q^3}, \dots$  are also roots of  $f(x)$ .

$$\text{Proof: } 0 = f(\beta) = f_0 + f_1\beta + \dots + f_m\beta^m$$

$$\Rightarrow 0 = \left( \sum_{i=0}^m f_i \beta^i \right)^q = \sum_{i=0}^m f_i^q \beta^{qi} = \sum_{i=0}^m f_i \beta^{qi} = f(\beta^q)$$

$$\text{since } f_i^q = f_i.$$

□

- (d) Note that  $\beta^q, \beta^{q^2}, \beta^{q^3}, \dots$  are called conjugates of  $\beta$  over  $F_q$ .

○ Minimal polynomial

- (a) A polynomial  $f(x) = f_0 + f_1x + \dots + f_mx^m$  over  $F_q$  is called the *minimal polynomial* of  $\beta$  over  $F_q$  if

$$(1) \ f(x) \text{ is monic } (f_m = 1) \text{ and } f(\beta) = 0,$$

$$(2) \ f(x) \text{ is irreducible over } F_q.$$

Notation:  $m_\beta(x)$  = minimal polynomial of  $\beta$  over  $F_q$

- (b) Note that the minimal polynomial  $m_\beta(x)$  of  $\beta$  over  $F_q$  is the polynomial of minimum degree over  $F_q$ , having  $\beta$  as its root.
- (c) If  $s$  is the least integer such that  $\beta^{q^s} = \beta$ , then

$$m_{\beta}(x) = \prod_{i=0}^{s-1} (x - \beta^{q^i}).$$

Example: Minimal polynomial of  $\beta \in F_8$  over  $F_2$

$F_8$  defined by  $\alpha^3 + \alpha + 1$

elements	minimal polynomial	conjugates
0	$x$	0
1	$x + 1$	1
$\alpha$	$x^3 + x + 1$	$\alpha, \alpha^2, \alpha^4$
$\alpha^2$	$x^3 + x + 1$	$\alpha, \alpha^2, \alpha^4$
$\alpha^3$	$x^3 + x^2 + 1$	$\alpha^3, \alpha^6, \alpha^5$
$\alpha^4$	$x^3 + x + 1$	$\alpha, \alpha^2, \alpha^4$
$\alpha^5$	$x^3 + x^2 + 1$	$\alpha^3, \alpha^6, \alpha^5$
$\alpha^6$	$x^3 + x^2 + 1$	$\alpha^3, \alpha^6, \alpha^5$

Note:  $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$

$$= (x + 1)(x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

$$\Rightarrow F_8 = \text{set of roots of } x^8 + x$$

Example: Relation between  $F_{16}$  and its subfields

$$\begin{array}{ccc}
 F_{16} & & F_{16} \\
 | \Leftarrow & x^4 + x + 1 & | \Leftarrow x^2 + x + \gamma \\
 F_4 & & F_4 \\
 | \Leftarrow & & | \Leftarrow x^2 + x + 1 \\
 F_2 & & F_2
 \end{array}$$

$\gamma$ : primitive element of  $F_4$  ( $\gamma^2 + \gamma + 1 = 0$ )

$\alpha$ : primitive element of  $F_{16}$  ( $\alpha^4 + \alpha + 1 = \alpha^2 + \alpha + \gamma = 0$ )

$$F_4 = \{0, 1, \gamma, \gamma^2 = \gamma + 1\}$$

$$= \{0, 1, \alpha^5, \alpha^{10}\}$$

Note that  $\gamma = \alpha^5$ .

elt. $\beta$	over $F_2$ (1 $\alpha$ $\alpha^2$ $\alpha^3$ )	additive representation over $F_4$	over $F_4$ (1 $\alpha$ )
0	0 0 0 0	0	0 0
1	1 0 0 0	1	1 0
$\alpha$	0 1 0 0	$\alpha$	0 1
$\alpha^2$	0 0 1 0	$\alpha^2 = \gamma + \alpha$	$\gamma$ 1
$\alpha^3$	0 0 0 1	$\alpha^3 = \gamma\alpha + \alpha^2 = \gamma + (\gamma + 1)\alpha = \gamma + \gamma^2\alpha$	$\gamma$ $\gamma^2$
$\alpha^4$	1 1 0 0	$\alpha^4 = \gamma\alpha + \gamma^2\alpha^2 = 1 + \alpha$	1 1
$\alpha^5$	0 1 1 0	$\alpha^5 = \alpha + \alpha^2 = \gamma$	$\gamma$ 0
$\alpha^6$	0 0 1 1	$\alpha^6 = \gamma\alpha$	0 $\gamma$
$\alpha^7$	1 1 0 1	$\alpha^7 = \gamma\alpha^2 = \gamma^2 + \gamma\alpha$	$\gamma^2$ $\gamma$
$\alpha^8$	1 0 1 0	$\alpha^8 = \gamma^2\alpha + \gamma\alpha^2 = \gamma^2 + \alpha$	$\gamma^2$ 1
$\alpha^9$	0 1 0 1	$\alpha^9 = \gamma^2\alpha + \alpha^2 = \gamma + \gamma\alpha$	$\gamma$ $\gamma$
$\alpha^{10}$	1 1 1 0	$\alpha^{10} = \gamma\alpha^2 + \gamma\alpha = \gamma^2$	$\gamma^2$ 0
$\alpha^{11}$	0 1 1 1	$\alpha^{11} = \gamma^2\alpha$	0 $\gamma^2$
$\alpha^{12}$	1 1 1 1	$\alpha^{12} = \gamma^2\alpha^2 = 1 + \gamma^2\alpha$	1 $\gamma^2$
$\alpha^{13}$	1 0 1 1	$\alpha^{13} = \alpha + \gamma^2\alpha^2 = 1 + \gamma\alpha$	1 $\gamma$
$\alpha^{14}$	1 0 0 1	$\alpha^{14} = \alpha + \gamma\alpha^2 = \gamma^2 + \gamma^2\alpha$	$\gamma^2$ $\gamma^2$
$\alpha^{15}$	1 0 0 0		$x + \alpha^{14}$

Example: Minimal polynomial of  $\beta \in F_{16}$  over  $F_2$

elt. $\beta$	$m_\beta(x)$ over $F_2$	$m_\beta(x)$ over $F_4$	$m_\beta(x)$ over $F_{16}$
0	$x$	$x$	$x$
1	$x + 1$	$x + 1$	$x + 1$
$\alpha$	$x^4 + x + 1$	$x^2 + x + \gamma$	$x + \alpha$
$\alpha^2$	$x^4 + x + 1$	$x^2 + x + \gamma^2$	$x + \alpha^2$
$\alpha^3$	$x^4 + x^3 + x^2 + x + 1$	$x^2 + \gamma^2 x + 1$	$x + \alpha^3$
$\alpha^4$	$x^4 + x + 1$	$x^2 + x + \gamma$	$x + \alpha^4$
$\alpha^5$	$x^2 + x + 1$	$x + \gamma$	$x + \alpha^5$
$\alpha^6$	$x^4 + x^3 + x^2 + x + 1$	$x^2 + \gamma x + 1$	$x + \alpha^6$
$\alpha^7$	$x^4 + x^3 + 1$	$x^2 + \gamma x + \gamma$	$x + \alpha^7$
$\alpha^8$	$x^4 + x + 1$	$x^2 + x + \gamma^2$	$x + \alpha^8$
$\alpha^9$	$x^4 + x^3 + x^2 + x + 1$	$x^2 + \gamma x + 1$	$x + \alpha^9$
$\alpha^{10}$	$x^2 + x + 1$	$x + \gamma^2$	$x + \alpha^{10}$
$\alpha^{11}$	$x^4 + x^3 + 1$	$x^2 + \gamma^2 x + \gamma^2$	$x + \alpha^{11}$
$\alpha^{12}$	$x^4 + x^3 + x^2 + x + 1$	$x^2 + \gamma^2 x + 1$	$x + \alpha^{12}$
$\alpha^{13}$	$x^4 + x^3 + 1$	$x^2 + \gamma x + \gamma$	$x + \alpha^{13}$
$\alpha^{14}$	$x^4 + x^3 + 1$	$x^2 + \gamma^2 x + \gamma^2$	$x + \alpha^{14}$
$\alpha^{15}$	$x + 1$		



Note:

- (a)  $x^{2^m} + x = \text{product of all monic irreducible polynomials over } F_2 \text{ of degree } s \text{ such that } s \text{ divides } m.$

Example:  $x^8 + x = x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$

- (b)  $x^m + 1 \mid x^n + 1 \Leftrightarrow m \mid n \text{ over } F_2.$

○ Cyclotomic coset:

- (a) If  $f(x)$  is an irreducible polynomial over  $F_2$  and  $f(\beta) = 0$ ,  
 $f(\beta^2) = f(\beta^{2^2}) = f(\beta^{2^3}) = \dots = 0$ , that is,  $\beta^2, \beta^{2^2}, \beta^{2^3}, \dots$   
 are also roots of  $f(x)$ .
- (b) If  $r = 2^i s \pmod{2^m - 1}$  for an integer  $i$ ,  
 $m_{\alpha^s}(x) = m_{\alpha^r}(x)$  where  $\alpha$  is a primitive element of  $F_{2^m}$ .
- (c) Cyclotomic coset mod  $2^m - 1$ :

$$C_s = \{r \mid r = 2^i s \pmod{2^m - 1} \text{ for an integer } i\}.$$

Example:  $F_{16} = F_{2^4}$  and let  $N = 2^4 - 1 = 15$

Cyclotomic cosets mod  $N$ :

$$\begin{aligned} C_0 &= \{0\} && \longleftrightarrow && \{1\} \\ C_1 &= \{1, 2, 4, 8\} && \longleftrightarrow && \{\alpha^1, \alpha^2, \alpha^4, \alpha^8\} \\ C_3 &= \{3, 6, 12, 9\} && \longleftrightarrow && \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\} \\ C_5 &= \{5, 10\} && \longleftrightarrow && \{\alpha^5, \alpha^{10}\} \\ C_7 &= \{7, 14, 13, 11\} && \longleftrightarrow && \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\} \end{aligned}$$

○ Relation between minimal polynomials and cyclotomic cosets

(a) Minimal polynomial of  $\alpha^s$  over  $F_2$ :

$$m_{\alpha^s}(x) = \prod_{r \in C_s} (x - \alpha^r)$$

(b) Example: In  $F_{16}$ ,

$$m_{\alpha}(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8) = x^4 + x + 1$$

$$m_{\alpha^3}(x) = (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9) = x^4 + x^3 + x^2 + x + 1$$

$$m_{\alpha^5}(x) = (x + \alpha^5)(x + \alpha^{10}) = x^2 + x + 1$$

$$m_{\alpha^7}(x) = (x + \alpha^7)(x + \alpha^{14})(x + \alpha^{13})(x + \alpha^{11}) = x^4 + x^3 + 1$$

○ Reciprocal polynomial of  $f(x)$  with degree  $m$

(a) Definition of  $f_r(x)$  (or  $f^*(x)$ )

$$f^*(x) = x^m \cdot f(x^{-1})$$

(b) If  $\beta$  is a root of  $f(x)$ , then  $\beta^{-1}$  is a root of  $f^*(x)$ .

Note:

(a)  $f(x)$  is irreducible over  $F_2$  and  $f(\beta) = 0$ .

$$\Rightarrow f(\beta^2) = f(\beta^4) = \dots = 0$$

$$\Rightarrow f(x) = (x - \beta)(x - \beta^2)(x - \beta^4) \dots (x - \beta^{2^{s-1}})$$

where  $s$  is the least integer such that  $\beta^{2^s} = \beta$ .

Note that  $s = \deg f(x)$ .

(b)  $m_\beta(x)$  = minimal polynomial of  $\beta$  over  $F_q$

$$\Rightarrow m_\beta(x) = m_{\beta^q}(x) = m_{\beta^{q^2}}(x) = \dots$$

○ Number of primitive elements in the finite field  $F_{2^m}$

(a) If  $\alpha$  is primitive in  $F_{2^m}$  and  $\gcd(2^m - 1, s) = 1$ , then  $\alpha^s$  is primitive in  $F_{2^m}$ .

(b) Euler's phi function:

$$\varphi(n) = |\{1 \leq i \leq n \mid \gcd(i, n) = 1\}|$$

Note that  $\varphi(n)$  is the number of positive integers less than  $n$ , which are relatively prime to  $n$ .

(c) Number of primitive elements in the finite field  $F_{2^m}$

$$= \varphi(2^m - 1)$$

○ Number of primitive polynomials over  $F_2$

(a) Each primitive polynomial of degree  $m$  over  $F_2$  has  $m$  distinct primitive elements as its roots.

(b) Number of primitive polynomials of degree  $m$  over  $F_2$

$$= \varphi(2^m - 1)/m$$

Example:  $\varphi(2^6 - 1) = \varphi(63) = (7 - 1)(3^2 - 3^1) = 6 \cdot 6 = 36$

Number of primitive elements in  $F_{64} = 36$

Number of primitive polynomials of degree 6 over  $F_2 = 6$

## □ Implementation of Finite Field Representation

Example: Representation of the finite field  $F_8$

elements	additive representation	multiplicative representation	one's complement
0	0 0 0	1 1 1	0 0 0 (= 0)
$\alpha^0=1$	1 0 0	0 0 0	1 1 1 (= 7)
$\alpha$	0 1 0	0 0 1	1 1 0 (= 6)
$\alpha^2$	0 0 1	0 1 0	1 0 1 (= 5)
$\alpha^3$	1 1 0	0 1 1	1 0 0 (= 4)
$\alpha^4$	0 1 1	1 0 0	0 1 1 (= 3)
$\alpha^5$	1 1 1	1 0 1	0 1 0 (= 2)
$\alpha^6$	1 0 1	1 1 0	0 0 1 (= 1)

### ○ Operations in the finite field $F_8$

(a) Addition :  $\alpha^i + \alpha^i = 0 \pmod{2}$  and  $\alpha^i + \alpha^j = \alpha^k$

(b) Multiplication :  $\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod (2^m-1)}$

### ○ Multiplicative representation

- Multiplication is easy.
- Addition is difficult: Use a conversion table.
- Use (111...11) to denote the element "0".

### ○ Additive representation

(a) Addition is easy.

Multiplication is difficult: Use a conversion table.

One's complement can be used since the element "0" is not the same as the integer "0".

(b) Addition needs one instruction cycle : easy

$$\alpha^i = (c_{i1}, c_{i2}, c_{i3}, c_{i4}) = \underline{c}_i$$

$$\alpha^j = (c_{j1}, c_{j2}, c_{j3}, c_{j4}) = \underline{c}_j$$

$$\alpha^i + \alpha^j = (c_{i1} + c_{j1}, c_{i2} + c_{j2}, c_{i3} + c_{j3}, c_{i4} + c_{j4})$$

$\Rightarrow$  Componentwise modulo 2 addition

(c) Multiplication: Use ROM table.

(i)  $\underline{c}_i \rightarrow (\text{ROM}) \rightarrow i$  (exponent of  $\alpha^i$ )

(ii)  $\underline{c}_j \rightarrow (\text{ROM}) \rightarrow j$  (exponent of  $\alpha^j$ )

(iii)  $i + j = k \pmod{2^m - 1}$

(iv)  $k \rightarrow (\text{ROM}) \rightarrow \underline{c}_k$

○ Zech algorithm (add-one table)

(a) In the multiplicative representation, we can tabulate

$$1 + \alpha^n = \alpha^{z(n)}, \quad n \geq 1$$

in order to make addition easier.

(b)  $\alpha^m + \alpha^n = \alpha^m(1 + \alpha^{n-m}) = \alpha^m \cdot \alpha^{z(n-m)} = \alpha^{m+z(n-m)}$

Example: Zech table in the finite field  $F_8$

$n$	$z(n)$
1	3
2	6
3	1
4	5
5	4
6	2

Addition:

$$\alpha^4 + \alpha^5 = \alpha^{4+z(1)} = \alpha^7 = 1$$

$$\alpha^1 + \alpha^6 = \alpha^{1+z(5)} = \alpha^5$$

## □ Interpretation of Cyclic Codes by Finite Fields

○  $[n, k]$  cyclic code  $C$  over  $F_q$ :

(a) Any code polynomial  $c(x)$  can be expressed as

$$c(x) = a(x)g(x)$$

for some polynomial  $a(x)$  over  $F_q$ , where  $g(x)$  is the generator polynomial for  $C$ .

(b) If  $g(\beta) = 0$ , then  $c(\beta) = 0$  for any code polynomial  $c(x)$ .

$$c(\beta) = 0 = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{n-1}\beta^{n-1}$$

$$\Rightarrow \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} = 0.$$

(c) If  $g(\beta_1) = g(\beta_2) = \cdots = g(\beta_r) = 0$ , then

$$\begin{bmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ & & \vdots & & \\ 1 & \beta_r & \beta_r^2 & \cdots & \beta_r^{n-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = 0.$$