Introduction to Finite Fields

Yunghsiang S. Han

Department of Electrical Engineering,
National Taiwan University of Science and Technology
Taiwan

E-mail: yshan@mail.ntust.edu.tw

Groups

- Let G be a set of elements. A *binary operation* $*$ on G is a rule that assigns to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.
- A binary operation $*$ on G is said to be *associative* if, for any a, b, and c in G,
$$a * (b * c) = (a * b) * c.$$
- A set G on which a binary operation $*$ is defined is called a *group* if the following conditions are satisfied:
  1. The binary operation $*$ is associative.
  2. G contains an element e, an *identity* element of G, such that, for any $a \in G$,
  $$a * e = e * a = a.$$
  3. For any element $a \in G$, there exists another element $a' \in G$

such that

$$a * a' = a' * a = e.$$

a and a' are *inverse* to each other.

- A group G is called to be *commutative* if its binary operation $*$ also satisfies the following condition: for any a and b in G,

$$a * b = b * a.$$

Properties of Groups

- The identity element in a group G is unique.

  Proof: Suppose there are two identity elements e and e' in G. Then

  $$e' = e' * e = e.$$

- The inverse of a group element is unique.

Example of Groups

- $(Z, +)$. $e = 0$ and the inverse of i is $-i$.
- $(Q - \{0\}, \cdot)$. $e = 1$ and the inverse of a/b is b/a.
- $(\{0, 1\}, \oplus)$, where $\oplus$ is exclusive-OR operation.
- The *order* of a group is the number of elements in the group.
- Additive group: $(\{0, 1, 2, \ldots, m-1\}, \boxplus)$, where $m \in Z^+$, and $i \boxplus j \equiv i + j \bmod m$.
  - $(i \boxplus j) \boxplus k = i \boxplus (j \boxplus k)$.
  - $e = 0$.
  - $\forall 0 < i < m$, $m - i$ is the inverse of i.
  - $i \boxplus j = j \boxplus i$.
- Multiplicative group: $(\{1, 2, 3, \ldots, p-1\}, \boxdot)$, where p is a prime and $i \boxdot j \equiv i \cdot j \bmod p$.

Proof: Since p is a prime, $gcd(i,p)=1$ for all $0<i<p$. By Euclid's theorem, $\exists a,b\in Z$ such that $a\cdot i+b\cdot p=1$. Then $a\cdot i=-b\cdot p+1$. If $0<a<p$, then $a\boxdot i=i\boxdot a=1$. Assume that $a\geq p$. Then $a=q\cdot p+r$, where $r<p$. Since $gcd(a,p)=1$, $r\neq 0$. Hence, $r\cdot i=-(b+q\cdot i)p+1$, i.e., $r\boxdot i=i\boxdot r=1$.

Subgroups

- H is said to be a *subgroup* of G if (i) $H \subset G$ and $H \neq \emptyset$. (ii) H is closed under the group operation of G and satisfies all the conditions of a group.
- Let $G = (Q, +)$ and $H = (Z, +)$. Then H is a subgroup of G.

Fields

- Let F be a set of elements on which two binary operations, called addition "+" and multiplication "·", are defined. The set F together with the two binary operations $+$ and $\cdot$ is a field if the following conditions are satisfied:
  1. $(F, +)$ is a commutative group. The identity element with respect to addition is called the *zero* element or the additive identity of F and is denoted by 0.
  2. $(F - \{0\}, \cdot)$ is a commutative group. The identity element with respect to multiplication is called the *unit* element or the multiplicative identity of F and is denoted by 1.
  3. Multiplication is *distributive* over addition; that is, for any three elements a, b and c in F,
  $$a \cdot (b + c) = a \cdot b + a \cdot c.$$
- The *order* of a field is the number of elements of the field.

- A field with finite order is a *finite field*.
- $a - b \equiv a + (-b)$, where $-b$ is the additive inverse of b.
- $a \div b \equiv a \cdot b^{-1}$, where b^{-1} is the multiplicative inverse of b.

Properties of Fields

- $\forall a \in F,\ a \cdot 0 = 0 \cdot a = 0.$

  Proof: $a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0.$
  $0 = -a + a = -a + (a + a \cdot 0)$. Hence, $0 = 0 + a \cdot 0 = a \cdot 0.$

- Let $\forall a, b \in F$ and $a, b \neq 0$. Then $a \cdot b \neq 0$.

- $a \cdot b = 0$ and $a \neq 0$ imply that $b = 0$.

- $\forall a, b \in F$, $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$.

  Proof: $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. Similarly, we can prove that $-(a \cdot b) = a \cdot (-b)$.

- Cancellation law: $a \neq 0$ and $a \cdot b = a \cdot c$ imply that $b = c$.

  Proof: Since $a \neq 0$, $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$. Hence, $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$, i.e., $b = c$.

Examples of Fields

- $(R, +, \cdot)$.
- $(\{0,1\}, \boxplus, \boxdot)$, binary field $(GF(2))$.
- $(\{0,1,2,3\ldots,p-1\}, \boxplus, \boxdot)$, prime field $(GF(p))$, where p is a prime.
- There is a prime field for any prime.
- It is possible to extend the prime field $GF(p)$ to a field of p^m elements, $GF(p^m)$, which is called an extension field of $GF(p)$.
- Finite fields are also called Galois fields.

Properties of Finite Fields

- Let 1 be the unit element in $GF(q)$. Since there are only finite number of elements in $GF(q)$, there must exist two positive integers m and n such that $m < n$ and

$$\sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1.$$

  Hence, $\displaystyle\sum_{i=1}^{n-m} 1 = 0.$

- There must exist a smallest positive integer λ such that $\displaystyle\sum_{i=1}^{\lambda} 1 = 0$. This integer λ is called the *characteristic* of the field $GF(q)$.

- λ is a prime.

Proof: Assume that $\lambda = km$, where $1 < k, m < \lambda$. Then

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i=1}^{m} 1\right) = \sum_{i=1}^{km} 1 = 0.$$

Then $\sum_{i=1}^{k} 1 = 0$ or $\sum_{i=1}^{m} 1 = 0$. Contradiction.

- $\sum_{i=1}^{k} 1 \neq \sum_{i=1}^{m} 1$ for any $k, m < \lambda$ and $k \neq m$.
- $1 = \sum_{i=1}^{1} 1, \sum_{i=1}^{2} 1, \ldots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1 = 0$ are λ distinct elements in $GF(q)$. It cab be proved that these λ elements is a field, $GF(\lambda)$, under the addition and multiplication of $GF(q)$. $GF(\lambda)$ is called a *subfield* of $GF(q)$.
- If $q \neq \lambda$, then q is a power of λ.

Proof: We have $GF(\lambda)$ a subfield of $GF(q)$. Let $\omega_1 \in GF(q) - GF(\lambda)$. There are λ elements in $GF(q)$ of the form $a_1\omega_1$, $a_1 \in GF(\lambda)$. Since $\lambda \neq q$, we choose $\omega_2 \in GF(q)$ not of the form $a_1\omega_1$. There are λ^2 elements in $GF(q)$ of the form $a_1\omega_1 + a_2\omega_2$. If $q = \lambda^2$, we are done. Otherwise, we continue in this fashion and will exhaust all elements in $GF(q)$.

- Let a be a nonzero element in $GF(q)$. Then the following powers of a,

$$a^1 = a, a^2 = a \cdot a, a^3 = a \cdot a \cdot a, \cdots$$

  must be nonzero elements in $GF(q)$. Since $GF(q)$ has only finite number of elements, there must exist two positive integers k and m such that $k < m$ and $a^k = a^m$. Hence, $a^{m-k} = 1$.

- There must exist a smallest positive integer n such that $a^n = 1$. n is called the *order* of the finite field element a.

- The powers $a^1, a^2, a^3, \ldots, a^{n-1}, a^n = 1$ are all distinct.
- The set of these powers form a group under multiplication of $GF(q)$.
- A group is said to be *cyclic* if there exists an element in the group whose powers constitute the whole group.
- Let a be a nonzero element in $GF(q)$. Then $a^{q-1} = 1$.

  Proof: Let $b_1, b_2, \ldots, b_{q-1}$ be the $q-1$ nonzero elements in $GF(q)$. Since $a \cdot b_1, a \cdot b_2, \ldots, a \cdot b_{q-1}$ are all distinct nonzero elements, we have

$$(a \cdot b_1) \cdot (a \cdot b_2) \cdots (a \cdot b_{q-1}) = b_1 \cdot b_2 \cdots b_{q-1}.$$

  Then,

$$a^{q-1} \cdot (b_1 \cdot b_2 \cdots b_{q-1}) = b_1 \cdot b_2 \cdots b_{q-1},$$

  and then $a^{q-1} = 1$.
- If n is the order of a nonzero element a, then $n | q-1$.

Proof: Assume that $q-1=kn+r$, where $0<r<n$. Then

$$1=a^{q-1}=a^{kn+r}=(a^n)^k\cdot a^r=a^r.$$

Contradiction.

Primitive Element

- In $GF(q)$, a nonzero element a is said to be primitive if the order of a is $q-1$.
- The powers of a primitive element generate all the nonzero elements of $GF(q)$.
- Every finite field has a primitive element.

  Proof: Assume that $q > 2$. Let $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the prime factor decomposition of $h = q-1$. For every i, the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $GF(q)$. Hence, there is at least one nonzero element in $GF(q)$ that is not a root of this polynomial. Let a_i be such an element and set

  $$b_i = a_i^{h/\left(p_i^{r_i}\right)}.$$

  We have $b_i^{p_i^{r_i}} = 1$ and the order of b_i is a divisor of $p_i^{r_i}$.

On the other hand,

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1.$$

And so the order of b_i is $p_i^{r_i}$. We claim that the element $b = b_1 b_2 \cdots b_m$ has order h. Suppose that the order of b is a proper divisor of h and is therefore a divisor of at least one of the m integers h/p_i, $1 \leq i \leq m$, say of h/p_1. Then we have

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Now, for $1 < i$, $p_i^{r_i}$ divides h/p_1, and hence $b_i^{h/p_1} = 1$. Therefore, $b_1^{h/p_1} = 1$. This implies that the order of b_1 must divide h/p_1. Contradiction.

- Consider $GF(7)$. We have

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

Hence, 3 is a primitive element. Since

$$4^1 = 4, 4^2 = 2, 4^3 = 1$$

the order of 4 is 3 and $3|7-1$.

- $GF(q) - \{0\}$ is a finite cyclic group under multiplication.
- The number of primitive elements in $GF(q)$ is $\psi(q-1)$, where ψ is the Euler's function.

Binary Field Arithmetic

- Let $f(x) = \sum_{i=0}^{n} f_i x^i$ and $g(x) = \sum_{i=0}^{m} g_i x^i$, where $f_i, g_i \in GF(2)$.
- $f(x) \boxplus g(x) \equiv f(x) + g(x)$ with coefficients modulo by 2.
- $f(x) \boxdot g(x) \equiv f(x) \cdot g(x)$ with coefficients modulo by 2.
- $f(x) \boxdot 0 = 0$.
- $f(x)$ is said to be *irreducible* if it is not divisible by any polynomial over $GF(2)$ of degree less than n but greater than zero.
- $x^2, x^2 + 1, x^2 + x$ are reducible over $GF(2)$.
  $x + 1, x^2 + x + 1, x^3 + x + 1$ are irreducible over $GF(2)$.
- For any $m > 1$, there exists an irreducible polynomial of degree m.
- Any irreducible polynomial over $GF(2)$ of degree m divides

$x^{2^m-1}+1$. It will be easy to prove when we learn the construction of an extension field.

- $x^3+x+1|x^7+1$, i.e., $x^7+1=(x^4+x^2+x+1)(x^3+x+1)$.
- An irreducible polynomial $p(x)$ of degree m is said to be *primitive* if the smallest positive integer n for which $p(x)$ divides x^n+1 is $n=2^m-1$, i.e., $p(x)|x^{2^m-1}+1$.
- Since $x^4+x+1|x^{15}+1$, x^4+x+1 is primitive. $x^4+x^3+x^2+x+1$ is not since $x^4+x^3+x^2+x+1|x^5+1$.
- For a given m, there may be more than one primitive polynomial of degree m.
- For all $\ell \geq 0$, $[f(x)]^{2^\ell}=f(x^{2^\ell})$.

  Proof:

$$\begin{aligned} f^2(x) &= (f_0+f_1x+\cdots+f_nx^n)^2 \\ &= [f_0+(f_1x+f_2x^2+\cdots+f_nx^n)]^2 \end{aligned}$$

$$= \quad f_0^2 + (f_1 x + f_2 x^2 + \cdots + f_n x^n)^2$$

Expanding the equation above repeatedly, we eventually obtain

$$f^2(x) = f_0^2 + (f_1 x)^2 + (f_2 x^2)^2 + \cdots + (f_n x^n)^2.$$

Since $f_i = 0$ or 1, $f_i^2 = f_i$. Hence, we have

$$f^2(x) = f_0 + f_1 x^2 + f_2 (x^2)^2 + \cdots + f_n (x^2)^n = f(x^2).$$

List of Primitive Polynomials

m		m	
3	$1 + X + X^3$	14	$1 + X + X^6 + X^{10} + X^{14}$
4	$1 + X + X^4$	15	$1 + X + X^{15}$
5	$1 + X^2 + X^5$	16	$1 + X + X^3 + X^{12} + X^{16}$
6	$1 + X + X^6$	17	$1 + X^3 + X^{17}$
7	$1 + X^3 + X^7$	18	$1 + X^7 + X^{18}$
8	$1 + X^2 + X^3 + X^4 + X^8$	19	$1 + X + X^2 + X^5 + X^{19}$
9	$1 + X^4 + X^9$	20	$1 + X^3 + X^{20}$
10	$1 + X^3 + X^{10}$	21	$1 + X^2 + X^{21}$
11	$1 + X^2 + X^{11}$	22	$1 + X + X^{22}$
12	$1 + X + X^4 + X^6 + X^{12}$	23	$1 + X^5 + X^{23}$
13	$1 + X + X^3 + X^4 + X^{13}$	24	$1 + X + X^2 + X^7 + X^{24}$

Construction of $GF(2^m)$

- Initially, we have two elements 0 and 1 from $GF(2)$ and a new symbol α. Define a multiplication $\cdot$ as follows:

  1.
  $$0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1$$
  $$0 \cdot \alpha = \alpha \cdot 0 = 0, \quad 1 \cdot \alpha = \alpha \cdot 1 = \alpha$$

  2. $\alpha^2 = \alpha \cdot \alpha$ $\alpha^3 = \alpha \cdot \alpha \cdot \alpha$ $\cdots$ $\alpha^j = \alpha \cdot \alpha \cdot \cdots \cdot \alpha$ (j times)
  3. $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}$.

- Let $p(x)$ be a primitive polynomial of degree m over $GF(2)$. Assume that $p(\alpha) = 0$. Since $p(x) | x^{2^m - 1} + 1$, $x^{2^m - 1} + 1 = q(x)p(x)$. Hence, $\alpha^{2^m - 1} + 1 = q(\alpha)p(\alpha) = q(\alpha) \cdot 0 = 0$, $\alpha^{2^m - 1} = 1$, and α^i is not 1 for $i < 2^m - 1$.

- Let
$$F^* = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}.$$
- It can be proved that $F^* - \{0\}$ is a communicative group under "$\cdot$".
- $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$ represent $2^m - 1$ distinct elements.
- Next we define an additive operation "+" on F^* such that F^* forms a communicative group under "+".
- For $0 \leq i < 2^m - 1$, we have
$$x^i = q_i(x)p(x) + a_i(x), \tag{1}$$
where
$a_i(x) = a_{i0} + a_{i1}x + a_{i2}x^2 + \cdots + a_{i(m-1)}x^{m-1}$ and $a_{ij} \in \{0, 1\}$.
Since x^i and $p(x)$ are relatively prime, we have $a_i(x) \neq 0$.
- For $0 \leq i \neq j < 2^m - 1$, $a_i(x) \neq a_j(x)$.

Proof: Suppose that $a_i(x) = a_j(x)$. Then

$$\begin{aligned} x^i + x^j &= [q_i(x) + q_j(x)]p(x) + a_i(x) + a_j(x) \\ &= [q_i(x) + q_j(x)]p(x). \end{aligned}$$

This implies that $p(x)$ divides $x^i(1 + x^{j-i})$ (assuming that $j > i$). Since x^i and $p(x)$ are relatively prime, $p(x)$ must divide $x^{j-i} + 1$. This is impossible since $j - i < 2^m - 1$ and $p(x)$ is a primitive polynomial of degree m which does not divide $x^n + 1$ for $n < 2^m - 1$. Contradiction.

- We have $2^m - 1$ distinct nonzero polynomials $a_i(x)$ of degree $m - 1$ or less.
- Replacing x by α in (1) we have

$$\alpha^i = a_i(\alpha) = a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \cdots + a_{i(m-1)}\alpha^{m-1}.$$

- The $2^m - 1$ nonzero elements, $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{2^m-2}$ in F^* can be represented by $2^m - 1$ distinct nonzero polynomials of α over $GF(2)$ with degree $m-1$ or less.

- The 0 in F^* can be represented by the zero polynomial.
- Define an addition "+" as follows:
  1. $0 + 0 = 0$.
  2. For $0 \le i, j < 2^m - 1$,

$$0 + \alpha^i = \alpha^i + 0 = \alpha^i,$$

$$\begin{aligned} \alpha^i + \alpha^j &= (a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \cdots + a_{i(m-1)}\alpha^{m-1}) + \\ &\quad (a_{j0} + a_{j1}\alpha + a_{j2}\alpha^2 + \cdots + a_{j(m-1)}\alpha^{m-1}) \\ &= (a_{i0} + a_{j0}) + (a_{i1} + a_{j1})\alpha + (a_{i2} + a_{j2})\alpha^2 + \cdots + \\ &\quad (a_{i(m-1)} + a_{j(m-1)})\alpha^{m-1}, \end{aligned}$$

where $a_{i\ell} + a_{j\ell}$ is carried out in modulo-2 addition.

3. For $i \neq j$,

$$(a_{i0}+a_{j0})+(a_{i1}+a_{j1})\alpha+(a_{i2}+a_{j2})\alpha^2+\cdots+(a_{i(m-1)}+a_{j(m-1)})\alpha^{m-1}$$

is nonzero and must be the polynomial expression for some α^k in F^*.

- It is easy to see that F^* is a commutative group under "+" and polynomial multiplication satisfies distribution law.
- F^* is a finite field of 2^m elements.

Three representations for the elements of $GF(2^4)$ generated by $p(x) = 1 + x + x^4$

Power representation	Polynomial representation	4-Tuple representation
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

$\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16} \equiv \alpha$

$\alpha^3\ \alpha^6\ \alpha^{12}\ \underline{\alpha}^{24}\ \alpha^{48} \equiv \alpha^3$

$\equiv \alpha^9$

Representations of GF(2^4). $p(z) = z^4 + z + 1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	$x + 1$
α^1	z	0010	2	$x^4 + x + 1$
α^2	z^2	0100	4	$x^4 + x + 1$
α^3	z^3	1000	8	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^4	$z + 1$	0011	3	$x^4 + x + 1$
α^5	$z^2 + z$	0110	6	$x^2 + x + 1$
α^6	$z^3 + z^2$	1100	12	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^7	$z^3 + z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$z^2 + 1$	0101	5	$x^4 + x + 1$
α^9	$z^3 + z$	1010	10	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{10}	$z^2 + z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$z^3 + z^2 + z + 1$	1110	14	$x^4 + x^3 + 1$
α^{12}	$z^3 + z^2 + z + 1$	1111	15	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{13}	$z^3 + z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$z^3 + 1$	1001	9	$x^4 + x^3 + 1$

Examples of Finite Fields

GF(2)

+	0	1	*	0	1
0	0	1	0	0	0
1	1	0	1	0	1

GF(3)

+	0	1	2	*	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

$GF(2)[\alpha] / \alpha^2+\alpha+1$

Primitive polynomial over GF(2)

$GF(2^2)$, $p(x) = 1 + x + x^2$

($p(\alpha) = 1 + \alpha + \alpha^2 = 0$)

GF(4)

+	0	1	2	3	*	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	0	3	2	1	0	3	1	2
2	2	3	0	1	2	0	1	2	3
3	3	2	1	0	3	0	2	3	1

0	0	00	0
1	1	10	2
α	α	01	1
α^2	$1+\alpha$	11	3

Examples of Finite Fields

GF(4) →

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

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

0	0	0	0
1	0	1	1
2	1	0	α
3	1	1	$\alpha+1$

$\equiv GF(2)[\alpha] / \alpha^2+\alpha+1$

$GF(4^2) \equiv GF(4)[z]/z^2+z+2$, $p(z) = z^2+z+2$

Primitive polynomial over GF(4)

$\alpha = z$

$\alpha^{15} = 1$

Operate on GF(4)

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	00	0	
α^0	1	01	1	$x + 1$
α^1	z	10	4	$x^2 + x + 2$
α^2	$z + 2$	12	6	$x^2 + x + 3$
α^3	$3z + 2$	32	14	$x^2 + 3x + 1$
α^4	$z + 1$	11	5	$x^2 + x + 2$
α^5	2	02	2	$x + 2$
α^6	$2z$	20	8	$x^2 + 2x + 1$
α^7	$2z + 3$	23	11	$x^2 + 2x + 2$
α^8	$z + 3$	13	7	$x^2 + x + 3$
α^9	$2z + 2$	22	10	$x^2 + 2x + 1$
α^{10}	3	03	3	$x + 3$
α^{11}	$3z$	30	12	$x^2 + 3x + 3$
α^{12}	$3z + 1$	31	13	$x^2 + 3x + 1$
α^{13}	$2z + 1$	21	9	$x^2 + 2x + 2$
α^{14}	$3z + 3$	33	15	$x^2 + 3x + 3$

Properties of $GF(2^m)$

- In $GF(2)$ $x^4 + x^3 + 1$ is irreducible; however, in $GF(2^4)$, $x^4 + x^3 + 1 = (x + \alpha^7)(x + \alpha^{11})(x + \alpha^{13})(x + \alpha^{14})$.
- Let $f(x)$ be a polynomial with coefficients from $GF(2)$. Let β be an element in extension field $GF(2^m)$. If β is a root of $f(x)$, then for any $\ell \geq 0$, β^{2^ℓ} is also a root of $f(x)$.
- The element β^{2^ℓ} is called a *conjugate* of β.
- The $2^m - 1$ nonzero elements of $GF(2^m)$ form all the roots of $x^{2^m-1} + 1$.

  Proof: Let β be a nonzero element in $GF(2^m)$. It has been shown that $\beta^{2^m-1} = 1$. Then $\beta^{2^m-1} + 1 = 0$. Hence, every nonzero element of $GF(2^m)$ is a root of $x^{2^m-1} + 1$. Since the degree of $x^{2^m-1} + 1$ is $2^m - 1$, the $2^m - 1$ nonzero elements of $GF(2^m)$ form all the roots of $x^{2^m-1} + 1$.

- The elements of $GF(2^m)$ form all the roots of $x^{2^m} + x$.
- Let $\phi(x)$ be the polynomial of smallest degree over $GF(2)$ such that $\phi(\beta) = 0$. The $\phi(x)$ is called the *minimal polynomial* of β.
- $\phi(x)$ is unique.
- The minimal polynomial $\phi(x)$ of a field element β is irreducible.

  Proof: Suppose that $\phi(x)$ is not irreducible and that $\phi(x) = \phi_1(x)\phi_2(x)$, where degrees of $\phi_1(x), \phi_2(x)$ are less than that of $\phi(x)$. Since $\phi(\beta) = \phi_1(\beta)\phi_2(\beta) = 0$, either $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$. Contradiction.
- Let $f(x)$ be a polynomial over $GF(2)$. Let $\phi(x)$ be the minimal polynomial of a field element β. If β is a root of $f(x)$, then $f(x)$ is divisible by $\phi(x)$.

  Proof: Let $f(x) = a(x)\phi(x) + r(x)$, where the degree of $r(x)$ is less than that of $\phi(x)$. Since $f(\beta) = \phi(\beta) = 0$, we have $r(\beta) = 0$. Then $r(x)$ must be 0 since $\phi(x)$ is the minimal polynomial of β.

- The minimal polynomial $\phi(x)$ of an element β in $GF(2^m)$ divides $x^{2^m} + x$.
- Let $f(x)$ be an irreducible polynomial over $GF(2)$. Let β be an element in $GF(2^m)$. Let $\phi(x)$ be the minimal polynomial of β. If $f(\beta) = 0$, then $\phi(x) = f(x)$.
- Let β be an element in $GF(2^m)$ and let e be the smallest non-negative integer such that $\beta^{2^e} = \beta$. Then

$$f(x) = \prod_{i=0}^{e-1}(x + \beta^{2^i})$$

is an irreducible polynomial over $GF(2)$.

Proof: Consider

$$[f(x)]^2 = \left[\prod_{i=0}^{e-1}(x+\beta^{2^i})\right]^2 = \prod_{i=0}^{e-1}(x+\beta^{2^i})^2.$$

Since $(x+\beta^{2^i})^2 = x^2+\beta^{2^{i+1}}$,

$$\begin{aligned}[f(x)]^2 &= \prod_{i=0}^{e-1}(x^2+\beta^{2^{i+1}}) = \prod_{i=1}^{e}(x^2+\beta^{2^i}) \\ &= \left[\prod_{i=1}^{e-1}(x^2+\beta^{2^i})\right](x^2+\beta^{2^e})\end{aligned}$$

Since $\beta^{2^e}=\beta$, then

$$[f(x)]^2 = \prod_{i=0}^{e-1}(x^2+\beta^{2^i}) = f(x^2).$$

Let $f(x) = f_0 + f_1 x + \cdots + f_e x^e$, where $f_e = 1$. Expand

$$
\begin{aligned}
[f(x)]^2 &= (f_0 + f_1 x + \cdots + f_e x^e)^2 \\
&= \sum_{i=0}^{e} f_i^2 x^{2i} + (1+1) \sum_{i=0}^{e} \sum_{\substack{j=0 \\ i \neq j}}^{e} f_i f_j x^{i+j} \\
&= \sum_{i=0}^{e} f_i^2 x^{2i}.
\end{aligned}
$$

Then, for $0 \leq i \leq e$, we obtain

$$f_i = f_i^2.$$

This holds only when $f_i = 0$ or 1.

Now suppose that $f(x)$ is no irreducible over $GF(2)$ and $f(x) = a(x)b(x)$. Since $f(\beta) = 0$, either $a(\beta) = 0$ or $b(\beta) = 0$. If $a(\beta) = 0$, $a(x)$ has $\beta, \beta^2, \ldots, \beta^{2^{e-1}}$ as roots, so $a(x)$ has degree e and $a(x) = f(x)$. Similar argument can be applied to the case

$b(\beta) = 0$.

- Let $\phi(x)$ be the minimal polynomial of an element β in $GF(2^m)$. Let e be the smallest integer such that $\beta^{2^e} = \beta$. Then
$$\phi(x) = \prod_{i=0}^{e-1} (x + \beta^{2^i}).$$
- Let $\phi(x)$ be the minimal polynomial of an element β in $GF(2^m)$. Let e be the degree of $\phi(x)$. Then e is the smallest integer such that $\beta^{2^e} = \beta$. Moreover, $e \leq m$.
- The degree of the minimal polynomial of any element in $GF(2^m)$ divides m.

Minimal polynomials of the elements in $GF(2^4)$ generated by $p(x)=x^4+x+1$

Conjugate roots	minimal polynomials
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1

e.g. $X^{15}-1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ over $GF(2)$

$X^{15}-1=(x-\alpha^0)\ \underline{(x-\alpha^5)(x-\alpha^{10})}\ \underline{(x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)}$ over $GF(2^4)$

$\alpha^{15}=1$ $\qquad \underline{(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})}\ \underline{(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)}$

- If β is a primitive element of $GF(2^m)$, all its conjugates $\beta^2, \beta^{2^2}, \ldots,$ are also primitive elements of $GF(2^m)$.

  Proof: Let n be the order of β^{2^ℓ} for $\ell > 0$. Then

  $$(\beta^{2^\ell})^n = \beta^{n2^\ell} = 1.$$

  It has been proved that n divides $2^m - 1$, $2^m - 1 = k \cdot n$. Since β is a primitive element of $GF(2^m)$, its order is $2^m - 1$. Hence, $2^m - 1 | n2^\ell$. Since 2^ℓ and $2^m - 1$ are relatively prime, n must be divisible by $2^m - 1$, say

  $$n = q \cdot (2^m - 1).$$

  Then $n = 2^m - 1$. Consequently, β^{2^ℓ} is also a primitive element of $GF(2^m)$.

- If β is an element of order n in $GF(2^m)$, all its conjugates have the same order n.

$\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16} \equiv \alpha$

$\alpha^3\ \alpha^6\ \alpha^{12}\ \underline{\alpha}^{24}\ \alpha^{48} \equiv \alpha^3$

$\equiv \alpha^9$

Representations of $GF(2^4)$. $p(z) = z^4 + z + 1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	$x + 1$
α^1	z	0010	2	$x^4 + x + 1$
α^2	z^2	0100	4	$x^4 + x + 1$
α^3	z^3	1000	8	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^4	$z + 1$	0011	3	$x^4 + x + 1$
α^5	$z^2 + z$	0110	6	$x^2 + x + 1$
α^6	$z^3 + z^2$	1100	12	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^7	$z^3 + z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$z^2 + 1$	0101	5	$x^4 + x + 1$
α^9	$z^3 + z$	1010	10	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{10}	$z^2 + z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$z^3 + z^2 + z + 1$	1110	14	$x^4 + x^3 + 1$
α^{12}	$z^3 + z^2 + z + 1$	1111	15	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{13}	$z^3 + z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$z^3 + 1$	1001	9	$x^4 + x^3 + 1$