

## Chapter 3

# Finite Fields

Finite fields are used in most of the known constructions of pseudorandom sequences, and analysis of periods, correlations, and linear spans of linear feedback shift register (LFSR) sequences and nonlinear generated sequences. They are also important in many cryptographic primitive algorithms, such as the Diffie-Hellman key exchange, the Digital Signature Standard (DSS), the ElGamal public-key encryption, elliptic curve public-key cryptography, and LFSR (or Torus) based public-key cryptography. Finite fields and shift register sequences are also used in algebraic error-correcting codes, in code-division multiple-access (CDMA) communications, and many other applications beyond the scope of this book. This chapter gives a description of these fields and some properties which are frequently used in sequence design and cryptography. Section 1 introduces definitions of algebraic structures of groups, rings and fields, and polynomials. Section 2 shows the construction of the finite field  $GF(p^n)$ . Section 3 presents the basic theory of finite fields. Section 4 discusses minimal polynomials. Section 5 introduces subfields, trace functions, bases and computation of the minimal polynomials over intermediate subfields. Computation of a power of a trace function is shown in Section 6. And, the last section presents some counting numbers related to finite fields.

### 3.1 Algebraic Structures

In this section, we give the definitions of the algebraic structures of groups, rings and fields, polynomials, and some concepts which will be needed for the study of finite fields in the later sections.

We use the following notations for the sets of numbers:  $\mathbb{N}$ , the set of natural numbers (positive integers);  $\mathbb{Z}$ , the set of integers;  $\mathbb{Q}$ , the set of rational numbers;  $\mathbb{R}$ , the set of real numbers; and  $\mathbb{C}$ , the set of complex numbers.

#### A. Groups

**Binary operation:** Let  $S$  be a set and let  $S \times S$  denote the set of all ordered

pairs  $(s, t)$  with  $s \in S$  and  $t \in S$ . Then a mapping from  $S \times S$  into  $S$  is called a *(binary) operation* on  $S$ . Under this definition we require that the image of  $(s, t) \in S \times S$  must be in  $S$ . This is the *closure property* of an operation.

**Algebraic structure:** A set  $S$  together with one or more operations on  $S$  is called an *algebraic structure*.

**Definition 3.1** A group is a set  $G$  together with a binary operation  $*$  on  $G$  such that the following three properties hold:

(i)  $*$  is associative; that is, for any  $a, b, c \in G$ ,

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

(ii) There is an identity (or unit) element  $e$  in  $G$  such that for all  $a \in G$ ,

$$a * e = e * a = a$$

(iii) For each  $a \in G$ , there exists an inverse element  $a^{-1} \in G$  such that

$$a * a^{-1} = a^{-1} * a = e.$$

Sometimes, we denote the group as a triple  $(G, *, e)$ . If the group also satisfies

(iv) For all  $a, b \in G$ ,

$$a * b = b * a,$$

then the group is called Abelian or commutative.

*Note.* From the definition, the identity element  $e$  of  $G$  is unique, and the inverse element of any element  $a \in G$  is also unique.

For simplicity, we will frequently use the notation of ordinary multiplication to designate the operation in the group, writing simply  $ab$  instead of  $a * b$ . But it must be emphasized that by doing so we do not assume that the operation actually is ordinary multiplication. If  $G$  is an Abelian group, we also write  $a + b$  instead of  $a * b$  and  $-a$  instead of  $a^{-1}$ , i.e., using additive notation.

The associative law guarantees that expressions such as  $a_1 a_2 \cdots a_n$  with  $a_j \in G$ ,  $1 \leq j \leq n$ , are unambiguous, since no matter how we insert parentheses, the expression will always represent the same element of  $G$ . To indicate the  $n$ -fold composition of an element  $a \in G$  with itself, where  $n \in \mathbb{N}$ , we will write

$$a^n = aa \cdots a, \quad (n \text{ factors } a)$$

if using multiplicative notation, and we call  $a^n$  the  $n$ th power of  $a$ . If using additive notation for the operation  $*$  on  $G$ , we write

$$na = a + a + \cdots + a \quad (n \text{ summands } a)$$

and sometimes it is called  $n$  times  $a$ .

Following customary notation, we have the following rules:

Multiplicative Notation	Additive Notation
$a^{-n} = (a^{-1})^n$	$(-n)a = n(-a)$
$a^n a^m = a^{n+m}$	$na + ma = (n+m)a$
$(a^n)^m = a^{nm}$	$m(na) = (mn)a$

For  $n = 0 \in \mathbb{Z}$ , we adopt  $a^0 = e$  by convention in multiplicative notation and  $0a = 0$  in additive notation, where the last “zero” represents the identity element of  $G$ .

**Example 3.1** The following number sets together with ordinary addition and multiplication are groups:  $(\mathbb{Z}, +, 0)$ ,  $(\mathbb{R}, +, 0)$ , and  $(\mathbb{R}, \cdot, 1)$  are groups. We denote by  $\mathbb{Z}_n$  the set of the remainders of all integers on division by  $n$  where  $n$  is a positive integer, i.e.,  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ , and  $\mathbb{Z}_n^*$  is the set of nonzero elements in  $\mathbb{Z}_n$  which are coprime to  $n$ . Let  $a + b$  and  $ab$  be the ordinary sum and product of  $a$  and  $b$  reduced modulo  $n$ , respectively. Then we have

- (a)  $(\mathbb{Z}_2, +, 0)$ ,  $(\mathbb{Z}_6, +, 0)$  and  $(\mathbb{Z}_5, +, 0)$  are groups with respect to addition.
- (b)  $(\mathbb{Z}_5^*, \cdot, 1)$  forms a group with respect to multiplication.

In general, we have the following results.

**Proposition 3.1** *With the notation above,*

- (a)  $(\mathbb{Z}_n, +, 0)$  forms a group for any positive integer  $n$ , which is called the additive group of integers modulo  $n$ .
- (b)  $(\mathbb{Z}_p^*, \cdot, 1)$  forms a group for any prime  $p$ , which is called the multiplicative group of integers modulo  $p$ .

Before we give a proof for this proposition, we list the following basic fact on integers whose proof can be found in any book on number theory, say [89] [106].

**Fact 3.1** *Let  $p$  be a prime number. For any integer  $a : 0 < a < p$ ,  $a$  and  $p$  are coprime. In other words, the greatest common divisor of  $a$  and  $p$ , denoted by  $\gcd(a, p)$ , is equal to 1. Moreover, there exist two integers  $u$  and  $v$  such that  $au + pv = 1$  where  $0 < u < p$ .*

*Proof of Proposition 3.1.* Let  $a \pmod{n}$  denote the remainder of  $a$  when divided by  $n$ .

(a) For  $a, b \in \mathbb{Z}_n$ ,  $a + b$  is the remainder on division by  $n$  of the ordinary sum of  $a$  and  $b$ . So,  $a + b \in \mathbb{Z}_n$ . (i). For  $a, b, c \in \mathbb{Z}_n$ , now consider  $a, b, c$  as integers. Then  $a + (b + c) = (a + b) + c$ , as does  $a + (b + c) \equiv (a + b) + c \pmod{n}$ . (ii). For any  $a \in \mathbb{Z}_n$ ,  $a + 0 = 0 + a = a$ , so 0 is the identity element in  $\mathbb{Z}_n$ . (iii). For each  $a \in \mathbb{Z}_n$ , there exists a positive integer  $b \in \mathbb{Z}_n$  such that  $a + b = n$ . Note

that  $n \equiv 0 \pmod{n}$ . So,  $a + b = b + a = 0$ . Thus  $b$  is the inverse element of  $a$  in  $\mathbb{Z}_n$ .

(b) For  $a, b \in \mathbb{Z}_p$ ,  $ab$  is the remainder on division by  $p$  of the ordinary product of  $a$  and  $b$ . So,  $ab \in \mathbb{Z}_p^*$ . (i). For  $a, b, c \in \mathbb{Z}_p^*$ , now consider  $a, b, c$  as integers. Then  $a(bc) = (ab)c$ , as does  $a(bc) \equiv (ab)c \pmod{p}$ , which means that  $\mathbb{Z}_p^*$  satisfies the associative law. (ii). It is obvious that 1 is the identity element in  $\mathbb{Z}_p^*$ . (iii). For any  $a \in \mathbb{Z}_p^*$ , since  $p$  is a prime, according to Fact 1, there exist two integers  $u$  and  $v$  such that

$$au + pv = 1$$

where  $0 < u < p$ . Note that  $au + pv \equiv au \pmod{p}$ . Therefore we get  $au \equiv 1 \pmod{p} \implies a^{-1} = u \in \mathbb{Z}_p^*$ . Thus  $u$  is the inverse of  $a$  in  $\mathbb{Z}_p^*$ .  $\square$

**Definition 3.2** A multiplicative group (resp. additive group)  $G$  is said to be cyclic if there is an element  $a \in G$  such that for any  $b \in G$  there is some integer  $i$  with  $b = a^i$  (resp.  $b = ia$ ). Such an element  $a$  is called a generator of the cyclic group, and we write  $G = \langle a \rangle$ .

**Example 3.2** The following groups are cyclic.

- (a) For  $(\mathbb{Z}, +, 0)$ , the additive group of integers, both 1 and  $-1$  are generators.
- (b) For  $(\mathbb{Z}_6, +, 0)$ , the additive group of integers modulo 6; 1 and 5 are generators.
- (c) For  $(\mathbb{Z}_3^*, \cdot, 1)$ , the multiplicative group of integer modulo 3; 2 is the generator.
- (d) For  $(\mathbb{Z}_5^*, \cdot, 1)$ , the multiplicative group of integers modulo 5; 2 and 3 are generators, i.e.,

$$\begin{aligned} \mathbb{Z}_5^* &= \langle 2 \rangle = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 \equiv 3 \pmod{5}\} \\ &\quad (\text{where } 2^4 \equiv 1 \pmod{5}) \\ &= \langle 3 \rangle = \{3^0 = 1, 3^1 = 3, 3^2 \equiv 4, 3^3 \equiv 2 \pmod{5}\} \\ &\quad (\text{where } 3^4 \equiv 1 \pmod{5}) \end{aligned}$$

**Definition 3.3** A group is called finite (resp. infinite) if it contains finitely (resp. infinitely) many elements. The number of elements in a finite group is called the order of the group  $G$ . We will write  $|G|$  for the order of the finite group  $G$ .

## B. Rings and Fields

In most of the number systems used in elementary arithmetic there are two distinct binary operations: addition and multiplication. Examples are provided by the integers, the rational numbers, and the real numbers. We now define a type of algebraic structure known as a ring that shares some of the basic properties of these number systems.

**Definition 3.4** A ring  $(R, +, \cdot)$  is a set  $R$ , together with two binary operations, denoted by  $+$  and  $\cdot$ , such that:

- (i)  $R$  is an Abelian group with respect to  $+$ .
- (ii)  $\cdot$  is associative, that is,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in R$ .
- (iii) The distributive laws hold; that is, for all  $a, b, c \in R$  we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and } (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

**Example 3.3** The following are examples of rings from number systems.

- (a)  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ , and  $(\mathbb{C}, +, \cdot)$  are rings.
- (b)  $(\mathbb{Z}_4, +, \cdot)$  forms a ring of 4 elements. (This is the algebraic structure which underlies  $\mathbb{Z}_4$  code.)
- (c)  $(\mathbb{Z}_n, +, \cdot)$  forms a ring, called the *residue class ring modulo  $n$* .

Let  $(F, +, \cdot)$  be a ring, and let  $F^* = \{a \in R \mid a \neq 0\}$ , the set of nonzero elements of  $F$ .

**Definition 3.5** A field is a ring  $(F, +, \cdot)$  such that  $F^*$  together the multiplication  $\cdot$  forms a commutative group.

According to the definition, a *field* is a set  $F$  on which two binary operations, called *addition and multiplication*, are defined and which contains two distinct elements  $0$  and  $1$  (we denote the multiplicative identity  $e$  by  $1$ ) with  $0 \neq 1$ . Furthermore,  $(F, +, 0)$  is an Abelian group with respect to addition having  $0$  as the identity element, and  $(F^*, \cdot, 1)$  forms an Abelian group with respect to multiplication having  $1$  as the identity element. The two operations of addition and multiplication are linked by the distributive law  $a(b + c) = ab + ac$ . The second distributive law  $(b + c)a = ba + ca$  follows automatically from the commutativity of multiplication. The element  $0$  is called the *zero element* and  $1$  is called the *multiplicative identity element* or simply the *identity*.

**Definition 3.6** A finite field is a field that contains a finite number of elements. This number is called the order of the field.

Finite fields are also called *Galois fields* after their discoverer, Evariste Galois (1811-1832).

**Example 3.4** The following structures are fields or finite fields.

- (a)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  and  $(\mathbb{C}, +, \cdot)$  are fields.
- (b)  $(\mathbb{Z}_2, +, \cdot)$  forms a finite field of order 2. The elements of this field are  $0$  and  $1$ , and the operation tables are shown as follows:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

The elements 0 and 1 are called *binary elements*.

- (c)  $(\mathbb{Z}_5, +, \cdot)$  forms a finite field of order 5. The elements of this field are 0, 1, 2, 3 and 4, and the operation tables are shown as follows:

+	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

·	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

In general, we have the following result.

**Proposition 3.2**  $(\mathbb{Z}_p, +, \cdot)$  is a field if  $p$  is a prime.

*Proof.* From Proposition 1, both  $(\mathbb{Z}_p, +, 0)$  and  $(\mathbb{Z}_p^*, \cdot, 1)$  are Abelian groups. Since integers satisfy the distributive law, then  $a(b+c) = ab+ac$  for any  $a, b, c \in \mathbb{Z}_p$ , so that their remainders are equal. Hence  $\mathbb{Z}_p$  satisfies the distributive law. According to the definition of fields,  $(\mathbb{Z}_p, +, \cdot)$  is a field. □

*Note.* The converse of the proposition is also true, i.e. if  $(\mathbb{Z}_n, +, \cdot)$  is a field where  $n > 1$  is an positive integer, then  $n$  must be a prime.

We denote  $(\mathbb{Z}_p, +, \cdot)$  simply by  $\mathbb{Z}_p$ , or  $GF(p)$ , which is called the *residue class field modulo  $p$* . These are the first examples of finite fields that we encounter.

### C. Polynomials

Let  $R$  be an arbitrary ring. A *polynomial* over  $R$  is an expression of the form

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where  $n$  is a nonnegative integer, the coefficients  $a_i, 0 \leq i \leq n$ , are elements of  $R$ , and  $x$  is a symbol not belonging to  $R$ , called an *indeterminate* over  $R$ . We adopt the convention that a term  $a_i x^i$  with  $a_i = 0$  need not be written down. In particular, the polynomial  $f(x)$  above may then also be given in the equivalent form  $f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + \cdots + 0x^{n+h}$ , where  $h$  is any positive integer. When comparing two polynomials  $f(x)$  and  $g(x)$  over  $R$ , it is therefore possible to assume that they both involve the same powers of  $x$ .

(a) The polynomials

$$f(x) = \sum_{i=0}^n a_i x^i \text{ and } g(x) = \sum_{i=0}^n b_i x^i$$

over  $R$  are considered *equal* if and only if  $a_i = b_i$  for  $0 \leq i \leq n$ .

(b) The *sum* of  $f(x)$  and  $g(x)$  is defined by

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i) x^i.$$

(c) To define the *product* of two polynomials over  $R$ , let

$$f(x) = \sum_{i=0}^n a_i x^i \text{ and } g(x) = \sum_{i=0}^m b_i x^i$$

and set

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ where } c_k = \sum_{0 \leq i < k} a_i b_{k-i}.$$

It is easily seen that with these operations the set of polynomials over  $R$  forms a ring.

**Definition 3.7** *The ring formed by the polynomials over  $R$  with the above operations is called the polynomial ring over  $R$  and denoted by  $R[x]$ , i.e.,*

$$R[x] = \left\{ \sum_{i=0}^n a_i x^i \mid a_i \in R, n \geq 0 \right\}.$$

The zero element of  $R[x]$  is the polynomial all of whose coefficients are 0. This polynomial is called the *zero polynomial* and denoted by 0.

**Definition 3.8** *Let  $\sum_{i=0}^n a_i x^i$  be a polynomial over  $R$  that is not the zero polynomial, so that we can suppose  $a_n \neq 0$ . Then  $a_n$  is called the leading coefficient of  $f(x)$  and  $a_0$  the constant term, while  $n$  is called the degree of  $f(x)$ , denoted by  $n = \deg(f(x)) = \deg(f)$ . By convention, we set  $\deg(0) = -\infty$ . Polynomials of degree  $\leq 0$  are called constant polynomials. If the leading coefficient of  $f(x)$  is 1, then  $f(x)$  is called a monic polynomial.*

In the following, we consider polynomials over fields. Let  $F$  denote a field (not necessarily finite).

**Theorem 3.1** *Let  $f, g \in F[x]$ . Then*

$$\begin{aligned} \deg(f + g) &\leq \max\{\deg(f), \deg(g)\}, \\ \deg(fg) &= \deg(f) + \deg(g). \end{aligned}$$

A proof of this theorem can be easily carried out by computing the leading coefficient of the sum and the product of two polynomials, which is omitted here.

**Divisibility.** The polynomial  $g \in F[x]$  divides the polynomial  $f \in F[x]$  if there exists a polynomial  $h \in F[x]$  such that  $f = gh$ . We also say that  $g$  is a *divisor* of  $f$ , or  $f$  is a *multiple* of  $g$ , or  $f$  is *divisible* by  $g$ .

**Theorem 3.2** (Division Algorithm) *Let  $g \neq 0$  be a polynomial in  $F[x]$ . Then for any  $f \in F[x]$  there exist polynomials  $q, r \in F[x]$  such that*

$$f = qg + r, \text{ where } \deg(r) < \deg(g).$$

**Definition 3.9** *Let  $f, g \in F[x]$  not both of which are 0. If  $d \in F[x]$  satisfying the following conditions: (i)  $d$  divides  $f$  and  $g$ ; (ii) any polynomial  $c \in F[x]$  dividing both  $f$  and  $g$  divides  $d$ , then  $d$  is called the greatest common divisor of two polynomials  $f$  and  $g$ , denoted by  $d = \gcd(f, g)$ . If  $\gcd(f, g) = 1$ , then the two polynomials  $f$  and  $g$  are said to be relatively prime.*

**Theorem 3.3** *Let  $d = \gcd(f, g)$  with  $f, g, d \in F[x]$ . Then  $d$  can be expressed in the form*

$$d(x) = u(x)f(x) + g(x)v(x) \text{ with } u(x), v(x) \in F[x].$$

*Proof.* The greatest common divisor  $d$  of two polynomials  $f, g \in F[x]$  can be computed by the *Euclidean algorithm* as follows. Without loss of generality, we may suppose that  $g \neq 0$  and  $g \nmid f$ . We then repeatedly use the division algorithm in the following manner:

$$\begin{aligned} f &= q_1g + r_1, & \deg(r_1) < \deg(g), & & r_1 \neq 0 \\ g &= q_2r_1 + r_2, & \deg(r_2) < \deg(r_1), & & r_2 \neq 0 \\ r_1 &= q_3r_2 + r_3, & \deg(r_3) < \deg(r_2), & & r_3 \neq 0 \\ & \vdots & & & \\ r_{s-2} &= q_sr_{s-1} + r_s, & \deg(r_s) < \deg(r_{s-1}), & & r_{s-1} \neq 0 \\ r_{s-1} &= q_{r+1}r_s. \end{aligned}$$

Here  $q_1, \dots, q_{s+1}$  and  $r_1, \dots, r_s$  are polynomials in  $F[x]$ . Since  $\deg(g)$  is finite, the procedure must stop after finitely many steps. If the last nonzero remainder  $r_s$  has the leading coefficient  $b$ , then  $d = b^{-1}r_s$ . (This step is to make the leading coefficient of  $d$  is equal to 1.) The polynomials  $u$  and  $v$  can be found by working backward from the above identities and substituting the  $r_s, r_{s-1}, \dots, r_1$  into  $d = b^{-1}r_s$ .  $\square$

**Definition 3.10** *A polynomial  $p \in F[x]$  is called irreducible over  $F$  if  $p$  has positive degree and  $p = bc$  with  $b, c \in F[x]$  implies that either  $b$  or  $c$  is a constant polynomial. Otherwise,  $p$  is called reducible over  $F$ .*

Irreducible polynomials are of fundamental importance for the structure of the ring  $F[x]$ , and the structure of linear feedback shift register sequences, since polynomials in  $F[x]$  can be written as products of irreducible polynomials in an essentially unique manner. We list this result in the following theorem without proof. The proof can be found in [147] or [117].

**Theorem 3.4** (UNIQUE FACTORIZATION IN  $F[x]$ ) *Any polynomial  $f \in F[x]$  of positive degree can be written in the form*

$$f = ap_1^{e_1}p_2^{e_2} \cdots p_k^{e_k},$$

where  $a \in F$ ,  $p_1, \dots, p_k$  are distinct monic irreducible polynomials in  $F[x]$ , and  $e_1, \dots, e_k$  are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

**Definition 3.11** *An element  $b \in F$  is called a root (or zero) of the polynomial  $f \in F[x]$  if  $f(b) = 0$ .*

The following concept regarding polynomials over  $F$  corresponds to the period of the corresponding sequences.

**Definition 3.12** *For a polynomial  $f(x)$  over  $F$ , the period (or order) of  $f(x)$  is the least positive integer  $t$  such that  $f(x) \mid (x^t - 1)$ , denoted by  $\text{per}(f) = t$ .*

For example,  $f(x) = x^3 + x + 1$  over  $\mathbb{Z}_2$ , has period 7 by noticing that  $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ . But if  $f(x) = x^5 + x^2$  over  $\mathbb{Z}_2$ , then  $f(x)$  cannot be a factor of  $x^t + 1$  for any positive integer  $t$ , i.e., the period of  $f$  does not exist. However, we have the following result whose proof is omitted.

**Fact 3.2** *For  $f(x) \in F[x]$  where  $F$  is finite, if  $f(0) \neq 0$ , then the period of  $f(x)$  exists.*

## 3.2 Construction of $GF(p^n)$

In this section, we show the construction for the finite field  $GF(p^n)$ . In Section 3.1, we have already seen the finite field  $GF(p) = \mathbb{Z}_p$  of order  $p$  where  $p$  is a prime. The elements of  $GF(p)$  are  $\{0, 1, \dots, p-1\}$ , and the addition  $+$  and multiplication  $\cdot$  are carried out modulo  $p$ . We need the following fact (see [?]) in order to construct the finite field  $GF(p^n)$ .

**Fact 3.3** *For every prime  $p$ , and every degree  $n > 1$ , there is at least one irreducible polynomial of degree  $n$  over  $\mathbb{Z}_p$ .*

Let  $n$  be a positive integer. To construct the finite field  $GF(p^n)$  of order  $p^n$ , we choose  $f(x)$  to be an irreducible polynomial over  $GF(p)$  of degree  $n$ . Let us agree that  $\alpha$  is a formal symbol that satisfies  $f(\alpha) = 0$ . Let

$$GF(p^n) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in GF(p)\}.$$

We define two operations:  $+$  and  $\cdot$  on  $GF(p^n)$  as follows. For  $g(\alpha), h(\alpha) \in GF(p^n)$ ,

$$g(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i \text{ and } h(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i,$$

$$\text{Addition: } g(\alpha) + h(\alpha) = \sum_{i=0}^{n-1} (a_i + b_i) \alpha^i \in GF(p^n)$$

$$\text{Multiplication: } g(\alpha) \cdot h(\alpha) = r(\alpha)$$

where  $r(\alpha)$  is computed as follows:

(i) Multiply  $g(\alpha)$  and  $h(\alpha)$  according to the multiplication of polynomials, i.e.,

$$\begin{aligned} g(\alpha)h(\alpha) &= \sum_{i=0}^{n-1} a_i \alpha^i \sum_{j=0}^{n-1} b_j \alpha^j \\ &= \sum_{k=0}^{2n} c_k \alpha^k = c(\alpha) \end{aligned}$$

where

$$c_k = \sum_{i+j=k} a_i b_j.$$

(ii) Applying the division algorithm to  $c(\alpha)$  and  $f(\alpha)$ , we can get two polynomials  $q(\alpha)$  and  $r(\alpha)$  such that

$$c(\alpha) = q(\alpha)f(\alpha) + r(\alpha) \text{ with } \deg(r(\alpha)) < n.$$

Since  $\alpha$  satisfies  $f(\alpha) = 0$ , we have  $c(\alpha) = r(\alpha) \in GF(p^n)$ . In other words,  $r(x)$  is the remainder of the product  $g(x)h(x)$  divided by  $f(x)$ .

**Theorem 3.5** *The set  $GF(p^n)$  together with the two operations defined above forms a finite field, and the order of this field is  $p^n$ .*

*Proof.* Using the same argument as we did for the polynomial ring  $GF(p)[x]$ , it is clear that  $(GF(p^n), +, \cdot)$ , where two operations  $+$  and  $\cdot$  are defined above, forms a ring. So, we only need to prove that for each  $g \neq 0 \in GF(p^n)$ , there exists  $g^{-1} \in GF(p^n)$  such that  $gg^{-1} = 1$ . Since  $f(x)$  is irreducible over  $GF(p)$  of degree  $n$  and  $\deg(g(x)) \leq n-1$ , then  $g(x)$  is relatively prime to  $f(x)$ , i.e.,  $\gcd(f(x), g(x)) = 1$ . According to Theorem 3.3, there exist two polynomials  $u(x), v(x) \in GF(p)[x]$  such that

$$g(x)u(x) + f(x)v(x) = 1.$$

Substituting  $\alpha$  into the above identity,

$$g(\alpha)u(\alpha) + f(\alpha)v(\alpha) = 1.$$

Since  $f(\alpha) = 0$ , we get  $g(\alpha)u(\alpha) = 1$ . Note that if  $\deg(u) \geq n$ , applying the division algorithm to  $u(x)$  and  $f(x)$ , we then have  $u(x) = q_1(x)f(x) + r_1(x)$

where  $\deg(r_1) < n$ . By substituting  $\alpha$ , it follows that  $u(\alpha) = r_1(\alpha) \in GF(p^n)$ . So, we can suppose that  $\deg(u) \leq n - 1$ . Hence we have  $g(\alpha)u(\alpha) = 1$  where  $u(\alpha) \in GF(p^n) \implies g^{-1} = u(\alpha)$ .

□

The polynomial  $f(x)$  is called a *defining polynomial* of  $GF(p^n)$  and  $\alpha$  is called a *defining element* of  $GF(p^n)$  over  $GF(p)$ . The finite field  $GF(p^n)$  is also called a *Galois field*. From the construction of  $GF(p^n)$ ,  $f(\alpha) = 0$ . Thus  $\alpha$  is a root of  $f(x)$  in  $GF(p^n)$ . We also say that  $GF(p^n)$  is obtained from  $GF(p)$  by adjoining to  $GF(p)$  a zero of  $f(x)$  or  $GF(p^n)$  is a *finite extension* of  $GF(p)$ .

**Example 3.5** Let  $p = 2$  and  $f(x) = x^3 + x + 1$ . Then  $f(x)$  is irreducible over  $GF(2)$ . Let  $\alpha$  be a root of  $f(x)$ , i.e.,  $f(\alpha) = 0$ . The finite field  $GF(2^3)$  is defined by

$$GF(2^3) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in GF(2)\}.$$

$GF(2^3)$ , defined by  $f(x) = x^3 + x + 1$  and  $f(\alpha) = 0$

as a 3-tuple	as a polynomial	as a power of $\alpha$
000 =	0	= 0
001 =	1	= 1
010 =	$\alpha$	= $\alpha$
100 =	$\alpha^2$	= $\alpha^2$
110 =	$1 + \alpha$	= $\alpha^3$
011 =	$\alpha + \alpha^2$	= $\alpha^4$
111 =	$1 + \alpha + \alpha^2$	= $\alpha^5$
101 =	$1 + \alpha^2$	= $\alpha^6$
$\alpha^7 = 1$		

Note that  $GF(2^3)^* = \langle \alpha \rangle$ , i.e., the nonzero elements of  $GF(2^3)$  form a cyclic group of order 7 with generator  $\alpha$ , where  $\alpha^7 = 1$ .

**Example 3.6** Let  $p = 2$  and  $f(x) = x^4 + x + 1$ . Then  $f(x)$  is irreducible over  $GF(2)$ . Let  $\alpha$  be a root of  $f(x)$ , i.e.,  $f(\alpha) = 0$ . The finite field  $GF(2^4)$  is defined by

$$GF(2^4) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in GF(2)\}.$$

(a) A table of  $GF(2^4)$  is given below.

$GF(2^4)$ , defined by  $f(x) = x^4 + x + 1$  and  $f(\alpha) = 0$

0 0 0 0	=	0 = $\alpha^\infty$
1 0 0 0	=	1 = $\alpha^0$
0 1 0 0	=	$\alpha$
0 0 1 0	=	$\alpha^2$
0 0 0 1	=	$\alpha^3$
1 1 0 0	=	$\alpha^4$
0 1 1 0	=	$\alpha^5$
0 0 1 1	=	$\alpha^6$
1 1 0 1	=	$\alpha^7$
1 0 1 0	=	$\alpha^8$
0 1 0 1	=	$\alpha^9$
1 1 1 0	=	$\alpha^{10}$
0 1 1 1	=	$\alpha^{11}$
1 1 1 1	=	$\alpha^{12}$
1 0 1 1	=	$\alpha^{13}$
1 0 0 1	=	$\alpha^{14}$

$$(\alpha^{15} = 1)$$

(b) To add and multiply  $1 + \alpha$  and  $\alpha + \alpha^3$ :

$$(1 + \alpha) + (\alpha + \alpha^3) = 1 + \alpha^3$$

We may use the definition of multiplication in  $GF(p^n)$  to multiply these two elements. But here we will introduce a simpler way to do that. Note that  $1 + \alpha = \alpha^4$  and  $\alpha + \alpha^3 = \alpha^9$ . Hence

$$(1 + \alpha) \cdot (\alpha + \alpha^3) = \alpha^4 \alpha^9 = \alpha^{4+9} = \alpha^{13} = 1 + \alpha^2 + \alpha^3.$$

So, the polynomial representation is efficient for performing addition, while the exponential representation is best for multiplication. Note that we also have  $GF(2^4)^* = \langle \alpha \rangle$ , i.e.,  $GF(2^4)^*$  is a cyclic group of order 15 with generator  $\alpha$ , where  $\alpha^{15} = 1$ .

### 3.3 The Basic Theory of Finite Fields

#### A. The characteristic of a finite field

**Definition 3.13** *If  $F$  is a finite field and there exists a positive integer  $m$  such that  $m\beta = 0$  for every  $\beta \in F$ , then the least such positive integer  $m$  is called the characteristic of  $F$  and  $F$  is said to have characteristic  $m$ .*

**Theorem 3.6** *Let  $F$  be a finite field. Then the characteristic of  $F$  is a prime.*

*Proof.* Let  $|F| = q$ .  $F$  contains the identity element 1. Since  $F$  is finite, the elements  $1, 1 + 1 = 2, 1 + 1 + 1 = 3, \dots$  cannot be all distinct. Therefore, there

is the smallest number  $p$  such that  $p = 1 + 1 + \cdots + 1$  ( $p$  times)  $= 0$ . This  $p$  must be a prime number (for if  $rs = 0$  then  $r = 0$  or  $s = 0$ ).

□

Let  $F$  be a field. A subset  $K$  of  $F$  that is itself a field under the operations of  $F$  will be called a *subfield* of  $F$ .  $F$  is called an *extension (field)* of  $K$ . If  $K \neq F$ , we say that  $K$  is a *proper subfield* of  $F$ . So,  $GF(p^n)$  has characteristic  $p$  and contains  $GF(p)$  as a subfield.

### B. Structures of Finite Fields

**Theorem 3.7** *Let  $F$  be a finite field and  $|F| = q$  with characteristic  $p$ . Then  $F = GF(p)$  if  $q = p$  or  $F$  is a vector space of dimension  $n$  over  $GF(p)$  if  $q > p$ , that is  $q = p^n$ .*

*Proof.* If  $q = p$ , since  $GF(p)$  is a subfield of  $F$ , we get  $F = GF(p)$ . Supposing  $q > p$ , we choose a maximal set of elements of  $F$  which are linearly independent over  $GF(p)$ , say  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ . Then  $F$  contains all the elements

$$a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1}, \quad a_i \in GF(p),$$

and no others. Thus  $F$  is a vector space of dimension  $n$  over  $GF(p)$ , and contains  $q = p^n$  elements.

□

Theorem 3.7 shows that if  $F$  is a finite field of order  $q$  and  $p$  is the characteristic of  $F$ , then  $q = p$  or  $q = p^n$  ( $n \geq 1$ ). Two finite fields  $F$  and  $G$  are said to be *isomorphic* if there is a one-to-one mapping from  $F$  onto  $G$  which preserves addition and multiplication. All finite fields of order  $p^n$  are isomorphic (we omit the proof here). So, we only have two different types of finite fields: one is  $GF(p)$ , the residue class field modulo  $p$ , and the other is  $GF(p^n)$ , the extension field obtained by adjoining a zero of an irreducible polynomial of degree  $n$  over  $GF(p)$  to  $GF(p)$ . Sometimes we denote  $F$  with order  $q$  by  $\mathbb{F}_q$ . For a finite field  $F$  we denote by  $F^*$  the multiplicative group of the nonzero elements of  $F$ .

**Definition 3.14** *Let  $G$  be a group. For  $\alpha \in G$ , if  $r$  is the smallest positive integer such that  $\alpha^r = 1$ , then  $r$  is called the order of  $\alpha$ , denoted by  $\text{ord}(\alpha) = r$ .*

In the following, we will establish the cyclic structure of the multiplicative group of a finite field. For doing this, we need the following fact about orders of the elements in a commutative group.

**Fact 3.4** *Let  $\alpha, \beta \in F^*$  with  $\text{ord}(\alpha) = r$  and  $\text{ord}(\beta) = s$ . Then*

- (i)  $\text{ord}(\alpha^m) = r/\text{gcd}(r, m)$ . Moreover  $\text{ord}(\alpha^m) = \text{ord}(\alpha)$  if and only if  $\text{gcd}(m, r) = 1$ .
- (ii) If  $\text{gcd}(r, s) = 1$ , then  $\text{ord}(\alpha\beta) = rs$ .

Note that the above fact is not true for non-commutative groups.

**Theorem 3.8** *For every finite field  $F$  the multiplicative group  $F^*$  (nonzero elements of  $F$ ) is cyclic.*

*Proof.* Let  $|F| = q$ . We need to prove that there is an element in  $F^*$  which has order  $q - 1$ . We first show the following assertion.

*If we choose  $\alpha \in F^*$  such that the order  $r$  of  $\alpha$  is the maximum one, then the order  $s$  of any element  $\beta \in F^*$  divides  $r$ , i.e.,  $s|r$ .*

From Fact 3.4-(ii) and the assumption about  $r$ , we know that  $\gcd(r, s) \neq 1$ . For any common prime divisor of  $s$  and  $r$ , we may write  $r = p_1^d a$  and  $s = p_1^e b$  where  $a$  and  $b$  are not divisible by  $p_1$  and  $d, e \geq 1$ . According to Fact 3.4-(i),  $\text{ord}(\alpha^{p_1^d}) = a$ ,  $\text{ord}(\beta^b) = p_1^e$  and  $\text{ord}(\alpha^{p_1^d} \beta^b) = p_1^e a$ . Hence  $e \leq d$  or else  $r$  would not be maximum. Thus every prime power that is a divisor of  $s$  is also a divisor of  $r$ , and so  $s|r$ . Next we prove that  $r = q - 1$ . It is clear  $r \leq q - 1$ . Let  $g(x) = \prod_{\beta \in F^*} (x - \beta)$ . Then  $\deg(g) = q - 1$ . From the above assertion, every  $\beta \in F^*$  satisfies the equation  $x^r - 1 = 0$ . Consequently,  $x^r - 1$  is divisible by  $g(x) \implies q - 1 = \deg(g) \leq \deg(x^r - 1) = r$ . But  $r \leq q - 1$ , hence  $r = q - 1$ . Thus  $F^* = \langle \alpha \rangle$ . □

**Definition 3.15** *A generator of the cyclic group  $GF(p^n)^*$  is called a primitive element of  $GF(p^n)$ . An irreducible polynomial over  $GF(p)$  having a primitive element in  $GF(p^n)$  as a zero is called a primitive polynomial over  $GF(p)$ .*

Note that not all irreducible polynomials are primitive. For example,  $x^4 + x^3 + x^2 + x + 1$  is irreducible over  $GF(2)$ , so it can be used to generate the field  $GF(2^4)$ . However, it is not a primitive polynomial. According to the definition, if  $F$  is a finite field of order  $p^n$ , an element  $\alpha$  of  $F$  is a primitive element if it has order  $p^n - 1$ .

**Corollary 3.1** *Every finite field contains a primitive element.*

*Proof.* Take  $\alpha$  to be a generator of the cyclic group  $F^*$ . □

The following corollary follows directly from the proof of Theorem 3.8.

**Corollary 3.2** (FERMAT'S THEOREM) *Every element  $\beta$  of a finite field of order  $p^n$  satisfies the identity*

$$\beta^{p^n} = \beta,$$

*or equivalently, it is a root of the equation*

$$x^{p^n} - x = 0.$$

*Thus*

$$x^{p^n} - x = \prod_{\beta \in F} (x - \beta).$$

**Lemma 3.1** *In any finite field of characteristic  $p$ ,*

$$(x + y)^p = x^p + y^p.$$

*Proof.* Use the binomial expansion,

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^{p-k} y^k$$

where

$$\binom{p}{0} = \binom{p}{p} = 1.$$

Now if  $1 \leq k \leq p-1$ , then  $\gcd(k!, p) = 1$ . Thus

$$\begin{aligned} \binom{p}{k} &= \frac{p(p-1)\cdots(p-k+1)}{k!} \\ &= p \frac{(p-1)\cdots(p-k+1)}{k!} \equiv 0 \pmod{p}. \end{aligned}$$

□

The following result is easily proved by mathematical induction.

**Corollary 3.3** *In any finite field of characteristic  $p$ ,*

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}$$

for any  $m \geq 1$ .

### C. Representations of Elements

According to Theorem 3.7,  $GF(p^n)$  is a vector space of dimension  $n$  over  $GF(p)$ . Any set of  $n$  linearly independent elements can be used as a basis for this vector space. There are two important bases for  $GF(p^n)$ . One is the *polynomial basis*  $\{1, \alpha, \dots, \alpha^{n-1}\}$ , which is used to construct  $GF(p^n)$  from an irreducible polynomial  $f(x)$  over  $GF(p)$  of degree  $n$  with  $f(\alpha) = 0$  (see Section 3.1). Another is called a *normal basis*  $\{\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}\}$  if these are linearly independent over  $GF(p)$ . Normal bases for  $GF(p^n)$  always exist (see [117]). We also know that  $GF(p^n)^*$  is a cyclic group. Let  $\alpha$  be a primitive element of  $GF(p^n)$  and  $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$  be a basis of  $GF(p^n)$  over  $GF(p)$ . Then we can write  $GF(p^n)$  as follows:

$$\begin{aligned} GF(p^n) &= \{a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1} \mid a_i \in GF(p)\} \\ &\quad \text{(Vector Representation)} \\ &= \{\alpha^i \mid 0 \leq i \leq p^n - 2 \text{ or } i = \infty\} \\ &\quad \text{(Exponential Representation)} \end{aligned}$$

where we denote  $0 = \alpha^\infty$ .

**Example 3.7** For the finite field  $GF(2^3)$ , defined by  $f(x) = x^3 + x + 1$ , we have the following representations.

Poly. Basis			Normal Basis			$\alpha^r = 1$ Exp.
1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^6$	$\alpha^5$	
0	0	0	0	0	0	$0 = \alpha^\infty$
1	0	0	1	1	1	$1 = \alpha^0$
0	1	0	0	1	1	$\alpha$
0	0	1	1	0	1	$\alpha^2$
1	1	0	1	0	0	$\alpha^3$
0	1	1	1	1	0	$\alpha^4$
1	1	1	0	0	1	$\alpha^5$
1	0	1	0	1	0	$\alpha^6$

#### D. Computation of $GF(p^n)$

Let  $\alpha$  be a primitive element of  $GF(p^n)$ . For  $0 \neq \beta \in GF(p^n)$ , then  $\beta = \alpha^i$  for some  $i \geq 0$ . The nonnegative integer  $i$  is called a *logarithm* of  $\beta$  (to the base  $\alpha$ ). For small finite fields, we have the following look-up table methods for performing computations in  $GF(p^n)$ , which are much more efficient than using the method from the definition of the multiplication.

**Method 1:** Using the log and anti-log tables, the elements of  $GF(p^n)$  are obtained from the vector representation.

*Addition:* Using a vector representation: For  $\beta = b_0\alpha_0 + b_1\alpha_1 + \cdots + b_{n-1}\alpha_{n-1}$ , and  $\gamma = c_0\alpha_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha_{n-1}$ ,

$$\beta + \gamma = (b_0 + c_0)\alpha_0 + (b_1 + c_1)\alpha_1 + \cdots + (b_{n-1} + c_{n-1})\alpha_{n-1}$$

where  $b_i + c_i$  is performed in  $GF(p)$ , i.e., modulo  $p$ .

*Multiplication:* Using an exponential representation for which the elements are converted from the log and anti-log tables: First, by look-up in the anti-log table to obtain

$$\beta = \alpha^r \quad \text{and} \quad \gamma = \alpha^s;$$

then compute

$$\beta\gamma = \alpha^{r+s}$$

where  $r + s$  is reduced modulo  $p^n - 1$ , finally, by look-up in the log table, the vector representation of  $\alpha^{r+s}$  is retrieved.

**Method 2:** Using the *trinomial table* (or “Zech’s logarithm”), and the elements of  $GF(p^n)$  are presented by the exponential representation. For  $0 < t < p^n - 1$ , there exists a unique  $\tau(t)$  such that

$$1 + \alpha^t = \alpha^{\tau(t)}.$$

$\tau(t)$  is called the *Zech’s logarithm* of  $\alpha^t$ . The table containing  $\tau(t)$  for  $0 < t < p^n - 1$  is called the *trinomial table* of  $GF(p^n)$  (or *add-one table*). Then to add and multiply  $\alpha^t$  and  $\alpha^s$ :

$$\begin{aligned}
 \text{Addition: } \quad \alpha^t + \alpha^s &= \alpha^t(1 + \alpha^{s-t}) = \alpha^t \cdot \alpha^{\tau(s-t)} \\
 &= \alpha^{t+\tau(s-t)} \quad (\text{using the trinomial table}) \\
 \text{Multiplication: } \quad \alpha^t \alpha^s &= \alpha^{t+s}.
 \end{aligned}$$

**Example 3.8** (a) For the finite field  $GF(2^4)$ , given by Example 3.6, we have the following trinomial table:

$t$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\tau(t)$	4	8	14	1	10	13	9	2	7	5	12	11	6	3.

For multiplying  $\alpha^3$  times  $\alpha^5$ , it is easy because it just involves addition of the exponents, i.e.,  $\alpha^3 \cdot \alpha^5 = \alpha^{3+5} = \alpha^8$ . For computing  $\alpha^3 + \alpha^5$ , we use the above trinomial table:

$$\alpha^3 + \alpha^5 = \alpha^3(1 + \alpha^2) = \alpha^{3+\tau(2)} = \alpha^{3+8} = \alpha^{11}.$$

(b) Let  $GF(2^5)$  be defined by the primitive polynomial  $f(x) = x^5 + x^3 + 1$ , and let  $\alpha$  be a root of  $f(x)$ . Then  $\alpha$  is a primitive element of  $GF(2^5)$ .

Table 3.1:  $GF(2^5)$  defined by  $\alpha^5 + \alpha^3 + 1 = 0$  and its trinomial table

$\alpha^t$	Vector Representation	$\tau(t)$	$\alpha^t$	Vector Representation	$\tau(t)$
0	1 0 0 0 0	$\infty$	16	0 0 1 1 0	7
1	0 1 0 0 0	14	17	0 0 0 1 1	18
2	0 0 1 0 0	28	18	1 0 0 1 1	17
3	0 0 0 1 0	5	19	1 1 0 1 1	8
4	0 0 0 0 1	25	20	1 1 1 1 1	12
5	1 0 0 1 0	3	21	1 1 1 0 1	27
6	0 1 0 0 1	10	22	1 1 1 0 0	15
7	1 0 1 1 0	16	23	0 1 1 1 0	11
8	0 1 0 1 1	19	24	0 0 1 1 1	9
9	1 0 1 1 1	24	25	1 0 0 0 1	4
10	1 1 0 0 1	6	26	1 1 0 1 0	29
11	1 1 1 1 0	23	27	0 1 1 0 1	21
12	0 1 1 1 1	20	28	1 0 1 0 0	25
13	1 0 1 0 1	30	29	0 1 0 1 0	28
14	1 1 0 0 0	1	30	0 0 1 0 1	13
15	0 1 1 0 0	22			

In Table 3.1, the first column (also the fourth column) lists the exponent  $i$  in  $\alpha^i$ , the second column (and the fifth column) the coefficients of  $\alpha^i$  under the basis  $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ , and the third column (also the sixth column), the trinomial table, i.e., the values of  $\tau(i)$ ,  $i = 1, \dots, 30$ , where  $1 + \alpha^i = \alpha^{\tau(i)}$ . Therefore,

$$\begin{aligned} \alpha^8 + \alpha^{27} &= \alpha^8(1 + \alpha^{19}) = \alpha^{8+\tau(19)} = \alpha^{8+8} = \alpha^{16}, \\ &\quad (\tau(19) = 8 \text{ by look-up table}) \\ \alpha^8 \cdot \alpha^{27} &= \alpha^{8+27} = \alpha^4. \end{aligned}$$

The second method only needs to store the trinomial table, which contains the values of  $\tau(t)$  for  $1 \leq t < p^n - 1$  (see the above example). This is much more efficient for performing computations in small finite fields, say  $p^n \leq 2^{40}$ , than the first method (which needs to store two tables). In general, for coding applications, the sizes of finite fields are small which fall in this range. However, for cryptographical applications, the fields are usually large, with sizes at least having  $\log(p^n) \geq 1024$ . Thus the look-up table methods are not applicable to this type of application. So, one has to perform multiplication by the Euclidean algorithm (see the definition of the multiplication in a finite field in Section 3.2).

### 3.4 Minimal Polynomials

Fermat's theorem (Corollary 3.2) implies that every element  $\alpha$  of  $GF(q)$  where  $q$  is a prime or a power of a prime, say  $q = p^n$ , satisfies the equation

$$x^q - x = 0. \quad (3.1)$$

This polynomial has all its coefficients from the prime field  $GF(p)$ , and is monic. However,  $\alpha$  may satisfy an equation with a lower degree than (3.1).

**Definition 3.16** *Let  $\alpha$  be an element in  $GF(p^n)$ . The minimal polynomial of  $\alpha$  over  $GF(p)$  is defined as the lowest degree monic polynomial  $m(x) \in GF(p)[x]$  such that  $m(\alpha) = 0$ .*

*Note.* The minimal polynomial of any element in  $GF(p^n)$  is unique.

**Example 3.9** In  $GF(2^4)$ , defined by  $\alpha^4 + \alpha + 1 = 0$ , the minimal polynomials, having coefficients equal to 0 or 1, are listed in the following table.

Element	Minimal Polynomial
0	$x$
1	$x + 1$
$\alpha$	$x^4 + x + 1$
$\alpha^{-1} = \alpha^{14}$	$x^4 + x^3 + 1$
$\alpha^3$	$x^4 + x^3 + x^2 + x + 1$
$\alpha^5$	$x^2 + x + 1$

We will show a method for finding minimal polynomials later.

### A. Properties of Minimal Polynomials

Assume that  $m(x)$  is the minimal polynomial of  $\alpha \in GF(p^n)$ .

**Property 3.1** (IRREDUCIBILITY)  $m(x)$  is irreducible.

*Proof.* If  $m(x) = g(x)h(x)$  where the degrees of both  $g(x)$  and  $h(x)$  are greater than zero, then  $m(\alpha) = g(\alpha)h(\alpha) = 0$ . Thus either  $g(\alpha) = 0$  or  $h(\alpha) = 0$ , which contradicts the fact that  $m(x)$  is the lowest degree polynomial with  $\alpha$  as a root.  $\square$

**Property 3.2** (DIVISIBILITY) For any  $f(x) \in GF(p)[x]$ , if  $f(\alpha) = 0$ , then  $m(x) | f(x)$ .

*Proof.* Applying the division algorithm to divide  $f(x)$  by  $m(x)$ , then there exist  $q(x), r(x) \in GF(p)[x]$  such that

$$f(x) = q(x)m(x) + r(x), \deg(r(x)) < \deg(m(x)).$$

Substituting  $x = \alpha$ , this becomes

$$0 = 0 + r(\alpha).$$

Hence,  $r(x)$  is a polynomial of lower degree than  $m(x)$ , but has  $\alpha$  as a root. This is a contradiction unless  $r(x) = 0$ , and then  $m(x) | f(x)$ .  $\square$

**Property 3.3**

$$m(x) | (x^{p^n} - x).$$

*Proof.* From Corollary 3.2,  $\alpha \in GF(p^n) \implies \alpha^{p^n} - \alpha = 0$ . Applying Property 3.2,  $m(x) | (x^{p^n} - x)$ .  $\square$

**Property 3.4**  $\deg(m(x)) \leq n$ .

*Proof.*  $GF(p^n)$  is a vector space of dimension  $n$  over  $GF(p)$ . Therefore any  $n+1$  elements, such as  $1, \alpha, \dots, \alpha^n$ , are linearly dependent, i.e, there exist coefficients  $a_i \in GF(p)$ , not all zero, such that

$$\sum_{i=0}^n a_i \alpha^i = 0.$$

Thus  $\sum_{i=0}^n a_i x^i \in GF(p)[x]$  is a polynomial of degree  $\leq n$  having  $\alpha$  as a root. Therefore  $\deg(m(x)) \leq n$ .  $\square$

**Property 3.5** *The minimal polynomial of a primitive element of  $GF(p^n)$  has degree  $n$ .*

*Proof.* Let  $\alpha$  be a primitive element of  $GF(p^n)$ , with minimal polynomial  $m(x)$  of degree  $d$ . As in Theorem 3.5 we may use  $m(x)$  to generate a field  $F$  of order  $p^d$ . For  $F$  contains  $\alpha$ , and hence all of  $GF(p^n)$ , then  $d \geq n$ . By Property 3.5, it follows that  $d = n$ . □

### B. Conjugates and Cyclotomic Cosets

**Property 3.6**  *$\alpha$  and  $\alpha^p$  have the same minimal polynomial. In particular, in  $GF(p^n)$ ,  $\alpha$  and  $\alpha^{p^2}$  have the same minimal polynomial.*

*Proof.* Let  $m_\alpha(x) = \sum a_i x^i$  and  $m_{\alpha^p}(x) = \sum b_i x^i$ ,  $a_i, b_i \in GF(p)$ , be the minimal polynomials of  $\alpha$  and  $\alpha^p$  over  $GF(p)$ . Note that  $a_i = a_i^p$ . Using Lemma 3.1,

$$\begin{aligned} m_\alpha(\alpha^p) &= \sum a_i (\alpha^p)^i = \sum a_i^p (\alpha^i)^p = \sum (a_i \alpha^i)^p \\ &= \left( \sum a_i \alpha^i \right)^p = m_\alpha(\alpha)^p = 0. \end{aligned}$$

According to Property 3.2,  $m_{\alpha^p}(x) \mid m_\alpha(x)$ . From Property 3.1,  $m_\alpha(x)$  is irreducible, so  $m_\alpha(x) = m_{\alpha^p}(x)$ . □

**Definition 3.17** *Let  $\alpha \in GF(p^n)$ . Then the elements  $\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}$  are called conjugates of  $\alpha$  with respect to  $GF(p)$ .*

From Property 3.6 all conjugates of  $\alpha$  have the same minimal polynomial.

**Definition 3.18** *A (cyclotomic) coset  $C_s$  modulo  $p^n - 1$  (with respect to  $p$ ) is defined to be*

$$C_s = \{s, sp, \dots, sp^{n_s-1}\},$$

where  $n_s$  is the smallest positive integer such that  $s \equiv sp^{n_s} \pmod{p^n - 1}$ . The subscript  $s$  is chosen as the smallest integer in  $C_s$ , and  $s$  is called the coset leader of  $C_s$ .

*Note.* In group theory, all cosets of a subgroup  $H$  of a group  $G$  have the same number of elements. The *cyclotomic cosets* are generalized cosets of a cyclic subgroup of the multiplicative group  $\mathbb{Z}_m^*$ , extended to the entire ring  $\mathbb{Z}_m$ , and have sizes which divide the order of the cyclic subgroup.

We introduce the following notation related to the cyclotomic cosets.

$$\begin{aligned} \Gamma_p(n) &= \{ \text{all coset leaders in } \mathbb{Z}_{p^n-1} \}, \text{ and} \\ \Omega_p(n) &= \{C_s \mid s \in \Gamma_p(n)\}. \end{aligned}$$

Then  $|\Gamma_p(n)| = |\Omega_p(n)|$ . Note that the operation of multiplying the elements in  $\mathbb{Z}_{p^n-1}$  by  $p$  results in a partition of  $\mathbb{Z}_{p^n-1}$ , i.e.,

$$\mathbb{Z}_{p^n-1} = \bigcup_{s \in \Gamma_p(n)} C_s.$$

**Example 3.10** We compute the cyclotomic cosets modulo  $2^n - 1$  with respect to 2 for  $n = 4, 5, 6$  and 7.

(a). For  $n = 4$  and  $p = 2$ , the cyclotomic cosets modulo 15 are:

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

Moreover, we have

$$\mathbb{Z}_{15} = C_0 \cup C_1 \cup C_3 \cup C_5 \cup C_7$$

and  $\Gamma_2(4) = \{0, 1, 3, 5, 7\}$ .

(b) For  $n = 5$  and  $p = 2$ , the cyclotomic cosets modulo 31 are given as follows:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8, 16\} \\ C_3 &= \{3, 6, 12, 24, 17\} \\ C_5 &= \{5, 10, 20, 9, 18\} \\ C_7 &= \{7, 14, 28, 25, 19\} \\ C_{11} &= \{11, 22, 13, 26, 21\} \\ C_{15} &= \{15, 30, 29, 27, 23\}. \end{aligned}$$

The set  $\Gamma_2(5)$ , consisting of all coset leaders modulo 31, is given by

$$\Gamma_2(5) = \{0, 1, 3, 5, 7, 11, 15\}.$$

(c) In the following, the cosets modulo 63 and 127, respectively, have the coset leaders listed in the first columns.

Cyclotomic cosets modulo 63

0					
1	2	4	8	16	32
3	6	12	24	48	33
5	10	20	40	17	34
7	14	28	56	49	35
9	18	36			
11	22	44	25	50	37
13	26	52	41	19	38
15	30	60	57	51	39
21	42				
23	46	29	58	53	43
27	54	45			
31	62	61	59	55	47

Cyclotomic cosets modulo 127

0						
1	2	4	8	16	32	64
3	6	12	24	48	96	65
5	10	20	40	80	33	66
7	14	28	56	112	97	67
9	18	36	72	17	34	68
11	22	44	88	49	98	69
13	26	52	104	81	35	70
15	30	60	120	113	99	71
19	38	76	25	50	100	73
21	42	84	41	82	37	74
23	46	92	57	114	101	75
27	54	108	89	51	102	77
29	58	116	105	83	39	78
31	62	124	121	115	103	79
43	86	45	90	53	106	85
47	94	61	122	117	107	87
55	110	93	59	118	109	91
63	126	125	123	119	111	95

For  $\alpha \in GF(p^n)$ , all  $\alpha^j$ 's where  $j$  runs through a cyclotomic coset have the same minimal polynomial. This leads to the following method for finding minimal polynomials.

### C. Finding Minimal Polynomials

#### Algorithm 3.1 AN ALGORITHM FOR FINDING MINIMAL POLYNOMIALS

*Input:*  $f(x)$ , a primitive polynomial over  $GF(p)$  of degree  $n$ .  
*Output:* All irreducible polynomials over  $GF(p)$  whose degrees divides  $n$

procedure\_MP( $f$ ):

1. Generate the finite field  $GF(p^n)$  by  $f(\alpha) = 0$ .
2. Compute all coset leaders mod  $(p^n - 1)$ :  $\Gamma_p(n)$ .
3. For each  $s \in \Gamma_p(n)$ , compute

$$m_s(x) = \prod_{i \in C_s} (x - \alpha^i)$$

4. Return all  $m_s(x)$  for  $s \in \Gamma_p(n)$ .

The polynomial  $m_s(x)$ , computed in Algorithm 3.1, is the minimal polynomial of  $\alpha^s$  and its conjugates. According to Fact 3.4, if  $\gcd(s, p^n - 1) = 1$ , then

$ord(\alpha^s) = ord(\alpha) = p^n - 1$ . Thus  $\alpha^s$  is a primitive element of  $GF(p^n)$ . Hence  $m_s(x)$  is a primitive polynomial over  $GF(p)$  of degree  $n$ . We list the following formula without proof. The readers may write it out for themselves.

$$x^{p^n} - x = \text{product of all monic polynomials,} \\ \text{irreducible over } GF(p), \text{ whose} \\ \text{degrees divide } n.$$

So, Algorithm 3.1 gives all of such irreducible polynomials. Thus we have established the following property:

**Property 3.7**

$$x^{p^n} - x = x \prod_{s \in \Gamma_p(n)} m_s(x)$$

where the size of a coset  $C_s$  is equal to the degree of the minimal polynomial of  $\alpha^s$  over  $GF(p)$  and  $\deg(m_s(x))|n$  for every  $s \in \Gamma_p(n)$ .

**Example 3.11** (a) Let  $n = 4$ ,  $p = 2$ , and  $GF(2^4)$  be defined by  $\alpha^4 + \alpha + 1 = 0$ . The minimal polynomials of the elements of  $GF(2^4)$  are listed in Table 3.2.

Table 3.2: Minimal polynomials of the elements of  $GF(2^4)$

Coset	Element	Minimal Polynomial
	0	$x$
$C_0 = \{0\}$	1	$m_0(x) = x + 1$
$C_1 = \{1, 2, 4, 8\}$	$\alpha, \alpha^2, \alpha^4, \alpha^8$	$m_1(x) = x^4 + x + 1$
$C_3 = \{3, 6, 12, 9\}$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$m_3(x) = x^4 + x^3 + x^2 + x + 1$
$C_5 = \{5, 10\}$	$\alpha^5, \alpha^{10}$	$m_5(x) = x^2 + x + 1$
$C_7 = \{7, 14, 13, 11\}$	$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$m_7(x) = x^4 + x^3 + 1$

Furthermore,

$$\begin{aligned} x^{2^4} + x &= x m_0(x) m_1(x) m_3(x) m_5(x) m_7(x) \\ &= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1) \\ &\quad (x^4+x^3+x^2+x+1). \end{aligned}$$

(b) Let  $n = 5$ ,  $p = 2$ , and  $GF(2^5)$  be defined by  $\alpha^5 + \alpha^3 + 1 = 0$  from Example 3.8. The minimal polynomials of the elements of  $GF(2^5)$  are listed in Table 3.3.

Table 3.3: Minimal polynomials of the elements of  $GF(2^5)$ 

Coset	Element	Minimal Polynomial
	0	$x$
$C_0 = \{0\}$	1	$m_0(x) = x + 1$
$C_1 = \{1, 2, 4, 8, 16\}$	$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$	$m_1(x) = x^5 + x^3 + 1$
$C_3 = \{3, 6, 12, 24, 17\}$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$	$m_3(x) = x^5 + x^3 + x^2 + x + 1$
$C_5 = \{5, 10, 20, 9, 18\}$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}$	$m_5(x) = x^5 + x^4 + x^3 + x + 1$
$C_7 = \{7, 14, 28, 25, 19\}$	$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$	$m_7(x) = x^5 + x^4 + x^3 + x^2 + 1$
$C_{11} = \{11, 22, 13, 26, 21\}$	$\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}$	$m_{11}(x) = x^5 + x^4 + x^2 + x + 1$
$C_{15} = \{15, 30, 29, 27, 23\}$	$\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}$	$m_{15}(x) = x^5 + x^2 + 1$

Therefore

$$\begin{aligned}
 x^{2^5} + x &= x m_0(x) m_1(x) m_3(x) m_5(x) m_7(x) m_{11}(x) m_{15}(x) \\
 &= x(x+1)(x^5+x^3+1)(x^5+x^3+x^2+x+1) \\
 &\quad (x^5+x^4+x^3+x^2+1)(x^5+x^4+x^3+x+1) \\
 &\quad (x^5+x^4+x^2+x+1)(x^5+x^2+1)
 \end{aligned}$$

The tables of the minimal polynomials of the elements in  $GF(2^n)$  for  $n = 6, 7, 8, 9$  and  $10$  are provided in Appendix C. Next we introduce the concept of reciprocal polynomials, which is frequently used in sequence analysis.

#### D. Reciprocal Polynomials

**Definition 3.19** Let  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ ,  $a_i \in GF(p^n)$  and  $a_0 \neq 0$ . The reciprocal polynomial of  $f(x)$  is defined as  $\frac{x^n}{a_0}f(x^{-1})$ , denoted by  $f^{-1}(x)$ , i.e.,  $f^{-1}(x) = \frac{x^n}{a_0}f(x^{-1})$ . In particular, if  $p = 2$ , then the reciprocal polynomial of  $f(x)$  is given by

$$f^{-1}(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + 1,$$

i.e.,  $f^{-1}(x)$  is obtained by reversing the order of the coefficients of  $f(x)$ .

From the definition, the following result is immediate.

**Property 3.8** For  $\alpha \in GF(p^n)$ , the minimal polynomials of  $\alpha$  and  $\alpha^{-1}$  are a pair of reciprocal polynomials.

**Example 3.12** From Example 3.11, we compute the pairs of reciprocal polynomials shown in Table 3.4.

Table 3.4: Pairs of reciprocal polynomials

$n$	$f(x)$	$f^{-1}(x)$
4	$m_1(x) = x^4 + x + 1$	$m_1^{-1}(x) = m_7(x) = x^4 + x^3 + 1$
	$m_3(x) = x^4 + x^3 + x^2 + x + 1$	$m_3^{-1}(x) = m_3(x) = x^4 + x^3 + x^2 + x + 1$
	$m_5(x) = x^2 + x + 1$	$m_5^{-1}(x) = m_5(x) = x^2 + x + 1$
5	$m_1(x) = x^5 + x^3 + 1$	$m_1^{-1}(x) = m_{15}(x) = x^5 + x^2 + 1$
	$m_3(x) = x^5 + x^3 + x^2 + x + 1$	$m_3^{-1}(x) = m_7(x) = x^5 + x^4 + x^3 + x^2 + 1$
	$m_5(x) = x^5 + x^4 + x^3 + x + 1$	$m_5^{-1}(x) = m_{11}(x) = x^5 + x^4 + x^2 + x + 1$

Notice that for  $n = 4$ , the reciprocal polynomial of  $x^4 + x^3 + x^2 + x + 1$  is itself.

### E. Periods of the Minimal Polynomials

For  $\alpha \in GF(p^n)$  with order  $r$ , from the definition of the order,  $r$  is the smallest integer satisfying  $\alpha^r = 1$ . Let  $m_\alpha(x)$  be the minimal polynomial of  $\alpha$ . Then

$$m_\alpha(x) \mid (x^r - 1) \quad (3.2)$$

and  $r$  is the smallest integer such that (3.2) is true. According to the definition of the period of polynomials,  $r$  is the period of  $m_\alpha(x)$ . Thus we have established the following assertion.

**Theorem 3.9** *For any  $0 \neq \alpha \in GF(p^n)$ , the period of the minimal polynomial of  $\alpha$  is equal to the order of  $\alpha$ , i.e.,*

$$\text{per}(m_\alpha) = \text{ord}(\alpha).$$

For example, for  $n = 4$ , from Table 3.2, the minimal polynomial of  $\alpha$  is  $x^4 + x + 1$  which has period 15, and the order of  $\alpha$  is 15 since it is a primitive element.

## 3.5 Trace Functions

### A. Subfields

We list the following result without proof.

**Fact 3.5** *Suppose that  $F$  is a finite extension field of  $GF(p)$  which contains all the zeros of  $x^{p^n} - x$ . Then these zeros form a finite field of order  $p^n$ .*

**Theorem 3.10** Let  $F$  be the finite field with  $q = p^n$  elements, where  $p$  is prime.

(a)  $F = GF(p^n)$  contains a subfield  $GF(p^m)$  if and only if  $m$  is a positive divisor of  $n$ .

(b) If  $\alpha \in GF(p^n)$  then  $\alpha \in GF(p^m)$  if and only if  $\alpha^{p^m} = \alpha$ .

In order to prove Theorem 3.10, we need the following lemma.

**Lemma 3.2** If  $a, s, t$  are integers with  $a \geq 2, s, t \geq 1$ , then

$$(a^s - 1) \mid (a^t - 1) \iff s \mid t.$$

(Recall that the vertical bar means “divides”.)

*Proof.* We write  $t = qs + r$ , where  $0 \leq r < s$ . Then

$$\frac{a^t - 1}{a^s - 1} = a^r \cdot \frac{a^{qs} - 1}{a^s - 1} + \frac{a^r - 1}{a^s - 1}.$$

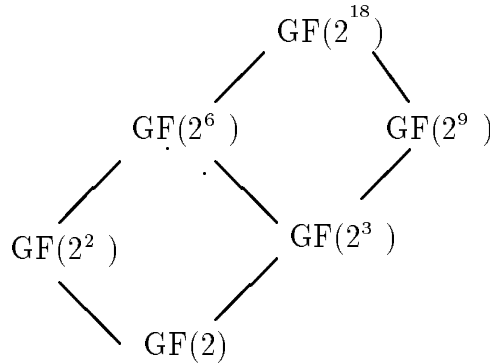
$a^{qs} - 1$  is always divisible by  $a^s - 1$  since  $a^{qs} - 1 = (a^s - 1)(a^{(q-1)s} + \dots + a^s + 1)$ . The last term is less than 1, and so it is an integer if and only if  $r = 0$ . □

*Proof of Theorem 3.10.* (a) If  $m \mid n$ , from Fact 3.5, then  $GF(p^n)$  contains a subfield  $GF(p^m)$ . Conversely, let  $\alpha$  be a primitive element of  $GF(p^m)$ . Then

$$\alpha^{p^m - 1} = 1 \text{ and } \alpha^{p^n - 1} = 1.$$

So  $(p^m - 1) \mid (p^n - 1) \implies m \mid n$  from Lemma 3.2. (b) is immediate from Corollary 3.2. □

**Example 3.13** The subfields of  $GF(2^{18})$  can be determined by listing all positive divisors of 18. The containment relations between these various subfields are displayed in the following diagram.



According to Theorem 3.10, the containment relations are equivalent to divisibility relations among the positive divisors of 18. Subfields are the basic tools for the constructions of (cascaded, generalized) GMW sequences.

*Note.* All results discussed in this chapter related to  $GF(p)$  or  $GF(p^n)$  are true when the prime  $p$  is replaced by a power of a prime, say  $q = p^h$ . From now on, we will discuss the properties of finite fields using the general notation  $GF(q)$ .

## B. Trace Functions

**Definition 3.20** Let  $q$  be a prime or a power of a prime. For  $\alpha \in F = GF(q^n)$  and  $K = GF(q)$ , the trace function  $Tr_{F/K}(x)$ ,  $x \in F$ , is defined by

$$Tr_{F/K}(x) = x + x^q + \cdots + x^{q^{n-1}}, x \in F.$$

If  $\alpha \in F$ ,  $Tr_{F/K}(\alpha)$  is called the trace of  $\alpha$  over  $K$ , simply denoted as  $Tr(\alpha)$  if the context is clear.

In the following, we simply write  $(Tr_{F/K}(x))^q = Tr_{F/K}(x)^q$ . Note that

$$Tr_{F/K}(x)^q = \sum_{i=0}^{n-1} x^{q^{i+1}} = Tr_{F/K}(x).$$

From Theorem 3.10-(b),  $Tr_{F/K}(x) \in K$ . Hence  $Tr_{F/K}(x)$  is a mapping from  $F$  to  $K$ . If  $q = 2$ , then  $Tr_{F/K}(x)$  is either 0 or 1, i.e.,

$$Tr_{F/K}(x) = x + x^2 + \cdots + x^{2^{n-1}} \in GF(2) \text{ for all } x \in GF(2^n).$$

**Example 3.14** Let  $GF(2^3)$  and  $GF(2^4)$  be defined by  $\alpha^3 + \alpha + 1 = 0$  and  $\alpha^4 + \alpha + 1 = 0$ , respectively (see Examples 3.5 and 3.6 for the tables of these finite fields). Here  $\alpha$  denotes a primitive elements in both fields, respectively. We compute the trace functions of the elements of  $GF(2^3)$  and  $GF(2^4)$  as follows.

$GF(2^3)$								
$x$	0	1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
$Tr(x)$	0	1	0	0	1	0	1	1

$GF(2^4)$																
$x$	0	1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$	$\alpha^7$	$\alpha^8$	$\alpha^9$	$\alpha^{10}$	$\alpha^{11}$	$\alpha^{12}$	$\alpha^{13}$	$\alpha^{14}$
$Tr(x)$	0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1

**Theorem 3.11** Let  $F = GF(q^n)$  and  $K = GF(q)$ . Then the trace function  $Tr_{F/K}$  satisfies the following properties:

- (a)  $Tr_{F/K}(x + y) = Tr_{F/K}(x) + Tr_{F/K}(y)$  for all  $x, y \in F$ .
- (b)  $Tr_{F/K}(cx) = cTr_{F/K}(x)$  for all  $c \in K, x \in F$ .

- (c)  $Tr_{F/K}$  is a linear transformation from  $F$  onto  $K$  (i.e., a linear functional), where both  $F$  and  $K$  are viewed as vector spaces over  $K$ .
- (d)  $Tr_{F/K}(c) = nc$  for all  $c \in K$ .
- (e)  $Tr_{F/K}(x^q) = Tr_{F/K}(x)$  for all  $x \in F$  and  $Tr_{F/K}(x^p) = Tr_{F/K}(x)^{p^i}$  for  $q = p^h$  and any positive integer  $i$ .
- (f)  $Tr_{F/K}(yx^q) = Tr_{F/K}(y^{q^{n-1}}x)$  for all  $x, y \in F$ .

*Proof.* (a) For  $x, y \in F$  we use Corollary 3.3 to get

$$\begin{aligned} Tr_{F/K}(x+y) &= (x+y) + (x+y)^q + \cdots + (x+y)^{q^{n-1}} \\ &= x+y + x^q + y^q + \cdots + x^{q^{n-1}} + y^{q^{n-1}} \\ &= Tr_{F/K}(x) + Tr_{F/K}(y). \end{aligned}$$

(b) For  $c \in K$  we have  $c^{q^j} = c$  for all  $j \geq 0$  by Theorem 3.10-(b). Therefore

$$\begin{aligned} Tr_{F/K}(cx) &= cx + c^q x^q + \cdots + c^{q^{n-1}} x^{q^{n-1}} \\ &= c Tr_{F/K}(x). \end{aligned}$$

(c) The properties (a) and (b), together with the fact that  $Tr_{F/K}(x) \in K$  for all  $x \in F$ , show that  $Tr_{F/K}(x)$  is a linear transformation from  $F$  into  $K$ . To prove that this mapping is onto, it suffices then to show existence of an  $\alpha \in F$  with  $Tr_{F/K}(\alpha) \neq 0$ . Now  $Tr_{F/K}(\alpha) = 0$  if and only if  $\alpha$  is a root of the polynomial  $x^{q^{n-1}} + \cdots + x^q + x$  in  $F$ . Since this polynomial can have at most  $q^{n-1}$  roots in  $F$  and  $F$  has  $q^n$  elements, the result follows.

(d) This follows immediately from the definitions of the trace function and Theorem 3.10-(b).

(e) For  $x \in F$  we have  $x^{q^n} = x$  by Corollary 3.2, and so  $Tr_{F/K}(x^q) = x^q + x^{q^2} + \cdots + x^{q^n} = Tr_{F/K}(x)$ . Thus, the first assertion is established. For the second assertion, we only write the proof for  $i = 1$ . (For  $i > 1$ , the proof is similar to that for  $i = 1$ .) Applying Lemma 1 in Section 3, we have

$$\begin{aligned} Tr_{F/K}(x^p) &= x^p + x^{qp} + \cdots + x^{q^{n-1}p} \\ &= Tr_{F/K}(x^p) = (x + x^q + \cdots + x^{q^{n-1}})^p \\ &= Tr_{F/K}(x)^p. \end{aligned}$$

(f) Again, using Corollary 3.2, and then the result (e), it follows that

$$Tr_{F/K}(yx^q) = Tr_{F/K}(y^{q^n}x^q) = Tr_{F/K}(y^{q^{n-1}}x)^q = Tr_{F/K}(y^{q^{n-1}}x).$$

□

**Theorem 3.12** (TRANSITIVITY OF TRACE) *Let  $K$  be a finite field,  $F$  a finite extension of  $K$ , and  $E$  a finite extension of  $F$ , i.e.,  $K \subset F \subset E$ . Then*

$$\text{Tr}_{E/K}(x) = \text{Tr}_{F/K}(\text{Tr}_{E/F}(x)) \text{ for all } x \in E.$$

*In other words, the trace function from  $E$  to  $K$  is a composition of the trace function from  $E$  to  $F$  and the trace function from  $F$  to  $K$ .*

*Proof.* We can suppose that  $K = GF(q)$ ,  $F = GF(q^n)$  and  $E = GF(q^{nm})$ . Then for  $x \in E$  we have

$$\begin{aligned} \text{Tr}_{F/K}(\text{Tr}_{E/F}(x)) &= \sum_{i=0}^{n-1} \text{Tr}_{E/F}(x)^{q^i} = \sum_{i=0}^{n-1} \left( \sum_{j=0}^{m-1} x^{q^{nj}} \right)^{q^i} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x^{q^{nj+i}} = \sum_{k=0}^{nm-1} x^{q^k} = \text{Tr}_{E/K}(x). \end{aligned}$$

□

### C. Norms

Another function from a finite field to one of its subfields is obtained by forming the product of the conjugates of an element of the field with respect to the subfield.

**Definition 3.21** *For  $\alpha \in F = GF(q^n)$  and  $K = GF(q)$ , the norm  $N_{F/K}(\alpha)$  of  $\alpha$  over  $K$  is defined by*

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \dots \cdot \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

Note that  $N_{F/K}(\alpha) \in K$ . Thus  $N_{F/K}(x)$  is a mapping from  $F$  to  $K$ .

### D. Dual Bases

**Definition 3.22** *Let  $K = GF(q)$  and  $F = GF(q^n)$ . Then two bases  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta_1, \dots, \beta_n\}$  of  $F$  over  $K$  are said to be dual (or complementary) bases if for  $1 \leq i, j \leq n$ :*

$$\text{Tr}_{F/K}(\alpha_i \beta_j) = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j. \end{cases}$$

**Theorem 3.13** *Let  $K = GF(q)$  and  $F = GF(q^n)$ , and let two bases  $\{\alpha_1, \dots, \alpha_n\}$  and  $\{\beta_1, \dots, \beta_n\}$  of  $F$  over  $K$  be dual bases. If*

$$x = x_1 \alpha_1 + x_2 \alpha_2 + \dots + x_n \alpha_n \in F, \text{ where } x_j \in K, \quad (3.3)$$

*then the coefficients  $x_j$  under the basis  $\{\alpha_i\}$  are given by*

$$x_j = \text{Tr}(\beta_j x), 1 \leq j \leq n.$$

*Proof.* Multiplying  $\beta_j$  times the two sides of the identity (3.3), and then applying the definition of the dual bases, the result follows.

**Example 3.15** Let  $GF(2^3) = \{\alpha^3 + \alpha + 1 = 0\}$ . Then  $\{1, \alpha, \alpha^2\}$  and  $\{1, \alpha^2, \alpha\}$  are a pair of the dual bases over  $GF(2)$ . For  $\alpha^6$ , we write

$$\alpha^6 = x_0 + x_1\alpha + x_2\alpha^2, x_i \in GF(2),$$

and then we compute the  $x_i$ 's by Theorem 3.13,

$$x_0 = Tr(1\alpha^6) = 1, x_1 = Tr(\alpha^2\alpha^6) = Tr(\alpha) = 0, x_2 = Tr(\alpha\alpha^6) = Tr(1) = 1.$$

Thus,  $\alpha^6 = 1 + \alpha^2$ , the same result as we obtained before.

### E. Minimal Polynomials over Intermediate Subfields

Usually, it is easier to write a program for finding primitive polynomials over  $GF(q)$  when  $q$  is a prime than in the case when  $q$  is a power of a prime. In the following theorem, we provide a method for computing primitive polynomials over  $GF(q^m)$  in terms of known primitive polynomials over  $GF(q)$ .

**Theorem 3.14** Let  $f(x)$  be a primitive polynomial over  $GF(q)$  of degree  $n$  and let  $\alpha$  be a root of  $f(x)$  in the extension field  $GF(q^n)$ . If  $m|n$  and  $1 \leq m < n$ , let  $Q = q^m$  and  $l = n/m$ . Then the minimal polynomial  $g(x)$  of  $\alpha$  over  $GF(q^m)$  has degree  $l$ , and is given by

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^Q) \cdots (x - \alpha^{Q^{l-1}}) \\ &= x^l + \sum_{j=0}^{l-1} c_j x^j, c_j \in GF(Q). \end{aligned} \quad (3.4)$$

Furthermore,  $f(x)$  can be factored into  $m$  primitive polynomials over  $\mathbb{F}_Q$  of degree  $l$  as follows:

$$f(x) = \prod_{i=0}^{m-1} \sigma_i(g(x)) \quad (3.5)$$

where  $\sigma_i$  is the Frobenius map which raises the coefficients of  $g(x)$  to the power  $q^i$  and keeps the primitivity of  $g(x)$ , i.e.,

$$\sigma_i(g(x)) = \sum_{j=0}^{l-1} c_j^{q^i} x^j,$$

which is primitive over  $GF(Q)$ .

*Proof.* Since  $\alpha$  is a primitive element in  $GF(q^n)$ , the minimal polynomial of  $\alpha$  over  $GF(Q)$  has degree  $l$ . Note that  $g(\alpha) = 0$ , i.e.,  $\alpha$  is a root of  $g(x)$ . Thus we only need to show that  $g(x)$  is a polynomial over  $GF(Q)$ , i.e., the coefficients of  $g(x)$  belong to  $GF(Q)$ . From the construction of  $g(x)$  in (3.5),

we know that  $c_j$  is a symmetric polynomial in  $\alpha^{Q^k}$ ,  $k = 0, 1, \dots, l-1$ . Thus  $c_j^Q = c_j \implies g(x) \in GF(Q)[x]$ . Thus,  $g(x)$  is the minimal polynomial of  $\alpha$  over  $GF(Q)$ . For the second assertion, it is easy to see that  $\sigma_i(g(x)) \in GF(Q)[x]$  since  $g(x) \in GF(Q)[x]$ . Note that  $\alpha^{q^i}$  is a root of  $\sigma_i(g(x))$ . Thus  $\sigma_i(g(x))$  is the minimal polynomial of  $\alpha^{q^i}$  over  $GF(Q)$ . Notice that  $\{\alpha^{q^i Q^j} = \alpha^{q^{i+mj}} \mid 0 \leq i < m; 0 \leq j < l\}$  constitutes all roots of  $f(x)$ . It follows that (3.5) is true.  $\square$

From Theorem 3.14, we have the following algorithm to compute primitive polynomials over  $GF(q^m)$  in terms of the primitive polynomials over  $GF(q)$ .

**Algorithm 3.2** AN ALGORITHM FOR FINDING PRIMITIVE POLYNOMIALS OVER  $GF(q^m)$

*Input:*  $f(x)$ , a primitive polynomial over  $GF(q)$  of degree  $n$ ;  $1 < m < n$ , a proper divisor of  $n$ .

*Output:* A primitive polynomial  $g(x)$  over  $GF(q^m)$  of degree  $l = n/m > 1$ .

procedure\_MP( $f, g$ ):

1. Generate  $GF(q^n)$  from  $f(x)$ , and set  $\alpha$  to be a root of  $f(x)$  in  $GF(q^n)$ .
2. Set  $\beta = \alpha^d$  where  $d = (q^n - 1)/(q^m - 1)$ . Then  $\beta$  is a primitive element in  $GF(q^m)$ . Compute the minimal polynomial of  $\beta$ , say  $h(x)$ ,

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

( $h(x)$  is a primitive polynomial over  $GF(q)$  of degree  $m$ .) We now use  $h(x)$  as a defining polynomial for  $GF(q^m)$ .

3. Compute  $g(x)$ , the minimal polynomial of  $\alpha$  over  $GF(q^m)$ :

$$g(x) = \prod_{i=0}^{l-1} (x - \alpha^{q^{mi}}), l = n/m.$$

$g(x)$  is a primitive polynomial over  $GF(q^m)$  of degree  $l$ .

4. Return  $g(x)$

**Example 3.16** Find a primitive polynomial over  $GF(2^3)$  of degree 2. We will apply Algorithm 3.2 to this question where the computation is done using the software package Maple.

1. Select  $f(x) = x^6 + x + 1$ , a primitive polynomial over  $GF(2)$  of degree 6, set  $\alpha$  a root of  $f(x)$  in  $GF(2^6)$  where  $GF(2^6)$  is defined by  $f(x)$ .
2. For  $m = 3$ , set  $d = (2^6 - 1)/(2^3 - 1) = 9$  and  $\beta = \alpha^9$ ; compute

$$h(x) = (x - \beta)(x - \beta^2)(x - \beta^4) = x^3 + x^2 + 1.$$

3. In  $GF(2^3)$ , defined by  $\beta^3 + \beta^2 + 1 = 0$ , compute

$$g(x) = (x - \alpha)(x - \alpha^8) = x^2 + (\alpha + \alpha^8)x + \alpha^9 = x^2 + \alpha^{2^7}x + \alpha^9 = x^2 + \beta^3x + \beta$$

which is a primitive polynomial over  $GF(2^3)$  of degree 2.

*Note.* This algorithm has important applications for implementation of GMW sequences and interleaved sequences. In Appendix B of this chapter, we compute a table consisting of primitive polynomials over  $GF(2^m)$  of degree  $l$  for  $lm < 32$  by Algorithm 3.2.

### 3.6 Powers of Trace Functions

In this section, we will describe how to compute a power of a trace function, and give a formula for the exponents in the expansion. This expansion has important applications for computing linear spans of GMW sequences, generalized GMW sequences, bent function sequences, and geometric sequences, *etc.*

Let  $p$  be a prime,  $q = p^r$ , and let  $f(x)$  be a function from  $GF(q^n)$  to  $GF(q)$ . By the Lagrange interpolation formula and  $x^{q^n} = x$  for  $x \in GF(q^n)$ , we can write  $f(x)$  in a polynomial form  $f(x) = \sum_{i=0}^{q^n-1} c_i x^i$ ,  $c_i \in GF(q)$  (we will discuss this representation in detail in Chapter 6). The *weight* of  $f(x)$ , denoted as  $w(f)$ , is defined as the number of nonzero coefficients of  $f(x)$ , i.e.,

$$w(f) = |\{i \mid c_i \neq 0, 0 \leq i < q^n\}|. \quad (3.6)$$

Any number in  $\mathbb{Z}_{p^t}$  can be written as a number in the  $p$ -ary number system. In other words, for  $x \in \mathbb{Z}_{p^t}$ , we can write it as  $x = \sum_{i=0}^{t-1} x_i p^i$ ,  $0 \leq x_i < p$ . The Hamming weight of  $x$ , as a  $p$ -ary number, is defined as the number of nonzero coefficients of  $x$  with respect to the base  $\{1, p, \dots, p^{t-1}\}$ , i.e.,  $w(x) = |\{i \mid x_i \neq 0, 0 \leq i < t\}|$ . For  $y \in \mathbb{Z}_{p^t}$ ,  $y = \sum_{i=0}^{t-1} y_i p^i$ ,  $0 \leq y_i < p$ , we have the following property on the uniqueness of the  $p$ -ary number system.

**Property 3.9** (UNIQUENESS OF  $p$ -ARY NUMBERS) *With the above notation,*

$$x = y \iff x_i = y_i, i = 0, 1, \dots, t-1.$$

For  $m|n$ , we have a field tower:

$$GF(q) \subset GF(q^m) \subset GF(q^n).$$

We simply denote by  $Tr_m^n(x)$  the trace function  $Tr_{GF(q^n)/GF(q^m)}(x) = x + x^Q + \dots + x^{Q^{l-1}}$  where  $n = ml$  and  $Q = q^m$ . The objective of this section is to obtain the prototype of exponents of  $x$  in the expansion of a power of the trace function, i.e., the exponents of  $x$  in the expansion of  $(Tr_m^n(x))^s$ , shortened as  $Tr_m^n(x)^s$ , where  $1 < s < q^m$ .

#### A. Binary case

We first investigate the simple case:  $q = 2$ .

**Theorem 3.15** (POWER OF TRACE: BINARY CASE) *With the above notation, for  $q = 2$  and  $1 < s < 2^m - 1$ , we write  $s = 2^{i_1} + \dots + 2^{i_k}$ , a binary number. Then*

(a)

$$\begin{aligned} \text{Tr}_m^n(x)^s &= (x + x^Q + \dots + x^{Q^{l-1}})^s && (\text{here } Q = 2^m) \\ &= \sum_{\mathbf{t} \in \mathbb{Z}_l^k} x^{\tau_s(\mathbf{t})}, \end{aligned} \quad (3.7)$$

where  $\mathbf{t} = (t_1, t_2, \dots, t_k)$ ,  $0 \leq t_j < l$ , or equivalently,  $\mathbf{t} \in \mathbb{Z}_l^k = \{(t_1, \dots, t_k) \mid t_k \in \mathbb{Z}_l\}$  and

$$\tau_s(\mathbf{t}) = 2^{i_1 + mt_1} + \dots + 2^{i_k + mt_k}. \quad (3.8)$$

(b)  $\tau_s(\mathbf{t}) < 2^n - 1$ , for all  $\mathbf{t} \in \mathbb{Z}_l^k$ .

(c)  $\tau_s(\mathbf{t})$  is a one-to-one map from  $\mathbb{Z}_l^k$  to  $\mathbb{Z}_{2^m-1}$ . In other words, we have

$$\tau_s(\mathbf{t}) \neq \tau_s(\mathbf{t}') \iff \mathbf{t} \neq \mathbf{t}' \in \mathbb{Z}_l^k.$$

(d)  $\tau_s(\mathbf{t}) \equiv s \pmod{2^m - 1}$  for all  $\mathbf{t} \in \mathbb{Z}_l^k$ .

(e)  $w(\text{Tr}_m^n(x)^s) = l^k$ .

*Proof.* (a) Expanding  $\text{Tr}_m^n(x)^s$ , then

$$\begin{aligned} \text{Tr}_m^n(x)^s &= (x + x^Q + \dots + x^{Q^{l-1}})^s \\ &= \prod_{j=1}^k (x^{2^{i_j}} + x^{2^{i_j}Q} + \dots + x^{2^{i_j}Q^{l-1}}). \end{aligned}$$

Since  $Q = 2^m$ , we have

$$\text{Tr}_m^n(x)^s = \prod_{j=1}^k (x^{2^{i_j}} + x^{2^{i_j+m}} + \dots + x^{2^{i_j+(l-1)m}}). \quad (3.9)$$

The exponent of  $x$  in the expansion of (3.9) is a sum of  $k$  elements where each is taken from a different row of the following matrix:

$$A = \begin{bmatrix} 1 & 2^m & 2^{2m} & \dots & 2^{(l-1)m} \\ 2 & 2^{1+m} & 2^{1+2m} & \dots & 2^{1+(l-1)m} \\ \vdots & & & & \\ 2^{m-1} & 2^{m-1+m} & 2^{m-1+2m} & \dots & 2^{m-1+(l-1)m} \end{bmatrix}_{m \times l}.$$

In other words, any exponent of  $x$  in the expansion (3.9) can be represented as

$$\begin{array}{ccccccc} \tau_s(\mathbf{t}) & = & 2^{i_1+mt_1} & + & 2^{i_2+mt_2} & + & \dots & + & 2^{i_k+mt_k} \\ & & \downarrow & & \downarrow & & \dots & & \downarrow \\ & & \text{taken from row } i_1 & & \text{from row } i_2 & & \dots & & \text{taken from row } i_k \end{array}$$

where  $t_1 \in \mathbb{Z}_l, \dots, t_k \in \mathbb{Z}_l$ , i.e.,  $\mathbf{t} = (t_1, \dots, t_k) \in \mathbb{Z}_l^k$ . Thus assertion 1 is established.

(b) Note that the numbers in matrix  $A$  are the base of binary numbers in  $\mathbb{Z}_{2^n-1}$ . Since  $s < 2^m - 1$ , then  $k < m$ . Thus the binary number  $\tau_s(\mathbf{t})$  has the Hamming weight  $k < m < n$ . So

$$\tau_s(\mathbf{t}) < 2^n - 1, \text{ for all } \mathbf{t} \in \mathbb{Z}_l^k.$$

(c) From Property 3.9, any integer in  $\mathbb{Z}_{2^n}$  has a unique binary representation. Together with assertion 2, it follows that

$$\tau_s(\mathbf{t}) \neq \tau_s(\mathbf{t}'), \text{ for all } \mathbf{t} \neq \mathbf{t}' \in \mathbb{Z}_l^k.$$

(d) Note that  $2^{jm} \equiv 1 \pmod{2^m - 1}$ . From (3.8), we have

$$\tau_s(\mathbf{t}) \equiv 2^{i_1} + \dots + 2^{i_k} \equiv s \pmod{2^m - 1}, \text{ for all } \mathbf{t} \in \mathbb{Z}_l^k.$$

(e) This is immediate from assertion 3 since there are  $l^k$  elements in  $\mathbb{Z}_l^k$ .  $\square$

**Corollary 3.4** *With the notation in Theorem 3.15, if  $s' \neq s$  with  $1 < s, s' < 2^m - 1$ , then*

$$\tau_s(\mathbf{t}) \neq \tau_{s'}(\mathbf{t}')$$

for every pair  $\mathbf{t}, \mathbf{t}' \in \mathbb{Z}_l^k$ .

*Proof.* If  $\tau_s(\mathbf{t}) = \tau_{s'}(\mathbf{t}')$  for some pair  $\mathbf{t}, \mathbf{t}' \in \mathbb{Z}_l^k$ , then they are equal modulo  $2^m - 1$ . In other words, we have

$$\tau_s(\mathbf{t}) \equiv \tau_{s'}(\mathbf{t}') \pmod{2^m - 1}.$$

From Theorem 3.15-(d),  $\tau_s(\mathbf{t}) \equiv s \pmod{2^m - 1}$  and  $\tau_{s'}(\mathbf{t}') \equiv s' \pmod{2^m - 1}$ . Consequently

$$s \equiv s' \pmod{2^m - 1},$$

which is a contradiction to  $s \neq s'$  with  $1 < s, s' < 2^m - 1$ .  $\square$

**Example 3.17** Let  $n = ml$ .

(a) For  $n = 6, m = 3$  and  $l = 2$ , we choose  $s = 3 = 1 + 2 \implies k = 2$  and  $(i_1, i_2) = (0, 1)$ . In this case, we have the following field tower:

$$GF(2) \subset GF(2^3) \subset GF(2^6)$$

and  $\mathbf{t} = (t_1, t_2) \in \mathbb{Z}_2^2$ . We will use the formula (3.7) to expand  $Tr_3^6(x)^3$ .

$\mathbf{t} = (t_1, t_2) \in \mathbb{Z}_2^2$	$\tau_3(t_1, t_2) = 2^{3t_1} + 2^{1+3t_2}$	$(\text{mod } 7)$
(0, 0)	$1 + 2 = 3$	3
(0, 1)	$1 + 2^4 = 17$	3
(1, 0)	$2^3 + 2 = 10$	3
(1, 1)	$2^3 + 2^4 = 24$	3

Then

$$Tr_3^6(x)^3 = x^3 + x^{17} + x^{10} + x^{24}.$$

(b) When  $n = 8, m = 4, l = 2, s = 7 = 1 + 2 + 2^2 \implies k = 3, (i_1, i_2, i_3) = (0, 1, 2)$  and  $(t_1, t_2, t_3) \in \mathbb{Z}_2^3$ , we have

$\mathbf{t} = (t_1, t_2, t_3) \in \mathbb{Z}_2^3$	$\tau_3(t_1, t_2, t_3) = 2^{4t_1} + 2^{1+4t_2} + 2^{2+4t_3}$	(mod 15)
(0, 0, 0)	$1 + 2 + 2^2 = 7$	7
(0, 0, 1)	$1 + 2 + 2^6 = 67$	7
(0, 1, 0)	$1 + 2^5 + 2^2 = 37$	7
(0, 1, 1)	$1 + 2^5 + 2^6 = 97$	7
(1, 0, 0)	$2^4 + 2 + 2^2 = 22$	7
(1, 0, 1)	$2^4 + 2 + 2^6 = 82$	7
(1, 1, 0)	$2^4 + 2^5 + 2^2 = 52$	7
(1, 1, 1)	$2^4 + 2^5 + 2^6 = 112$	7

Therefore,

$$Tr_4^8(x)^7 = x^7 + x^{67} + x^{37} + x^{97} + x^{22} + x^{82} + x^{52} + x^{112}.$$

(c) When  $n = 9, m = 3, l = 3, s = 3 = 1 + 2 \implies k = 2, (i_1, i_2) = (0, 1)$ , and  $(t_1, t_2) \in \mathbb{Z}_3^2$ , we have

$\mathbf{t} = (t_1, t_2) \in \mathbb{Z}_3^2$	$\tau_3(t_1, t_2) = 2^{3t_1} + 2^{1+3t_2}$	(mod 7)
(0, 0)	$1 + 2 = 3$	3
(0, 1)	$1 + 2^4 = 17$	3
(0, 2)	$1 + 2^7 = 129$	3
(1, 0)	$2^3 + 2 = 10$	3
(1, 1)	$2^3 + 2^4 = 24$	3
(1, 2)	$2^3 + 2^7 = 136$	3
(2, 0)	$2^6 + 2 = 66$	3
(2, 1)	$2^6 + 2^4 = 80$	3
(2, 2)	$2^6 + 2^7 = 192$	3

Thus, we get

$$Tr_3^9(x)^3 = x^3 + x^{17} + x^{129} + x^{10} + x^{24} + x^{136} + x^{66} + x^{80} + x^{192}.$$

**B. Non-binary Case**

We are now in a position to discuss a power of the trace function for the general case of  $q > 2$ . First we introduce the multinomial coefficients.

**Definition 3.23** Let  $x_i$  be indeterminates,  $i = 1, \dots, l$  and  $s > 0$ .

$$(x_1 + x_2 + \dots + x_l)^s = \sum_{i_1, \dots, i_l} \binom{s}{i_1, \dots, i_l} x_1^{i_1} \dots x_l^{i_l}$$

where the summation is taken over all nonnegative integer-valued vectors  $(i_1, \dots, i_l)$  such that  $i_1 + \dots + i_l = s$  and

$$\binom{s}{i_1 \dots i_l} = \frac{s!}{i_1! \dots i_l!},$$

which is called a multinomial coefficient and represents the number of possible divisions of  $s$  distinct objects into  $l$  distinct groups of respective sizes  $i_1, i_2, \dots, i_l$ . (By convention,  $0! = 1$ .)

Recall  $Q = q^m$  and  $q = p^r$ . Let  $0 < s < p$ . Applying the multinomial formula to  $\text{Tr}_m^n(x)^s$  with  $x_i = x^{Q^i}$ , we have

**Lemma 3.3**

$$\text{Tr}_m^n(x)^s = (x + x^Q + \dots + x^{Q^{l-1}})^s = \sum \binom{s}{i_1 \dots i_l} x^{i_1 + i_2 Q + \dots + i_l Q^{l-1}}$$

where the summation is taken over all nonnegative integer-valued vectors  $(i_1, \dots, i_l)$  such that  $i_1 + \dots + i_l = s$ . Furthermore, for such a vector,

$$\binom{s}{i_1 \dots i_l} \neq 0,$$

and the number of monomials in the expansion, or equivalently,  $w(\text{Tr}_m^n(x)^s)$ , is given by

$$w(\text{Tr}_m^n(x)^s) = \binom{l + s - 1}{l - 1}.$$

**Theorem 3.16** (POWER OF TRACE: NONBINARY CASE) Let  $s < q^m - 1$ , and  $s = \sum_{i=0}^{r^m-1} s_i p^i$ ,  $0 \leq s_i < p$ , a  $p$ -ary number.

(a)

$$\begin{aligned} \text{Tr}_m^n(x)^s &= (x + x^Q + \dots + x^{Q^{l-1}})^s \\ &= \sum_B d_B x^{\text{tr}(AB)} \end{aligned} \quad (3.10)$$

where the summation is taken over all matrices  $B$  defined as follows:

$$B = \begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,rm-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,rm-1} \\ \vdots & & & \\ b_{l-1,0} & b_{l-1,1} & \cdots & b_{l-1,rm-1} \end{bmatrix}_{l \times rm}$$

in which the  $j$ th column of  $B$  is a nonnegative integer-valued vector such that

$$b_{0,j} + b_{1,j} + \cdots + b_{l-1,j} = s_j, j = 0, 1, \dots, rm - 1, \quad (3.11)$$

the matrix  $A$  is given by

$$A = \begin{bmatrix} 1 & p^{rm} & \cdots & p^{rm(l-1)} \\ p & p^{1+rm} & \cdots & p^{1+rm(l-1)} \\ \vdots & & & \\ p^{rm-1} & p^{rm-1+rm} & \cdots & p^{rm-1+rm(l-1)} \end{bmatrix}_{rm \times l},$$

the notation  $\text{tr}(AB)$  denotes the trace of the  $rm \times rm$  matrix  $AB$ , i.e., if we write  $AB = (u_{ij})_{rm \times rm}$ , then

$$\text{tr}(AB) = \sum_{i=0}^{rm-1} u_{i,i},$$

and the coefficient  $d_B$  is given by

$$d_B = \prod_{j=0}^{rm-1} \binom{s_j}{b_{0,j}, b_{1,j}, \dots, b_{l-1,j}} \not\equiv 0 \pmod{p}. \quad (3.12)$$

(b) Let  $M(s)$  be the set of all such  $l \times rm$  matrices  $B$  with (3.11), i.e.,

$$M(s) = \{B = (b_{ij})_{l \times rm} \mid 0 \leq b_{ij} \in \mathbb{Z} \text{ with (3.11)}\}.$$

Then

(i)  $\text{tr}(AB) < q^n - 1$  for any  $B \in M(s)$ .

(ii)  $\text{tr}(AB) \neq \text{tr}(AC)$  if  $B \neq C \in M(s)$ .

(iii)  $\text{tr}(AB) \equiv s \pmod{q^m - 1}$  for every  $B \in M(s)$ .

(c) The number of the monomials in (3.10) is given by

$$w(\text{Tr}_m^n(x)^s) = |M(s)| = \prod_{i=0}^{rm-1} \binom{l + s_i - 1}{l - 1}.$$

*Proof.* (a) For  $s = \sum_{i=0}^{rm-1} s_i p^i$ ,  $0 \leq s_i < p$ , notice that  $Q = q^m = p^{rm}$ , and we have

$$\text{Tr}_m^n(x)^s = (x + x^Q + \cdots + x^{Q^{l-1}})^s = \prod_{i=0}^{rm-1} P_i \quad (3.13)$$

where

$$P_i = \left( x^{p^i} + x^{p^{i+rm}} + \cdots + x^{p^{i+rm(l-1)}} \right)^{s_i}.$$

According to Lemma 3.3, for a fixed  $i$ , an exponent of  $x$  in  $P_i$  is the inner product of the  $i$ th row  $A_i = (p^i, p^{i+rm}, \dots, p^{i+rm(l-1)})$  of  $A$  and the  $i$ th column  $B_i = (b_{0,i}, b_{1,i}, \dots, b_{l-1,i})^T$  of  $B$ , i.e.,

$$u_{i,i} = (A_i \cdot B_i) = b_{0,i} p^i + b_{1,i} p^{i+rm} + \cdots + b_{l-1,i} p^{i+rm(l-1)}, \quad (3.14)$$

where  $B_i$  is a nonnegative integer-valued solution of (3.11). Thus, every exponent of  $x$  in the expansion of (3.13) is the sum of  $u_{i,i}$ ,  $i = 0, 1, \dots, m-1$ , which is  $\text{tr}(AB)$ . From Lemma 3.3, each factor in  $d_B$  is not congruent to zero modulo  $p$ . Thus  $d_B \not\equiv 0 \pmod{p}$  for any  $B \in M(s)$ . Therefore the assertion 1 is true.

(b) Note that the entries in matrix  $A$  are the base of the  $p$ -ary number system in  $\mathbb{Z}_{q^n-1}$  and

$$0 \leq b_{i,j} \leq s_j < p \implies \text{tr}(AB) < q^n - 1 = p^{rm} - 1.$$

From the uniqueness of the  $p$ -ary number system,  $\text{tr}(AB) \neq \text{tr}(AC)$  if and only if  $B \neq C$ ,  $C \in M(s)$ . From (3.14), note that  $q^{mj} = p^{rmj} \equiv 1 \pmod{q^m - 1}$ , and then

$$u_{i,i} \equiv b_{0,i} p^i + b_{1,i} p^i + \cdots + b_{l-1,i} p^i \equiv p^i \sum_{j=0}^{l-1} b_{j,i} \equiv s_i p^i \pmod{q^m - 1}.$$

So, it follows that

$$\text{tr}(AB) \equiv \sum_{i=0}^{rm-1} s_i p^i \equiv s \pmod{q^m - 1}$$

which completes the proof of assertion 2.

(c) From assertion 1, we have  $d_B \not\equiv 0 \pmod{p}$  for any  $B \in M(s)$ . Since there are  $\binom{l + s_i - 1}{l - 1}$  ways to choose the  $i$ th column of  $B$ , there are

$$|M(s)| = \prod_{i=0}^{rm-1} \binom{l + s_i - 1}{l - 1}$$

ways to form  $B$  satisfying (3.11). Thus the number of monomials in (3.13) is given by this formula.  $\square$

**Corollary 3.5** *With the notation in Theorem 3.16, if  $s \neq t < q^m - 1$ , then*

$$\text{tr}(AB) \neq \text{tr}(AC)$$

where  $B \in M(s)$  and  $C \in M(t)$ .

*Proof.* From Theorem 3.16,

$$\text{tr}(AB) \equiv s \pmod{q^m - 1} \quad \text{and} \quad \text{tr}(AC) \equiv t \pmod{q^m - 1}.$$

If  $\text{tr}(AB) = \text{tr}(AC)$ , then  $\text{tr}(AB) \equiv \text{tr}(AC) \pmod{q^m - 1}$  which implies that  $s \equiv t \pmod{q^m - 1}$ .  $\square$

For Theorems 3.15 and 3.16, we considered the case  $1 < s < q^m - 1$ . In the following, we look at the case  $s = q^m - 1$ . Note that

$$q^m - 1 = \begin{cases} (p-1) + (p-1)p + \cdots + (p-1)p^{r^m-1}, & p > 2 \\ 1 + 2 + \cdots + 2^{r^m-1}, & p = 2. \end{cases}$$

For the case  $p = 2$ , we have

$$Tr_m^n(x)^{2^{r^m-1}} = \sum_{\mathbf{t} \in \mathbb{Z}_l^{r^m}} x^{\tau_s(\mathbf{t})}$$

and

$$w(Tr_m^n(x)^{2^{r^m-1}}) = |\{\tau_{2^{r^m-1}}(\mathbf{t}) \mid \mathbf{t} \in \mathbb{Z}_l^{r^m}\}| = l^{r^m}.$$

Since the Hamming weight of  $\tau_{2^{r^m-1}}(\mathbf{t})$  is equal to  $rm$ ,  $\tau_{2^{r^m-1}}(\mathbf{t}) \neq \tau_i(\mathbf{t}')$  for any  $i$  with  $1 \leq i < 2^{r^m} - 1$ . For the case of  $p > 2$ , we have

$$Tr_m^n(x)^{q^m-1} = Tr_m^n(x)^{p^{r^m-1}} = \sum_{B \in M(p^{r^m-1})} d_B x^{Tr(AB)}, \quad \text{and}$$

$$w(Tr_m^n(x)^{q^m-1}) = w(Tr_m^n(x)^{p^{r^m-1}}) = |M(p^{r^m} - 1)| = \binom{l+p-2}{l-1}^{r^m},$$

in which  $\text{tr}(AB) \neq \text{tr}(AC)$  for  $B \in M(p^{r^m} - 1)$  and  $C \in M(i)$  where  $1 < i < q^m - 1$ .

### C. Composition of Trace Functions and Arbitrary Functions

Let  $g(x)$  be a function from  $GF(q^m)$  to  $GF(q)$ . We can write

$$g(x) = \sum_{i=0}^{q^m-1} c_i x^i, \quad c_i \in GF(q^m).$$

From the above discussion, we have established the following theorem on expansion of the composition of  $g(x)$  and  $Tr_m^n(x)$ , denoted by  $g \circ Tr_m^n(x)$ , a function from  $GF(q^n)$  to  $GF(q)$ .

**Theorem 3.17** *Let*

$$f(x) = g \circ Tr_m^n(x).$$

For  $p = 2$  and  $q = 2^r$ ,

$$f(x) = \sum_{c_i \neq 0} c_i \sum_{\mathbf{t} \in \mathbb{Z}_l^{w(i)}} x^{\tau_{w(i)}(\mathbf{t})}$$

and

$$w(f) = \sum_{c_i \neq 0} l^{w(i)}. \quad (3.15)$$

For  $p > 2$ ,

$$f(x) = \sum_{c_i \neq 0} c_i \sum_{B \in M(i)} d_B x^{tr(AB)}$$

and the number of nonzero monomials in the expansion is given by

$$w(f) = \sum_{c_i \neq 0} |M(i)|. \quad (3.16)$$

These functions are illustrated in the following commutative diagram.

$$GF(p^n) \longrightarrow \boxed{Tr_m^n(x)} \xrightarrow{GF(p^m)} \boxed{g(x)} \longrightarrow GF(p)$$

Figure 3.1: Commutative diagram of  $f$  and  $g \circ Tr_m^n$

**Remark 3.1** The results shown in Theorems 3.15-3.17 have important applications for computation of linear spans of GMW sequences and many other sequences. In fact, this value is just the number of nonzero coefficients of  $f$  represented relative to the basis  $(1, x, \dots, x^{q^n-1})$ . In Chapter 6, we will show that  $f(x)$  corresponds to a sequence over  $GF(q)$ , and  $w(f)$  is equal to *the linear span* of the sequence.

**Remark 3.2** (MAXIMUM WEIGHT) Note that the function  $g$  has maximum weight when all coefficients  $c_i$ 's are nonzero. In this case,  $f$  has maximum weight which is derived as follows.

$$\begin{aligned} w(f) &= \sum_{s=1}^{q^m-1} |M(s)| + 1 \\ &= \sum_{s=1}^{q^m-1} \prod_{i=1}^{rm-1} \binom{l+s_i-1}{l-1} + 1 \quad \left( s = \sum_{i=0}^{rm-1} s_i p^i, 0 \leq s_i < p \right) \\ &= 1 + \sum_{i=1}^{p-1} \binom{rm}{1} \binom{l+i-1}{l-1} \end{aligned}$$

$$\begin{aligned}
& + \binom{rm}{2} \sum_{0 < i, j < p} \binom{l+i-1}{l-1} \binom{l+j-1}{l-1} + \cdots \\
& + \binom{rm}{t} \sum_{0 < i_1, \dots, i_t < p} \binom{l+i_1-1}{l-1} \cdots \binom{l+i_t-1}{l-1} \\
& + \cdots + \binom{rm}{rm} \binom{l+p-2}{l-1}^{rm}.
\end{aligned}$$

In particular, if  $p = 2$ , then the above formula becomes

$$w(f) = (l+1)^{rm}.$$

Therefore,  $f$  has maximum weight if and only if  $g$  has maximum weight.

**Example 3.18** Let  $n = 4$ ,  $m = l = 2$ ,  $q = p = 3$  and  $s = 5$ . Then  $s = 2+3 \implies s_0 = 2$  and  $s_1 = 1$ . Directly expanding  $Tr_2^4(x)^5$ , we have

$$\begin{aligned}
Tr_2^4(x)^5 &= (x + x^9)^5 \\
&= (x + x^9)^{2+3} \\
&= (x + x^9)^2(x^3 + x^{27}) \\
&= (x^2 + 2x^{10} + x^{18})(x^3 + x^{27}) \\
&= x^5 + x^{29} + 2x^{13} + 2x^{37} + x^{21} + x^{45}
\end{aligned}$$

Using Theorem 3.16,

$$Tr_2^4(x)^5 = \sum_{B \in \mathcal{M}(5)} d_B x^{tr(AB)}$$

where

$$A = \begin{bmatrix} 1 & 3^2 \\ 3 & 3^3 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix},$$

where  $(b_{0,0}, b_{1,0})$  is a nonnegative integer-valued solution of  $b_{0,0} + b_{1,0} = 2$  and  $(b_{0,1}, b_{1,1})$  is a nonnegative integer-valued solution of  $b_{0,1} + b_{1,1} = 1$ . Thus we have  $(b_{0,0}, b_{1,0}) \in \{(2, 0), (0, 2), (1, 1)\}$  and  $(b_{0,1}, b_{1,1}) \in \{(0, 1), (1, 0)\}$ . We list all the corresponding matrices  $B$  (here the brackets for matrices are omitted),

$d_B$  and  $tr(AB)$  values in the following table.

$B$	$d_B$	$tr(AB)$	(mod 8)
$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$	1	29	5
$\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$	1	5	5
$\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix}$	1	45	5
$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$	1	21	5
$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	2	13	5
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	2	37	5

Therefore, we have

$$Tr_2^4(x)^5 = x^{29} + x^5 + x^{45} + x^{21} + 2x^{13} + 2x^{37}.$$

For small values of  $n$ ,  $q$  and  $s$ , one may directly expand a power of a trace function, which seems simpler. However, for large  $n$ , the exponents in the expansion of a power of a trace function can be easily calculated by computer using the representation of the exponents in Theorems 3.15 and 3.16. These representations also provide insight into the properties of those exponents in certain algebraic forms.

*Note.* The formula (3.16) also includes the binary case in Theorem 3.15. For the binary case, each column of the matrix  $B$  has only one non-zero entry (which is one) and the other entries in the column are zero.

### 3.7 The Numbers of Irreducible Polynomials and Coset Leaders

In the section, we will give the formulae for determining the number of irreducible or primitive polynomials over  $\mathbb{F}_q$  of degree  $n$ . Let  $I_q(n)$  be the number of irreducible polynomials over  $\mathbb{F}_q$  of degree  $n$ . Then

$$I_q(n) = \frac{1}{n} \sum_{m|n} \mu(m) q^{n/m}$$

### 3.7. THE NUMBERS OF IRREDUCIBLE POLYNOMIALS AND COSET LEADERS 69

where  $\mu(x)$  is the Möbius function defined by

$$\mu(x) = \begin{cases} 1 & \text{if } x = 1 \\ (-1)^r & \text{if } x \text{ is the product of } r \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

This result can be found in many books, say [61]. As an example, we have

$$\begin{aligned} I_2(2) &= \frac{1}{2}(\mu(1)2^2 + \mu(2)2) = \frac{1}{2}(4 - 2) = 1 \\ I_2(3) &= \frac{1}{3}(\mu(1)2^3 + \mu(3)2) = \frac{1}{3}(8 - 2) = 2 \\ I_2(4) &= \frac{1}{4}(\mu(1)2^4 + \mu(2)2^2) = \frac{1}{4}(16 - 4) = 3 \\ I_2(5) &= \frac{1}{5}(\mu(1)2^5 + \mu(5)2) = \frac{1}{5}(32 - 2) = 6 \\ I_2(6) &= \frac{1}{6}(\mu(1)2^6 + \mu(2)2^3 + \mu(3)2^2 + \mu(6)2) \\ &= \frac{1}{6}(64 - 8 - 4 + 2) = 9. \end{aligned}$$

The number of primitive polynomials over  $\mathbb{F}_q$  of degree  $n$ ,  $P_q(n)$ , is given by

$$P_q(n) = \frac{\phi(q^n - 1)}{n}$$

where  $\phi(x)$  is the Euler phi function which denotes the number of integers in the range from 1 to  $x$  which are coprime to  $x$ . From Property 3.7,  $I_q(m)$  is equal to the number of the cosets modulo  $q^n - 1$  with respect to  $q$  which have size  $m$ . Therefore, we have

$$|\Gamma_q(n)| = \sum_{m|n} I_q(m).$$

In other words, the number of coset leaders modulo  $q^n - 1$  with respect to  $q$  is equal to the sum of the number of irreducible polynomials over  $GF(q)$  of degree  $m$  where  $m$  runs through all divisors of  $n$ . Thus, we have

$$\sum_{m|n} I_q(m) = q^n. \quad (3.17)$$

In the following table, we present the values of  $I_2(n)$ ,  $\Gamma_2(n)$ , and  $P_2(n)$  for  $1 \leq n \leq 30$ .

Values of  $I_2(n)$ ,  $\Gamma_2(n)$ , and  $P_2(n)$  for  $1 \leq n \leq 30$ 

$n$	$2^n - 1$	$I_2(n)$	$\Gamma_2(n)$	$P_2(n)$
1	1	1	1	1
2	3	1	2	1
3	7	2	3	2
4	15	3	5	2
5	31	6	7	6
6	63	9	13	6
7	127	18	19	18
8	255	30	35	16
9	511	56	59	48
10	1023	99	107	60
11	2047	186	187	176
12	4095	335	351	144
13	8191	630	631	630
14	16383	1161	1181	756
15	32767	2182	2191	1800
16	65535	4080	4115	2048
17	131,071	7710	7711	7710
18	262,143	14532	14601	7776
19	524,287	27594	27595	27594
20	1,048,575	52377	52487	24000
21	2,097,151	99858	99879	84672
22	4,194,303	190,557	190,745	120,032
23	8,388,607	364,722	364,723	356,960
24	16,777,215	698,870	699,251	276,480
25	33,554,431	1,342,176	1,342,183	1,296,000
26	67,108,863	2,580,795	2,581,427	1,719,900
27	134,217,727	4,971,008	4,971,067	4,202,496
28	268,435,455	9,586,395	9,587,579	4,741,632
29	536,870,911	18,512,790	18,512,791	18,407,808
30	1,073,741,823	35,790,267	35,792,567	17,820,000
31	2,147,483,647	69,273,666	69,273,667	69,273,666

**Remark 3.3** We provide some tables in Appendix B, which contain primitive polynomials over  $GF(2)$  of degree up to 32, primitive polynomials over  $GF(p)$  of degree  $n$  where  $2 < p \leq 127$  and  $p^n \leq 2^{32}$ , and primitive polynomials over  $GF(2^m)$  of degree  $l$  where  $m \in \{2, 3, \dots, 8\}$  and  $l \cdot m \leq 32$ .

**Note.**

For more detailed treatments about the relationships among irreducible polynomials, cyclotomic cosets and combinatorial necklaces, see [63]. For further references on finite fields, see [117] [128] [125].

## Appendix A. A Maple Program for Step 3 in Algorithm 3.1

**Comments:** In this Maple program, we set the parameters for computing the minimal polynomial of  $\alpha^3$  in  $GF(2^4)$  defined by the primitive polynomial  $f(x) = x^4 + x + 1$  where  $\alpha$  is a root of  $f(x)$ . So, for computing the minimal polynomials for different elements in different fields, one should reset the parameters.

```
writeto('output-file'):
n:=4;
p:=2;
q:=p^n-1;
alias(alpha=RootOf(z^4+z+1)):
C:=[3, 6, 12, 9]; #coset with coset leader 3 modulo 15
m:=1: # a variable that holding the minimal polynomial
for d in C do
    m:=Expand(m*(x+alpha^d)) mod p
od:
print(m);
quit;
```

## Appendix B. Primitive Polynomials

In Table 3.5, we list specific primitive polynomials over  $GF(2)$  of every degree up to 31. (These were taken from [130].) In the second column of Table 3.5, we represent a primitive polynomial  $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$  as a vector  $(c_0, c_1, \dots, c_{n-1})$ . For example, for  $n = 4$ , the primitive polynomial is  $f(x) = x^4 + x + 1$ . Table 3.6 contains primitive polynomials over  $GF(p)$  of degree  $n$  where  $p$  is a prime with  $2 < p \leq 127$  and  $p^n < 2^{32}$ . (These were computed by Amr Youssef.) The primitive polynomials over  $GF(2^m)$  of degree  $n$  where  $m \in \{2, 3, \dots, 8\}$  and  $n = ml \leq 32$  are listed in Table 3.7. (These were computed using Theorem 3.14.) The data listed in Table 3.7 were taken from the course projects of the graduate course: Sequence Design and Cryptography, Spring 2002, University of Waterloo. The notation used in Table 3.7 is as follows:

- $f(x)$  is a primitive polynomial over  $GF(2)$  of degree  $n$  and  $\alpha$  is a root of  $f(x)$  in the extension  $GF(2^n)$ .
- $n$  is a composite number and  $n = ml$  where both  $m$  and  $l$  are proper factors of  $n$ .
- $\beta = \alpha^d$  where  $d = \frac{2^n - 1}{2^m - 1}$  is a primitive element of  $GF(2^m)$  and  $h(x)$  is the minimal polynomial of  $\beta$  which is used as the defining polynomial of  $GF(2^m)$ .

- $g(x) = \prod_{i=0}^{l-1} (x - \alpha^{Q^i})$ , where  $Q = 2^m$  is the minimal polynomial of  $\alpha$  over  $GF(2^m)$  of degree  $l$ , which is primitive over  $GF(2^m)$  of degree  $l$ .

## Appendix C. Minimal Polynomials

Minimal polynomials have important applications in the implementation of many binary sequences with good correlation, such as 3-term sequences, 5-term sequences, most of the signal sets with low cross-correlation, and the boolean functions transformed from trace representations of sequences. For these applications, we need to compute the minimal polynomials of elements in finite fields. In this Appendix, we list the minimal polynomials of elements in  $\mathbb{F}_{2^n}$  for  $5 \leq n \leq 10$ . For example, for  $\alpha^i \in \mathbb{F}_{2^n}$ , the corresponding minimal polynomial of  $\alpha^i$  is equal to the polynomial

$$f_{\alpha^i}(x) = \prod_{j=0}^{s-1} (x + \alpha^{i2^j}) = c_0 + c_1x + \cdots + c_{s-1}x^{s-1} + x^s, \quad c_i \in \mathbb{F}_2$$

where  $s$  is the smallest number such that  $i2^s \equiv i \pmod{2^n - 1}$ . We represent this as a vector  $(c_0, c_1, \dots, c_{s-1}, c_s)$  where  $s|n$ . For example, for  $n = 6$  in Table 3.8, the minimal polynomial of  $\alpha^3$  is given as  $f_{\alpha^3}(x) = 1 + x + x^2 + x^4 + x^6 \leftrightarrow 1110101$ , and the minimal polynomial of  $\alpha^9$  is given as  $f_{\alpha^9}(x) = 1 + x^2 + x^3 \leftrightarrow 1011$ .

3.7. THE NUMBERS OF IRREDUCIBLE POLYNOMIALS AND COSET LEADERS 73

Table 3.5: Specific primitive polynomials over  $GF(2)$  of degree  $n$ :  $1 \leq n \leq 31$

$n$	$(c_0, c_1, \dots, c_{n-1})$
1	1
2	11
3	110
4	1100
5	10010
6	110000
7	1100000
8	10111000
9	100010000
10	1001000000
11	10100000000
12	110010100000
13	1101100000000
14	11010100000000
15	110000000000000
16	1011010000000000
17	10010000000000000
18	111001000000000000
19	1110010000000000000
20	10010000000000000000
21	101000000000000000000
22	1100000000000000000000
23	10000100000000000000000
24	110110000000000000000000
25	1001000000000000000000000
26	11100010000000000000000000
27	111001000000000000000000000
28	1001000000000000000000000000
29	10100000000000000000000000000
30	110010100000000000000000000000
31	10010000000000000000000000000000

Table 3.6: Primitive polynomials over  $GF(p)$  of degree  $n$  with  $2 < p$  (a prime)  $< 127$  and  $p^n < 2^{32}$ 

$p$	$f(x)$	$p$	$f(x)$	$p$	$f(x)$
3	$x^2 + x + 2$	13	$x^2 + x + 2$	47	$x^2 + x + 13$
3	$x^3 + 2x^2 + 1$	13	$x^3 + x^2 + 2$	47	$x^3 + x^2 + 2$
3	$x^4 + x^3 + 2$	13	$x^4 + x^3 + x^2 + 6$	47	$x^4 + x^3 + 5$
3	$x^5 + x^4 + x^2 + 1$	13	$x^5 + x^4 + x^3 + 6$	47	$x^5 + x^4 + 6$
3	$x^6 + x^5 + 2$	13	$x^6 + x^5 + x^3 + 6$	53	$x^2 + x + 5$
3	$x^7 + x^6 + x^4 + 1$	13	$x^7 + x^4 + 2$	53	$x^3 + x^2 + 2$
3	$x^8 + x^5 + 2$	13	$x^8 + x^7 + x^6 + 11$	53	$x^4 + x^3 + 2$
3	$x^9 + x^7 + x^5 + 1$	17	$x^2 + x + 3$	53	$x^5 + x^4 + 12$
3	$x^{10} + x^9 + x^7 + 2$	17	$x^3 + x^2 + 7$	59	$x^2 + x + 2$
3	$x^{11} + x^{10} + x^4 + 1$	17	$x^4 + x^3 + 5$	59	$x^3 + x^2 + 9$
3	$x^{12} + x^{11} + x^7 + 2$	17	$x^5 + x^4 + 5$	59	$x^4 + x^3 + 18$
3	$x^{13} + x^{12} + x^6 + 1$	17	$x^6 + x^5 + 3$	59	$x^5 + x^4 + 4$
3	$x^{14} + x^{13} + 2$	17	$x^7 + x^6 + 7$	61	$x^2 + x + 2$
3	$x^{15} + x^{14} + x^4 + 1$	19	$x^2 + x + 2$	61	$x^3 + x^2 + 6$
3	$x^{16} + x^9 + 2$	19	$x^3 + x^2 + 6$	61	$x^4 + x^3 + 17$
3	$x^{17} + x^{16} + x^8 + 1$	19	$x^4 + x^3 + 2$	61	$x^5 + x^4 + 55$
3	$x^{18} + x^{17} + x^5 + 2$	19	$x^5 + x^4 + 5$	67	$x^2 + x + 12$
5	$x^3 + x^2 + 2$	19	$x^6 + x^5 + 15$	67	$x^3 + x^2 + 6$
5	$x^4 + x^3 + x + 3$	19	$x^7 + x^6 + 5$	67	$x^4 + x^3 + 12$
5	$x^5 + x^2 + 2$	23	$x^2 + x + 7$	71	$x^2 + x + 11$
5	$x^6 + x^5 + 2$	23	$x^3 + x^2 + 6$	71	$x^3 + x^2 + 8$
5	$x^7 + x^6 + 2$	23	$x^4 + x^3 + 20$	71	$x^4 + x^3 + 13$
5	$x^8 + x^5 + x^3 + 3$	23	$x^5 + x^4 + 6$	73	$x^2 + x + 11$
5	$x^9 + x^7 + x^6 + 3$	23	$x^6 + x^5 + 7$	73	$x^3 + x^2 + 5$
5	$x^{10} + x^9 + x^7 + 3$	29	$x^2 + x + 3$	73	$x^4 + x^3 + 33$
5	$x^{11} + x^{10} + 2$	29	$x^3 + x^2 + 3$	79	$x^2 + x + 3$
5	$x^{12} + x^7 + x^4 + 3$	29	$x^4 + x^3 + 2$	79	$x^3 + x^2 + 2$
7	$x^2 + x + 3$	29	$x^5 + x^4 + 2$	79	$x^4 + x^3 + 7$
7	$x^3 + x^2 + x + 2$	29	$x^6 + x^5 + 11$	83	$x^2 + x + 2$
7	$x^4 + x^3 + x^2 + 3$	31	$x^2 + x + 12$	83	$x^3 + x^2 + 11$
7	$x^5 + x^4 + 4$	31	$x^3 + x^2 + 9$	83	$x^4 + x^3 + 24$
7	$x^6 + x^5 + x^4 + 3$	31	$x^4 + x^3 + 13$	89	$x^2 + x + 6$
7	$x^7 + x^5 + 4$	31	$x^5 + x^4 + 10$	89	$x^3 + x^2 + 6$
7	$x^8 + x^7 + 3$	31	$x^6 + x^5 + 12$	89	$x^4 + x^3 + 14$
7	$x^9 + x^8 + x^3 + 2$	37	$x^2 + x + 5$	97	$x^2 + x + 5$
7	$x^{10} + x^9 + x^8 + 3$	37	$x^3 + x^2 + 17$	97	$x^3 + x^2 + 5$
11	$x^2 + x + 7$	37	$x^4 + x^3 + 22$	97	$x^4 + x^3 + 15$
11	$x^3 + x^2 + 3$	37	$x^5 + x^4 + 2$		
11	$x^4 + x^3 + 8$	41	$x^2 + x + 12$		
11	$x^5 + x^4 + x^3 + 3$	41	$x^3 + x^2 + 11$		
11	$x^6 + x^5 + x + 7$	41	$x^4 + x^3 + 26$		
11	$x^7 + x^6 + 4$	41	$x^5 + x^4 + 11$		
11	$x^8 + x^7 + x^6 + 7$				
101	$x^2 + x + 3$	107	$x^2 + x + 5$	113	$x^2 + x + 10$
101	$x^3 + x^2 + 27$	107	$x^3 + x^2 + 10$	113	$x^3 + x^2 + 10$
101	$x^4 + x^3 + 11$	107	$x^4 + x^3 + 8$	113	$x^4 + x^3 + 6$
103	$x^2 + x + 5$	109	$x^2 + x + 6$	127	$x^2 + x + 3$
103	$x^3 + x^2 + 7$	109	$x^3 + x^2 + 6$	127	$x^3 + x^2 + 15$
103	$x^4 + x^3 + 44$	109	$x^4 + x^3 + 24$	127	$x^4 + x^3 + 3$

3.7. THE NUMBERS OF IRREDUCIBLE POLYNOMIALS AND COSET LEADERS 75

Table 3.7: Primitive polynomials over  $GF(2^m)$  of degree  $l$  with  $n = ml \leq 32$

$l$	$h(x)$	$g(x)$
$GF(2^2)$		
2	$x^2 + x + 1$	$x^2 + x + \beta$
3	$x^2 + x + 1$	$x^3 + x^2 + \beta^2 x + \beta$
4	$x^2 + x + 1$	$x^4 + x^3 + \beta x^2 + \beta x + \beta$
5	$x^2 + x + 1$	$x^5 + x^4 + \beta^2 x^3 + \beta x^2 + \beta$
6	$x^2 + x + 1$	$x^6 + x^2 + x + \beta$
7	$x^2 + x + 1$	$x^7 + x^6 + \beta x^5 + \beta^2 x^4 + \beta^2 x^2 + x + \beta$
8	$x^2 + x + 1$	$x^8 + x^7 + \beta^2 x^6 + \beta^2 x^5 + x^4 + x^3 + x^2 + \beta$
$GF(2^3)$		
2	$x^3 + x^2 + 1$	$x^2 + \beta^3 x + \beta$
3	$x^3 + x + 1$	$x^3 + \beta x^2 + \beta^5 x + \beta$
4	$x^3 + x + 1$	$x^4 + \beta x^3 + \beta^3 x^2 + x + \beta$
5	$x^3 + x + 1$	$x^5 + \beta^2 x^3 + \beta^2 x^2 + x + \beta$
6	$x^3 + x^2 + 1$	$x^6 + \beta^3 x^5 + x^4 + x^3 + \beta^3 x^2 + \beta^2 x + \beta$
7	$x^3 + x^2 + 1$	$x^7 + \beta^3 x^6 + \beta^2 x^5 + x^4 + \beta^3 x^3 + \beta^4 x + \beta$
8	$x^3 + x^2 + 1$	$x^8 + \beta^3 x^6 + \beta^3 x^5 + \beta x^4 + x^3 + \beta x^2 + \beta x + \beta$
$GF(2^4)$		
2	$x^4 + x + 1$	$x^2 + \beta^2 x + \beta$
3	$x^4 + x + 1$	$x^3 + \beta^{10} x^2 + \beta^{13} x + \beta$
4	$x^4 + x + 1$	$x^4 + \beta^4 x^3 + \beta x^2 + \beta^6 x + \beta$
5	$x^4 + x^3 + 1$	$x^5 + x^4 + \beta^5 x^3 + \beta^{14} x^2 + x + \beta$
6	$x^4 + x^3 + 1$	$x^6 + \beta^{10} x^5 + \beta^4 x^4 + \beta^{14} x^3 + \beta^{11} x^2 + \beta^9 x + \beta$
$GF(2^5)$		
2	$x^5 + x^4 + x^3 + x^2 + 1$	$x^2 + \beta^{23} x + \beta$
3	$x^5 + x^3 + x^2 + x + 1$	$x^3 + \beta^{20} x + \beta$
4	$x^5 + x^2 + 1$	$x^4 + \beta^2 x^3 + \beta x^2 + \beta^8 x + \beta$
5	$x^5 + x^3 + x^2 + x + 1$	$x^5 + \beta^8 x^4 + \beta^{30} x^3 + \beta^{21} x^2 + \beta^{19} x + \beta$
$GF(2^6)$		
2	$x^6 + x^5 + 1$	$x^2 + \beta^{30} x + \beta$
3	$x^6 + x^5 + x^4 + x + 1$	$x^3 + \beta^{56} x^2 + x + \beta$
4	$x^6 + x^5 + x^4 + x + 1$	$x^4 + \beta^{54} x^3 + \beta^{34} x^2 + \beta^{54} x + \beta$
$GF(2^7)$		
2	$x^7 + x^6 + 1$	$x^2 + \beta^{91} x + \beta$
3	$x^7 + x^5 + x^3 + x + 1$	$x^3 + \beta^{115} x^2 + \beta^{66} x + \beta$
4	$x^7 + x^6 + x^5 + x^2 + 1$	$x^4 + \beta^{66} x^3 + \beta^{92} x^2 + \beta^{113} x + \beta$
$GF(2^8)$		
2	$x^8 + x^4 + x^3 + x^2 + 1$	$x^2 + \beta^{50} x + \beta$
3	$x^8 + x^7 + x^3 + x^2 + 1$	$x^3 + \beta^{84} x^2 + \beta^{36} x + \beta$
4	$x^8 + x^6 + x^5 + x^2 + 1$	$x^4 + \beta^{37} x^3 + \beta^{49} x^2 + \beta^{18} x + \beta$

Table 3.8: Minimal polynomials of elements in  $\mathbb{F}_{2^5}$  and  $\mathbb{F}_{2^6}$ 

$n = 5$		$n = 6$	
coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$
1	100101	1	1100001
3	111101	3	1110101
5	110111	5	1110011
7	101111	7	1001001
11	111011	9	1011
15	101001	11	1011011
		13	1101101
		15	1010111
		21	111
		23	1100111
		27	1101
		31	1000011

Table 3.9: Minimal polynomials of elements in  $\mathbb{F}_{2^7}$ 

coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$
1	11000001	21	11010011
3	11010101	23	11100101
5	11110001	27	11101111
7	10111111	29	10001001
9	10011101	31	10101011
11	10010001	43	11001011
13	10100111	47	10001111
15	11111101	55	10111001
19	11110111	63	10000011

3.7. THE NUMBERS OF IRREDUCIBLE POLYNOMIALS AND COSET LEADERS 77

Table 3.10: Minimal polynomials of elements in  $\mathbb{F}_{2^8}$

coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$
1	101110001	23	110001101	53	111000011
3	111011101	25	110110001	55	100011011
5	110011111	27	111111001	59	101100101
7	100101101	29	101100011	61	111100111
9	101111011	31	101101001	63	101110111
11	111001111	37	111110101	85	111
13	110101001	39	100111111	87	110001011
15	111010111	43	110000111	91	101011111
17	11001	45	100111001	95	111110011
19	101001101	47	100101011	111	110111101
21	110100011	51	11111	119	10011
				127	100011101

Table 3.11: Minimal polynomials of elements in  $\mathbb{F}_{2^9}$

coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$
1	1000100001	41	1100111011	93	1001111101
3	1001101001	43	1101001111	95	1001110111
5	1000110011	45	1011111001	103	1111010101
7	1001100101	47	1101101011	107	1100010101
9	1100100011	51	1010101111	109	1111111011
11	1011010001	53	1010100101	111	1111100011
13	1110111001	55	1011110101	117	1111001011
15	1000011011	57	1010111101	119	1100000001
17	1101101101	59	1111001101	123	1110000101
19	1010000111	61	1111101001	125	1000101101
21	1110100001	63	1010011001	127	1001011001
23	1001011111	73	1101	171	1010110111
25	1100011111	75	1101111111	175	1000010111
27	1111000111	77	1001001011	183	1101110011
29	1101011011	79	1110001111	187	1001101111
31	1101100001	83	1010100011	191	1100110001
35	1000000011	85	1110110101	219	1011
37	1111011001	87	1010010101	223	1100010011
39	1011001111	91	1101001001	239	1011011011
				255	1000010001

Table 3.12: Minimal polynomials of elements in  $\mathbb{F}_{2^{10}}$ 

coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$	coset leader $i$	$f_{\alpha^i}$
1	1001000001	73	1001111111	175	11110110001
3	1111000001	75	11110101001	179	11010101101
5	10110000101	77	10101100001	181	10110010111
7	10011111111	79	11110110001	183	11011111101
9	11110101001	83	11010101101	187	11010111111
11	10101100001	85	10110010111	189	11011000001
13	11110110001	87	11011111101	191	11000100101
15	11010101101	89	11010111111	205	11011110111
17	10110010111	91	11011000001	207	10001100101
19	11011111101	93	11000100101	213	11000100011
21	11010111111	95	11011110111	215	11001000011
23	11011000001	101	10001100101	219	11000110111
25	11000100101	103	11000100011	221	11100010001
27	11011110111	105	11001000011	223	10100111101
29	10001100101	107	11000110111	235	10011000101
31	11000100011	109	11100010001	237	10001100011
35	11001000011	111	10100111101	239	11111110011
37	11000110111	115	10011000101	245	10101010111
39	11100010001	117	10001100011	247	11100110101
41	10100111101	119	11111110011	251	11110001101
43	10011000101	121	10101010111	253	11010100111
45	10001100011	123	11100110101	255	10001010011
47	11111110011	125	11110001101	343	10111000111
49	10101010111	127	11010100111	347	11001111111
51	11100110101	147	10001010011	351	10110101011
53	11110001101	149	10011100111	367	10000011101
55	11010100111	151	11001111111	375	11001011011
57	10001010011	155	10110101011	379	11100010111
59	10011100111	157	10000011101	383	11111000101
61	11001111111	159	11001011011	439	11010000101
63	10110101011	167	11100010111	447	11100111001
69	10000011101	171	11111000101	479	11001001111
71	11001011011	173	11010000101	511	11100011101
33	101111	99	111011	165	100101
231	110111	363	101001	495	111101
341	111				

### Exercises for Chapter 3

1. Give a proof for Corollary 3.3 in Section 3.2. In other words, prove that in any finite field of characteristic  $p$ ,

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}$$

for any  $m \geq 1$ .

2. Let  $GF(2^6)$  be defined by the primitive polynomial  $f(x) = x^6 + x + 1$  and let  $\alpha$  be a root of  $f(x)$ . Compute:  $\alpha^9 + \alpha^{23}$ ,  $\alpha^9 \cdot \alpha^{23}$ , and  $1 + \alpha^7$ .
3. Let  $p$  be a prime number. Prove that

$$x^{p^n} - x = \text{product of all monic polynomials,} \\ \text{irreducible over } GF(p), \text{ whose} \\ \text{degree divides } n.$$

4. The cyclotomic coset containing  $s$  consists of

$$C_s = \{s, sp, sp^2, \dots, sp^{n_s-1}\}$$

where  $n_s$  is the smallest positive integer such that  $p^{n_s}s \equiv s \pmod{p^n - 1}$ . Prove that  $n_s \mid n$ .

5. Let  $\alpha$  be a primitive element in  $GF(p^n)$ . Prove that  $m_s(x)$  defined in the Algorithm in Section 3.4 is a polynomial over  $GF(p)$ . In other words, if

$$m_s(x) = \prod_{i \in C_s} (x - \alpha^i)$$

where  $C_s$  is the cyclotomic coset modulo  $p^n - 1$  containing  $s$  as the coset leader, then the coefficients of  $m_s(x)$  belong to  $GF(p)$ .

6. Let  $GF(2^5)$  be defined by the primitive polynomial  $f(x) = x^5 + x^3 + 1$  and let  $\alpha$  be a root of  $f(x)$ .
- (1) Compute the cyclotomic cosets modulo 31 which contain 5 and 13, respectively.
  - (2) Compute the minimal polynomials of  $\alpha^5$  and  $\alpha^{13}$ .
  - (3) What are orders of  $\alpha^5$  and  $\alpha^{13}$ ? What are periods of these two polynomials?
  - (4) Are these two polynomials a pair of reciprocal polynomials?
7. Let  $GF(2^6)$  be defined by the primitive polynomial  $f(x) = x^6 + x + 1$  and let  $\alpha$  be a root of  $f(x)$ . Compute:  $Tr(1), Tr(\alpha), Tr(\alpha^2), Tr(\alpha^3), Tr(\alpha^4), Tr(\alpha^6)$ .

8. Let  $GF(2^3)$  be defined by the primitive polynomial  $g(x) = x^3 + x^2 + 1$  and  $\alpha$  is a root of  $g(x)$ . Let  $f(x) = x^2 + \alpha^3x + \alpha$ . Then  $f(x)$  is a primitive polynomial over  $GF(2^3)$  of degree 2. We can construct the finite field  $GF(2^6)$  in an alternative way: constructing  $GF(q^2)$  where  $q = 8$  by  $f(x)$ . Let  $\beta$  be a root of  $f(x)$ . Then  $GF(q^2)$  can be considered as a vector space over  $GF(q)$  of dimension 2.

- (1) Write the first six elements

$$1, \beta, \beta^2, \beta^3, \beta^4, \beta^5$$

in the vector representation forms under the basis  $\{1, \beta\}$ . For example,

$$\beta^2 = \alpha^3\beta + \alpha,$$

so the vector representation of  $\beta^2$  is  $(\alpha, \alpha^3)$ ; and

$$\begin{aligned} \beta^3 &= \beta \cdot \beta^2 = \beta(\alpha^3\beta + \alpha) \\ &= \alpha^3\beta^2 + \alpha\beta \\ &= \alpha^3(\alpha^3\beta + \alpha) + \alpha\beta \\ &= \alpha^6\beta + \alpha^4 + \alpha\beta = \alpha^2\beta + \alpha^4 \end{aligned}$$

so, the vector representation of  $\beta^3$  is  $(\alpha^2, \alpha^4)$ .

- (2) What is the minimal polynomial of  $\beta$  over  $GF(2)$ ?