Appendix B: Galois Fields GF(q)

This appendix is devoted to an introduction to finite fields, usually called Galois fields GF(q). A related algebraic structure called a group is first described. The aim of this appendix is to define polynomial operations over these algebraic structures. The main concept in terms of its utility for designing error-control codes is that a polynomial defined over a finite field GF(p_{prime}) has roots in that field, or in one of its extensions GF(q). In the same way, each element a of the extended finite field GF(q) is a root of some polynomials with coefficients in the finite field GF(p_{prime}). The polynomial of minimum degree that satisfies this condition is called a minimum polynomial of a.

B.1 Groups

A group G_{r} is defined as a set of elements that are related by some specific operations. For a given group G_{r} of elements, the binary operation $*$ is defined as an assignment rule for any two elements of this group, a and b. In this rule these two elements are assigned a unique element c of the same group, such that $c = a^*b$. This operation is said to be closed over the group G_{r} because its result is another element of the same group. This operation is said to be associative if it satisfies

$$a * (b * c) = (a * b) * c \tag{1}$$

B.1.1 Definition of a Group G_{r}

A set of elements G_{r} over which the binary operation $*$ is defined is said to be a group, if the following conditions are satisfied:

1. The binary operation $*$ is associative.
2. The set of elements G_{r} contains an element e, such that for every element of the set $a \in G_{\text{r}}$,

$$e * a = a * e = a \tag{2}$$

The element e is called the identity for the binary operation $*$.

Essentials of Error-Control Coding Jorge Castiñeira Moreira and Patrick Guy Farrell
 ISBN: 0-470-02920-X

3. For every element of the set $a \in G_r$, there is another element of the same set $a' \in G_r$, such that

$$a * a' = a' * a = e \tag{3}$$

The element a' is called the inverse element of a.

A group G_r is said to be commutative if, for every pair of its elements $a, b \in G_r$, it is true that

$$a * b = b * a \tag{4}$$

It can be shown that both the inverse element a' of an element a and the identity e of the binary operation defined over the group G_r are unique.

B.2 Addition and Multiplication Modulo *m*

For a set of elements $G_r = \{0, 1, 2, \ldots, i, j, \ldots, m-1\}$ that satisfies the conditions for being a group, the addition operation $\oplus$ between any two of its elements i and j is defined as

$$\begin{aligned} i \oplus j &= r \\ r &= (i + j) \text{mod}(m) \end{aligned} \tag{5}$$

that is, the addition of any two elements of the group i and j is the remainder of the division of the arithmetic addition $(i + j)$ by m. This operation is called modulo-m addition.

Modulo-2 addition, for instance, is defined over the group $G_r = \{0, 1\}$:

$$0 \oplus 0 = 0,$$
$$1 \oplus 1 = 0,$$
$$0 \oplus 1 = 1,$$
$$1 \oplus 0 = 1,$$

As an example, the last result comes from the calculation of $1 + 0 = 1$, and $1/2 = 0$ with remainder 1, then $1 \oplus 0 = 1$. A group constituted of p_{prime} elements $G_r = \{1, 2, 3, \ldots, p_{\text{prime}} - 1\}$, where p_{prime} is a prime number. $p_{\text{prime}} : 2, 3, 5, 7, 11, \ldots$ is a commutative group under modulo-p_{prime} addition.

Multiplication modulo-p_{prime} between any two elements i and j is defined as

$$\begin{aligned} i \otimes j &= r \\ r &= ij \bmod p_{\text{prime}} \end{aligned} \tag{6}$$

For the binary group $G_r = \{0, 1\}$, this operation is determined by the following table:

$$0 \otimes 0 = 0$$
$$1 \otimes 1 = 1$$
$$0 \otimes 1 = 0$$
$$1 \otimes 0 = 0$$

Table B.1 Modulo-2 addition

$\oplus$	0	1
0	0	1
1	1	0

As an example, the last result of the above table comes from the calculation of $1 \times 0 = 0$, and $0/2 = 0$ with remainder 0, then $1 \otimes 0 = 0$.

B.3 Fields

The definition of groups is useful for introducing the definition of what is called a finite field. A field is a set of elements F for which addition, multiplication, subtraction and division performed with its elements result in another element of the same set. Once again, the definition of a field is based on the operations described over such a field. For addition and multiplication operations, the following conditions define a field:

1. F is a commutative group with respect to the addition operation. The identity element for the addition is called '0'.
2. F is a commutative group for the multiplication operation. The identity element for multiplication is called '1'.
3. Multiplication is distributive with respect to addition:

$$a(b + c) = ab + ac \tag{7}$$

The number of elements of a field is called the order of that field. A field with a finite number of elements is usually called a finite field, or Galois field GF.

The inverse for the addition operation of an element of the field $a \in F$ is denoted as $-a$, and inverse for the multiplication operation of an element of the field is denoted as a^{-1}. Subtraction and division operations are defined as a function of the inverse elements as

$$\begin{aligned} a - b &= a + (-b) \\ a/b &= a(b^{-1}) \end{aligned} \tag{8}$$

The set $G_r = \{0, 1\}$ defined under addition and multiplication modulo 2 is such that $G_r = \{0, 1\}$ is a commutative group with respect to the addition operation, and is also a commutative group with respect to the multiplication operation. This is the so-called binary field GF(2).

Operations in this binary field are defined by Tables B.1 and B.2.

Table B.2 Modulo-2 multiplication

$\bullet$	0	1
0	0	0
1	0	1

For a given prime number p_{prime}, the set of integer numbers $\{0, 1, 2, 3, \ldots, p_{\text{prime}} - 1\}$ is a commutative group with respect to modulo-p_{prime} addition. The set of integer numbers $\{1, 2, 3, \ldots, p_{\text{prime}} - 1\}$ is a commutative group with respect to multiplication modulo p_{prime}. This set is therefore a field of order p_{prime}. They are also called prime fields GF (p_{prime}).

An extension of a prime field GF(p_{prime}) is called an extended finite field GF(q) = GF(p_{prime}^m), with m a positive integer number. This extended field is also a Galois field. Particular cases of practical interest are the finite fields of the form GF(2^m), with m a positive integer number.

For a given finite field GF(q), and for an element of this field $a \in$ GF(q), the powers of this element are also elements of the finite field, since the multiplication operation is a closed operation. Therefore,

$$a^1 = a, \qquad a^2 = a \bullet a, \qquad a^3 = a \bullet a \bullet a \ldots$$

are also elements of the same finite field GF(q). However, these powers will start to repeat because the field is a finite field, and its order is a finite number.

In other words, there should exist two integer numbers k and m, such that $m > k$ and $a^m = a^k$. Since a^{-k} is the multiplicative inverse of a^k, $a^{-k}a^m = a^{-k}a^k$, or $a^{m-k} = 1$. There is therefore a number n such that $a^n = 1$, and this number is called the order of the element a. Thus, powers $a^1, a^2, a^3, \ldots, a^{n-1}$ are all different and form a group under multiplication in GF(q).

It can be shown that if a is a non-zero element of the finite field GF(q), then $a^{q-1} = 1$. It is also true that if a is a non-zero element of the finite field GF(q), and if n is the order of that element, then n divides $q - 1$.

A non-zero element a of a finite field GF(q) is said to be a primitive element of that field if the order of that element is $q - 1$. All the powers of a primitive element $a \in$ GF(q) of a field generate all the non-zero elements of that field GF(q). Every finite field has at least one primitive element.

B.4 Polynomials over Binary Fields

The most commonly used fields are extensions of the binary field GF(2), and they are called Galois fields GF(2^m). Binary arithmetic uses addition and multiplication modulo 2. A polynomial $f(X)$ defined over GF(2) is of the form

$$f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n \tag{9}$$

where the coefficients f_i are either 0 or 1. The highest exponent of the variable X is called the degree of the polynomial. There are 2^n polynomials of degree n. Some of them are

$$\begin{aligned} n &= 1 \qquad X, X + 1 \\ n &= 2 \qquad X^2, 1 + X^2, X + X^2, 1 + X + X^2 \end{aligned}$$

Polynomial addition and multiplication are done using operations modulo 2, and satisfy the commutative, associative and distributive laws. An important operation is the division of two polynomials. As an example, the division of polynomial $X^3 + X + 1$ by the polynomial $X + 1$

is done as follows:

$$
\begin{array}{rl|l}
X^3 & +X+1 & X+1 \\
\multicolumn{3}{r}{---------} \\
X^3+X^2 & & X^2+X \\
\multicolumn{3}{r}{---------} \\
\multicolumn{2}{r}{X^2+X+1} & \\
\multicolumn{2}{r}{X^2+X} & \\
\multicolumn{2}{r}{-----} & \\
\multicolumn{2}{r}{r(X)=1} &
\end{array}
$$

The division is of the form

$$f(X) = q(X)g(X) + r(X) \tag{10}$$

where, in this example,

$$r(X) = 1$$
$$q(X) = X + X^2$$

Definition B.1: An element of the field a is a zero or root of a polynomial $f(X)$ if $f(a) = 0$. In this case a is said to be a root of $f(X)$ and it also happens that $X - a$ is factor of this polynomial $f(X)$.

Thus, for example, $a = 1$ is a root of the polynomial $f(X) = 1 + X^2 + X^3 + X^4$, and so $X + 1$ is a factor of this polynomial $f(X)$. The division of $f(X)$ by $X + 1$ has the quotient polynomial $q(X) = 1 + X + X^3$. Remember that the additive inverse of a, $-a$, is equal to a, $a = -a$, for modulo-2 operations.

Definition B.2: A polynomial $p(X)$ defined over GF(2), of degree m, is said to be irreducible, if $p(X)$ has no factor polynomials of degree higher than zero and lower than m.

For example, the polynomial $1 + X + X^2$ is an irreducible polynomial, since neither X nor $X + 1$ are its factors. A polynomial of degree 2 is irreducible if it has no factor polynomials of degree 1. A property of irreducible polynomials over the binary field GF(2), of degree m, is that they are factors of the polynomial $X^{2^m-1} + 1$. For example, the polynomial $1 + X + X^3$ is a factor of $X^{2^3-1} + 1 = X^7 + 1$.

Furthermore, an irreducible polynomial $p_i(X)$ of degree m is a primitive polynomial if the smallest integer number n, for which $p_i(X)$ is a factor of $X^n + 1$, is $n = 2^m - 1$. For example, the polynomial $X^4 + X + 1$ is a factor of $X^{2^4-1}+1 = X^{15}+1$, and it is not a factor of any other polynomial of the form $X^n + 1$, where $1 \leq n < 15$. This means that the polynomial $X^4 + X + 1$ is a primitive polynomial.

Another interesting property of polynomials over GF(2) is that

$$(f(X))^{2^l} = f(X^{2^l}) \tag{11}$$

B.5 Construction of a Galois Field GF(2^m)

An extended Galois field contains not only the binary elements '0' and '1' but also the element α and its powers. For this new element,

$$\begin{aligned} 0\alpha &= \alpha 0 = 0 \\ 1\alpha &= \alpha 1 = \alpha \\ \alpha^2 &= \alpha\alpha, \qquad \alpha^3 = \alpha\alpha^2 \\ \alpha^i\alpha^j &= \alpha^{i+j} = \alpha^j\alpha^i \end{aligned}$$

A set of these elements is

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^k, \ldots\} \tag{12}$$

which contains 2^m elements. Since a primitive polynomial $p_i(X)$, over GF(2) of degree m, is a factor of $X^{2^m-1}+1$, and taking into account that $p_i(\alpha) = 0$,

$$\begin{aligned} X^{2^m-1} + 1 &= p(X)q(X) \\ \alpha^{2^m-1} + 1 &= p(\alpha)q(\alpha) = 0 \\ \alpha^{2^m-1} &= 1 \end{aligned} \tag{13}$$

Therefore the set F is a finite set of 2^m elements:

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\} \tag{14}$$

The condition

$$i + j < 2^m - 1 \tag{15}$$

should be satisfied to make the set be closed with respect to the multiplication operation. This means that if any two elements of the set α^i and α^j are multiplied, the result $\alpha^k = \alpha^i\alpha^j$ should be an element of the same set; that is, $k < 2^m - 1$.

If

$$i + j = (2^m - 1) + r, \quad 0 \le r < 2^m - 1 \tag{16}$$

then

$$\alpha^i\alpha^j = \alpha^{(i+j)} = \alpha^{(2^m-1)+r} = \alpha^r$$

and this result shows that the set is closed with respect to the multiplication operation. On the other hand, for a given integer number i, such that $0 < i < 2^m - 1$,

$$\alpha^{2^m-1-i} \text{ is the multiplicative inverse of } \alpha^i \tag{17}$$

Thus, the set $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$ is a group of order $2^m - 1$ with respect to the multiplication operation. To ensure that the set F is a commutative group under addition, the

operation of addition in the set must be defined. For $0 \leq i < 2^m - 1$, X^i is divided by $p(X)$, resulting in

$$X^i = q_i(X)p(X) + a_i(X) \tag{18}$$

$a_i(X)$ is of degree $m-1$ or less, and $a(X) = a_{i0} + a_{i1}X + a_{i2}X^2 + \cdots + a_{i,m-1}X^{m-1}$. For $0 \leq i,\ j < 2^m - 1$,

$$a_i(X) \neq a_j(X) \tag{19}$$

If $i = 0, 1, 2, \ldots, 2^m - 2$, there are $2^m - 1$ different polynomials $a_i(X)$:

$$\begin{aligned} \alpha^i &= q_i(\alpha)p(\alpha) + a_i(\alpha) = a_i(\alpha) \\ \alpha^i &= a_{i0} + a_{i1}X + a_{i2}X^2 + \cdots + a_{i,m-1}X^{m-1} \end{aligned} \tag{20}$$

These polynomials represent $2^m - 1$ non-zero elements $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{2^m-2}$.

There are $2^m - 1$ different polynomials in α over GF(2) which represent the $2^m - 1$ different non-zero elements of the set F. This leads to a binary representation for each element of the set.

The addition operation is defined as

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus \alpha^i &= \alpha^i \oplus 0 = \alpha^i \end{aligned}$$

and

$$\alpha^i \oplus \alpha^j = (a_{i0} \oplus a_{j0}) + (a_{i1} \oplus a_{j1})X + (a_{i2} \oplus a_{j2})X^2 + \cdots + (a_{i,m-1} \oplus a_{j,m-1})X^{m-1} \tag{21}$$

where addition element by element is done modulo 2. This is the same as saying that the addition of any two elements of the set $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$ is the exclusive-OR bitwise operation between the binary representation of those two elements, which are equivalent to the corresponding polynomial expressions in α.

This set F of elements defined as above is commutative with respect to the addition operation, and the set of non-zero elements of F is commutative with respect to the multiplication operation. Therefore the set

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$$

is a Galois field or finite field of 2^m elements, GF(2^m).

Example B.1: Let $m = 3$, and $p_i(X) = 1 + X + X^3$ a primitive polynomial over GF(2). Since $p_i(\alpha) = 1 + \alpha + \alpha^3 = 0$, then $\alpha^3 = 1 + \alpha$. The field GF(2^3) can be constructed, making use of the above expression, in order to determine all the non-zero elements of that field. Thus, for example, $\alpha^4 = \alpha\alpha^3 = \alpha(1 + \alpha) = \alpha + \alpha^2$.

Table B.3 shows all the elements of the Galois field GF(2^3) generated by $p_i(X) = 1 + X + X^3$. Examples of the product and sum of two elements in this field are calculated as follows:

$$\begin{aligned} \alpha^4\alpha^6 &= \alpha^{10} = \alpha^{10-7} = \alpha^3 \\ \alpha^2 + \alpha^4 &= \alpha^2 + \alpha + \alpha^2 = \alpha \end{aligned}$$

Table B.3 The Galois field GF(2^3) generated by $p_i(X) = 1 + X + X^3$

Exp. representation	Polynomial representation	Vector representation
0	0	0 0 0
1	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1 + \alpha$	1 1 0
α^4	$\alpha + \alpha^2$	0 1 1
α^5	$1 + \alpha + \alpha^2$	1 1 1
α^6	$1 + \alpha^2$	1 0 1

The most commonly used way of determining the sum of two elements of a Galois field is by doing the bitwise exclusive-OR operation over the binary representations of these two elements.

Example B.2: Determine the table of the elements of the Galois field GF(2^4) generated by the primitive polynomial $p_i(X) = 1 + X + X^4$.

According to the expression for the primitive polynomial, $p_i(\alpha) = 1 + \alpha + \alpha^4 = 0$, or $\alpha^4 = 1 + \alpha$. The generated field GF(2^4) is shown in Table B.4.

B.6 Properties of Extended Galois Fields GF(2^m)

Polynomials defined over the binary field GF(2) can have roots that belong to an extended field GF(2^m). This is the same as what happens in the case of polynomials defined over the

Table B.4 The Galois field GF(2^4) generated by $p_i(X) = 1 + X + X^4$

Exp. representation	Polynomial representation	Vector representation
0	0	0 0 0 0
1	1	1 0 0 0
α	α	0 1 0 0
α^2	α^2	0 0 1 0
α^3	α^3	0 0 0 1
α^4	$1 + \alpha$	1 1 0 0
α^5	$\alpha + \alpha^2$	0 1 1 0
α^6	$\alpha^2 + \alpha^3$	0 0 1 1
α^7	$1 + \alpha + \alpha^3$	1 1 0 1
α^8	$1 + \alpha^2$	1 0 1 0
α^9	$\alpha + \alpha^3$	0 1 0 1
α^{10}	$1 + \alpha + \alpha^2$	1 1 1 0
α^{11}	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1
α^{13}	$1 + \alpha^2 + \alpha^3$	1 0 1 1
α^{14}	$1 + \alpha^3$	1 0 0 1

set of real numbers, which can have roots outside that set; that is, roots that are complex numbers.

As an example, the polynomial $p_i(X) = 1 + X^3 + X^4$ is irreducible over GF(2) since it has no roots in that field, but it has, however, its four roots in the extended Galois field GF(2^4). By simply replacing the variable X in the expression for the polynomial with the elements as given in Table B.4 of the Galois field GF(2^4), it can be verified that α^7, α^{11}, α^{13} and α^{14} are indeed the roots of that polynomial. As a consequence of this,

$$\begin{aligned} p_i(X) &= 1 + X^3 + X^4 \\ &= (X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\ &= [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}] \\ &= [X^2 + (\alpha^8)X + \alpha^3][X^2 + (\alpha^2)X + \alpha^{12}] \\ &= X^4 + (\alpha^8 + \alpha^2)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)X + \alpha^{15} \\ &= X^4 + X^3 + 1 \end{aligned}$$

The following theorem determines a condition to be satisfied by the roots of a polynomial taken from an extended field. This theorem allows determination of all the roots of a given polynomial as a function of one of these roots β.

Theorem B.1: Let $f(X)$ be a polynomial defined over GF(2). If an element β of the extended Galois field GF(2^m) is a root of the polynomial $f(X)$, then for any positive integer $l \geq 0$, β^{2^l} is also a root of that polynomial.

Demonstration of this theorem is based on equation (11), and is done by simply replacing the variable X in the polynomial expression of $f(X)$ with the corresponding root

$$(f(\beta))^{2^l} = (0)^{2^l} = f(\beta^{2^l}) = 0$$

The element β^{2^l} is called the conjugate of β.

This theorem states that if β is an element of the extended field GF(2^m) and also a root of the polynomial $f(X)$, its conjugates are also elements of the same field and roots of the same polynomial.

Example B.3: The polynomial $p_i(X) = 1 + X^3 + X^4$ defined over GF(2) has α^7 as one of its roots. This means that, by applying Theorem B.1, $(\alpha^7)^2 = \alpha^{14}$, $(\alpha^7)^4 = \alpha^{28} = \alpha^{13}$ and $(\alpha^7)^8 = \alpha^{56} = \alpha^{11}$ are also roots of that polynomial. This is the whole set of roots since the next operation $(\alpha^7)^{16} = \alpha^{112} = \alpha^7$ repeats the value of the original root.

In this example it is also verified that the root $\beta = \alpha^7$ satisfies the condition $\beta^{2^m-1} = \beta^{15} = (\alpha^7)^{15} = \alpha^{105} = \alpha^0 = 1$. In general, it is verified that $\beta^{2^m-1} = 1$, because for an element $a \in GF(q)$, it is true that $a^{q-1} = 1$. Equivalently,

$$\beta^{2^m-1} + 1 = 0$$

that is, β is a root of the polynomial $X^{2^m-1} + 1$. In general, every non-zero element of the Galois field GF(2^m) is a root of the polynomial $X^{2^m-1} + 1$. Since the degree of the polynomial

$X^{2^m-1}+1$ is 2^m-1, the 2^m-1 non-zero elements of GF(2^m) are all roots of $X^{2^m-1}+1$. Since the zero element 0 of the field GF(2^m) is the root of the polynomial X, it is possible to say that the elements of the field GF(2^m) are all the roots of the polynomial $X^{2^m}+X$.

B.7 Minimal Polynomials

Since every element β of the Galois field GF(2^m) is a root of the polynomial $X^{2^m}+X$, the same element could be a root of a polynomial defined over GF(2) whose degree is less than 2^m.

Definition B.3: The minimum-degree polynomial $\phi(X)$, defined over GF(2) that has β as its root, is called the minimal polynomial of β. This is the same as to say that $\phi(\beta)=0$.

Thus, the minimal polynomial of the zero element 0 is X, and the minimum polynomial of the element 1 is $1+X$.

B.7.1 Properties of Minimal Polynomials

Minimal polynomials have the following properties [1]:

Theorem B.2: The minimum polynomial of an element β of a Galois field GF(2^m) is an irreducible polynomial.

Demonstration of this property is based on the fact that if the minimal polynomial was not irreducible, it could be expressed as the product of at least two other polynomials $\phi(X)=\phi_1(X)\,\phi_2(X)$, but since $\phi(\beta)=\phi_1(\beta)\,\phi_2(\beta)=0$, it should be true that either $\phi_1(\beta)=0$ or $\phi_2(\beta)=0$, which is contradictory with the fact that $\phi(X)$ is of minimum degree.

Theorem B.3: For a given polynomial $f(X)$ defined over GF(2), and $\phi(X)$ being the minimal polynomial of β, if β is a root of $f(X)$, it follows that $\phi(X)$ is a factor of $f(X)$.

Theorem B.4: The minimal polynomial $\phi(X)$ of the element β of the Galois field GF(2^m) is a factor of $X^{2^m}+X$.

Theorem B.5: Let $f(X)$ be an irreducible polynomial defined over GF(2), and $\phi(X)$ be the minimal polynomial of an element β of the Galois field GF(2^m). If $f(\beta)=0$, then $f(X)=\phi(X)$.

This last theorem means that if an irreducible polynomial has the element β of the Galois field GF(2^m) as its root, then that polynomial is the minimal polynomial $\phi(X)$ of that element.

Theorem B.6: Let $\phi(X)$ be the minimal polynomial of the element β of the Galois field GF(2^m), and let e be the smallest integer number for which $\beta^{2^e}=\beta$, then the minimal polynomial of β is

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

Table B.5 Minimal polynomials of all the elements of the Galois field GF(2^4) generated by $p_i(X) = 1 + X + X^4$

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

Example B.4: Determine the minimal polynomial $\phi(X)$ of $\beta = \alpha^7$ in GF(2^4). As seen in Example B.3, the conjugates $\beta^2 = (\alpha^7)^2 = \alpha^{14}$, $\beta^{2^2} = (\alpha^7)^4 = \alpha^{28} = \alpha^{13}$ and $\beta^{2^3} = (\alpha^7)^8 = \alpha^{56} = \alpha^{11}$ are also roots of the polynomial for which $\beta = \alpha^7$ is a root. Since $\beta^{2^e} = \beta^{16} = (\alpha^7)^{16} = \alpha^{112} = \alpha^7 = \beta$, then $e = 4$ so that

$$\begin{aligned}
\phi(X) &= (X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\
&= [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}] \\
&= [X^2 + (\alpha^8)X + \alpha^3][X^2 + (\alpha^2)X + \alpha^{12}] \\
&= X^4 + (\alpha^8 + \alpha^2)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)X + \alpha^{15} \\
&= X^4 + X^3 + 1
\end{aligned}$$

The construction of the Galois field GF(2^m) is done by considering that the primitive polynomial $p_i(X)$ of degree m has α as its root, $p_i(\alpha) = 0$. Since all the powers of α generate all the elements of the Galois field GF(2^m), α is said to be a primitive element.

All the conjugates of α are also primitive elements of the Galois field GF(2^m). In general, it can be said that if β is a primitive element of the Galois field GF(2^m), then all its conjugates β^{2^l} are also elements of the Galois field GF(2^m).

Table B.5 shows the minimal polynomials of all the elements of the Galois field GF(2^4) generated by $p_i(X) = 1 + X + X^4$, as seen in Example B.2.

Bibliography

[1] Lin, S. and Costello, D. J., Jr., *Error Control Coding: Fundamentals and Applications*, Prentice Hall, Englewood Cliffs, New Jersey, 1983.

[2] Allenby, R. B. J., *Rings, Fields and Groups: An Introduction to Abstract Algebra*, Edward Arnold, London, 1983.

[3] Hillma, A. P. and Alexanderson, G. L., *A First Undergraduate Course in Abstract Algebra*, 2nd Edition, Wadsworth, Belmont, California, 1978.

[4] McEliece, R. J., *Finite Fields for Computer Scientists and Engineers*, Kluwer, Massachusetts, 1987.