EE512: Error Control Coding

Solution for Assignment on Finite Fields

February 16, 2007

1. (a) Addition and Multiplication tables for $GF(5)$ and $GF(7)$ are shown in Tables 1 and 2.

+	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

Table 1: Tables for GF(5)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 2: Tables for GF(7)

(b) $GF(4) = \{0, 1, \alpha, \alpha^2\}$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$. The addition and multiplication tables are shown in Table 3.

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

×	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Table 3: Tables for GF(4)

2. Construction of $GF(16)$ using three different irreducible polynomials:

(a) Using $\pi_1(x) = x^4 + x + 1$: Let α be a root of $\pi_1(x) = 0$; $\alpha^4 = \alpha + 1$. Table 4 shows the construction.

(b) Using $\pi_2(x) = x^4 + x^3 + 1$: Let β be a root of $\pi_2(x) = 0$; $\beta^4 = \beta^3 + 1$. Table 4 shows the construction.

(c) Using $\pi_3(x) = x^4 + x^3 + x^2 + x + 1$: Let γ be a root of $\pi_3(x) = 0$; $\gamma^4 = \gamma^3 + \gamma^2 + \gamma + 1$. Table 5 shows the powers of γ. Note that γ is not a primitive element of $GF(16)$, since order of γ

Power	Polynomial	Vector
$\alpha^{-\inf}$	0	0000
α^0	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001

Power	Polynomial	Vector
$\beta^{-\inf}$	0	0000
β^0	1	0001
β	β	0010
β^2	β^2	0100
β^3	β^3	1000
β^4	β^3+1	1001
β^5	$\beta^3+\beta+1$	1011
β^6	$\beta^3+\beta^2+\beta+1$	1111
β^7	$\beta^2+\beta+1$	0111
β^8	$\beta^3+\beta^2+\beta$	1110
β^9	β^2+1	0101
β^{10}	$\beta^3+\beta$	1010
β^{11}	$\beta^3+\beta^2+1$	1101
β^{12}	$\beta+1$	0011
β^{13}	$\beta^2+\beta$	0110
β^{14}	$\beta^3+\beta^2$	1100

Table 4: GF(16) using $\pi_1(x)$ and $\pi_2(x)$.

is 5. It can be noticed that the polynomial $\pi_3(x) = x^4 + x^3 + x^2 + x + 1$ can be written as $\pi_3(x) = (1 + x)^4 + (1 + x)^3 + 1 = \pi_2(1 + x)$. Thus $(1 + \gamma)$ is a root of $\pi_2(x)$, and it has to be a primitive element, since $\pi_2(x)$ is a primitive polynomial. Table 5 shows the construction of $GF(16)$ using $(1 + \gamma)$ as the primitive element.

Power	Polynomial
$\gamma^{-\inf}$	0
γ^0	1
γ	γ
γ^2	γ^2
γ^3	γ^3
γ^4	$\gamma^3+\gamma^2+\gamma+1$
γ^5	1

Power	Polynomial	Vector
$(1+\gamma)^{-\inf}$	0	0000
$(1+\gamma)^0$	1	0001
$(1+\gamma)$	$1+\gamma$	0011
$(1+\gamma)^2$	$1+\gamma^2$	0101
$(1+\gamma)^3$	$1+\gamma+\gamma^2+\gamma^3$	1111
$(1+\gamma)^4$	$\gamma+\gamma^2+\gamma^3$	1110
$(1+\gamma)^5$	$1+\gamma^2+\gamma^3$	1101
$(1+\gamma)^6$	γ^3	1000
$(1+\gamma)^7$	$1+\gamma+\gamma^2$	0111
$(1+\gamma)^8$	$1+\gamma^3$	1001
$(1+\gamma)^9$	γ^2	0100
$(1+\gamma)^{10}$	$\gamma^2+\gamma^3$	1100
$(1+\gamma)^{11}$	$1+\gamma+\gamma^3$	1011
$(1+\gamma)^{12}$	γ	0010
$(1+\gamma)^{13}$	$\gamma+\gamma^2$	0110
$(1+\gamma)^{14}$	$\gamma+\gamma^3$	1010

Table 5: $GF(16)$ using $\pi_3(x)$.

(d) Isomorphism between two fields is a one-one and onto mapping of the elements of one field to another such that all the operations of the fields are preserved. If ϕ is an isomorphism from $F_1 \rightarrow F_2$, $\phi(a_1 * a_2) = \phi(a_1) o \phi(a_2)$, where $a_1, a_2 \in F_1$, $*$ is the operation defined in F_1, and o is the operation defined in F_2. Observing the elements of $GF(16)$ constructed using $\pi_1(x)$, α^7 is a root of $\pi_2(x)$. Thus mapping $\alpha^7 \in GF_1 \rightarrow \beta \in GF_2$ is an isomorphism between GF_1 and GF_2. Similarily, α^3 is a root of $\pi_3(x)$. Thus mapping $\alpha^3 \in GF_1 \rightarrow \gamma \in GF_3$ is an isomorphism between GF_1 and GF_3.

3. (a) Finding all polynomials of degree 2 and degree 3 that are irreducible over GF(2) and GF(3):

i. $x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $GF(2)$. $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the irreducible polynomials of degree 3 over $GF(2)$. To check if the irreducible polynomial of degree m over $GF(p)$, $f(x)$ is primitive, it is required to find the smallest number n such that $f(x)$ divides $x^n - 1$. If $n = p^m - 1$, then $f(x)$ is primitive, If $n < p^m - 1$, then $f(x)$ is not primitive. Since there is just one irreducible polynomial of degree 2 over $GF(2)$, it has to be primitive. Both the irreducible polynomials of degree 3 over $GF(2)$ are also primitive.

ii. $x^2 + x + 2$, $x^2 + 2x + 2$ and $x^2 + 1$ are the irreducible polynomials of degree 2 over $GF(3)$. It can be seen that $x^2 + 1$ divides $x^4 - 1$ over $GF(3)$; thus, it is not a primitive polynomial. It can be verified that the other two irreducible polynomials of degree 2 over $GF(3)$are primitive. $x^3 + 2x + 1$,$x^3 + 2x^2 + 1$,$x^3 + x^2 + 2$,$x^3 + 2x + 2$,$x^3 + x^2 + x + 2$ and $x^3 + 2x^2 + 2x + 2$ are the irreducible polynomilas of degree 3 over $GF(3)$. $x^3 + 2x + 1$ and $x^3 + 2x^2 + 1$ are the primitive polynomials of degree 3 over $GF(3)$, the rest of the irreducible polynomials are not primitive (It can be verified that they divide $x^{13} - 1$).

(b) Construction of $GF(9)$ in two different ways:

i. Construction using primitive polynomial: Consider the primitive polynomial $\pi_1(x) = x^2 + x + 2$. Let α be a root of $\pi_1(x) = 0$; therefore, $\alpha^2 = 2\alpha + 1$.

Power	Polynomial	Vector(with basis [1,α])
0	0	00
1	1	01
α	α	10
α^2	$2\alpha + 1$	21
α^3	$2\alpha + 2$	22
α^4	2	02
α^5	2α	20
α^6	$\alpha + 2$	12
α^7	$\alpha + 1$	11

Table 6: $GF_1(9)$

ii. Construction using non-primitive polynomial: Consider the non-primitive polynomial $\pi_2(x) = x^2 + 1$. Let β be a root of $\pi_2(x) = 0$. Since $\pi_2(x)$ is not a primitive polynomial, β will not be a primitive element of $GF(9)$. $\pi_2(x)$ can be written as, $\pi_2(x) = (x + 1)^2 + (x + 1) + 2$, Thus $(1 + \beta)$ is a primitive element of $GF(9)$.

Power	Polynomial	Vector(with basis [1,β])
0	0	00
1	1	01
$(1 + \beta)$	$\beta + 1$	11
$(1 + \beta)^2$	2β	20
$(1 + \beta)^3$	$2\beta + 1$	21
$(1 + \beta)^4$	2	02
$(1 + \beta)^5$	$2\beta + 2$	22
$(1 + \beta)^6$	β	10
$(1 + \beta)^7$	$\beta + 2$	12

Table 7: $GF_2(9)$

To find the isomorphism between GF_1 and GF_2, note that $\alpha^2 \in GF_1$ is a root of $\pi_2(x)$, thus $\alpha^2 \to \beta$ is an isomorphism.

4. (a) Let $GF(9) = \{0, 1, \alpha, \alpha^2, ..., \alpha^7\}$, where α is the root of the primitive polynomial $\pi(x) = x^2 + x + 2$. The multiplicative group $GF^*(9) = \{1, \alpha, \alpha^2, ..., \alpha^7\}$. Ord$(\alpha^i) = n/(n, i)$, where n

is the order of the multiplicative group (8 in this case) and (n, i) denotes the GCD of n and i. Primitive elements are the elements with order 8.
Elements of order 2 = $\{\ \alpha^4\}$;
Elements of order 4 = $\{\ \alpha^2, \alpha^6\}$;
Elements of order 8 = $\{\ \alpha, \alpha^3, \alpha^5, \alpha^7\}$ (primitive).
Similarly, let $GF(16) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14},\ \alpha^4 = \alpha + 1$.
Elements of order 3 = $\{\alpha^5, \alpha^{10}\}$;
Elements of order 5 = $\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$;
Elements of order 15 = $\{\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}\}$ (primitive).

(b) Order of elements in GF(32): Order of the Multiplicative group $GF^*(32)$ is $n = 31$. Since n is prime, $(n, i) = 1$ for all $i \Longrightarrow$ all elements are primitive. For all non-zero, non-unity elements of $GF(p^m)$ to be primitive, $p^m - 1$ should be prime.

5. (a) Multiplication and addition in GF(p)are defined modulo p. Thus, order of an element a is the smallest number n such that $a^n = 1 \mod p$. Using this condition, order of every element can be determined. Moreover, order of any element should divide the order of the multiplicative group $p - 1$. An element is primitive if its order is equal to $p - 1$.
GF(7): Elements of order 2 = { 6}; Elements of order 3 = { 2,4}; Elements of order 6 (primitive) = { 3,5}.
GF(11): Elements of order 2 = { 10}; Elements of order 5 = { 3,4,5,9}; Elements of order 10 (primitive) = { 2,6,7,8}.

(b) All non-zero, non-unity elements of $GF(p)$ cannot be primitive for $p > 3$ since $(p - 1)$ would not be prime, and there would be elements with order less than $(p - 1)$. In $GF(3)$ there is only one non-zero, non-unity element and it has to be primitive.

6. (a) Let $\alpha \in GF(2^m)$. We know that $\alpha^{2^m} = \alpha$. Therefore, $\left(\alpha^{2^{m-1}}\right)^2 = \alpha$. Hence, $\alpha^{2^{m-1}}$ is a square root of α.

(b) Proof is similar to that for the previous part.

7. In GF(16),
$$(x + y)^3 = x^3 + y^3 + 3x^2y + 3xy^2 = x^3 + y^3 + xy(x + y).$$
Using the given values for $x + y$ and $x^3 + y^3$, we get that $(\alpha^{14})^3 = \alpha + xy(\alpha^{14})$. Simplifying, we get $xy = \alpha^{14}$ or $y = \alpha^{14}/x$. Using in $x + y = \alpha^{14}$, we get
$$x + \frac{\alpha^{14}}{x} = \alpha^{14},$$
or the quadratic equation $f(x) = x^2 + \alpha^{14}x + \alpha^{14} = 0$.
By trial and error, we see that the roots of $f(x)$ in GF(16) are α^6 and α^8. Hence, possible solutions for (x, y) are (α^6, α^8) or (α^8, α^6).

8. (a) Since $x + y = \alpha^3$,
$$(x + y)^2 = x^2 + y^2 = (\alpha^3)^2 = \alpha^6$$
. We see that the second equation is consistent with and fully dependent on the first equation. The set of solutions is $\{(x, x + \alpha^3) : x \in \text{GF}(16)\}$.

(b) The second equation is inconsistent with the first equation. Hence, no solution exists.

9. We are given that $x^3 + y^3 + z^3 = 0$ for $x, y, x \in \text{GF}(64)$. Note that $x^{63} = y^{63} = z^{63} = 1$.
Since $(a + b)^2 = a^2 + b^2$ for $a, b \in \text{GF}(64)$, we see that $(a + b)^{32} = a^{32} + b^{32}$. Using this, we get
$$(x^3 + y^3 + z^3)^{32} = 0.$$
Simplifying the LHS above, we get that $x^{33} + y^{33} + z^{33} = 0$.

10. Suppose $\beta \in \mathrm{GF}(q)$ is an element of order 5. Then, β is a root of $x^5 - 1$, since $\beta^5 - 1 = 0$. Notice that β^2, β^3, β^4 and $\beta^5 = 1$ are all distinct and additional roots of $x^5 - 1$. Since $x^5 - 1$ can have no further roots in $\mathrm{GF}(q)$, we get

$$x^5 - 1 = (x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)(x-\beta^5).$$

(a) If $\alpha \in \mathrm{GF}(16)$ is a primitive element, we see that $\mathrm{Ord}(\alpha^3) = 5$. Hence,

$$x^5 + 1 = (x+\alpha^3)(x+\alpha^6)(x+\alpha^9)(x+\alpha^{12})(x+1)$$

in $\mathrm{GF}(16)[x]$.
In $\mathrm{GF}(2)[x]$,

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

is a complete factorization into irreducibles.
In GF(11), we see from Problem (5a) that 3 is an element of order 5. Hence,

$$\begin{aligned} x^5 - 1 &= (x-3)(x-3^2)(x-3^3)(x-3^4)(x-3^5), \\ &= (x-3)(x-9)(x-5)(x-4)(x-1). \end{aligned}$$

(b) $x^5 - 1$ factors into linear factors over $\mathrm{GF}(p)$ when $p-1$ is a multiple of 5.

11. (a) i. Cyclotomic Decomposition of GF(9) (α: primitive): $S = \{\alpha^0\} \cup \{\alpha, \alpha^3\} \cup \{\alpha^2, \alpha^6\} \cup \{\alpha^4\} \cup \{\alpha^5, \alpha^7\}$. Table 8 lists the minimal poynomials.

Element	Minimal Polynomial
0	x
1	$x+1$
α, α^3	$x^2 + x + 2$
α^2, α^6	$x^2 + 1$
α^4	$x + 2$
α^5, α^7	$x^2 - x + 2$

Table 8: Minimal polynomials of GF(9).

ii. Cyclotomic Decomposition of GF(16) (α: primitive): $S = \{\alpha^0\} \cup \{\alpha, \alpha^2, \alpha^4, \alpha^8\} \cup \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\} \cup \{\alpha^5, \alpha^2\} \cup \{\alpha^7, \alpha^{14}\, \alpha^{13}, \alpha^{11}\}$. Table 9 lists the minimal poynomials.

Element	Minimal Polynomial
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$x^4 + x^3 + 1$

Table 9: Minimal polynomials of GF(16).

(b) Not neccessarily. As a counterexample, the minimal polynomial of $\alpha^3 \in \mathrm{GF}(16)$ (order 5, nonprimitive element) has degree 4.