EE 229B ERROR CONTROL CODING **Spring 2005**

Lecture notes on finite fields
Venkat Anantharam
(based on scribe notes by Rohit Puri, Aaron Wagner, Anand Raghavan, Payam Pakzad, and Marc Ibanez)

Warning : Use at your own risk ! These notes have not been sufficiently carefully screened.

1 Characteristic and size of a finite field

We first prove the following :
Fact : For a finite field F, there is a prime p and an integer $m \geq 1$ such that $|F| = p^m$.

Subsequently, we will focus on the case $p = 2$.

Definition: *Characteristic* of F : Consider (1, 1+1, 1+1+1, ...). Since F is finite, we must have,

$$\underbrace{1+1+\ldots+1}_{k} = \underbrace{1+1\ldots+1}_{l} \tag{1}$$

for some $l > k$. This means $\underbrace{1+1+\ldots+1}_{l-k} = 0$, and $l - k > 0$. There must therefore be a smallest $m > 0$ s.t. $\underbrace{1+1+\ldots+1}_{m} = 0$.

Lemma: m must be a prime number ≥ 2.
Proof: Since $1 \neq 0$ we have $m \geq 2$. Suppose $m = m_1 \cdot m_2$ where $m_1 > 1, m_2 > 1$.
Then, $\underbrace{1+1+\ldots+1}_{m} = (\underbrace{1+1+\ldots+1}_{m_1}) \cdot (\underbrace{1+1+\ldots+1}_{m_2})$. But L.H.S equals 0 which implies that at least one of the R.H.S terms equals 0, which is a contradiction. Hence m must be a prime number. This is called the *characteristic* of the field. We denote it by p from now on.

Note that the set $\{1,\ 1+1,\ 1+1+1,\ \ldots \underbrace{1+1+\ldots+1}_{p-1},\ 0\}$, which is a subset of F, is itself a field with the operations of F, and in fact is just a copy of GF(p). This is because the product of two sums of 1's is also a sum of 1's. We can view the set F as a vector space over GF(p) as follows:
Vector Addition: To define the vector addition we need to describe how to add elements of F. We take this addition operation to be the same as one already defined for F when it is viewed as a field.
Scalar Multiplication: Given $k \in GF(p), x \in F$, we want to define $k \cdot x \in F$. $k \cdot x$ is defined as $(\underbrace{1+1+\ldots+1}_{k}) \cdot x$, where the operation on the R.H.S. is just the field multiplication, which is already defined in F.
It is straightforward to verify that the properties required of vector addition and scalar multiplication are satisfied by the definitions we just made and so we have indeed described F as a vector space over $GF(p)$. Now note that we have proved that $|F| = p^m$ for some $m \geq 1$! Indeed, m here is the dimension of F viewed as a vector space over GF(p). F must have such a dimension and since p^m is the total number of distinct linear combinations of m linearly independent basis vectors in a vector space over the field GF(p), it follows that F must have exactly p^m elements.

.	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

+	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

2 Field of characteristic 2

From now on we restrict ourselves to fields of characteristic 2. So far we have learned that if there exists a field of characteristic 2, then we must have $|F| = 2^m$ for some $m \geq 1$. We will construct such a field for every m. This is of importance in coding theory.

For $m = 1$, we know an F exists, namely GF(2) $= \{0, 1\}$. Let us try to construct such a field for $m = 2$. Here the set F is $\{0, 1, \alpha, \_\}$. Consider $\alpha \cdot \alpha$. Now $\alpha \cdot \alpha \neq 0$ (else $\alpha = 0$), $\alpha \cdot \alpha \neq \alpha$ (else $\alpha = 1$). $\alpha \cdot \alpha = 1$ is possible. But in this case, let the fourth element be β. Then $\beta \cdot \alpha \neq 0$ (else $\beta = 0$ or $\alpha = 0$). Moreover $\beta \cdot \alpha \neq 1$ (else $\beta = \alpha$, because we already assumed that $\alpha \cdot \alpha = 1$), $\beta \cdot \alpha \neq \alpha$ (else $\beta = 1$) and $\beta \cdot \alpha \neq \beta$ (else $\alpha = 1$). Thus $\alpha \cdot \alpha = 1$ is not possible. Hence $\alpha \cdot \alpha$ must be the fourth element of the field. Denote it by α^2. We can verify that addition and multiplication tables for this field are as above.

In coming up with the above tables we used the identity $\alpha^2 = 1 + \alpha$. This identity must hold because $1 + \alpha \neq 0$ (else $\alpha = 1$), $1 + \alpha \neq 1$ (else $\alpha = 0$), and $1 + \alpha \neq \alpha$ (else $1 = 0$). The only remaining choice is $1 + \alpha = \alpha^2$.

The calculations done above involve powers of α. This is like dealing with polynomials in α. Indeed, all that is going on is that any power of α bigger than 2 can be replaced by a polynomial in α of degree at most 1, using the identity $\alpha^2 = 1+\alpha$. Using this observation, it can be verified that the addition and multiplication tables are consistent with addition and multiplication of polynomials in α and so all the necessary properties of a field, including the less obvious ones such as distributivity of multiplication over addition can be seen to hold.

Note that if the elements $\{0, 1, \alpha, \alpha^2\}$ are mapped respectively to two bit symbols {00,01,10,11} then the addition tables just correspond to bitwise addition. The multiplication tables are somewhat more strange, but the thing to focus on is that they come from using the relation $1 + \alpha = \alpha^2$.

3 Finite Fields through polynomials

The set of polynomials over GF(2) is denoted GF(2)[X] :

$\{a_0 + a_1 \cdot X \ldots + a_d \cdot X^d; \;\; d \geq 0; \;\; a_0, a_1, \ldots a_d \;\epsilon\; \{0,1\}\}$

We can add and multiply as usual with coefficients added and multiplied as in GF(2).
e.g, $(X^2 + X + 1) \cdot (X^4 + X^2 + 1) = X^6 + X^5 + X^3 + X + 1$.
Definition: A polynomial over GF(2) is called irreducible over $GF(2)$ if it has no non-trivial factors, e.g,
Reducible : $X^2 + 1 = (X + 1)(X + 1)$ so $X^2 + 1$ is reducible.
Irreducible : $X^2 + X + 1$ is irreducible (because neither 0 nor 1 is a root). $X^3 + X + 1$ and also $X^3 + X + 1$ are irreducible (in each case, at least one of the factors would have degree 1 but these polynomials have no roots in GF(2)).
Also consider $X^4 + X + 1$. It has no roots, so any nontrivial factorization would be into two factors each of degree 2, and each of these factors would have leading coefficient 1 and constant coefficient 1. Suppose we had $X^4 + X + 1 = (X^2 + a \cdot X + 1) \cdot (X^2 + b \cdot X + 1)$
$= X^4 + (a + b) \cdot X^3 + ab \cdot X^2 + (a + b) \cdot X + 1$. This would require $a + b = 1$ and $a + b = 0$ which is impossible. Hence $X^4 + X + 1$ is irreducible over $GF(2)$.

Theorem: Given an irreducible polynomial over GF(2), $m(x)$, of degree d, we can construct a field of characteristic 2 and size 2^d.
Define F to be the set of polynomials with GF(2) coefficients with degree $\leq d - 1$ with the usual addition, and with multiplication defined modulo $m(x)$. I.e, $p(x) \cdot q(x)$ is defined to be the remainder of the usual product when divided by $m(x)$. This field is denoted
$GF(2)[X]/ < m(X) >$.
Example : $d = 3$, $m(X) = X^3 + X + 1$, $F = \{a_0 + a_1 \cdot X + a_2 \cdot X^2 : a_0, a_1, a_2 \;\epsilon\; GF(2)\}$.
Multiplication : We know that

$$(1 + X^2) \times (1 + X + X^2) = (X^3 + X + 1) \times (X + 1) + (X^2 + X) \tag{2}$$

in case of regular multiplication with coefficients from GF(2). Hence, under the field multiplication operation '.',

$$(1 + X^2) \cdot (1 + X + X^2) = (X^2 + X) \tag{3}$$

For d = 2, with $m(X) = X^2 + X + 1$, $GF(2)[X]/ < m(X) >$ is just the example we constructed by hand (of GF(4)) with X being written for what we called α. You can check this from the addition and multiplication tables.

Note that, given an irreducible polynomial $m(X)$ of degree d over GF(2),
$GF(2)[X]/ < m(X) >$ is a set of 2^d elements. As mentioned, addition is defined coordinate-wise, and multiplication is modulo m(X).
Claim : This is a field.
Proof: The additive identity is zero polynomial $(0 + 0 \cdot X + \ldots 0 \cdot X^{d-1})$.
The additive inverse of p(X) is just p(X) (coefficients are from GF(2) !).
Commutativity and associativity of addition are obvious.
The multiplicative Identity is 1 $(1 + 0 \cdot X + \ldots + 0 \cdot X^{d-1})$
Commutativity and associativity of multiplication are obvious.
Multiplication distributes over addition : this is because, to find the remainder of $p(X)q(X)$ when divided by $m(X)$ we can first find the remainders of $p(X)$ and $q(X)$ when divided by m(X) (this is

not necessary if p(X) and q(X) are already of degree at most d-1), and then find the remainder of the product of these remainders, when divided by m(X).
What about the existence of a multiplicative inverses for non-zero elements ?

To show the existence of a multiplicative inverse for a nonzero element $p(x) \in F$, we make use of the Euclidean Division Algorithm, which provides us with an $a(x), b(x) \in F$ such that

$$a(x)p(x) + b(x)m(x) = \text{GCD}(p(x), m(x)) = 1 \text{ (Bezout Identity)}$$

and degree$(a(x)) \leq d-1$.

$a(x)$ is then the multiplicative inverse of $p(x)$ in F. Note that $\text{GCD}(p(x), m(x)) = 1$ since $m(x)$ is irreducible. □

Example: Find the inverse of $1+x$ in GF(2)[x]/$< x^2+x+1 >$.

$$\begin{aligned} x^2+x+1 &= x(x+1)+1 \\ (x+1) &= (x+1)1+0 \end{aligned}$$

Then working backward:

$$1 \cdot (x^2+x+1) + x(x+1) = 1$$

so $x(x+1) = 1$ *mod* x^2+x+1, so x is the multiplicative inverse of $x+1$.

Example: What is $(1+x+x^2)^{-1}$ in GF(2)$[x]/< x^3+x^2+1 >$?

$$\begin{aligned} x^3+x^2+1 &= x(1+x+x^2)+(x+1) \\ x^2+x+1 &= x(x+1)+1 \\ (x+1) &= 1(x+1)+0 \end{aligned}$$

Then working backward, we replace $(x+1)$ in the second equation using the first equation:

$$\begin{aligned} x^2+x+1 &= x(x^3+x^2+1)+x^2(1+x+x^2)+1 \\ (1+x^2)(x^2+x+1)+x(x^3+x^2+1) &= 1 \end{aligned}$$

So $(x^2+x+1)^{-1} = 1+x^2$ *mod* x^3+x^2+1.

A large number of practical codes are based on these finite fields.

We will presently show:

I. Every field F of size 2^m must be "of this kind."

II. For every $m \geq 1$, there is an irreducible polynomial of degree m, hence there is a field of size 2^m. Of course, this polynomial may not be unique, however,

III. Irrespective of which irreducible polynomial of degree m is used, the resulting field is the same up to relabeling of the elements.

We note an analogy between the construction of these finite fields and the construction of the complex numbers from the reals. In the latter case, the polynomial $x^2 + 1$ is irreducible over $\Re$, and we form the field of complex numbers using $\Re[x]/ < x^2 + 1 >$. By creating the symbol i to represent the solution to $x^2 + 1 = 0$, we force the complete factorization: $x^2 + 1 = (x + i)(x - i)$.

Analogously, GF(2^m) is the unique finite field of size 2^m obtained by forcing the complete factorization of $x^{2^m-1} - 1$ (i.e. regardless of how we choose $m(x)$, the nonzero elements will be precisely the $2^m - 1$ solutions of $x^{2^m-1} = 1$).

Definition 1 *Let F be a finite field of size n. Let $\alpha \in F, \alpha \neq 0$. Consider $\alpha, \alpha^2, \alpha^3, \ldots$. Since the field is finite, we must have $\alpha^l = \alpha^k$ for some $l \neq k$, so we must have $\alpha^j = 1$ from some $j \neq 0$. The smallest such j is called the* order *of α, denoted ord(α).*

Lemma 1 *(Lagrange) For every $\alpha \in F$, ord(α) divides $n - 1$.*

Proof: The $n - 1$ nonzero elements of F form a group under field multiplication. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{j-1}\}$ is a subgroup of this group. The disjoint union of the cosets of this subgroup gives F. Thus j divides $n - 1$, which we denote $j|(n - 1)$. □

This shows that every nonzero element α of a finite field F of size n must solve the equation $x^{n-1} - 1 = 0$ (since $\alpha^j = 1$ and $j|(n + 1)$). We will take $n = 2^m$ giving $x^{2^m-1} - 1 = 0$. Our field will consist of the $2^m - 1$ solutions to this equation and the zero element.

Definition 2 *A nonzero element of a finite field whose order is $n - 1$ is called* primitive.

Example: If there is a primitive element in a field of size 16, then there must be a nonprimitive element, namely the primitive element cubed. Some fields have only the zero, unity, and primitive elements, like the field with cardinality eight.

Consider a nonzero, nonunity element of GF(8), α. Since α is primitive (because $n - 1 = 7$ is a prime), the elements of GF(8) can be written as $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$. We will construct a field of size 8 in 2 ways and see that they are the same up to a renaming of the elements.

One way to construct this field is to use GF(2)[x]/$< x^3 + x + 1 >$. We will denote $ax^2 + bx + c$ by abc. Addition over this field is done coordinate-wise in GF(2). To specify the multiplication rule, we could multiply all elements of GF(2)[x] and then divide by $x^3 + x + 1$ and take the remainder. However, a more intelligent method is to remember that the elements can be written as $\{0, 1, x, x^2, \ldots, x^6\}$. We then find the representations of the various powers of x as polynomials of x of degree ≤ 2. Since x^3 *mod* $(x^3 + x + 1) = x + 1$, we can obtain the following:

$$\begin{aligned} 1 &= 1 \\ x &= x \\ x^2 &= x^2 \\ x^3 &= x + 1 \end{aligned}$$

$$\begin{aligned} x^4 &= x^3 \cdot x = (x+1)x = x^2 + x \\ x^5 &= x^3 \cdot x^2 = (x+1)x^2 = x^2 + x + 1 \\ x^6 &= x^5 \cdot x = x^3 + x^2 + x = x^2 + 1 \end{aligned}$$

Then

$$\begin{aligned} 110 \cdot 101 &= (x^2 + x) \cdot (x^2 + 1) \\ &= x^4 \cdot x^6 = x^{10} = x^3 \\ &= x + 1 = 011 \end{aligned}$$

This allows us to fill in the entire multiplication table for our field:

$\cdot$	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	011	001	111	101
011	000	011	110	101	111	100	001	010
100	000	100	011	111	110	010	101	001
101	000	101	001	100	010	111	011	110
110	000	110	111	001	101	011	010	100
111	000	111	101	010	001	110	001	011

Note that 010 (x), 100 (x^2), and 110 (x^4) solve the equation $m(x) = x^3 + x + 1 = 0$. It is easily verified that the other three nonzero, nonunity elements, 011 (x^3), 101 (x^6), 111 ($x^{12} = x^5$) solve the other third–order irreducible polynomial, $\hat{m}(y) = y^3 + y^2 + 1 = 0$. If we constructed the field using $\hat{m}(y)$ in place of $m(x)$, then y would replace x^3, giving the one-to-one mapping:

000	001	010	100	011	110	111	101
0	1	x	x^2	x^3	x^4	x^5	x^6
0	1	y^5	y^3	y	y^6	y^4	y^2
000	001	011	101	010	110	111	100

(Here we used the rule $y^3 = y^2 + 1$ to derive the binary expansion in the bottom row). This verifies that these two ways of construction GF(8) are identical up to element relabeling. In the sequel we will see that

$$x^{2^m} - x = \prod_{d|m} \prod m(x),$$

where the inner product is over all irreducible polynomials $m(x)$ of degree d. For $m = 3$ we have

$$x^8 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

from which we conclude that $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the only irreducible polynomials of degree 3 (you could have also verified this directly, case by case). Thus, if you believe the claim (I) that every finite field of characteristic 2 and size 2^d has to be of the form $GF(2)[x]/ < m(X) >$ for some irreducible polynomial $m(x)$ of degree d, then the two constructions of $GF(8)$ described above exhaust all possible constructions, and, since they are identical, we conclude that GF(8) is unique. Note that the elements of GF(8) are precisely the solutions of $x^8 - x$. The nonzero elements of GF(8) are precisely the solutions $x^7 - 1$.

We will see:

I. Given a finite field F of characteristic 2 and size 2^m, it must be of the type $GF(2)[X]/ < m(X) >$ for some irreducible polynomial $m(X)$ of degree m.

II. For every $m \geq 1$ there exists at least one irreducible polynomial (over GF(2)) of degree m.

III. All constructions of the type $GF(2)[X]/ < m(X) >$, $m(X)$ irreducible, degree m, result in the same field, up to renaming of the elements.

Defn: *Euler ϕ Function:* This is a function defined on $\{1, 2, \ldots\}$ with $\phi(1) = 1$, and for $n \geq 2$ $\phi(n) =$ number of integers in $\{1, 2, \ldots, n-1\}$ that are relatively prime to n. (*i.e.* $gcd(k, n) = 1 \iff k$ is counted.)
Ex: $\phi(15) = 14 - \mid \{3, 6, 9, 12, 5, 10\} \mid = 14 - 6 = 8$.

Defn: *Mobius Function*(μ): This is a function defined on$\{1, 2, \ldots, \}$ with $\mu(1) = 1$. For $n \geq 2, n = \Pi_{i=1}^{l} p_i^{a_i}$.

$$\mu(n) \quad = \quad \begin{cases} (-1)^l, & \text{if } n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l} \; and \, a_i = 1, 1 \leq i \leq l \\ 0, & \text{otherwise} \end{cases}$$

Ex: $75 = 3^1.5^2,\ \mu(75) = 0.\ 210 = 2.3.5.7,\ \mu(210) = (-1)^4 = 1.$

Defn: *Dirichlet Product*: Given two functions f and g defined on $\{1, 2, \ldots\}$, their Dirichlet product, denoted fog, is defined as

$$f \, o \, g(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

Ex: $f \, o \, g(72) = f(1)g(72) + f(2)g(36) + f(3)g(24) + f(4)g(18) + f(6)g(12) + f(8)g(9) + f(9)g(8) + f(12)g(6) + f(18)g(4) + f(24)g(3) + f(36)g(2) + f(72)g(1)$

Fact: The Dirichlet product is commutative and associative.

Notation:
$\hat{1}$ is the function $\hat{1}$(n)=1 for all $n > 1$.
δ is the function $\delta(1) = 1, \delta(n) = 0 \, for \, n > 1$.

Fact: δ is the identity for the Dirichlet product. $\Rightarrow f \, o \, \delta = \delta \, o \, f = f$

$$\big[(f\, o\, \delta(n) = \sum_{d|n} f(d)\delta(\frac{n}{d}) = f(n)\delta(1) = f(n)\big].$$

Theorem: For the Dirichlet product μ is the inverse of $\hat{1}$ *i.e.* $\mu\, o\, \hat{1}$=$\hat{1}\, o\, \mu = \delta$.

Pf: $\mu\, o\, \hat{1}(1)$=$\mu(1)\hat{1}(1)$=1=$\delta(1)$. (by defn.)

For $n > 1$, $\mu\, o\, \hat{1}$(n)=$\sum_{d|n} \mu(d)\hat{1}(\frac{n}{d}) = \sum_{d|n} \mu(d)$. Now we need to show that $\sum_{d|n} \mu(d) = 0$.
Suppose $n = p_1^{a_1}p_2^{a_2}\dots p_l^{a_l}$. $d|n$ iff $d = p_1^{b_1}p_2^{b_2}\dots p_l^{b_l}$ for some $0 \le b_i \le a_i$. If any $b_i \ge 2$ then $\mu(d) = 0$ by definition.
The number of divisors d for which exactly j of the b_i are 1 and none are ≥ 2 is $\binom{l}{j}$.
So, $\sum_{d|n} \mu(d) = 1 + \binom{l}{1}(-1) + \binom{l}{2}(+1) + \dots + (-1)^l = (1 + (-1))^l = 0$.
Thus $\mu\, o\, \hat{1}$(n) $= \delta(n)$ for $n \ge 2$ also. Hence $\mu\, o\, \hat{1} = \delta$.

□

Theorem: *Möbius Inversion Formula:* Suppose g and f are functions on $\{1, 2, \dots\}$ satisfying $g(n) = \sum_{d|n} f(d)$, then we have

$$f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d})\ . \qquad (4)$$

Pf: The hypothesis is that $g = f\, o\, \hat{1}$= $\sum_{d|n} f(d)\hat{1}(\frac{n}{d}) = \sum_{d|n} f(d)$. So, $g\, o\, \mu = (f\, o\, \hat{1})\, o\, \mu = f\, o(\hat{1}\, o\, \mu) = f\, o\, \delta = f$. This is precisely equation(4).

□

Now we are ready to prove Claim I. We need two more lemmas for that.

Lemma: $\sum_{d|n} \phi(d) = n$, for any $n \ge 1$.

Pf: Consider all the fractions $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$. Reduce each of these to lowest terms. For each $d|n$ exactly $\phi(d)$ of these fractions will end up getting reduced to a fraction whose denominator is d. So, $\sum_{d|n} \phi(d) = n$.
This implies that $\phi(n) = \sum_{d|n} \mu(d)(\frac{n}{d})$ (by the Möbius Inversion Formula.)
If $n = p_1^{a_1}p_2^{a_2}\dots p_l^{a_l}$, then

$$\phi(n) = n\big[1 - \sum_{i=1}^{l} \frac{1}{p_i} + \sum_{i=1}^{l} \sum_{j=1, j\ne i}^{l} \frac{1}{p_i}\frac{1}{p_j} - \dots\big]= n\, \Pi_{i=1}^{l}\, (1 - \tfrac{1}{p_i}).$$

Therefore,

$$\phi(n) = n \prod_{i=1}^{l} (1 - \frac{1}{p_i}). \tag{5}$$

Note: $\phi(n) > 0$. (This can also be seen by simply noting that 1 is relatively prime to n.) The formula (5) can be interpreted as an inclusion-exclusion formula. First subtract 1 from $n =| \{0, 1, \ldots, n-1\} |$ $\frac{n}{p_i}$ times, $1 \leq i \leq l$. This is to remove all the integers in $\{0, 1, \ldots, n-1\}$ that are divisible by p_i. However, integers that are divisible by $p_i p_j$ for some $i \neq j$ have been overcounted, so we throw them back in, and so on.

□

Lemma: If $\alpha \in F$ (finite field of characteristic 2) and $ord(\alpha) = t$ (*i.e.* $\alpha^t = 1$ and t is the smallest such), and if $\beta = \alpha^i$, then

$$ord(\beta) = \tfrac{t}{gcd(t,i)}.$$

Ex: Consider $F = GF(16)$, i.e. $F = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{14}\}, t = 15$. $(\alpha^3)^5 = 1$, and we have $5 = \frac{15}{gcd(3,15)}$. Similarly, $(\alpha^{10})^3 = 1$, $3 = \frac{15}{gcd(10,15)}$.

Pf: Let u denote $ord(\beta)$. $\beta = \alpha^i$, *i.e.* $(\alpha^i)^u = 1$ and u is the smallest such.
Note: $(\alpha^i)^{\frac{t}{gcd(i,t)}} = (\alpha^t)^{\frac{i}{gcd(i,t)}} = (1)^{\frac{t}{gcd(i,t)}} = 1 \Rightarrow u | \frac{t}{gcd(i,t)}$.
Also, since $\alpha^t = 1$ and $(\alpha^i)^u = \alpha^{iu} = 1$, we have $t | iu$. So, $\frac{t}{gcd(i,t)} | \frac{i}{gcd(i,t)} u \Rightarrow \frac{t}{gcd(i,t)} | u$ since $\frac{t}{gcd(i,t)}$ and $\frac{i}{gcd(i,t)}$ have no common factors. So, $u | \frac{t}{gcd(i,t)}$.
Putting these together, we have $u = \frac{t}{gcd(i,t)}$.

□

Theorem: If F is a finite field of size 2^m, there are exactly $\phi(t)$ elements in F of order t for each t dividing $2^m - 1$.

Corollary: Any finite field of size 2^m can be written as $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m - 2}\}$ where α is a primitive element.
Pf: $\phi(2^m - 1) > 0 \Rightarrow F$ has an element of order $2^m - 1$, *i.e.* a primitive element.

□

Defn: In a finite field F, given $\beta \in F, \beta \neq 0$, the polynomial with coefficients in $GF(2)$ of least degree satisfied by β is called the minimal polynomial of β.
Ex: In $GF(8) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$, where α represents X in $GF(2)[X]/ < X^3 + X + 1 >$, $\alpha, \alpha^2, \alpha^4$ have minimal polynomial $X^3 + X + 1$ and $\alpha^3, \alpha^5, \alpha^6$ have minimal polynomial $X^3 + X^2 + 1$.

Claim: Given F, a finite field of size 2^m and β, a primitive element in F, its minimal polynomial has to have degree m. Call this minimal polynomial $m(X)$. Then F can be viewed as $GF(2)[X]/ < m(X) >$.

Pf. of claim (claim I): If β is a primitive element and β satisfies $b_0 + b_1X + \ldots + b_kX^k = 0$ with $k < m$, then every power of β is a nonzero linear combination with GF(2) coefficients of $1, \beta, \beta^2, \ldots, \beta^{k-1} \Rightarrow$ can have at most $(2^k - 1)$ distinct powers and we know that there are $(2^m - 1)$ distinct powers $\Rightarrow k \geq m$, which is a contradiction. Conversely, since F has dimension m over $GF(2)$, β^m should be expressible as a linear combination with $GF(2)$ coefficients of $1, \beta, \beta^2, \ldots, \beta^{m-1}$.

□

Pf. of Theorem: Let $\alpha \in F$, $\alpha \neq 0$, $\alpha \neq 1$. Let $t = ord(\alpha)$. Then $t|(2^m - 1)$.
Consider $1, \alpha, \alpha^2, \ldots, \alpha^{t-1}$. Each of these solves $X^t - 1 = 0$, and any element of F that solves $X^t - 1 = 0$ must be one of these, because this equation can have at most t solutions. In particular, any element of F of order t must be one of these (since any element of order t satisfies $X^t - 1 = 0$). Now, exactly $\phi(t)$ of these have order t since α^i has order t precisely if $gcd(i, t) = 1$ and there are exactly $\phi(t)$ such i. This means there are exactly $\phi(t)$ elements of F that have order t.
But, $\sum_{t|2^m-1} \phi(t) = 2^m - 1$. This means that for <u>each</u> $t|2^m - 1$ we have exactly $\phi(t)$ elements of F of order t (by counting).

□

We now prove Claim II. We will need the following

Theorem 1 *For each $m \geq 1$,*

$$x^{2^m} - x = \prod_{d|m} \prod_{\substack{p(x)\ irreducible \\ of\ degree\ d}} p(x)$$

Lemma 2 $\quad (x^l - 1)|(x^k - 1) \quad$ *iff* $\quad l|k$

Proof: Suppose $k = q \cdot l + r$ where q and r are the quotient and remainder after dividing k by l, so that $0 \leq r \leq l - 1$. Then:

$$\frac{x^k - 1}{x^l - 1} = \frac{(x^{q\,l} - 1)x^r}{x^l - 1} + \frac{x^r - 1}{x^l - 1} = (1 + x^l + \cdots + x^{(q-1)l})x^r + \frac{x^r - 1}{x^l - 1}$$

The second term on the right cannot be a polynomial since $r \leq l - 1$, so if $x^l - 1$ divides $x^k - 1$, we must have $\frac{x^r-1}{x^l-1} = 0$, i.e. $r = 0$, so l divides k.

The converse is trivial from the above representation. □

Lemma 3 $\quad (2^l - 1)|(2^k - 1) \quad$ *iff* $\quad l|k$

Proof: Same as above. Write 2 instead of x everywhere in the preceding proof. □

Lemma 4 *Let $g(x)$ be an irreducible polynomial dividing $x^{2^m} - x$. Then degree of $g(x)$ divides m.*

Proof: Let d be the degree of $g(x)$. Let $\hat{\mathcal{F}}$ be the quotient field $GF(2)[y]/{<}g(y){>}$. We saw before that the elements of $\hat{\mathcal{F}}$ are precisely the 2^d roots of $x^{2^d} - x$.

Take any element $a(y) \in \hat{\mathcal{F}}$, $a(y) = a_0 + a_1 y + \cdots + a_{d-1} y^{d-1}$ with $a_i \in GF(2)$. Note that each such element is a root of $x^{2^d} - x$, and since there are 2^d such elements, all distinct, these are all the roots of $x^{2^d} - x$ (in $\hat{\mathcal{F}}$). Then, using the fact that in a field of characteristic 2, $(u+v)^2 = u^2 + v^2$ (*Freshman's dream!*), and squaring consecutively we get, in the field $\hat{\mathcal{F}}$,

$$\begin{gathered}(a(y))^2 = a_0 + a_1 y^2 + \cdots + a_{d-1} y^{2(d-1)} = a(y^2) \\ \vdots \\ (a(y))^{2^m} = a(y^{2^m}) \overset{(a)}{=} a(y) \ ,\end{gathered}$$

where (a) is because $y^{2^m} = y$ modulo $g(y)$, from the hypothesis that $g(x)$ divides $x^{2^m} - x$, and $g(y) = 0$ in $\hat{\mathcal{F}}$. Thus $a(y)$ also solves $x^{2^m} - x = 0$.
So, in $\hat{\mathcal{F}}$, the roots of $x^{2^d} - x$ also solve $x^{2^m} - x$. This means $(x^{2^d} - x)|(x^{2^m} - x)$. Then by Lemma 1, $d \mid m$. □

Lemma 5 *Let $g(x)$ be any (irreducible) polynomial dividing $x^{2^m} - x$. Then $g(x)^2$ does not divide $x^{2^m} - x$.*

Definition: The *formal derivative*, $\frac{d}{dx}(\cdot)$ of a polynomial in $GF(2)[x]$ is the linear operator defined by:

$$\begin{cases} \frac{d}{dx}(x^{2m}) & \triangleq 0 \\ \frac{d}{dx}(x^{2m+1}) & \triangleq x^{2m} \end{cases}$$

It is easy to verify that the formal derivative has the *chain rule* property, i.e. $\frac{d}{dx}(p(x)q(x)) = p(x)\frac{d}{dx}(q(x)) + q(x)\frac{d}{dx}(p(x))$.

Proof of Lemma 4: Suppose we can write $x^{2^m} - x = (g(x))^2 f(x)$. Then, taking derivatives of both sides, we get:

$$1 = (g(x))^2 \frac{d}{dx}(f(x))$$

(using the chain rule and since $\frac{d}{dx}(g(x)^2) = 0$ in $GF(2)[x]$.)
but this is impossible unless $g(x) = 1$. □

Lemma 6 *Let d be a divisor of m. Then every irreducible polynomial, $g(x)$ of degree d divides $x^{2^m} - x$.*

Proof: Let $\hat{\mathcal{F}} = GF(2)[y]/ < g(y) >$. Then $\hat{\mathcal{F}}$ is a field of size 2^d. We claim that the minimal polynomial of y (viewed as a member of $\hat{\mathcal{F}}$) is $g(x)$. To see this, first notice that $g(y) = 0$ in $\hat{\mathcal{F}}$, so y solves $g(x) = 0$. Further, no polynomial of degree less than d can be solved by y, or else the dimension of $\hat{\mathcal{F}}$ would be less than d.

All the elements of $\hat{\mathcal{F}}$ are roots of $x^{2^d} - x$. In particular y is a root, and so its minimal polynomial, $g(x)$, must divide $x^{2^d} - x$. This is because, if it didn't divide $x^{2^d} - x$ it would have to be relatively prime to it (as polynomials in $GF(2)[x]$), so it would be possible to find polynomials $a(x), b(x) \in GF(2)[x]$ such that $a(x)g(x)+b(x)(x^{2^d}-x) = 1$, but this would lead to a contradiction, because, when this equation is applied to y (in the field $\hat{\mathcal{F}}$) we get the equation $0 = 1$. Now, by Lemma 2 we have $(2^d - 1) \mid (2^m - 1)$, because we assumed that $d \mid m$. Then by Lemma 1, $(x^{2^d-1} - 1) \mid (x^{2^m-1} - 1)$, so $(x^{2^d} - x) \mid (x^{2^m} - x)$. So $g(x)$ divides $x^{2^m} - x$. □

Proof of Theorem 1: Follows directly from Lemmas 3, 4 and 5. □

Proof of Claim II: Let N_d denote the number of irreducible polynomials of degree d. Then, equating the degrees of polynomials in Theorem 1, we get:

$$2^m = \sum_{d|m} d \cdot N_d$$

Then from *Möbius Inversion Formula*:

$$m \cdot N_m = \sum_{d|m} \mu(\frac{m}{d})2^d$$

The right-hand side is nonzero, since it is the sum of distinct powers of 2 with coefficients in $\{-1, 0, 1\}$, with at least one nonzero coefficient corresponding to $d = m$. Thus $N_m > 0$. □

We will prove Claim III in the sequel using the following concept :

Definition: A polynomial, $m(x)$ of degree m is called *primitive* if it is irreducible, and $\min\{t > 0 : m(x)|x^t - 1\} = 2^m - 1$,

and the following two lemmas :

Lemma 7 *The minimal polynomial of a primitive element is primitive.*

Lemma 8 *All the roots of a primitive polynomial are primitive.*

Then we will use all the results we have proved so far to get a deep understanding of the minimal polynomial of any element in any finite field of characteristic 2. This will be provided by the following :

Theorem 2 *Let $\mathcal{F}$ be a field of size 2^m. Given $\alpha \in \mathcal{F}, \alpha \neq 0, 1$, consider $\{\alpha, \alpha^2, \cdots, \alpha^{2^i}\}$:*

- *There exists a smallest integer $d > 0$ such that $\alpha = \alpha^{2^d}$.*
- *d divides m.*
- *The roots of the minimal polynomial of α are precisely $\{\alpha, \alpha^2, \cdots, \alpha^{2^{d-1}}\}$, i.e. the minimal polynomial of α is precisely*

  $$(x - \alpha)(x - \alpha^2) \dots (x - \alpha^{2^{d-1}}) \ .$$

  Note that this is a polynomial of degree d so one consequence is that the degree of the minimal polynomial of any element must divide m. Note also that when we claim that this polynomial is the minimal polynomial of α we are also claiming that its coefficients are in $GF(2)$ (which is not obvious at first sight).

Lemma 1 *Let F be a finite field, $|F| = 2^m$, and $char(F) = 2$. If $\alpha \in F$ is primitive (*i.e. *$ord(\alpha) = 2^m - 1$) its minimal polynomial $m(x)$ is primitive (*i.e. *the smallest t for which $m(x)$ divides $x^t - 1$ is $t = 2^m - 1$).*

Proof:

1. $m(x)$ must divide $x^{2^m-1} - 1$ because if not, since $m(x)$ is irreducible we have $\gcd(m(x), x^{2^m-1} - 1) = 1$, as polynomials in $GF(2)[x]$. So there exist $a(x)$ and $b(x)$ in $GF(2)[x]$ such that $a(x)m(x) + b(x)(x^{2^m-1} - 1) = 1$. Apply this to α, get $0 = 1$. This is a contradiction.
2. $m(x)$ cannot divide $x^t - 1$ for any $t < 2^m - 1$ because if it did, *i.e.* $x^t - 1 = m(x)g(x)$ for some $g(x) \in GF(2)[x]$, plug in α and get $\alpha^t - 1 = 0$, but this means α is not primitive.

□

Lemma 2 *Let $p(x)$ be a primitive polynomial. Then all its roots in F are primitive.*

Proof: Note that $p(x)$ is irreducible, because this is part of the definition of being primitive. Suppose $p(x)$ had a root β which was not primitive, *i.e.* $\beta^t = 1$ for some $t < 2^m - 1$, then either $\gcd(p(x), x^t - 1)$ is some nontrivial divisor of $p(x)$ or it equals $p(x)$. If the former, then $p(x)$ is not irreducible, and this is a contradiction. If the latter, then $p(x)$ divides $x^t - 1$, and we have $t < 2^m - 1$, so this is a contradiction to Lemma 1.

□

Corollary 1 *The number of primitive polynomials in $GF(2)[x]$ of degree m is exactly $\frac{\phi(2^m-1)}{m}$.*

Proof: Every primitive polynomials in $GF(2)[x]$ of degree m shows up exactly once as a factor of $x(x^{2^m-1} - 1)$. There are exactly $\phi(2^m - 1)$ primitive elements in a field of size 2^m and the nonzero elements of F are all roots of $x^{2^m-1} - 1$, so their minimal polynomials are factors of $x^{2^m-1} - 1$. The minimal polynomials of the primitive elements must be primitive and of degree m, and each of the m roots of a primitive polynomial is primitive, so there are exactly $\frac{\phi(2^m-1)}{m}$ primitive polynomials in $GF(2)[x]$ of degree m.

□

Corollary 2 *In particular, for each $m \geq 2$ there is at least one primitive polynomial in $GF(2)[x]$ of degree m.*

Proof: Since $\phi(2^m - 1) > 0$, the result follows from the preceding corollary. Alternately, as we have already proved that a field of size 2^m exists for each $m \geq 1$, and we have already proved that such a field has at least one primitive element, and we have proved that the minimal polynomial of a primitive element is primitive and of degree m, this proves the corollary.

□

4 Proof of III

Given F, $|F| = 2^m$, we saw it has at least one primitive element and, for any primitive element $\alpha \in F$, F can be viewed as $GF(2)[x]/\langle m(x)\rangle$ where $m(x)$ is the minimal polynomial of α (which has degree m, as we saw).

Recall that:

- the nonzero elements of F are all roots of $x^{2^m-1} - 1$
- $$x(x^{2^m-1} - 1) = \prod_{d|m} \prod_{\text{irreducible polynomials } p(x) \text{ of degree } d} p(x)$$
- there are $\phi(t)$ elements of degree t in the field

This means that for *any* primitive polynomial $\tilde{m}(x)$ of degree m, F contains some β (β is primitive) which has $\tilde{m}(x)$ as its minimum polynomial. So F can also be viewed as $GF(2)[x]/\langle\tilde{m}(x)\rangle$.

So for *any* F of size 2^m, it can be viewed as $GF(2)[x]/\langle\tilde{m}(x)\rangle$ for *any* primitive $\tilde{m}(x)$ of degree m. So all such F are "the same" (*i.e.* isomorphic).

5 Final Claim

Given F, $|F| = 2^m$, and given $\alpha \in F$, consider $\alpha, \alpha^2, \alpha^4, \ldots$

1. there will be a smallest d such that $\alpha^{2^d} = \alpha$
2. this $d \mid m$

3. the minimum polynomial of α, say $m(x)$, is precisely $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2^{d-1}})$ (it has degree d and its coefficients are in $GF(2)$). The roots of a given minimal polynomial are said to be *conjugate*. The corresponding powers of the primitive element, thought of as a subset of $0, 1, \ldots, 2^m - 2$, form what is called a *cyclotomic coset modulo* $2^m - 1$.

Proof:

1. Given α with $\mathrm{ord}(\alpha) = n$, consider $\alpha, \alpha^2, \alpha^4, \ldots$ There must be some $k < l$ with $\alpha^{2^k} = \alpha^{2^l}$. So $\alpha^{2^k(2^{l-k}-1)} = 1$ and n divides $2^k(2^{l-k}-1)$. But n is odd, so n divides $2^{l-k}-1$. So $\alpha^{2^{l-k}} = \alpha$ and there is a smallest d such that $\alpha^{2^d} = \alpha$.

2. Write $m = qd + r$ where $0 \le r \le d-1$.

$$\alpha = \alpha^{2^m} = \alpha^{2^{qd}\cdot 2^r} = \underbrace{((\overbrace{(((((\alpha^{2^d})^{2^d})^{\cdots})^{2^d}}^{q\text{ times}})^2)^{\cdots})^2}_{r\text{ outer braces}} = \alpha^{2^r}$$

Since $r < d$, this is a contradiction unless $r = 0$.

3. Let α have minimum polynomial $m(x) = x^j + a_{j-1}x^{j-1} + \cdots + a_0$ where $a_0, \ldots, a_{j-1} \in GF(2)$. We claim $\alpha^2, \alpha^4, \ldots, \alpha^{2^{d-1}}$ are also roots of $m(x)$ (because $(u+v)^2 = u^2 + v^2$ in char 2). To see this

$$m(\alpha^2) = (\alpha^2)^j + a_{j-1}(\alpha^2)^{j-1} + \cdots + a_0 = (m(\alpha))^2 = 0$$

But we see that $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2^{d-1}})$ is in $GF(2)[x]$. So this must be the minimum polynomial.

Why? Its coefficients are the elementary symmetric functions in $\alpha_0 = \alpha, \alpha_1 = \alpha^2, \cdots, \alpha_{d-1} = \alpha^{2^{d-1}}$.

i.e.

$$\begin{array}{rl}
\alpha_0 + \alpha_1 + \cdots + \alpha_{d-1} & (\text{coef of } x) \\
\displaystyle\sum_{1 \le i < j \le d} \alpha_i \alpha_j & (\text{coef of } x^2) \\
\displaystyle\sum_{1 \le i_1 < i_2 < i_3 \le d} \alpha_{i_1}\alpha_{i_2}\alpha_{i_3} & (\text{coef of } x^3) \\
& \text{etc.}
\end{array}$$

But

$$\begin{aligned}
(\alpha_0 + \alpha_1 + \cdots + \alpha_{d-1})^2 &= \alpha_0^2 + \cdots + \alpha_{d-1}^2 \\
&= \alpha_1 + \alpha_2 + \cdots + \alpha_{d-1} + \alpha_0 \\
&\text{etc.}
\end{aligned}$$

So the coefficients solve $x^2 = x$. So they must be 0 or 1, *i.e.* in $GF(2)$.

□

6 Examples

In the following, the appendices, page numbers etc. refer to the book of Wicker.

Note that in the text we have :

- Appendix A: primitive polynomials of different degrees
- Appendix C: structure of the minimal polynomials of the element in the fields up to $GF(2^{10})$

Recall the formulas we have proved :

$$N_m = \text{no. of irreducible polynomials of degree } m = \frac{1}{m}\sum_{d|m} \mu\left(\frac{m}{d}\right)2^d$$

$$\text{no. of primitive polynomials of degree } m = \frac{\phi(2^m-1)}{m}$$

- $m = 2$:

  $N_2 = \frac{1}{2}[\mu(2)\cdot 2 + \mu(1)\cdot 2^2] = \frac{1}{2}[-2+4] = \frac{1}{2}\cdot 2 = 1$

  $\frac{\phi(3)}{2} = \frac{2}{2} = 1$

  So there is one irreducible polynomial of degree 2 and this is primitive. This is x^2+x+1.

- $m = 3$:

  $N_3 = \frac{1}{3}[\mu(3)\cdot 2 + \mu(1)\cdot 2^3] = \frac{1}{3}[-2+8] = \frac{1}{3}\cdot 6 = 2$

  $\frac{\phi(7)}{3} = \frac{6}{3} = 2$

  So there are two irreducible polynomials of degree 3 and both are primitive. These are x^3+x+1 and x^3+x^2+1.

  To construct $GF(8)$ just write $\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$.

  Appendix C (on pg. 476) lists under “modulo 7”

  $$\begin{aligned}&\{0\},\\&\{1,2,4\},\{3,5,6\}\end{aligned}$$

  This is telling you that the factors of x^7-1 are

  $$\begin{aligned}(x-\alpha^0) &= (x-1)\\(x-\alpha)(x-\alpha^2)(x-\alpha^4) &= x^3+(\alpha+\alpha^2+\alpha^4)x^2+(\alpha^3+\alpha^5+\alpha^6)x+1\\(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) &= x^3+(\alpha^3+\alpha^5+\alpha^6)x^2+(\alpha+\alpha^2+\alpha^4)x+1\end{aligned}$$

  If we choose to interpret α as a root of the primitive polynomial x^3+x+1, this corresponds to setting $\alpha+\alpha^2+\alpha^4 = 0$ and $\alpha^3+\alpha^5+\alpha^6 = 1$, and this tells you how to add : $\alpha^3 = \alpha+1$. Alternatively, we could choose to interpret α as a root of the primitive polynomial x^3+x^2+1, which would mean setting $\alpha+\alpha^2+\alpha^4 = 1$ and $\alpha^3+\alpha^5+\alpha^6 = 1$ and now we add using $\alpha^3 = \alpha^2+1$

- $m = 4$:

  $N_4 = \frac{1}{4}[\mu(4) \cdot 2 + \mu(2) \cdot 2^2 + \mu(1) \cdot 2^4] = \frac{1}{4}[0 - 4 + 16] = \frac{1}{4} \cdot 12 = 3$

  $\frac{\phi(15)}{4} = \frac{8}{4} = 2$

  So there are three irreducible polynomials of degree 3, only two of which are primitive. $GF(16)$ can be constructed as $GF(2)[x]/\langle m(x) \rangle$ for any one of the *three* irreducible polynomials, but if we want to think of $GF(16)$ as $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, then α has to be primitive, so the minimal polynomial of α must be one of the *two* primitive polynomials.

$x^4 + x + 1$ and $x^4 + x^3 + 1$	are irreducible and primitive
$x^4 + x^3 + x^2 + x + 1$	is irreducible but not primitive

  Here is how we see that $x^4+x^3+x^2+x+1$ is irreducible. It has no roots in $GF(2)$, so if it were reducible we could write it as $(x^2+ax+1)(x^2+bx+1) = x^4+(a+b)x^3+(ab)x^2+(a+b)x+1$. This means $ab = 1$ and $a + b = 1$. This is impossible.

  $x^4 + x^3 + x^2 + x + 1$ is not primitive because it divides $x^5 - 1$ (*i.e.* $x^t - 1$ for $t < 15$).

  Appendix A (on pg. 445) lists under "4"

  10011
  11001

  This tells us the primitive polynomials of degree 4 : $x^4 + x + 1$ and $x^4 + x^3 + 1$

  Appendix C (on pg. 477) lists under "modulo 15"

  $\{0\}$,
  $\{5, 10\}$
  $\{1, 2, 4, 8\}, \{3, 6, 9, 12\}, \{7, 11, 13, 14\}$

  Where do these come from? We can actually construct them by hand. For example, in which list does α^7 belong? We can just write $\{\alpha^7, \alpha^{14}, \alpha^{13}(= \alpha^{28}), \alpha^{11}(= \alpha^{26})\}$.

  This means for $GF(16) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ the factors of $x^{15} - 1$ are

  $$\begin{array}{rcl} (x-1) & & \\ (x-\alpha^5)(x-\alpha^{10}) & \Rightarrow & \text{corresponds to } x^2+x+1 \\ (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) & \Rightarrow & \text{corresponds to } x^4+x+1 \text{ or } x^4+x^3+1 \\ (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) & \Rightarrow & \text{corresponds to } x^4+x^3+x^2+x+1 \\ (x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14}) & \Rightarrow & \text{corresponds to the other irreducible polynomial of degree 4.} \end{array}$$

- $m = 5$:

  $N_5 = \frac{1}{5}[\mu(5) \cdot 2 + \mu(1) \cdot 2^5] = \frac{1}{5}[-2 + 32] = \frac{1}{5} \cdot 30 = 6$

$\frac{\phi(31)}{5} = \frac{30}{5} = 6$

Thus there are 6 irreducible polynomials of degree 5, and they are all primitive. These are listed in Appendix A on page 445 of the text, where one reads, under "5",

$$\begin{array}{c} 100101 \\ 101001 \\ 101111 \\ 110111 \\ 111011 \\ 111101 \end{array}$$

This tells us the primitive polynomials of degree 5 : x^5+x^2+1, x^5+x^3+1, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, and $x^5+x^4+x^3+x^2+1$.

Appendix C (on pg. 477) lists under "modulo 31"

$$\begin{array}{l} \{0\}, \\ \{1,2,4,8,16\} \\ \{3,6,12,17,24\} \\ \{5,9,10,18,20\} \\ \{7,14,19,25,28\} \\ \{11,13,21,22,26\} \\ \{15,23,27,29,30\} \end{array}$$

This is a list that you could have generated yourself, as discussed earlier. This tells us the factorization of $x^{31}-1$: the factors are $x-1$ and the six irreducible polynomials of degree 5. $GF(32)$ can be viewed as :

$$\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{30}\} \ ,$$

and any root of any of the six irreducible polynomials of degree 5 could be taken to be α. How to add depends on this choice.