ELEC 6131: Error Detecting and Correcting Codes

Instructor:
Dr. M. R. Soleymani, Office: EV-5.125, Telephone: 848-2424 ext: 4103.
Time and Place: Tuesday, 17:45 – 20:15.
Office Hours: Tuesday, 15:00 – 17:00

LECTURE 2: Introduction to Algebra

Sets and Operations

- You are certainly familiar with the concept of "set".
- A set is a "shapeless" ensemble of objects. What gives shape (structure) to a set is a relationship between its elements or an operation transforming elements of the set to each other.
- A "binary" operation (it does not have anything to do with zero and one) is an operation that takes two elements (that is why it is called binary) and gives another element.
- Addition or multiplication are operations defined for the set of integers, reals, and rational numbers.

Sets and Operations

- A set is said to be closed under an operation if the result of applying the operation to two elements of the set results in an element in the set.
- Take a set G with operation $*$. We say G is closed under $*$ if:
  - for any $a, b \in G$ we have $a * b \in G$.
- **Example:** the set of positive integers is closed under addition but not closed under subtraction.
- **Example:** the set of integers is closed under multiplication but not under division.

Groups

- Definition: a set G with a binary operation * is a group if the set is closed under * and:

1. The binary operation is associative:

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

i.e., no need for parentheses.

2. G contains an element e such that:

$$\text{for all } a \rightarrow a * e = e * a = a$$

3. For any element $a \in G$ there is $a' \in G$ such that $a * a' = a' * a = e$.

a' is called the inverse of a.

Groups

- **Theorem:** the identity element of a group G is unique.
- **Proof:** assume that G has two identities, say e and $\hat{e}$. Then,

$$\hat{e} = \hat{e} * e = e.$$

- **Theorem:** the inverse of an element of group is unique.
- **Proof:** assume that $a \in G$ has two inverses a' and $a^{"}$. Then,

$$a' = a' * e = a' * \left(a * a^{"}\right) = (a' * a) * a^{"} = e * a^{"} = a^{"}.$$

Groups

- **Example:** the set of integers with operation + forms a group. The identity element is zero.
- **Example:** the set of integers with multiplication is not a group. Why?
- **Question:** is the set of rational numbers with multiplication a group? If not, what should we do to form a group under multiplication?

Finite Groups

- Take a set consisting of 5 elements, $G=\{0,1,2,3,4\}$. It is obvious that under addition (usual addition) this is not a group.
- For one thing it is not even closed under addition. For example, $3+2=5 \notin G$. Secondly, there is no way we can define inverse.
- To find an operation that when applied to G makes it a group, we can use addition followed by some “truncation” or in proper terms make “modulo” operation. This means to divide the result of ordinary addition by 5 and take the remainder as the modulo-5 sum.

Finite Groups

Modulo 5 addition:

$\boxplus_5$	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

Additive Groups

- In general, for $\boldsymbol{G}=\{\boldsymbol{0},\boldsymbol{1},\boldsymbol{2},\ldots,\boldsymbol{m}-\boldsymbol{1}\}$ we use modulo-m addition. That is, we divide the result $\boldsymbol{a}+\boldsymbol{b}$ by $\boldsymbol{m}$ and take the remainder $\boldsymbol{r}$ as the modulo-m sum.
- $\boldsymbol{G}=\{\boldsymbol{0},\boldsymbol{1},\boldsymbol{2},\ldots,\boldsymbol{m}-\boldsymbol{1}\}$ forms a group under modulo-m addition:
  - a. First of all, when we divide $a+b$ by m we get $a+b=mq+r$, where $0\le r\le m-1$. That is $r=a\boxplus b\in G$. So, G is closed under $\boxplus$.
  - b. Since the ordinary addition is associative we have $a+b+c=(a+b)+c=a+(b+c)$. Dividing $a+b+c$ by m, we get $a+b+c=qm+r$ with $0\le r<m$. Dividing $a+b$ by m, we get $a+b=q_1m+r_1$, where again $0\le r_1<m$. So $a\boxplus b$=r_1. Dividing r_1+c by m, we get

$$r_1+c=q_2m+r_2,\qquad 0\le r_2<m$$

- So $r_1\boxplus c=r_2$ and $(a\boxplus b)\boxplus c=r_2$. Adding $a+b=q_1m+r_1$ to $r_1+c=q_2m+r_2$, we get

$$a+b+c=(q_1+q_2)m+r_2$$

- Therefore, $(a\boxplus b)\boxplus c=r_2=\mathrm{r}$. We can also show that $a\boxplus(b\boxplus c)=\mathrm{r}$. Hence, $(a\boxplus b)\boxplus c=a\boxplus(b\boxplus c)$. That is modulo-m addition is associative.

Additive Groups

- c. 0 is the identity element since $0 \boxplus a = a \boxplus 0 = a$ for any $a \in G$.
- d. $a + (m - a) = m$ so $a \boxplus (m - a) = 0$. Therefore, $m - a$ is the inverse of a and since $0 \leq m - a \leq m - 1$, we can say that each element of G has an inverse.
- This is called an additive group.

Multiplicative Groups

- Let p be a prime. The set $G = \{1, 2, \dots, p-1\}$ under modulo-p multiplication $\boxdot$ form a group.
- $a \boxdot b$ is defined as the remainder of dividing the real multiplication result of $a \cdot b$ by p. Since $a \cdot b = qp + r$ for $0 < r < p$, the set G is closed under $\boxdot$.
- It is easy to show that $\boxdot$ is also commutative, associative, and the identity element is 1.
- Take $i \in G$. It is clear that since p is a prime, i and p are mutually prime and we can find a and b such that $a \cdot i + b \cdot p = 1$ or $a \cdot i = -b \cdot p + 1$. That is $a \boxdot i = i \boxdot a = 1$ for $i \in G$. For $i \notin G$, then we divide a by p to get $a = q \cdot p + r$ and r is the inverse of i since:
  - $a \cdot i = (q \cdot p + r)i = -b \cdot p + 1 \rightarrow r \cdot i = -(b + qi)p + 1$

Multiplicative Groups

Modulo 5 Multiplication

$\odot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Sub-groups

- A subset of G say H is said to be a sub-group of the group G if it is group under the group operation (of group G).
- 1) first of all, H has to be closed under the operation $*$.
- 2) secondly, any element of H should have an inverse with respect to $*$ that is in H.
- There is no need for checking other two properties since for $a \in H$ we have its inverse $a' \in H$ and therefore, $a * a' = e \in H$ (due to H being closed under $*$).
- Also, since elements of H are also elements of G, associative property holds automatically. So, we have:
- **Theorem 3:** Let G be a group under $*$ and let $H \subset G$. Then H is a subgroup of G iff:
- i) H is closed under $*$
- ii) for any $a \in H$, $a' \in H$ where a' is the inverse of a.

Sub-groups

- **Example:** The set of integers Z is a group under + (real addition).

a) set of even numbers is a subgroup of Z.

b) the set of odd numbers is not a subgroup of Z.

- **Definition:** let H be a subgroup of the group G. let a be an element of G.

- the set of elements $a * H = \{a * h : h \in H\}$ is called the **left coset** of H.
- the set of elements $H * a = \{h * a : h \in H\}$ is the **right coset** of H.

- If the group G is commutative (Abelian), then every left coset $a * H$ is identical to the right coset $H * a$. We refer to them as just cosets.

- The importance of the notation of coset is that cosets of a subgroup partition the elements of the original group. That is, they divide the elements of the original group into non-overlapping sets. The following theorems show this.

Sub-groups

- **Theorem 4:** Let H be a subgroup of a group G with operation $*$. No two elements of a coset of H are identical.

- **Proof:** consider the coset $a * H = \{a * h : h \in H\}$. Assume that two elements of $a * H$ say $a * h_1$ and $a * h_2$ are identical, where $h_1 \neq h_2$. Let a^{-1} be the inverse of a. Then,

$$a^{-1} * (a * h_1) = a^{-1} * (a * h_2)$$

or

:

$$(a^{-1} * a) * h_1 = (a^{-1} * a) * h_2$$

$$e * h_1 = e * h_2 \;\Rightarrow\; h_1 = h_2 \;\Rightarrow \text{ contradiction.}$$

Sub-groups

- **Theorem 5:** two different cosets are disjoint. That is, no two elements in two different cosets of a subgroup H of the group G are identical.
- **Proof:** let $a * H$ and $b * H$ be two different cosets of H with $a \in G$ and $b \in G$. Let $a * h_1$ and $b * h_2$ be two elements in $a * H$ and $b * H$, respectively. Assume that $a * h_1 = b * h_2$. Denote the inverse of h_1 by ${h_1}^{-1}$. Then,

$$(a * h_1) * {h_1}^{-1} = (b * h_2) * {h_1}^{-1}$$
$$\Rightarrow a * (h_1 * {h_1}^{-1}) = b * (h_2 * {h_1}^{-1}) \Rightarrow a * e = b * h_3$$
$$\Rightarrow a = b * h_3, \text{ where } h_3 = h_2 * {h_1}^{-1}.$$

- Now,

$$a = b * h_3 \;\Rightarrow\; a * H = (b * h_3) * H$$
$$= \{(b * h_3) * h : h \in H\} = \{b * (h * h_3) : h_3 \in H\}$$
$$= \{b * h_4 : h_4 \in H\} = b * H \Rightarrow \text{contradiction.}$$

- **Theorem 6 (Lagrange's theorem):** let G be a finite group of order n and let H be a subgroup of order m. Then, m divides n and the partition G/H consists of $\frac{n}{m}$ cosets of H.
- **Proof:** due to Theorem 4, every coset of H consists of m elements of G. Let i be the number of cosets of H. Then, we have $n = i \cdot m$. Therefore, m divides n and $i = \frac{n}{m}$.

Fields

- A field is a set with two operations. These two operations can be called addition and multiplication. However, they do not need necessarily be identical to real addition and real multiplication as is the case in real field (set of real numbers under normal addition and multiplication).
- A field is roughly speaking a set of elements with two operations such that performing these two operations and their inverse we do not leave the set. In another word, the set is closed under two operations and their inverse.
- **Example:** the set of real numbers $\mathbb{R}$ under addition (and its inverse subtraction) and multiplication (also division) form a field.

Definition of a Field

- Let F be a set of elements. Let two operations "addition (+)" and "multiplication ($\cdot$)" be defined on elements of F. The set F together with + and . is a field if:
  - i) F is a commutative (Abelian) group under +. The identity element under + is called "zero element" or "additive identity".
  - ii) the set of non-zero elements of F form a commutative group under multiplication. The identity element with respect to $\cdot$ is called "unit element" or "multiplicative element". It is denoted by 1.
  - iii) multiplication is distributive with respect to addition. That is, for $a, b, c \in F$, we have:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Properties of Fields

- **Property I:** for every element $a \in F$, we have:

$$a \cdot 0 = 0 \cdot a = 0.$$

- **Proof:**

$$a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0 \qquad \text{(add } -a \text{ to both sides)}$$

$$-a + a = -a + a + a \cdot 0$$

$$\Rightarrow 0 = 0 + a \cdot 0 \Rightarrow a \cdot 0 = 0$$

- **Property II:** for $a \neq 0$ and $b \neq 0$, $a, b \in F$, we have $a \cdot b \neq 0$.
- **Proof:** since the set of non-zero elements of F is closed under multiplication, $a \cdot b \neq 0$.
- **Property III:** $a \cdot b = 0$ and $a \neq 0 \Rightarrow b = 0$.
- **Proof:** Direct consequence of II. Since if $b \neq 0$, then $a \cdot b \neq 0$.

Properties of Fields

- **Property IV:** for any two elements a and b of F, we have:

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$$

- **Proof:**

$$0 = 0 \cdot b = \big(a + (-a)\big) \cdot b = a \cdot b + (-a) \cdot b$$

So, $(-a) \cdot b$ is the additive inverse of $a \cdot b$, i.e., $-(a \cdot b) = (-a) \cdot b$.

Similarly, we can show $-(a \cdot b) = a \cdot (-b)$.

- **Property V:** for $a \neq 0$, $a \cdot b = a \cdot c \Rightarrow b = c$.

- **Proof:** let multiplication inverse of a be a^{-1}. Multiply both sides of $a \cdot b = a \cdot c$ by a^{-1}

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) \Rightarrow (a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$$

$$\Rightarrow 1 \cdot b = 1 \cdot c \Rightarrow b = c$$

Examples of Fields

Example: consider the set {0, 1} with modulo-2 addition:

+	0	1
0	0	1
1	1	0

and modulo-2 multiplication:

·	0	1
0	0	0
1	0	1

This is called the Galois Field and is denoted by GF(2).

Example: let p be a prime. The set $\{0, 1, 2, \cdots, p-1\}$ forms a commutative group under multiplication modulo-p.
Using the fact that real multiplication is distributive over real addition, we can easily show that modulo-p multiplication is distributive over modulo-p addition. So, the set $\{0, 1, 2, \cdots, p-1\}$ is a field of order p under modulo-p multiplication and addition. It is called a prime field since p is a prime. GF(2) is a special case of prime field for $p=2$.

Some properties of finite fields:

Take the finite field with q elements, say GF(q). Let's add 1 to itself to get the following sums:

$$\sum_{i=1}^{1} 1 = 1 \quad , \qquad \sum_{i=1}^{2} 1 = 1 + 1 \quad , \qquad \sum_{i=1}^{3} 1 = 1 + 1 + 1 \quad , \cdots$$

$$\sum_{i=1}^{k} 1 = 1 + 1 + \cdots + 1 \qquad k \text{ times}$$

Since the field is finite, all these sums cannot belong to it and be different. Since the field is closed under +, these sums have to belong to GF(q). So, they cannot be all different. Hence, for some $m < n$, we should have:

$$\sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1 \;\Rightarrow\; \sum_{i=1}^{n-m} 1 = 0.$$

So, there is a smallest number λ that $\sum_{i=1}^{\lambda} 1 = 0$. The number λ is called the characteristic of GF(q).

Some properties of finite fields:

Theorem 7: the characteristic λ of a finite field is prime.

Proof: assume that λ is not a prime. Therefore, $\lambda = km$ for integers k and m which are smaller than λ. Since the field is closed under multiplication,

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i=1}^{m} 1\right) \in GF(q).$$

From the distributive law, we have,

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

But since $\sum_{i=1}^{km} 1 = \sum_{i=1}^{\lambda} 1 = 0$, either $\sum_{i=1}^{k} 1$ or $\sum_{i=1}^{m} 1$ should be equal to zero. It contradicts the fact that λ is the smallest number such that $\sum_{i=1}^{\lambda} 1 = 0$.

Some properties of finite fields:

For any two integers k and $m < \lambda$ we have, $\sum_{i=1}^{k} 1 \neq \sum_{i=1}^{m} 1$. This is true since if $\sum_{i=1}^{k} 1 = \sum_{i=1}^{m} 1$, then $\sum_{i=1}^{m-k} 1 = 0$. But $m - k < \lambda$ and this contradicts the fact that λ is the characteristic of the field. So, the sums

$$1 = \sum_{i=1}^{1} 1, \sum_{i=1}^{2} 1, \sum_{i=1}^{3} 1, \cdots, \sum_{i=1}^{\lambda} 1 = 0$$

are λ distinct elements of $GF(q)$. This set of sums a subset of $GF(q)$ is itself a field under $+$ and $\cdot$ and is denoted by $GF(\lambda)$. It is a subfield of $GF(q)$.

Therefore, any finite field of q elements with characteristic λ has a subfield of λ elements. It can be proved that if $q \neq \lambda$, then q is a power of λ.

Some properties of finite fields:

Now, let's see how multiplication works when applied repeatedly. Take an element of the field say a

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

Since $GF(q)$ has a finite number of elements and also it is closed under multiplication, these products have to belong to $GF(q)$ and therefore, cannot be distinct. So, there must be some $k < m$ such that,

$$a^k = a^m \;\Rightarrow\; a^{m-k} = 1$$

So, there must be a smallest number n such that $a^n = 1$. This number, n, is called the order of the field element a.

Now, the products $a^1, a^2, \cdots, a^{n-1}, a^n = 1$ are all distinct. They form a field with n elements. Firstly, it has the unit element 1. Secondly, considering $a^i \cdot a^j = a^{i+j}$ if $i + j < n$ and $i + j = n + r$ if $i + j > n$ for some $r < n$.

So, $a^i \cdot a^j = a^{n+r} = a^n \cdot a^r = 1 \cdot a^r = a^r \in$ field of n elements. Also, $a^i \cdot a^{n-i} = a^n = 1$ so a^{n-i} is the inverse of a^i. The properties of associativity and commutativity are inherited from $GF(q)$. So, $a^n = 1, a^1, a^2, \cdots, a^{n-1}$ form a commutative group under multiplication.

A group such as this, i.e., one that has one element whose powers constitute the whole group is called cyclic.

Some properties of finite fields:

Theorem 8: let a be a non-zero element of a finite field $GF(q)$. Then, $a^{q-1} = 1$.

Proof: let $b_1, b_2, \cdots, b_{q-1}$ be the $q-1$ non-zero elements of $GF(q)$. Multiply each by a,

$$a \cdot b_1, a \cdot b_2, \cdots, a \cdot b_{q-1}.$$

These are non-zero and distinct. Multiply them to get

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

$$= b_1 \cdot b_2 \cdot \cdots \cdot b_{q-1}$$

$$\Rightarrow \quad a^{q-1} = 1$$

Theorem 9: let a be a non-zero element of $GF(q)$. The order of a, say n, divides $q-1$.

Proof: suppose n does not divide $q-1$. Then, $q-1 = k \cdot n + r$ for some $0 < r < n$. Then, $a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r = (a^n)^k \cdot a^r$. But $a^{q-1} = 1$ and $a^n = 1$. Therefore, $a^r = 1$. This contradicts the assumption that n is the order of a since $r < a$.

In a finite field $GF(q)$, a non-zero element is called primitive if its order is $q-1$. It is clear that powers of a primitive element generate all the non-zero elements of $GF(q)$.

Every finite field has a primitive element.

Some properties of finite fields:

Example: take $GF(7)$ with modulo-7 operations:

+	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

and

·	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

Take element 3

$$3^1 = 3, \qquad 3^2 = 3 \cdot 3 = 2, \qquad 3^3 = 6, \qquad 3^4 = 4, \qquad 3^5 = 5, \qquad 3^6 = 1.$$

So, 3 is a primitive element of $GF(7)$. But take 4,

$$4^1 = 4, \qquad 4^2 = 4 \cdot 4 = 2, \qquad 4^3 = 4 \cdot 4^2 = 1.$$

So, order of 4 is 3.

Some properties of finite fields:

Binary field:

Recall that we said (showed) that a finite field with q elements only exists when q is prime or it is a power of a prime. So, we have $GF(q)$ or $GF(q^m)$. The smallest prime is 2 and we saw that $GF(2)$ with respect to modulo-2 addition (in digital electronic and logic you may have seen it as exclusive OR: XOR) and modulo-2 multiplication (AND in digital logic) form a field.

In fact, this is the field that we will be most interested in (also its extended field $G(2^m)$) in this course.

$GF(2)$ has elements 0 and 1. Addition is performed modulo-2 that is 0+1=1, 1+1=0, and 1+1+1=1, etc. any equation relating variables in this field has coefficient 0 or 1. For example, $X + Y + Z = 1$. We do not have terms such as $2X$, $3Y$ etc, since $2X = X + X = 0$ and $3Y = Y + Y + Y = Y$.

Binary Field:

- Recall that we said (showed) that a finite field with q elements only exists when q is prime or it is a power of a prime. So, we have $GF(q)$ or $GF(q^m)$.
- The smallest prime is 2 and we saw that $GF(2)$ with respect to modulo-2 addition (in digital electronic and logic you may have seen it as exclusive OR: XOR) and modulo-2 multiplication (AND in digital logic) form a field.
- In fact, this is the field that we will be most interested in (also its extended field $G(2^m)$) in this course.
- $GF(2)$ has elements 0 and 1. Addition is performed modulo-2 that is 0+1=1, 1+1=0, and 1+1+1=1, etc. any equation relating variables in this field has coefficient 0 or 1.
- For example, $X + Y + Z = 1$. We do not have terms such as $2X$, $3Y$ etc, since $2X = X + X = 0$ and $3Y = Y + Y + Y = Y$.

Polynomials over $GF(2)$

Assume that you have a binary number $f = f_n f_{n-1} \cdots f_0$ written in a shift register. To find the value of f in decimal you add f_0 to $2f_1, 4f_2, \cdots$. That is,

$$f = f_0 + f_1 \cdot 2 + f_2 \cdot 2^2 + f_3 \cdot 2^3 + \cdots + f_n \cdot 2^n.$$

2 in fact is the shift operation in a shift register. Replacing 2 by a generic variable X, we get a polynomial in X with binary coefficients

$$f(X) = f_0 + f_1 X + f_2 X^2 + f_3 X^3 + \cdots + f_n X^n.$$

The largest power of X with non-zero coefficient is the degree of the polynomial. In $f(X)$ above if $f_n \neq 0$, then $f(X)$ has degree n. If we have $f_i = 0, i \geq 1$, then $f(X) = f_0$, i.e., it is constant function with degree zero. If $f_1 \neq 0$, but $f_i = 0$ for $i \geq 2$, then we have a polynomial of degree one:

$$f(X) = f_0 + f_1 X.$$

So, we have <u>two</u> degree one functions X and $1 + X$. For 2, we have four functions X^2, $1 + X^2$, $X + X^2$, and $1 + X + X^2$. In general, we have 2^n functions of degree n over $GF(2)$.

Addition and multiplication of Polynomials

Adding $f(X) = f_0 + f_1X + f_2X^2 + f_3X^3 + \cdots + f_nX^n$ to $g(X) = g_0 + g_1X + \cdots + f_mX^m \;\; m \leq n$ we get

$$f(X) + \; g(X) = (f_0 + g_0) + (f_1 + g_1)X + \cdots + (f_m + g_m)X^m + \cdots + f_nX^n.$$

For example, if $f(X) = 1 + X + X^3 + X^5$ and $g(X) = 1 + X^2 + X^3 + X^4 + X^7$, then

$$f(X) + \; g(X) = X + X^2 + X^4 + X^5 + X^7.$$

Multiplying $f(X)$ by $g(X)$ we get

$$f(X) \cdot \; g(X) = [f_0 + f_1X + f_2X^2 + f_3X^3 + \cdots + f_nX^n] \cdot [g_0 + g_1X + \cdots + f_mX^m]$$

$$= f_0g_0 + (f_0g_1 + g_0f_1)X + (f_0g_2 + f_1g_1 + f_2g_0)X^2 + \cdots + (f_0g_i + f_1g_{i-1} + \cdots + f_ig_0)X^i + \cdots + f_ng_mX^{n+m}.$$

Properties of polynomial operations over $GF(2)$

i) commutativity:

$$a(X) + b(X) = b(X) + a(X) \text{ and}$$

$$a(X) \cdot b(X) = b(X) \cdot a(X)$$

ii) associativity:

$$a(X) + [b(X) + c(X)] = [a(X) + b(X)] + c(X) \text{ and}$$

$$a(X) \cdot [b(X) \cdot c(X)] = [a(X) \cdot b(X)] \cdot c(X)$$

iii) distributivity of $\cdot$ over $+$:

$$a(X) \cdot [b(X) + c(X)] = a(X) \cdot b(X) + a(X) \cdot c(X).$$

Division of Polynomials

Dividing $f(X)$ by $g(X)$ we either get a remainder zero and say $g(X)$ divides $f(X)$ or we get a function $r(X)$ with degree less than that of $g(X)$. That is

$$f(X) = q(X) \cdot g(X) + r(X)$$

and $q(X)$ is called the quotient.

Example 1: Let's divide $f(X) = 1 + X + X^4 + X^5 + X^6$ by $g(X) = 1 + X + X^3$.

$$X^3 + X^2 = q(X)$$

$$X^3 + X + 1 \overline{)X^6 + X^5 + X^4 + X + 1}$$

$$X^6 + X^4 + X^3$$

$$\overline{X^5 + X^3 + X + 1}$$

$$X^5 + X^3 + X^2$$

$$\overline{X^2 + X + 1} = r(X)$$

So, $X^6 + X^5 + X^4 + X + 1 = (X^3 + X^2)(X^3 + X + 1) + X^2 + X + 1$.

Division of Polynomials

Example 2: Now, let's divide $f(X) = X^4 + X^3 + X^2 + 1$ by $X + 1$. What do you expect to get as remainder?
Let's see:

$$
\begin{array}{r}
X^3 + X + 1 \\
\hline
X + 1 \overline{)X^4 + X^3 + X^2 + 1} \\
X^4 + X^3 \\
\hline
X^2 + 1 \\
X^2 + X \\
\hline
X + 1 \\
X + 1 \\
\hline
0
\end{array}
$$

Could we have found out that $f(X)$ is dividable by $X + 1$ without doing the division?

Note that $X + 1 = 0 \Rightarrow X = 1$. Now, let $X = 1$ in $f(X)$.

$$f(1) = 1 + 1^2 + 1^3 + 1^4 = 1 + 1 + 1 + 1 = 0.$$

So, $X = 1$ is a root of $f(X)$ and therefore, it is divisible by $X + 1$.

Irreducible Polynomials

Definition: a polynomial is called irreducible if it is not divisible by any polynomial.

If the degree of $f(X)$ is n, we only need to check those with degrees in the range of 1 to $n-1$, i.e., $0 < k < n$.

Take the polynomial of degree 2, i.e.,

$$X^2,\ \ X^2+1,\ \ X^2+X, \text{and}\ \ X^2+X+1.$$

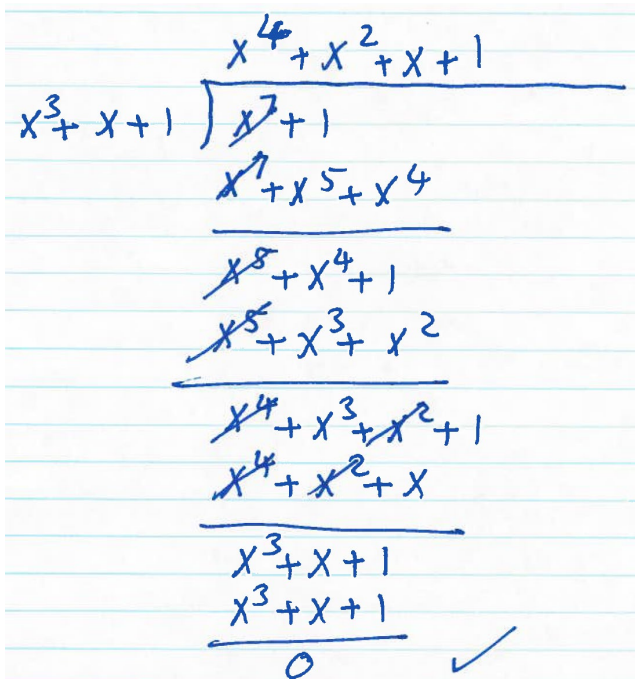
Only the last function X^2+X+1 is irreducible. The others have roots 1 or 0 and therefore, are divisible by X or $1+X$.

Theorem 10: any irreducible polynomial of degree m divides $X^{2^m-1}+1$.

Example: the polynomial $f(X)=X^3+X+1$ is irreducible since $f(0)=f(1)=1$ and therefore, it is not divisible by X and $X+1$. Note that we do not check for polynomials of degree 2 (why?).

According to Theorem 10, X^3+X+1 should divide $X^{2^3-1}+1=X^7+1$. Let's verify:

Primitive Polynomials



Definition: an irreducible polynomial $p(X)$ of degree m is called primitive if the smallest positive integer n for which $p(X)$ divides $X^n + 1$ is $n = 2^m - 1$.

Example: recall the example of $f(X) = X^2 + X + 1$ with degree 2. We showed that it is irreducible. We can see that the smallest n for which $f(X)$ divides $X^n + 1$ is $n = 2^m - 1 = 2^2 - 1 = 3$. So, $f(X) = X^2 + X + 1$ is a primitive polynomial.

$GF(4)$ or $GF(2^2)$ field:

We said that if q is a prime or power of a prime, then we can have a field $GF(q)$. It is obvious that we cannot form a field over integers 0, 1, 2, 3 with modulo-4 addition and multiplication due to the fact that 4 is not a prime and 1, 2, 3 cannot form a group under modulo-4 multiplication. So, we choose elements of $GF(4)$ as polynomials. Since the field will have only 3 non-zero elements, if we take an element α of it and form:

$$\alpha^0 = 1, \qquad \alpha^1 = \alpha, \qquad \alpha^2 = \alpha \cdot \alpha, \qquad \alpha^3 = \alpha \cdot \alpha^2, \ldots$$

so all these powers of α have to collapse into 3. This means that $\alpha^3 = \alpha \cdot \alpha^2$ has to be one of the non-zero elements $1, \alpha, \alpha^2$.

Letting $\alpha^3 = \alpha \cdot \alpha^2 = \alpha \Rightarrow \alpha^2 = 1 \Rightarrow$ not even 3 distinct elements.

And $\alpha^3 = \alpha \cdot \alpha^2 = \alpha^2 \Rightarrow \alpha = 1 \Rightarrow$ not a solution either.

Letting $\alpha^3 = \alpha \cdot \alpha^2 = 1 \Rightarrow \alpha^2 = \alpha^{-1}$.

$GF(4)$ or $GF(2^2)$ field:

So, we have the field:

$$GF(2^2) = \{0, 1, \alpha, \alpha^{-1}\} = \{0, 1, \alpha, \alpha^2\}.$$

$\alpha^2 = \alpha^{-1}$ needs to be the sum (modulo addition) of two other members $0 + 0 = 0$, $0 + 1 = 1$, $0 + \alpha = \alpha$, $1 + 1 = 0$, $1 + \alpha$. Among these only $1 + \alpha$ is different from the first three elements of $0, 1, \alpha$. So, we write $GF(2^2) = \{0, 1, \alpha, 1 + \alpha\}$.
That is $\alpha^2 = 1 + \alpha$ or $\alpha^2 + \alpha + 1 = 0$.

Important observation:

Recall that $p(X) = X^2 + X + 1$ is a primitive polynomial. In fact we have used this polynomial to generate $GF(4)$. The procedure is as follows:

Write $p(\alpha) = \alpha^2 + \alpha + 1 = 0$ and get $\alpha^2 = \alpha + 1$. Use this to generate:

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = 1 + \alpha$$

$$\alpha^3 = \alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1$$

etc.

Primitive Polynomials for several values of m:

$GF(4)$ is very important in Quantum Physics and Quantum Coding as they represent four Pauli Matrices $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ or I, X, Y, Z.

Here is a list of some primitive polynomials.

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

List of some primitive polynomials

A Useful Property of Polynomials over GF(2)

A useful property of polynomials over $GF(2)$: $f^2(X) = f(X^2)$. That is if $f(X) = f_0 + f_1X + f_2X^2 + \cdots + f_nX^n$ then, $f^2(X) = f_0 + f_1X^2 + f_2X^4 + \cdots + f_nX^{2n}$.

Proof: for $n = 0 \Rightarrow f(X) = f_0 \Rightarrow f^2(X) = f_0 \cdot f_0 = f_0$ and $f(X^2) = f_0 \Rightarrow f^2(X) = f(X^2)$

Induction step: if $f^2(X) = f(X^2)$ for $f(X) = f_0 + f_1X + \cdots + f_kX^k$ then, it is true for

$g(X) = f_0 + f_1X + \cdots + f_kX^k + f_{k+1}X^{k+1} = f(X) + f_{k+1}X^{k+1}$.

$$g^2(X) = [f(X) + f_{k+1}X^{k+1}]^2$$

$$g^2(X) = f^2(X) + f(X)f_{k+1}X^{k+1} + f(X)f_{k+1}X^{k+1} + f_{k+1}^2X^{2(k+1)}$$

$$= f^2(X) + f_{k+1}X^{2(k+1)}$$

$$= g(X^2).$$

So, since the property is true for $n = 0$, it is true for $n = 1$, and since it is true for $n = 1$, it is true for $n = 2$ and so on.

Constructing GF(2^m)

We saw earlier how to form $GF(4) = GF(2^2)$. Here, we extend the procedure to $GF(2^m)$ for any integer m.

We start with an element α and form:

$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha \cdot \alpha, \alpha^3 = \alpha \cdot \alpha^2, \cdots$. So, we will have the set

$$F = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^j, \cdots\}$$

However, we need to collapse the set somehow to have only 2^m distinct elements.

Take a primitive polynomial $p(X)$ and let $p(\alpha) = 0$. That is, let α be a root of $p(X)$. We know that $p(X)$ divides $X^{2^m-1} + 1$. So, $X^{2^m-1} + 1 = q(X)p(X)$. Let $X = \alpha$ to get $\alpha^{2^m-1} + 1 = q(\alpha)p(\alpha)$. Since $p(\alpha) = 0$, we have $\alpha^{2^m-1} + 1 = 0$ or $\alpha^{2^m-1} = 1$. So, the field will have elements $0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}$. That is,

$$GF(2^m) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$$

Constructing GF(2^m)

Example: $GF(2^4)$

We use the primitive polynomial $p(X) = 1 + X + X^4$. Letting $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, we get $\alpha^4 = \alpha + 1$.

The usefulness of having both polynomial and power representation is that we can use polynomial representation to do modulo-2 addition of bits of a symbol and the power representation performing multiplication using a log and an anti-log table to get the result.

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

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