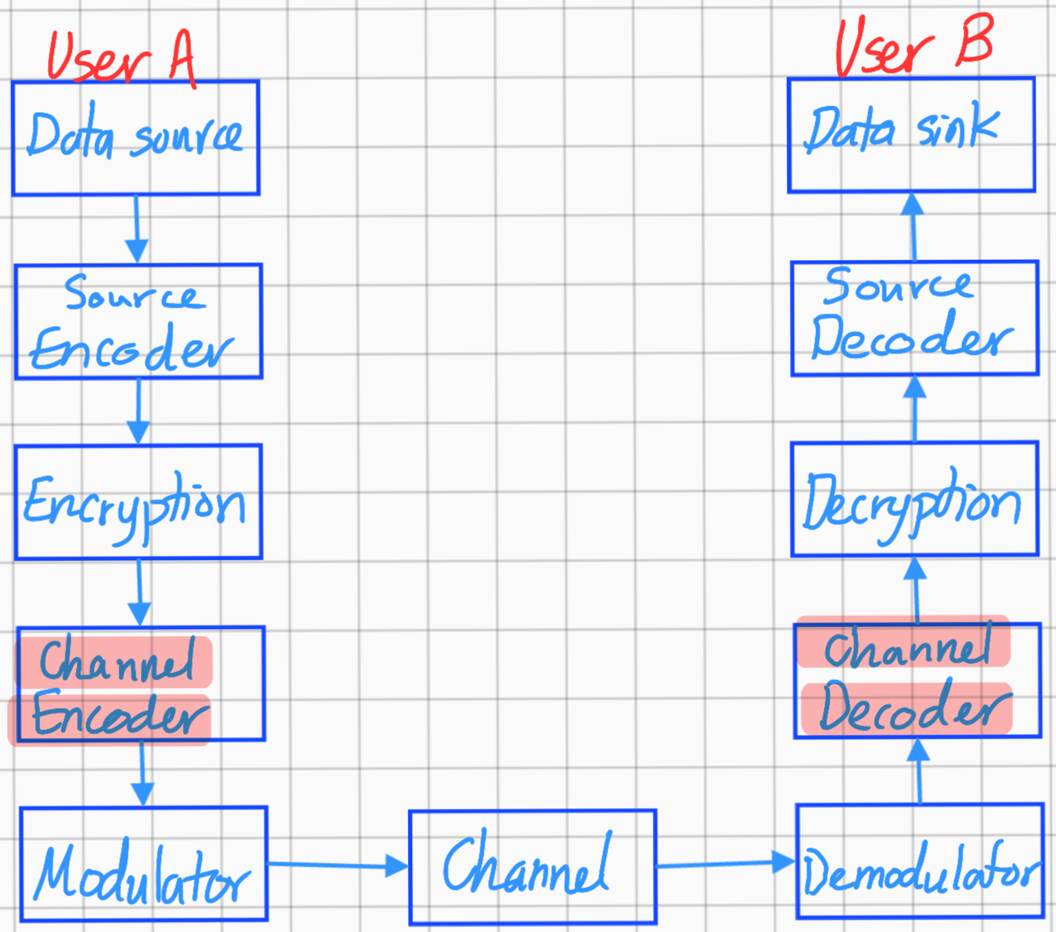
- Error control codes, also called channel codes, are used to format the transmitted information to increase its immunity to noise.
- This is accomplished by inserting controlled redundancy into the transmitted information stream allowing the receiver to detect and possibly correct errors.



- A Single-Error-Detecting Code:

Example: (Parity-Check Code)

For a binary data source, if we break it into k-bit message blocks. We can represent each block as:

$$m = (m_0, m_1, \dots, m_{k-1})$$

We can add a single redundant bit $\underline{b}$ at the end of each block.

The value of $\underline{b}$ is selected so that the binary sum of all the message bits and $\underline{b}$ in each block is zero. Then the transmitted blocks of message bits and redundant bit have the form

$C = (m_0, m_1, \dots, m_{k-1}, b)$ where $b = \sum_{j=0}^{k-1} m_j$

e.g. (a) $m = (1,0,1)$, $\text{sum} = 1+0+1 = 0$, $b = 0$

$\text{sum} + b = 0 + 0 = 0$

(b) $m = (1,1,1)$, $\text{sum} = 1+1+1 = 1$, $b = 1$

$\text{sum} + b = 1 + 1 = 0$

At the receiver, the received blocks are checked by adding bits. If the sum is not zero, then we know that one or an odd number of bits have been corrupted by the channel noise.

- A set is an arbitrary collection of objects or elements, without any predefined operations between set elements.
- Cardinality (card) of a set is defined as the number of distinct elements in the set.
- A binary operation is an operation that can be imposed on a set, along with a set of rules restricting the results of the operation. The binary operation operates on two elements from the set at a time, yielding a third element (not necessarily a distinct element).

- **Groups:**

A group G is a set of objects on which a binary operation "." has been defined. The binary operation must satisfy the following properties for G to be a group:

1. **Closure**: the binary operation takes any two elements in G and generates as its result an element that is also in G.
   i.e. For all $a, b \in G$, $a.b \in G$.

2. **Associativity**:
   $(a.b).c = a.(b.c)$ for all $a, b, c \in G$.
   Note: Since it's a binary operation we can't do $a.b.c$

3. **Identity** :

there exists an element $e \in G$ such that

$a.e = e.a = a$ for all $a \in G$

4. **Inverse** :

For each $a \in G$ there exists a unique element

$a^{-1} \in G$ such that $a.a^{-1} = a^{-1}.a = e$

(Note: e is the identity element under the binary operation)

For special groups :

A group can be commutative (تبديلي) if :

for all $a, b \in G$, $a.b = b.a$

in such case , the group is said to be

a commutative group or an abelian group.

The group operation for a commutative group is usually

represented with "+" symbol (called additive group).

Example: For the set of integers $\mathbb{Z}$ under integer addition, is it a group.

The properties integer addition should satisfy are:

1. Closure: for all $a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$
2. Associativity: for all $a, b, c \in \mathbb{Z}$
   $(a+b)+c = a+(b+c)$
3. Identity: the idenitity element under integer addition is zero, since $0 \in \mathbb{Z}$ such that
   $0+a = a+0 = a$ for all $a \in \mathbb{Z}$
4. Inverse: for each $a \in \mathbb{Z}$ there exists a unique element $-a \in \mathbb{Z}$ such that
   $a+(-a) = (-a)+a = 0$
   where 0 is the idenitity element under addition

As a result, $\mathbb{Z}$ is a group under addition.
Also, this group is commutative since for all $a, b \in \mathbb{Z}$, $a+b = b+a$.
Then the set of integers under integer addition is an infinite commutative group under integer addition.
Note: the set $\mathbb{Z}$ is not a group under integer multiplication since multiplication inverses for integers are not integers.

- **Definition :**

Order of a group is defined as

$|G| = \text{ord}(G) = \text{card}(G) =$ number of distinct elements in G.

- One of the simplest methods for constructing finite groups lies in the application of modular arithmetic to the set of integers.

- **Modular Arithmetic** :

1. Modular Addition
2. Modular Multiplication

1 Modular Addition:

Addition modulo m (or mod m) can be expressed as:

$$a + b \equiv c \bmod m$$

that is: a plus b is equivalent to c mod m.

The result c is obtained by summing a and b using standard integer addition and dividing the result by the modulus m, c is the positive remainder.

Example:

(a) $13 + 18 \equiv 11 \bmod 20$ $(13 + 18 = 31,\ 31 = 20 + 11$

(b) $3 + 8 \equiv 11 \bmod 20$

(c) $9 + 5 \equiv 4 \bmod 10$ $(9 + 5 = 14,\ 14 = 10 + 4)$

(d) $2 + 4 \equiv 0 \bmod 6$ $(2 + 4 = 6,\ 6 = 6 + 0)$

(e) $18 + 27 \equiv 0 \bmod 5$ $(18 + 27 = 45,\ 45 = 5(9) + 0)$

(f) $15 + 100 \equiv 50 \bmod 65$ $(15 + 100 = 115,\ 115 = 65 + 50)$

- Addition mod m groups the infinite set of integers into m distinct equivalence classes.
- For two integers a and b are in the same equivalence class mod m if a can be written as $a = km + b$ for some integer k.
- Elements in the same equivalence class mod m are equivalent, that is any element in a given class can be substituted for any other element in the same class without changing the outcome of a mod m operation
- An equivalence class of integers is labeled with its smallest nonnegative integer element.
- Each number in the same equivalence class differ by some multiple of m.

Example: Equivalence classes of integers under mod2 addition:

We have two equivalence classes,

Label $\leftrightarrow$ Equivalence class

$0 : \{0, \pm 2, \pm 4, \pm 6, \dots\}$, all even numbers

$1 : \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\}$, all odd numbers

Example: Equivalence classes of integers under mod5 addition:

We have 5 equivalence classes,

Label $\leftrightarrow$ Equivalence class

$0 : \{0, \pm 5, \pm 10, \pm 15, \pm 20, \dots\}$

$1 : \{1, 6, 11, 16, \dots; -4, -9, -14, -19, \dots\}$

$2 : \{2, 7, 12, 17, \dots; -3, -8, -13, -18, \dots\}$

$3 : \{3, 8, 13, 18, \dots; -2, -7, -12, -17, \dots\}$

$4 : \{4, 9, 14, 19, \dots; -1, -6, -11, -16, \dots\}$

Example: Equivalence classes of integers under mod 4 addition:

We have 4 equivalence classes,

Label $\leftrightarrow$ Equivalence class

$0 : \{0, \pm 4, \pm 8, \pm 12, \pm 16, \dots\}$

$1 : \{1, 5, 9, 13, 17, \dots; -3, -7, -11, -15, \dots\}$

$2 : \{2, 6, 10, 14, 18, \dots; -2, -6, -10, -14, \dots\}$

$3 : \{3, 7, 11, 15, 19, \dots; -1, -5, -9, -13, \dots\}$

- **Theorem**:

The equivalence classes $\{0, 1, 2, 3, \dots, m-1\}$ form a commutative group of order m under mod m integer addition for any positive integer m.

Proof:

- Since any element in an equivalence class can be substituted by the class's label, then we can consider just the labels, $G = \{0, 1, 2, \dots, m-1\}$, so $\text{ord}(G) = [(m-1) - 0] + 1 = m$.
- For the equivalence classes to form a commutitive group, they have to follow:

1. Closure: For $a, b \in G$, $a + b \equiv c \bmod m$ where $c \in G$ since $c < m$ and is an integer.
2. Associativity: Since integer addition is associative, mod m addition is also associative

3. Identity: the identity element in G is the additive identity zero, $e = 0 \in G$.

4. Inverse: for $a \in G$, there should be an $a^{-1} \in G$ such that $a + a^{-1} = e = 0$.

Since 0 & m are equivalent in the same equivalence class, then $m \equiv 0 \bmod m$.

So $a + a^{-1} = m \Rightarrow a^{-1} = m - a$.

If $a = 0$, then $a^{-1} = m \equiv m \bmod m = 0$ (zero is its own inverse).

If $a \in \{1, 2, 3, \dots, m-1\}$, then $a^{-1} = m - a$,

then $a^{-1} \in \{1, 2, 3, \dots, m-1\}$

Thus, all $a \in G$, there exists $a^{-1} \in G$.

5. Commutative: Since integer addition is commutative, then mod m addition is also commutative.

Example: The group of order 4 under mod 4 addition:

We will show how it is a commutative group:

The operation is shown in the following table:

(mod4) +	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1. Closure: for all $a, b \in G$, $a+b \in G$

2. Associativity: Since integer addition is associative, mod m addition is also associative

3. Identity: the identity element is the additive identity zero, $e=0$. For all $a \in \{0,1,2,3\}$, $a+e=a$.
(We have a zero in every row)

4. Inverse: For each $a \in \{0,1,2,3\}$ there exists a unique element $a^{-1} \in \{0,1,2,3\}$ such that

$a + a^{-1} = 0$.

e.g. $0^{-1} = 0$, $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 1$

5. Commutative: for all $a, b \in G$, $a + b = b + a$

since the addition table is symmetric about the main diagonal.

$\boxed{2}$ Modular Multiplication:

Multiplication mod m can be expressed as:

$$a \cdot b \equiv c \bmod m$$

that is: a times b is equivalent to c mod m.

The result c is obtained by multiplying a and b using standard integer multiplication and dividing the result by the modulus m, c is the positive remainder.

Example:

(a) Under mod 20 : $11 \cdot 5 = 55 \equiv 15 \bmod 20$

(b) Under mod 50 : $9 \cdot 7 = 63 \equiv 13 \bmod 50$

(c) Under mod 2 : $4 \cdot 17 = 68 \equiv 0 \bmod 2$, or since its even

(d) Under mod 18 : $6 \cdot 4 = 24 \equiv 6 \bmod 18$

(e) Under mod 10 : $2 \cdot 5 = 10 \equiv 0 \bmod 10$

(f) Under mod 6 : $6 \cdot 5 = 30 \equiv 0 \bmod 6$

- Modular multiplication does not always form a group under mod m for any integer m.
- For the number zero, it can not be included in a group under a multiplication operation. That is, under multiplication the set has to have multiplicative inverses for each element in the set, and since zero does not have a multiplicative inverse, then zero could not be in a group under multiplication.
- Since zero can not be an element in a group under mod m multiplication, and as $m \bmod m \equiv 0 \bmod m$, the group can not contain any element that divides m with a zero remainder. In such case, if $a \in G$ and the remainder $\text{rem}\left(\frac{m}{a}\right) = 0$, then there exists an element $b \in G$ where $a.b = m \equiv 0 \bmod m$.

Example: For $S=\{1,2,3,4,5,6,7\}$ under mod 8 integer multiplication, is it a group.

Since $4 \cdot 2 = 0 \bmod 8$ and 0 is not in the set, the mod 8 integer multiplication is not closed over S, then it is not a group.

Example: For $S=\{1,2,3,4\}$ under mod5 integer multiplication, is it a group.

The multiplication table is as follows:

(mod5) $\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1. Closure : for all $a, b \in S$, $a.b = c \bmod 5$ where $c \in S$.

2. Associativity : for all $a, b, c \in S$

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

as it follows from integer multiplication

3. Identity : the identity element is 1 since for all $a \in S$, $a.1 = 1.a = a$ (the multiplication identity)

4. Inverse : for all $a \in S$, there exists a unique element $a^{-1} \in S$ such that $a.a^{-1} = a^{-1}.a = 1$ as follows :

$$1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$$

5. Commutative : for all $a, b \in S$, $a.b = b.a \in S$ as it follows from integer multiplication and it is shown in the multiplication table where it is symmetric about the main diagonal.

As a result, S is a commutative group.

- Theorem:

The elements $S = \{1, 2, 3, \cdots, p-1\}$ form a commutative group of order $(p-1)$ under mod p multiplication if and only if p is a prime integer.

Proof:

1. Closure : If p is not a prime, then there exists $a, b \in S$ such that $a \cdot b = p \bmod p \equiv 0 \bmod p$, and since 0 is not in S, then S is not closed if p is not a prime. If p is a prime, then there is no such pair of elements and S is closed.
2. Associativity: it follows from integer multiplication
3. Identity: the identity element is 1 since it is the multiplication identity.

4. Inverse: For any $a \in S$, the multiplications

$$\{a.1, a.2, a.3, \ldots, a.(p-2), a(p-1)\}$$

are distinct since if they are not then there exists $b, c \in S$ such that

$$a.b = (a.c) \bmod p$$

$$a.(b-c) = 0 \bmod p$$

Thus, all $(p-1)$ multiplications are distinct.

Since the multiplications yeild $(p-1)$ distinct numbers, then $a.b = 1$ for some $b \in S$, then $a^{-1} = b$. As aresult, inverses are assured.

5. Commutative: for all $a, b \in S$, $a.b = b.a \in S$ as it follows from integer multiplication

As a result, it is a commutative group under mod p multiplication only if p is a prime.

Example: The group of order 6 under mod 7 multiplication

The multiplication table is as follows:

(mod 7) $\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. Closure: for all $a, b \in S$, $a \cdot b = c \bmod 5$ where $c \in S$.

2. Associativity: for all $a, b, c \in S$

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

as it follows from integer multiplication

3. Identity: the identity element is 1 since for all $a \in S$, $a.1 = 1.a = a$ (the multiplication identity)

4. Inverse: for all $a \in S$, there exists a unique element $a^{-1} \in S$ such that $a.a^{-1} = a^{-1}.a = 1$ as follows:

$1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$

5. Commutative: for all $a, b \in S$, $a.b = b.a \in S$ as it follows from integer multiplication and it is shown in the multiplication table where it is symmetric about the main diagonal.

As a result, it is a commutative group.

- **Definition: Order of a group element:**

Let a be an element in the group G with group operation "$\cdot$". The order of a is the smallest positive integer $ord(a)$ such that

$$a \cdot a \cdot \ldots \cdot a = e \qquad \text{"ord(a) times"}$$

where e is the group identity element.

- $ord(a) = 1$ if and only if $a = e$.

- An element in a group has an order that is a factor of the group's order.

Example: Find the order of the elements in the group of order 6 under mod 7 multiplication.

Elements	Order
1	$1^1 = 1 \bmod 7$, $\mathrm{ord}(1) = 1$
2	$2^3 = 8 \equiv 1 \bmod 7$, $\mathrm{ord}(2) = 3$
3	$3^6 = 729 = 7(104) + 1 \equiv 1 \bmod 7$, $\mathrm{ord}(3) = 6$
4	$4^3 = 64 = 7(9) + 1 \equiv 1 \bmod 7$, $\mathrm{ord}(4) = 3$
5	$5^6 = 15625 = 7(2232) + 1 \equiv 1 \bmod 7$, $\mathrm{ord}(5) = 6$
6	$6^2 = 36 = 7(5) + 1 \equiv 1 \bmod 7$, $\mathrm{ord}(6) = 2$

$\mathrm{ord}(G) = 6$

The factors of 6 are 1, 2, 3, 6

Example: Find the order of the elements in the group of order 8 under mod 8 addition.

Elements	Order
0	$\text{ord}(0) = 1$, $0 \equiv 8 \bmod 8 = \sum_{1} 8$
1	$\sum_{8} 1 = 8 \bmod 8 = 0 \bmod 8$, $\text{ord}(1) = 8$
2	$\sum_{4} 2 = 8 \bmod 8 = 0 \bmod 8$, $\text{ord}(2) = 4$
3	$\sum_{8} 3 = 24 \bmod 8 = 0 \bmod 8$, $\text{ord}(3) = 8$
4	$\sum_{2} 4 = 8 \bmod 8 = 0 \bmod 8$, $\text{ord}(4) = 2$
5	$\sum_{8} 5 = 40 \bmod 8 = 0 \bmod 8$, $\text{ord}(5) = 8$
6	$\sum_{4} 6 = 24 \bmod 8 = 0 \bmod 8$, $\text{ord}(6) = 4$
7	$\sum_{8} 7 = 56 \bmod 8 = 0 \bmod 8$, $\text{ord}(7) = 8$

$\text{ord}(G) = 8$

factors of 8 are 1, 2, 4, 8

Example: Find the order of the elements in the group of order 4 under mod 5 multiplication.

Elements	Order
1	$ord(1) = 1$
2	$2^4 = 16 \equiv 1 \bmod 5$, $ord(2) = 4$
3	$3^4 = 81 \equiv 1 \bmod 5$, $ord(3) = 4$
4	$4^2 = 16 \equiv 1 \bmod 5$, $ord(4) = 2$

$ord(G) = 4$

factors of 4 are 1, 2, 4

Subgroups:

For a group G under an operation "$\cdot$" : $(G, \cdot)$, S is a subgroup under the same operation "$\cdot$": $(S, \cdot)$ if it has all the properties that makes it a group.

That is, for $(S, \cdot)$ to be a subgroup, it has to be closed under its operation and contains the inverses along with the identity element. The associativity follows from G.

- **A proper subgroup**:

A subgroup S is a proper subgroup of G if $S \subset G$, but $S \neq G$.

Example: Proper Subgroups:

(a) The group of integers under mod 9 addition.

$\Rightarrow G = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

It contains the following proper subgroups:

$\{0\}$, $\{0, 3, 6\}$

(b) The group of integers under mod 16 addition.

$\Rightarrow G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$

It contains the following proper subgroups:

$\{0\}$, $\{0, 8\}$, $\{0, 4, 8, 12\}$, $\{0, 2, 4, 6, 8, 10, 12, 14\}$

- **Equivalence Classes vs. Cosets:**

- In mod m operation, two integers are in the same equivalence class and are equivalent if they differ by a multiple of m.

  This can be generalized to subgroups as follows. In subgroubs, equivalence classes are called cosets, and these cosets are equivalent when their elements differ by some element in G.

Theorem:

The distinct cosets of a subgroup S in a group G are disjoint.

Definition: Left and Right Cosets

Let S be a subgroup of G with operation "+".

A left coset of S in G is a subset of G whose elements can be expressed as

$$x + S = \{x + s, s \in S\}.$$

A right coset of S in G is a subset of G whose elements can be expressed as

$$S + x = \{s + x, s \in S\}$$

- If G is commutative, every left coset $x + S$ is identical to every right coset $S + x$.

  Here most groups are commutative, so all cosets will simply be referred to as cosets.

Example: Cosets

(a) The group of integers under mod 9 addition.

$\Rightarrow G = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

It contains the following proper subgroups:

$\{0\}$, $\{0, 3, 6\}$

- For the proper subgroup $S = \{0\}$, the distinct cosets of S in G are:

$C_0 = \{0\}$, $C_1 = \{1\}$, $C_2 = \{2\}$, $C_3 = \{3\}$, $C_4 = \{4\}$

$C_5 = \{5\}$, $C_6 = \{6\}$, $C_7 = \{7\}$, $C_8 = \{8\}$

- For the proper subgroup $S = \{0, 3, 6\}$, the distinct cosets of S in G are:

$C_0 = \{0, 3, 6\}$, $C_1 = \{1, 4, 7\}$, $C_2 = \{2, 5, 8\}$

(b) The group of integers under mod 16 addition.

$\Rightarrow G = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$

It contains the following proper subgroups:

$\{0\}$, $\{0,8\}$, $\{0,4,8,12\}$, $\{0,2,4,6,8,10,12,14\}$

- For the proper subgroup $S = \{0\}$, the distinct cosets of S in G are:

$C_0 = \{0\}$, $C_1 = \{1\}$, $C_2 = \{2\}$, $C_3 = \{3\}$, $C_4 = \{4\}$,

$C_5 = \{5\}$, $C_6 = \{6\}$, $C_7 = \{7\}$, $C_8 = \{8\}$, $C_9 = \{9\}$,

$C_{10} = \{10\}$, $C_{11} = \{11\}$, $C_{12} = \{12\}$, $C_{13} = \{13\}$, $C_{14} = \{14\}$,

$C_{15} = \{15\}$

- For the proper subgroup $S = \{0,8\}$, the distinct cosets of S in G are:

$C_0 = \{0,8\}$, $C_1 = \{1,9\}$, $C_2 = \{2,10\}$, $C_3 = \{3,11\}$, $C_4 = \{4,12\}$,

$C_5 = \{5,13\}$, $C_6 = \{6,14\}$, $C_7 = \{7,15\}$

- For the proper subgroub $S = \{0, 4, 8, 12\}$, the distinct cosets of S in G are :

$C_0 = \{0, 4, 8, 12\}$, $C_1 = \{1, 5, 9, 13\}$, $C_2 = \{2, 6, 10, 14\}$

$C_3 = \{3, 7, 11, 15\}$

- For the proper subgroup $S = \{0, 2, 4, 6, 8, 10, 12, 14\}$, the distinct cosets of S in G are :

$C_0 = \{0, 2, 4, 6, 8, 10, 12, 14\}$

$C_1 = \{1, 3, 5, 7, 9, 11, 13, 15\}$

Theorem: Lagrange's Theorem:

If S is a subgroup of G, then $ord(S) \mid ord(G)$.

(the notation $a|b$ denotes that a divides b without a remainder)

Proof:

For any subgroup S in a group G, it has n distinct disjoint cosets with $card(C_i)$ for the ith coset, with $card(C_i) = card(S)$.

Thus, $n\, card(C_i) = n\, card(S) = card(G)$

So $card(S) \mid card(G)$

$\Rightarrow ord(S) \mid ord(G)$.

Example: Subgroups and Cosets

(a) The group of integers G of order 4 under mod 4 addition contains the subgroup $S = \{0, 2\}$.

The distinct cosets of S in G are:

$C_0 = \{0, 2\}$, $C_1 = \{1, 3\}$.

The group G in terms of this coset decomposition is:

$$G = C_0 \cup C_1 = \{0, 2\} \cup \{1, 3\}$$

(b) The group of integers G of order 12 under mod 12 addition contains the subgroup $S = \{0, 4, 8\}$.

The distinct cosets of S in G are:

$C_0 = \{0, 4, 8\}$, $C_1 = \{1, 5, 9\}$, $C_2 = \{2, 6, 10\}$, $C_3 = \{3, 7, 11\}$.

The group G in terms of this coset decomposition is:

$$G = C_0 \cup C_1 \cup C_2 \cup C_3$$

Definition : Rings

A ring is a collection of elements R with two binary operations "+" and "$\cdot$" such that the following three properties hold:

1. R forms a commutative group under "+". The additive identity element is labeled "0".
2. The operation "$\cdot$" is associative: for all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. The operation "$\cdot$" is distributive over "+": for all $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

- A ring is a commutative ring if the operation "$\cdot$" is commuative: for all $a, b \in R$, $a \cdot b = b \cdot a$
- A ring is a ring with identity if the operation "$\cdot$" has an identity element, which is labeled "1"

- A ring is a commutative ring with identity if the operation "." is both commutative and has an identity element.

Example:

(a) The integers under mod m addition and multiplication form a commutative ring with identity.

(b) The set of all polynomials with binary coefficients forms a commutative ring with identity under standard polynomial addition and multiplication.

Definition : Fields

Let F be a set of objects on which two operations "+" and "." are defined.

F is a field if and only if :

1. F forms a commutative group under "+".
   The additive identity element is labeled "0".
2. $F - \{0\}$: the set F with the additive removed forms a commutative group under ".".
   The multiplicative identity element is labeled "1".
3. The operations "+" and "." distribute :

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

- A field can be viewed as a commutative ring with an identity element and multiplicative inverses.

- For a field, all its elements form a commutative group under "+", while its nonzero elements form a commutative group under ".".

Example:

(a) The real numbers form an infinite field.

(b) The integers do not form a field since integers do not have multiplication inverses as integers.

Definition: Vector Spaces

Let V be a set of elements called vectors.

Let F be a field of elements called scalars.

There are two operations defined between the field elements. Define two other operations,

1. let "+" be a binary additive operation among vectors, called vector addition, such that if $\vec{v}_1, \vec{v}_2 \in V$, then $\vec{v}_1 + \vec{v}_2 = \vec{v} \in V$

2. Let "." be a binary multiplicative operation, called scalar multiplication, such that if $a \in F$ and $\vec{v} \in V$, then $a.\vec{v} = \vec{w} \in V$.

Then V forms a vector space over F if the following five conditions are satisfied:

1. V forms a commutative group under "+".

2. For any element $a \in F$ and $\vec{v} \in V$, $a.\vec{v} = \vec{w} \in V$

   (closed under scalar multiplication)

3. The operations "+" and "." distribute:

   $a.(\vec{u} + \vec{v}) = a.\vec{u} + a.\vec{v}$ (additive vector operation)

and $(a+b).\vec{v} = a.\vec{v} + b.\vec{v}$ (additive field operation)

4. Associativity: for all $a, b \in F$ and all $\vec{v} \in V$,

   $(a.b).\vec{v} = a.(b.\vec{v})$

5. The multiplicative identity "1" in F is also the multiplicative identity in scalar multiplication:

   for all $\vec{v} \in V$ and $1 \in F$, $1.\vec{v} = \vec{v}.1 = \vec{v}$

- F is usually called the "scalar field" or the "ground field" of the vector space $(V, +, \cdot)$

Example: Vector Spaces

The set of binary n-tuples (V_n) forms a vector space over $F = \{0,1\} =: GF(2)$: Galois field of order 2.

Here each of the n coordinates in each vector can take on one of two values, $\{0,1\}$, independent of the other coordinates.

$|V_n| =: \text{card}(V_n) = 2^n$.

The n-tuple $\vec{v} = (v_0, v_1, \dots, v_{n-1})$, $\vec{v} \in V_n$ and for v_i elements, $v_i \in F$.

For all $\vec{v}, \vec{u} \in V_n$, and for all $v_i, u_i \in F$:

. The vector addition is:

$$\vec{u} + \vec{v} = (u_0 + v_0, u_1 + v_1, \dots, u_{n-1} + v_{n-1})$$

. The scalar multiplication for any $a \in F$:

$$a \cdot \vec{v} = (av_0, av_1, \dots, av_{n-1})$$

Example: V_3 over $GF(2)$ contains $2^3 = 8$ binary 3-tuples

- The linear combinations of vectors in a vector space are in the vector space:

Let vectors $\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{n-1}$ be in V.

Let scalars $a_0, a_1, \ldots, a_{n-1}$ be in F.

Then the following linear combination $\vec{v}$ is also in V:

$\vec{v} = a_0\vec{v}_0 + a_1\vec{v}_1 + \cdots + a_{n-1}\vec{v}_{n-1}$

Definition: Spanning Sets

For a vector space V, let $S = \{\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{m-1}\}$

where $S \subset V$ with $\mathrm{card}(S) = m$.

If there exists $\{a_0, a_1, \ldots, a_{m-1}\} \in F$ such that

for every vector $\vec{v} \in V$:

$$\vec{v} = \sum_{i=0}^{m-1} a_i \vec{v}_i$$

Then the set S is said to **span V** and S is called a **spanning set for V**.

Example: Spanning Sets

Does the vectors in $S = \{(1,1,0), (0,1,1), (1,0,1), (1,0,0)\}$ span the space V_3.

To check, make a list of all vectors in V_3, then generate the vectors by selecting (a_0, a_1, a_2, a_3) such that for every vector $\vec{v} \in V_3$, $\vec{v} = \sum_{i=0}^{3} a_i \vec{v_i}$.

The zero vector $\vec{0} =: (0,0,0)$ is obtained when all $a_i = 0$ that is $(a_0, a_1, a_2, a_3) = (0,0,0,0)$.

Also, in binary addition, the sum of any vector with itself is the zero vector $\vec{0}$. That is, every vector is its own inverse.

Since for $(a_0, a_1, a_2, a_3) = (1,1,0,0)$

$$\vec{v} = a_0 \cdot (1,1,0) + a_1 \cdot (0,1,1) + a_2 \cdot (1,0,1) + a_3 \cdot (1,0,0) = (1,0,1)$$

and $(1,0,1)$ is one of the vectors in S, then the vectors in S are not linearly independent.

Definition : Bases

A spanning set for V that has minimal cardinality is called a basis for V.

- From the definition of bases, since the cardinality should be minimum, the basis for V should be linearly independent; otherwise, the basis could be reduced.
- A vector space may have several possible bases that span V, however, all of the bases have the same cardinality.
- The canonical basis for a vector space V_n is the simplest basis. For example, the canonical basis for V_3 is $\{(1,0,0), (0,1,0), (0,0,1)\}$.
- One of the basis for V_5 : $\{(1,0,1,0,1), (0,1,0,1,1), (0,1,1,0,1), (0,0,1,1,1), (1,0,0,0,1)\}$.

Definition : **The Dimension of a Vector Space**

If a basis for a vector space V has k elements, then the vector space is said to have dimension k, $\dim(V) = k$.

Theorem :

Let $\{\vec{v}_i\}$ be a basis for a vector space V. For every vector $\vec{v} \in V$ there is a representation $\vec{v} = \sum_{i=0}^{k-1} a_i \vec{v}_i$.

This representation is unique.

Proof: We can proof this by contradiction.

Assume the representation is not unique. Then there can be two distinct representations for a vector $\vec{v}$, $\vec{v} = \sum_{i=0}^{k-1} a_i \vec{v}_i$ and $\vec{v} = \sum_{i=0}^{k-1} b_i \vec{v}_i$

So since $\vec{v} = \sum_{i=0}^{k-1} a_i \vec{v}_i = \sum_{i=0}^{k-1} b_i \vec{v}_i$

then $\sum_{i=0}^{k-1} a_i \vec{v}_i - \sum_{i=0}^{k-1} b_i \vec{v}_i = 0$

So $\sum_{i=0}^{k-1} (a_i - b_i) \vec{v}_i = 0 \quad \sim (1)$

Since the two representations are distinct, then there exists at least one term in (1) such that $(a_i - b_i)\vec{v}_i \neq 0$, and since $\sum_{i=0}^{k-1} (a_i - b_i)\vec{v}_i = 0$, then there exists some subset of $\{\vec{v}_i\}$ that represents the additive inverse of $(a_i - b_i)\vec{v}_i \neq 0$. As a result, the set $\{\vec{v}_i\}$ is not linearly independent, thus, it is not a basis since it is not with minimal cardinality. So the representation should be unique.

For example, for $k=2$, let the basis be $\{\vec{v}_0, \vec{v}_1\}$ so for the representations

$$\vec{v} = a_0\vec{v}_0 + a_1\vec{v}_1 \quad \text{and} \quad \vec{v} = b_0\vec{v}_0 + b_1\vec{v}_1$$

$$\vec{v} = a_0\vec{v}_0 + a_1\vec{v}_1 = b_0\vec{v}_0 + b_1\vec{v}_1 \Rightarrow (a_0 - b_0)\vec{v}_0 + (a_1 - b_1)\vec{v}_1 = 0$$

$$\Rightarrow c_0\vec{v}_0 + c_1\vec{v}_1 = 0 \quad \Rightarrow \quad c_0\vec{v}_0 = -c_1\vec{v}_1$$

$$\Rightarrow \vec{v}_0 = d_0\vec{v}_1$$, thus $\vec{v}_0$ & $\vec{v}_1$ are dependent.

- For a vector space V over a field F, with a dimension n, each distinct vector $\vec{v} \in V$ is associated with a unique ordered set $(a_0, a_1, \dots, a_{n-1})$ and vice versa. Then the cardinality of the vector space equals the number of possible choices for ordered set $(a_0, a_1, \dots, a_{n-1})$. That is,

$$\text{card}(V) = [\text{card}(F)]^n .$$

Example: The binary vector space V_n has cardinality

$$\text{card}(V_n) = [\text{card}(F)]^n = 2^n .$$

Definition : Vector Subspace

For a vector space V, S is a vector subspace of V if S itself is a vector space and $S \subseteq V$.

Theorem :

Let $\vec{v}_1$ and $\vec{v}_2$ be an arbitrary pair of vectors in the subset S of the vector space V over F. S is a vector subspace of V if and only if any linear combination of $\vec{v}_1$ and $\vec{v}_2$ is also in S.

(i.e. $a.\vec{v}_1 + b.\vec{v}_2 \in S$, $a,b \in F$)

Definition : Inner Product

The inner product is a binary operation that maps a pair of vectors in the vector space V over the field F onto scalars in F.

Let $\vec{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\vec{v} = (v_0, v_1, \ldots, v_{n-1})$ be vectors in the vector space V over the field F. The inner product $\vec{u} \cdot \vec{v}$ is defined as:

$$\vec{u} \cdot \vec{v} = \sum_{i=0}^{n-1} u_i \cdot v_i = u_0 \cdot v_0 + u_1 \cdot v_1 + \cdots + u_{n-1} \cdot v_{n-1}$$

with the following properties:

1. Commutativity : $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$

2. Associativity with scalar multiplication :

for $a \in F$ and $\vec{u}, \vec{v} \in V$, $a \cdot (\vec{u} \cdot \vec{v}) = (a \cdot \vec{u}) \cdot \vec{v}$

3. Distributivity with vector addition :

for $\vec{u}, \vec{v}, \vec{w} \in V$, $\vec{u} \cdot (\vec{v} + \vec{w}) = (\vec{u} \cdot \vec{v}) + (\vec{u} \cdot \vec{w})$

Definition : Dual Spaces of Vector Spaces

Let S be a subspace of a vector space V.
A set $S^{\perp}$ is called the dual space of S
if for all $\vec{u} \in S \subset V$ and all $\vec{w} \in S^{\perp} \subset V$,

$$\vec{u} \cdot \vec{w} = 0 .$$

Theorem :

The dual space $S^{\perp}$ of a vector subspace $S \subseteq V$
is itself a vector subspace of V.

- Note that : $0 \in S$ and $0 \in S^{\perp}$,
because both S and $S^{\perp}$ are vector subspaces of a vector space, and it follows from the definition of a vector subspace that it is a vector space, and a vector space should have the additive identity 0 since it is a group under "+".

Theorem: The dimension Theorem

Let S e a finite-dimensional vector subspace of V and let $S^{\perp}$ be the corresponding dual space. Then the dimension of S and the dimension of $S^{\perp}$ sum to the dimension of V.

$$\dim(S) + \dim(S^{\perp}) = \dim(V).$$

- Notice that since

$$\text{card}(S) = [\text{card}(F)]^{\dim(S)} \quad \text{and} \quad \text{card}(S^{\perp}) = [\text{card}(F)]^{\dim(S^{\perp})}$$

then:

$$\text{card}(S) + \text{card}(S^{\perp}) = [\text{card}(F)]^{\dim(S)} + [\text{card}(F)]^{\dim(S^{\perp})}$$

while:

$$\text{card}(V) = [\text{card}(F)]^{\dim(V)} = [\text{card}(F)]^{\dim(S)+\dim(S^{\perp})}$$

- If $\dim(S) = k$, $\dim(S^{\perp}) = t$, $\dim(V) = n$.

Then $\dim(S) = \dim(V) - \dim(S^{\perp}) = n - t = k$

and $\dim(S^{\perp}) = \dim(V) - \dim(S) = n - k = t$

where $(n-t) + (n-k) = (n-t) + t = n$

Example: Dual space and dimension theorem :

The vector space of binary 4-tuples

the following vector subspace :

$S = \{(0000), (0101), (0001), (0100)\}$

Notice since $(0001) + (0100) = (0101)$

and $(0001) + (0001) = (0000)$,

then the basis for S is $\{(0001), (0100)\}$.

So, $\dim(S) = 2$.

While, $S^{\perp} = \{(0000), (1010), (1000), (0010)\}$

and since $(1000) + (0010) = (1010)$,

and $(1000) + (1000) = (0000)$,

then the basis for $S^{\perp}$ is $\{(1000), (0010)\}$.

So, $\dim(S^{\perp}) = 2$.

$\dim(S) + \dim(S^{\perp}) = 4$

and $\dim(V_4) = 4$.

2.2 Elementary Properties of Galois Fields:

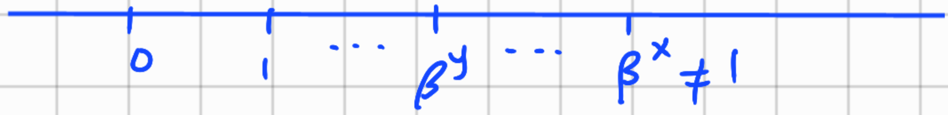
- The order of a Galois field completely specifies the field unlike a group. $GF(q)$ has an order q.

Theorem:

Let $\beta \in GF(q)$ and let "1" be the multiplicative identity. Consider the sequence $\{1, \beta, \beta^2, \beta^3, \dots\}$.
This sequence is repetitive and the first element to repeat is the element "1".

Proof: Since $\beta \in GF(q)$, and $\beta \cdot \beta \in GF(q)$, also $\beta \cdot (\beta \cdot \beta) = \beta^3 \in GF(q)$, so all $\beta^k \in GF(q)$.
So, since $GF(q)$ has an order q, then at some point elements must repeat.
To proof using contradition, assume that "1" is not the first element to repeat and let β^y be the first element to repeat and it equals β^x,

where $\beta^x = \beta^y \neq 1$ and $0 < y < x$.



So, $\beta^x = \beta^y \Rightarrow \beta^x \beta^{-y} = \beta^y \beta^{-y}$

$$\Rightarrow \beta^{x-y} = 1$$

This means that there exists an element β^{x-y} where $x-y < x$ that equals "1", which means $\beta^{x-y} = 1$ as the repeation of "1". Since we assumed that β^x is the first repeatition in the set for the element β^y and they do not equal to "1".

Thus, we have a contradiction. So, the assumption is not true. Thus, "1" is the first element to repeat.

Definition: The order of a Galois field element.

Let β be an element in $GF(q)$. The order of β ($ord(\beta)$) is the smallest integer m such that $\beta^m = 1$.

- Notice that the operation under which the order of a Galois field element is defined is the multiplicative operation.

- **Recall**: The nonzero elements of a field, $F - \{0\}$ form a commutative group under "$\cdot$" with the multiplicative identity element "1".

Theorem:

If $t = ord(\beta)$ for some $\beta \in GF(q)$, then $t \mid (q-1)$.

- This is: $ord(\beta) \mid$ # of nonzero elements of $GF(q)$

Proof: If $\beta \in GF(q)$ with $ord(\beta) = t$, then the set $S = \{\beta, \beta^2, \beta^3, \dots, \beta^t = 1\}$ forms a subgroub of $card(S) = ord(S) = ord(\beta) = t$, in the group of nonzero elements of $GF(q)$ under multiplication.

Lagrange's theorem states:

if S is a subgroup of G, then $ord(S) \mid ord(G)$.

Here, $ord(S) = t$ and $ord(G) = q-1$, the nonzero elements. Thus, $t \mid (q-1)$.

- The greatest common divisor of i and t is defined to be the largest positive integer m such that $m | i$ and $m | t$, it is denoted as $GCD(i,t)$.

Theorem:

Let α and β be elements in $GF(q)$ such that $\beta = \alpha^i$. If the $ord(\alpha) = t$,

$$ord(\beta) = \frac{t}{GCD(i,t)} =: \frac{ord(\alpha)}{GCD(i, ord(\alpha))}$$

Example: Consider GF(16).

Let the nonzero elements be $\{\alpha, \alpha^2, \alpha^3, \dots, \alpha^{15} = 1\}$.

The possible orders of any $\beta \in GF(16)$ can only have orders $\{1, 3, 5, 15\}$ since they divide 15 (i.e. $q-1 = 15$) without remainder.

The sequence of successive powers of β must be in GF(16), $\{\beta, \beta^2, \beta^3, \beta^4, \dots\}$

(a) For $\beta = \alpha^3$, the sequence

$\{\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \dots\}$ =

$\{\alpha^3, (\alpha^3)^2, (\alpha^3)^3, (\alpha^3)^4, (\alpha^3)^5, (\alpha^3)^6, \dots\}$ =

$\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15} = 1, \alpha^{18} = \alpha^{15} \cdot \alpha^3 = 1 \cdot \alpha^3, = \alpha^3, \dots\}$ =

$\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, 1\}$, $\mathrm{ord}(\beta) = \mathrm{ord}(\alpha^3) = 5$, $\mathrm{ord}(\alpha) = 15$,

$$\mathrm{ord}(\beta) = \frac{\mathrm{ord}(\alpha)}{GCD(i, \mathrm{ord}(\alpha))} \Rightarrow \mathrm{ord}(\beta) = \frac{15}{GCD(3, 15)} = \frac{15}{3} = 5$$

(b) For $\beta = \alpha^5$, the sequence

$\{\beta, \beta^2, \beta^3, \beta^4, \dots\} =$

$\{\alpha^5, (\alpha^5)^2, (\alpha^5)^3, (\alpha^5)^4, (\alpha^5)^6, \dots\} =$

$\{\alpha^5, \alpha^{10}, \alpha^{15} = 1\}$, $\text{ord}(\beta) = \text{ord}(\alpha^5) = 3$, $\text{ord}(\alpha) = 15$,

$$\text{ord}(\beta) = \frac{\text{ord}(\alpha)}{\text{GCD}(i, \text{ord}(\alpha))} \Rightarrow \text{ord}(\beta) = \frac{15}{\text{GCD}(5, 15)} = \frac{15}{5} = 3$$

(c) For $\beta = \alpha^{15}$, the sequence

$\{\beta, \beta^2, \beta^3, \dots\} = \{\alpha^{15} = 1\}$

$\text{ord}(\beta) = \text{ord}(\alpha^{15}) = 1$, $\text{ord}(\alpha) = 15$,

$$\text{ord}(\beta) = \frac{\text{ord}(\alpha)}{\text{GCD}(i, \text{ord}(\alpha))} \Rightarrow \text{ord}(\beta) = \frac{15}{\text{GCD}(15, 15)} = \frac{15}{15} = 1$$

(d) For $\beta = \alpha$, the sequence

$\{\beta, \beta^2, \beta^3, \dots\} = \{\alpha, \alpha^2, \alpha^3, \dots, \alpha^{15} = 1\}$, $\text{ord}(\beta) = \text{ord}(\alpha) = 15$

$$\text{ord}(\beta) = \frac{\text{ord}(\alpha)}{\text{GCD}(i, \text{ord}(\alpha))} \Rightarrow \text{ord}(\beta) = \frac{15}{\text{GCD}(1, 15)} = \frac{15}{1} = 15$$

Definition : The Euler ϕ Function :

The Euler ϕ function evaluated at an integer t, written $\phi(t)$, is the number of integers in the set $\{1, 2, \ldots, t-1\}$ that are relatively prime to t. (i.e. share no common divisors other than one).

- $\phi(t)$ is computed as follows :

if $t = 1$, $\phi(t) = 1$.

if $t > 1$, $\phi(t) = \text{card}\left[\{1 \leq i < t \mid GCD(i, t) = 1\}\right]$

$$\phi(t) = t \prod_{p \mid t} \left(1 - \frac{1}{p}\right)$$

This product is over all positive prime integers $p < t$ that divide t.

Example: The Euler ϕ Function:

(a) $\phi(9) = \phi(3.3)$

$= 9\left(1-\frac{1}{3}\right) = 9\left(\frac{2}{3}\right)$

$\phi(9) = 6$

That is, the number of integers in $\{1,2,3,\dots,8\}$ that are relatively prime to 9 are 6 numbers.

They are $\{1,2,4,5,7,8\}$.

(b) $\phi(30) = \phi(2.3.5)$

$= 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= \cancel{30}\left(\frac{2-1}{\cancel{2}}\right)\left(\frac{3-1}{\cancel{3}}\right)\left(\frac{5-1}{\cancel{5}}\right)$

$\phi(30) = 8$

and they are $\{1,7,11,13,17,19,23,29\}$.

(c) $\phi(56) = \phi(2.2.2.7)$

$= 56\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)$

$\phi(56) = 24$

(d) $\phi(256) = \phi(2^8)$

$$= 2^8\left(1 - \frac{1}{2}\right)$$

$$= 2^7(2-1)$$

$\phi(256) = 128$

Properties of the Euler ϕ function :

(1) If p is a prime, then $\phi(p) = p-1$, since all nonzero elements less than p are relatively prime to a prime.

(2) If $\phi(p_1 \cdot p_2) = \phi(p_1) \cdot \phi(p_2) = (p_1-1)(p_2-1)$ if p_1 and p_2 are distinct primes.

This is true for any number of primes.

(3) For a prime p, $\phi(p^m) = p^{m-1}(p-1)$.

(4) For distinct primes p_1 and p_2,

$$\phi(p_1^m p_2^n) = p_1^{m-1} p_2^{n-1}(p_1-1)(p_2-1)$$

Theorem: **The Multipliactive Structure of Galois Fields**:

Consider the Galois field $GF(q)$:

(1) If t does not divide $(q-1)$, then there are no elements of order t in $GF(q)$.

(2) If $t \mid (q-1)$, then there are $\phi(t)$ elements of order t in $GF(q)$.

Example: Consider $GF(11)$:

$q = 11$, $q-1 = 10$

Possible orders of elements in $GF(11)$ are $\{1,2,5,10\}$.

Order	Number of elements
1	$\phi(1) = 1$
2	$\phi(2) = 2(1-\frac{1}{2}) = 1$
5	$\phi(5) = 5(1-\frac{1}{5}) = 4$
10	$\phi(10) = \phi(2 \cdot 5) = \phi(2)\phi(5) = (1)(4) = 4$

Total number of elements $= 1+1+4+4 = 10$

The nonzero elements of GF(11) are :

$GF(11) - \{0\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10} = 1\}$

Since for any $\beta = \alpha^i \in GF(11)$, $ord(\alpha^i) = \frac{ord(\alpha)}{GCD(i, ord(\alpha))}$

1. $ord(\alpha) = 10$ since $\alpha^{10} = 1$.

2. $ord(\alpha^2) = \frac{ord(\alpha)}{GCD(2, ord(\alpha))} = \frac{10}{GCD(2,10)} = \frac{10}{2} = 5$

3. $ord(\alpha^3) = \frac{10}{GCD(3,10)} = \frac{10}{1} = 10$

4. $ord(\alpha^4) = \frac{10}{GCD(4,10)} = \frac{10}{2} = 5$

5. $ord(\alpha^5) = \frac{10}{GCD(5,10)} = \frac{10}{5} = 2$

6. $ord(\alpha^6) = \frac{10}{GCD(6,10)} = \frac{10}{2} = 5$

7. $ord(\alpha^7) = \frac{10}{GCD(7,10)} = \frac{10}{1} = 10$

8. $ord(\alpha^8) = \frac{10}{GCD(8,10)} = \frac{10}{2} = 5$

9. $\text{ord}(\alpha^9) = \dfrac{10}{GCD(9,10)} = \dfrac{10}{1} = 10$

10. $\text{ord}(1) = \text{ord}(\alpha^{10}) = \dfrac{10}{GCD(10,10)} = 1$

t (order)	$\phi(t)$	The elements of order t
1	1	1
2	1	α^5
5	4	$\alpha^2, \alpha^4, \alpha^6, \alpha^8$
10	4	$\alpha, \alpha^3, \alpha^7, \alpha^9$

The sets for all $\beta \in GF(11)$:

(1) of order 1, $\{1\}$

(2) of order 2, $\{\alpha^5, (\alpha^5)^2\} = \{\alpha^5, 1\}$

(3) of order 5, $\{\alpha^2, (\alpha^2)^2, (\alpha^2)^3, (\alpha^2)^4, (\alpha^2)^5\}$

$= \{\alpha^2, \alpha^4, \alpha^6, \alpha^8, 1\}$

and $\{\alpha^4, (\alpha^4)^2 = \alpha^8, (\alpha^4)^3 = \alpha^{12} = \alpha^{10} \cdot \alpha^2 = \alpha^2,$

$(\alpha^4)^4 = \alpha^{16} = \alpha^{10} \cdot \alpha^6 = \alpha^6, (\alpha^4)^5 = \alpha^{20} = \alpha^{10} \cdot \alpha^{10} = 1\}$

all distinct elements.

Similarly for α^6 and α^8.

(4) of order 10, $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10} = 1\}$

and $\{\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^3 = \alpha^9, (\alpha^3)^4 = \alpha^2, (\alpha^3)^5 = \alpha^5,$

$(\alpha^3)^6 = \alpha^8, (\alpha^3)^7 = \alpha, (\alpha^3)^8 = \alpha^4, (\alpha^3)^9 = \alpha^7, (\alpha^3)^{10} = 1\}$

all distinct elements.

Similarly for α^7 and α^9.

Definition: Primitive Elements in a Galois Field.

An element with order $(q-1)$ in $GF(q)$ is called a primitive element in $GF(q)$.

Theorem:

In every finite field $GF(q)$ there are exactly $\phi(q-1)$ primitive elements.

Example: The multiplicative structure of $GF(7)$:

$GF(7)$ nonzero elements construct a field under mod 7 multiplication since 7 is a prime.

- $GF(7)$ has $\phi(7-1) = \phi(6) = \phi(3.2)$

$$= 6\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right) = 2$$

So $GF(7)$ has 2 primitive elements.

* Under mod 7 multiplication:

- For element 1, since it is the identity element under multiplication, ord(1) = 1.
- For element 2, $2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 1 \bmod 7$, ord(2) = 3.
- For element 3, $3^1 = 3$, $3^2 = 9 = 2 \bmod 7$, $3^3 = 27 = 6 \bmod 7$, $3^4 = 81 = 7(11) + 4 = 4 \bmod 7$, $3^5 = 243 = 7(34) + 5 = 5 \bmod 7$, $3^6 = 729 = 7(104) + 1 = 1 \bmod 7$. So ord(3) = 6.

* Since 3 is a primitive element in GF(7) under multiplication, then 3^i for $i \in \{1, 2, \dots, 6\}$ will represent the 6 nonzero elements.

We can use the formula $\operatorname{ord}(\alpha^i) = \dfrac{\operatorname{ord}(\alpha)}{GCD(i, \operatorname{ord}(\alpha))}$

to find the order of the nonzero elements as follows since ord(3) = 6.

i	element represented in terms of 3^i	$ord(element) = ord(3^i)$
0	$3^0 = 1$	$ord(1) = 1$ (idmity element)
1	$3^1 = 3$	$ord(3) = 6$
2	$3^2 = 9 = 2 \bmod 7$	$ord(3^2) = \dfrac{ord(3)}{GCD(2, ord(3))} = \dfrac{6}{GCD(2,6)} = \dfrac{6}{2} = 3$ $ord(2) = 3$
3	$3^3 = 27 = 7(3) + 6$ $= 6 \bmod 7$	$ord(3^3) = \dfrac{ord(3)}{GCD(3, ord(3))} = \dfrac{6}{GCD(3,6)} = \dfrac{6}{3} = 2$ $ord(6) = 2$
4	$3^4 = 81 = 7(11) + 4$ $= 4 \bmod 7$	$ord(3^4) = \dfrac{6}{GCD(4,6)} = \dfrac{6}{2} = 3$ $ord(4) = 3$
5	$3^5 = 243 = 7(34) + 5$ $= 5 \bmod 7$	$ord(3^5) = \dfrac{6}{GCD(5,6)} = \dfrac{6}{1} = 6$ $ord(5) = 6$

6 $3^6 = 729 = 7(104)+1$
$= 1 \mod 7$

$ord(3^6) = \frac{6}{GCD(6,6)} = \frac{6}{6} = 1$

$ord(1) = 1$

t (order)	$\phi(t)$	The elements in GF(7) with order t.	
1	$\phi(1) = 1$	1	
2	$\phi(2) = (2-1) = 1$	6	
3	$\phi(3) = (3-1) = 2$	2, 4	
6	$\phi(6) = \phi(2)\phi(3) = 2$	3, 5	(primitive elements)

The Additive Structure of $GF(q)$:

$GF(q)$ elements construct a field with order q under addition.

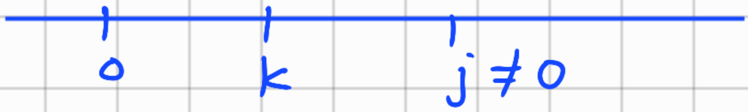
Since the order of an element $a \in GF(q)$ under addition is the smallest positive integer $ord(a)$ such that $a + a + \cdots + a = 0$ where 0 is the additive identity element, then in $GF(q)$ all q elements can be represented by $\sum_{i} 1$ such that $i \in \{1, 2, \dots, q\}$ since $\sum_{q} 1 = q \bmod q = 0 \bmod q$ (i.e. $ord(1) = q$).

For a positive integer m, let $\sum_{m} 1$ be denoted as $m(1)$, where m is the number of ones.

- The first element to repeat is the additive identity element "0".

Proof: By contradiction:

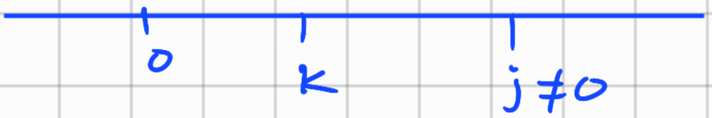
If $j(1) = k(1) \neq 0$ where $0 \leq k < j$



Then since $j(1) = k(1)$

$\Rightarrow j(1) - k(1) = 0$

$(j-k)(1) = 0$ where $(j-k) < j$



Then there exists an integer $(j-k)$ such that $(j-k)(1) = 0$ before $j(1) \neq 0$.

Contradiction since $j(1)$ should be the first to repeat before 0. Thus, 0 is first to repeat.

Definition: **Characteristic of GF(G)**

The characteristic of a $GF(q)$ is the smallest positive integer m such that $m(1) = 0$.

Theorem:

The characteristic of a Galois field is always a prime integer.

Proof: By contradiction:

For a $GF(q)$, if $k(1) = 0$ is the first element to repeat, then k is the characteristic of $GF(q)$.

Assume k is not a prime, then there exist two positive integers such that

$$k(1) = m(1) \cdot n(1) = 0$$

where $m < k$ and $n < k$.

Since the first element to repeat is 0, then $m(1) \neq 0$ and $n(1) \neq 0$.

Also $GF(q)$ has no multiplicatise inverse of the element 0, while $m(1) \cdot n(1) = 0$ with $m(1) \neq 0$ and $n(1) \neq 0$.

Contradiction since there are no such integers m and n with

$$m(1) \cdot n(1) = k(1) = 0 .$$

Thus, k is a prime.

Example: The additive structure of $GF(7)$:

$GF(7)$ elements construct a field under mod 7 addition.

element	ord(element)
0	$ord(0) = 1$, $0 \equiv 7 \bmod 7 = \sum_{1} 7$, also "0" identity element.
1	$\sum_{7} 1 = 7 = 0 \bmod 7$, $ord(1) = 7$
2	$\sum_{7} 2 = 14 = 0 \bmod 7$, $ord(2) = 7$
3	$\sum_{7} 3 = 21 = 0 \bmod 7$, $ord(3) = 7$
4	$\sum_{7} 4 = 28 = 0 \bmod 7$, $ord(4) = 7$
5	$\sum_{7} 5 = 35 = 0 \bmod 7$, $ord(5) = 7$
6	$\sum_{7} 6 = 42 = 0 \bmod 7$, $ord(5) = 7$

Theorem:

The order q of a Galois field $GF(q)$ must be a power of a prime.

- In other words, let p denote a prime, for a $GF(q)$ of order q, then $q = p^n$ for some positive integer n

  $n \in \{1, 2, 3, \dots\}$

2.3 Primitive Polynomials and Galois Fields of Order p^m

- The notation $GF(q)[x]$ is the set of all polynomials $a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_nx^n$ of an arbitrary degree n with coefficients $a_i \in GF(q)$.
- The additive and multiplicative operations are performed as expected with the coefficient operations performed using the operations in the field $GF(q)$, as follows. Let $A(x)$ and $B(x)$ be in $GF(q)[x]$ where $A(x) = \sum_{i=0}^{n} a_i x^i$ and $B(x) = \sum_{i=0}^{n} b_i x^i$.

Then $A(x) + B(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i$

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

and $A(x).B(x) = \left(\sum_{i=0}^{n} a_i x^i\right).\left(\sum_{i=0}^{m} b_i x^i\right) = (a_0.b_0) +$

$$\left[(a_1.b_0)+(a_0.b_1)\right]x + \left[(a_2.b_0)+(a_1.b_1)+(a_0.b_2)\right]x^2 + \dots + a_nb_mx^{n+m}$$

Example: In $GF(2)[x]$, let $A(x) = x^5 + x^2$ and $B(x) = x^2 + x + 1$.

$$A(x) + B(x) = (x^5 + x^2) + (x^2 + x + 1)$$
$$= x^5 + (1+1)x^2 + x + 1 \quad , (\text{in } GF(2),\ 1+1=0)$$
$$= x^5 + x + 1$$

Definition: **Irreducible Polynomials**

An irreducible polynomial over $GF(q)$ is a polynomial that cannot be factored in $GF(q)$ into a product of lower degree polynomials in $GF(q)[x]$.

Example: The polynomial $A(x) = x^2 + x + 1$:

(a) In $GF(2)[x]$, it is irreducible since

$A(0) = (0 \cdot 0) + 0 + 1 = 1$ (not a root)

$A(1) = (1 \cdot 1) + 1 + 1 = 1 + 1 + 1 = 1$ (not a root)

So $A(x)$ has no roots in $GF(2)$, it is irreducible.

(b) In $GF(4)[x]$, we will learn that

$$A(x) = x^2+x+1 = (x+\alpha)(x+\alpha^2)$$
$$= x^2 + (\alpha+\alpha^2)x + 1$$

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

So $A(s)$ is reducible.

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	$1+\alpha=\alpha^2$	$1+\alpha^2=\alpha$
α	α	$1+\alpha=\alpha^2$	0	$\alpha+\alpha^2=1$
α^2	α^2	$1+\alpha^2=\alpha$	$\alpha+\alpha^2=1$	0

Definition: Primitive Polynomials

An irreducible polynomial $p(x) \in GF(p)[x]$ of degree m is said to be primitive if the smallest positive integer n for which $p(x)$ divides $x^n - 1$ is $n = p^m - 1$.

Example: Primitive Polynomials

$p(x) = x^3 + x + 1 \in GF(2)[x]$ is primitive.

Here, $p = 2$, $m = 3$:

$$p(x) \mid x^{p^m - 1} - 1 \Rightarrow p(x) \mid x^{2^3 - 1} - 1 = p(x) \mid x^7 - 1.$$

This means that $p(x)$ will not divide $x^i - 1$ for all $i \in \{1, 2, 3, 4, 5, 6\}$ with zero remainder.

while $\text{Rem}\left\{\dfrac{x^7 - 1}{x^3 + x + 1}\right\} = 0$

where $x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$

Since

$$
\begin{array}{r|l}
 & x^4 + x^2 + x + 1 \\
\hline
x^3 + x + 1 & x^7 - 1 \\
 & \underline{x^7 + x^5 + x^4} \\
 & x^5 + x^4 - 1 \\
 & \underline{x^5 + x^3 + x^2} \\
 & x^4 + x^3 + x^2 - 1 \\
 & \underline{x^4 + x^2 + x} \\
 & x^3 + x - 1 \\
 & \underline{x^3 + x + 1} \\
 & 0
\end{array}
$$

- The primitive polynomials of m-degree in $GF(p)[x]$ are constructed from primitive elements in $GF(p^m)$ with a one-to-one mapping between the distinct powers of α and the set of polynomials in α of degree less than or equal to $(m-1)$ with coefficients in $GF(p)$.

That is, since for an m-degree primitive polynomial $p(x)$,

$p(x) = \sum_{i=0}^{m} a_i x^i$ where α is a root of $p(x)$,

then $p(\alpha) = \sum_{i=0}^{m} a_i \alpha^i = 0$

$$0 = a_m \alpha^m + \sum_{i=0}^{m-1} a_i \alpha^i$$

so for example if $p=2$, then

$$a_m \alpha^m = \sum_{i=0}^{m-1} a_i \alpha^i$$

$\Rightarrow$ the set of polynomials in α of degree less than or equal to $(m-1)$ is enough to map all p^m primitive elements under mod $p(\alpha)$

- In $GF(p^m)$ there are $\phi(p^m-1)$ primitive elements.

Their map into primitive polynomials in $GF(p)[x]$ is $\frac{\phi(p^m-1)}{m}$ primitive polynomials of m-degree.

- A list of binary primitive polynomials is in Appendix A.

Example: In $GF(4)$ the elements are $\{0, 1, \alpha, \alpha^2\}$,

$p(x) = x^2+x+1$ is a primitive polynomial in $GF(2)[x]$.

Let α be a root of $p(x)$, then $\alpha^2+\alpha+1 = 0$.

The map between the exponentials of α and the polynomial of $(m-1)$ degree or less is:

Exponential	Polynomial	Label	Vector space representation: $(1, \alpha)$
0	0	0	$(0,0)$
1	1	1	$(1,0)$
α	α	2	$(0,1)$
α^2	$\alpha+1$	3	$(1,1)$

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	$(\alpha+1=\alpha^2)$	$(\alpha^2+1=\alpha)$
α	α	$(\alpha+1=\alpha^2)$	0	$(\alpha^2+\alpha=1)$
α^2	α^2	$(\alpha^2+1=\alpha)$	$(\alpha^2+\alpha=1)$	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	$(1\cdot\alpha=\alpha)$	$(1\cdot\alpha^2=\alpha^2)$
α	0	$(1\cdot\alpha=\alpha)$	$(\alpha\cdot\alpha=\alpha^2)$	$(\alpha\cdot\alpha^2=\alpha^3=1)$
α^2	0	$(1\cdot\alpha^2=\alpha^2)$	$(\alpha\cdot\alpha^2=\alpha^3=1)$	$(\alpha^2\cdot\alpha^2=\alpha^3\cdot\alpha=\alpha)$

Using the labels,

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Here, integer labels are not usefull since the labels do not represent integers and the operations have no resemblance to modular integer operations.

Example: From page 445.

- For a binary primitive polynomial of degree $m=3$, 1011 and 1101 are primitive polynomials, this means that the smallest positive integer n for which these polynomials divide is when $n = p^m - 1 = 2^3 - 1 = 7$, which is $x^7 - 1$.

(a) for 1011, $P(x) = x^3 + x + 1$

(b) for 1101, $p(x) = x^3 + x^2 + 1$

- For $m=4$, 10011 and 11001 are primitive, this means that $n = 2^4 - 1 = 15$, where they divide $x^{15} - 1$ without a remainder.

(a) for 10011, $P(x) = x^4 + x + 1$

(b) for 11001, $P(x) = x^4 + x^3 + 1$

Example: $GF(8)$:

$p(X) = X^3 + X + 1$ is primitive in $GF(2)[X]$.

Let α be a root of $p(X)$, then $\alpha^3 + \alpha + 1 = 0$.

Exponential	Polynomial	Vector space: $(1, \alpha, \alpha^2)$
0	0	$(0,0,0)$
α	α	$(0,1,0)$
α^2	α^2	$(0,0,1)$
α^3	$\alpha+1$	$(1,1,0)$
α^4	$\alpha^3 . \alpha = (\alpha+1).\alpha = \alpha^2+\alpha$	$(0,1,1)$
α^5	$\alpha^4 . \alpha = (\alpha^2+\alpha).\alpha = \alpha^3+\alpha^2 = \alpha+1+\alpha^2 = \alpha^2+\alpha+1$	$(1,1,1)$
α^6	$\alpha^5 . \alpha = (\alpha^2+\alpha+1).\alpha = \alpha^3+\alpha^2+\alpha = \alpha+1+\alpha^2+\alpha = \alpha^2+1$	$(1,0,1)$
$\alpha^7 = 1$	1	$(1,0,0)$

- The Galois field vector-space representations for $GF(2^m)$ is listed in Appendix B.

Theorem:

The roots of a degree m primitive polynomial $p(x) \in GF(p)[x]$ have order $p^m - 1$.

Explanation:

The roots of a degree m primitive polynomial $p(x) \in GF(p)[x]$ are primitive elements in $GF(p^m)$. Since primitive elements in $GF(p^m)$ all have an order equal to the number of nonzero elements in such Galois field, then their order is

$$\text{card}[GF(p^m) - \{0\}] = p^m - 1.$$

Also, since the smallest positive integer n where $p(x) \mid x^n - 1$ is when $n = p^m - 1$, this means that for some $f(x)$, $p(x)f(x) = x^{p^m-1} - 1$

and since for some root α,

$p(\alpha)f(\alpha) = \alpha^{p^m-1} - 1 = 0$ (α is a root of $p(x)$).

Then $\alpha^{p^m-1} - 1 = 0$

$\alpha^{p^m-1} = 1$ where $n = p^m - 1$ is

the smallest positive integer.

Thus, the order of a primitive element α

is $p^m - 1$.

- Using vector space representation from the polynomial representation reduces field mathematics for $GF(p^m)$ addition to vector addition over $GF(p)$. This makes the software and hardware of the operations simpler.
- Galois fields of prime power order p^m, $GF(p^m)$, are called extensions of the field of prime order p, $GF(p)$. Also, $GF(p^m)$ contains $GF(p)$ and is constructed over $GF(p)$.
- Fields contain subfields, same as groups contain subgroups.
- A subfield S is a proper subfield in a field F if $S \subset F$ and $S \neq F$.
- $GF(p^m)$ contains all Galois fields of order p^b, where b divides m.

Example: Subfields and Proper Subfields:

(a) For $GF(64)$:

$GF(64) = GF(2^6)$

since 1, 2, 3, 6 divide 6 with zero remainder,

Subfields: $GF(2)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$

Proper subfields: all the above subfields except $GF(2^6)$

(b) For $GF(59049)$

$GF(59049) = GF(3^{10})$

since 1, 2, 5, 10 divide 10 with zero remainder,

Subfields: $GF(3)$, $GF(3^2)$, $GF(3^5)$, $GF(3^{10})$

Proper subfields: all the above subfields except $GF(3^{10})$

Theorem:

An element β in $GF(q^m)$ lies in the subfield $GF(q)$ if and only if $\beta^q = \beta$.

Proof: **Assume** that $\beta \in GF(q)$, then β is a root of the polynomial $x^{q-1} - 1$.

Then, $\beta^{q-1} - 1 = 0 \Rightarrow \beta^{q-1} = 1$

$$\beta^{q-1} \cdot \beta = 1 \cdot \beta$$

$$\beta^q = \beta .$$

Assume that $\beta^q = \beta$, then $\beta^{q-1} = 1$ which means that β has an order of $q-1$, this implies that β is a primitive element in $GF(q)$ that can construct the set of all nonzero elements in $GF(q)$ using the first $(q-1)$ consecutive powers of β.

Example: Subfield Elements in $GF(64)$:

$GF(64) = GF(2^6)$

Subfields: $GF(2), GF(2^2), GF(2^3), GF(2^6)$

Let α be a primitive element in $GF(64)$,

(a) For $GF(2)$:

$\beta \in GF(2)$ if and only if $\beta^q = \beta \Rightarrow \beta^2 = \beta$

which is when $\beta = 1$, this means that

$\beta = \alpha^i = 1$ when $i = 63$.

So $\beta = \alpha^{63} = 1$. Thus $GF(2) = \{0, \alpha^{63} = 1\}$

(b) For $GF(2^2)$:

$\beta \in GF(4)$ if and only if $\beta^4 = \beta \Rightarrow \beta^3 = 1$.

This means that $\beta^3 = (\alpha^i)^3 = 1$ when $3i = 63$

so $i = 21$. Thus $\beta = \alpha^{21}$.

$GF(4) = \{0, \alpha^{21}, (\alpha^{21})^2 = \alpha^{42}, (\alpha^{21})^3 = \alpha^{63} = 1\}$

$GF(4) = \{0, \alpha^{21}, \alpha^{42}, \alpha^{63} = 1\}$

(c) For $GF(2^3)$:

$\beta \in GF(8)$ if and only if $\beta^8 = \beta \Rightarrow \beta^7 = 1$.

This means that $\beta^7 = (\alpha^i)^7 = 1$ when $7i = 63$

so $i = 9$. Thus $\beta = \alpha^9$.

$GF(8) = \{0, \alpha^9, (\alpha^9)^2 = \alpha^{18}, (\alpha^9)^3 = \alpha^{27}, (\alpha^9)^4 = \alpha^{36},$
$(\alpha^9)^5 = \alpha^{45}, (\alpha^9)^6 = \alpha^{54}, (\alpha^9)^7 = \alpha^{63} = 1\}$

$GF(8) = \{0, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}, \alpha^{63} = 1\}$

(d) For $GF(2^6)$:

$\beta = \alpha$

Note: From the above example, $GF(p^m)$: $GF(2^6)$ can be represented as 6-dimensional subspace over $GF(p)$: $GF(2)$. Also, from above $GF(2^2)$ can be represented as 2-dimensional subspace over $GF(2)$, where $GF(2)$ is a

subfield of $GF(2^2)$ of prime 2 to a power.
So, in general, it is possible to represent $GF(q^m)$ as an m-dimensional subspace over $GF(q)$, where q is a prime to a power.

2.4 Zech's Logarithms:

In $GF(q)$ with q as a prime power, addition is not as simple as multiplication. A $q \times q$ table of all possible additions can be constructed and used. However, it is a large table for large q values. A more efficient use of memory is obtained by Zech's logarithms, it is also called add-one table.

It is a $q \times 2$ table. The first column contains the logarithm to the base α of all q elements with α as the primitive element. The second column contains the logarithm to the base α of all q elements after adding one to it.

- Add-one tables for $GF(8)$ through $GF(64)$ are included in Appendix B.

Example: Add-One Table for GF(8):

For the primitive polynomial $p(x) = x^3+x+1$ and with α as a root, then $p(\alpha) = \alpha^3+\alpha+1 = 0$.

x	$\log_\alpha x$	x in vector space $(1,\alpha,\alpha^2)$	$(x+1)$ in vector space $(x+(1,0,0))$ $(1,\alpha,\alpha^2)$	$\log_\alpha(x+1)$
α	1	(0,1,0)	(1,1,0)	3
α^2	2	(0,0,1)	(1,0,1)	6
α^3	3	(1,1,0)	(0,1,0)	1
α^4	4	(0,1,1)	(1,1,1)	5
α^5	5	(1,1,1)	(0,1,1)	4
α^6	6	(1,0,1)	(0,0,1)	2
$\alpha^7=1$	0	(1,0,0)	(0,0,0)	* : undefined
0	* : undefined	(0,0,0)	(1,0,0)	0

$\alpha^4 = \alpha^3 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2+\alpha$

$\alpha^5 = \alpha^4\cdot\alpha = (\alpha^2+\alpha)\cdot\alpha = \alpha^3+\alpha^2 = \alpha+1+\alpha^2 = \alpha^2+\alpha+1$

$\alpha^6 = \alpha^5\cdot\alpha = (\alpha^2+\alpha+1)\cdot\alpha = \alpha^3+\alpha^2+\alpha = \alpha+1+\alpha^2+\alpha = \alpha^2+1$

- The $\log_\alpha x$ and the $\log_\alpha(x+1)$ columns are stored in a read-only-memory (ROM) look-up table.
- To perform addition in $GF(p^m)$ using the add-one table, the following is done:

(1) Combine all terms that have the same exponent using mod addition in $GF(p)$.

(2) Arrange the resulting expression in a decreasing form in terms of exponents as:

$$\alpha^a + \alpha^b + \alpha^c + \cdots + \alpha^z$$

(3) Factor the expression into the form

$$\left(\cdots \left(\left((\alpha^{a-b}+1)\alpha^{b-c}+1 \right) \alpha^{c-d}+1 \right) \cdots \right) \alpha^z ,$$

then this expression can be solved as a series of add-one operations and Galois field multiplications.

Example: GF(8) Addition Using Add-One Table:

From the previous example:

x	$\log_\alpha x$	$\log_\alpha (x+1)$
α	1	3
α^2	2	6
α^3	3	1
α^4	4	5
α^5	5	4
α^6	6	2
$\alpha^7=1$	0	* : undefined
0	* : undefined	0

Solve the addition of:

$$\alpha^6+\alpha^5+\alpha^7+\alpha^6+\alpha^3+\alpha^3+\alpha^3+\alpha+1 =$$

$$(1+1)\alpha^6+\alpha^5+\alpha^7+(1+1+1)\alpha^3+\alpha+1 =$$

$$(0)\alpha^6+\alpha^5+\alpha^7+(1)\alpha^3+\alpha+1 =$$

$$\alpha^7+\alpha^5+\alpha^3+\alpha+1 =$$

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

OR $$((((((\alpha+0)\alpha+1)\alpha+0)\alpha+1)\alpha+0)\alpha+1)\alpha+1$$

Then for $(((\underbrace{\alpha^2+1}_{6\to\alpha^6})\alpha^2+1)\alpha^2+1)\alpha+1 =$

$$((\underbrace{\alpha^6.\alpha^2}_{\alpha}+1)\alpha^2+1)\alpha+1 =$$

$$((\underbrace{\alpha+1}_{3\to\alpha^3})\alpha^2+1)\alpha+1 =$$

$$(\underbrace{\alpha^5+1}_{4\to\alpha^4})\alpha+1 =$$

$$\alpha^5+1 = \boxed{\alpha^4}$$

Problems:

(2.1) Prove that the identity element e in a group G is unique.

Proof: Let $(G, \cdot)$ represent a group under the operation "$\cdot$". Suppose the identity element is not unique. Let e_1 and e_2 be two identity elements where $e_1 \neq e_2$. Then there exists an element $a \in G$ where

$a.e_1 = a$ (e_1 : identity element)

$a.e_2 = a$ (e_2 : identity element)

As $a = a$,

then $a.e_1 = a.e_2$

so $e_1 = e_2$ (contradiction).

Thus, the identity element is unique.

(2.5) Construct the operation table for the group of order 6 under modulo 6 addition.

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

(2.23) Prove that

$$\phi(p_1 \cdot p_2) = \phi(p_1) \cdot \phi(p_2) = (p_1 - 1)(p_2 - 1)$$

for distinct primes p_1 and p_2.

Proof:

Since $\phi(t) = \text{card}\left[\{1 \leq i < t \mid GCD(i, t) = 1\}\right]$

$$= t \prod_{p \mid t} \left(1 - \frac{1}{p}\right)$$

which is the number of integers in the set $\{1, 2, 3, \ldots, t-1\}$ that are relatively prime to t.

Then $\phi(p_1 \cdot p_2) = \text{card}\left[\{1 \leq i < p_1 \cdot p_2 \mid GCD(i, p_1 \cdot p_2) = 1\}\right]$

$$= p_1 \cdot p_2 \prod_{p \mid (p_1 \cdot p_2)} \left(1 - \frac{1}{p}\right)$$

$$= p_1 \cdot p_2 \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

$$= p_1 \cdot p_2 \left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)$$

$$= (p_1 - 1)(p_2 - 1)$$

(2.26) Prove that $\sum_{x|n} \phi(x) = n$.

Proof:

Let $n = p^m$ for some prime p and integer m, then all $x = p^r$, $r \in \{0, 1, \dots, m\}$ will divide n with zero remainder.

Then

$$\sum_{x|n} \phi(x) = \sum_{r \in \{0,1,\dots,m\}} \phi(p^r)$$

$$= \phi(1) + \phi(p) + \phi(p^2) + \phi(p^3) + \dots + \phi(p^{m-1}) + \phi(p^m)$$

since $\phi(p^r) = p^{r-1}(p-1)$ then

$$\sum_{x|n} \phi(n) = 1 + (p-1) + p(p-1) + p^2(p-1) + \dots + p^{m-2}(p-1) + p^{m-1}(p-1)$$

$$= 1 + p - 1 + p^2 - p + p^3 - p^2 + \dots + p^{m-1} - p^{m-2} + p^m - p^{m-1}$$

$$\sum_{x|n} \phi(n) = p^m = n$$

(2.19) V_5 is the vector space of binary 5-tuples.
The canonical vector space for V_5 is
$\{(10000), (01000), (00100), (00010), (00001)\}$.
Express the vector (11010) as a linear combination of the vectors in the canonical basis for V_5.

$$\begin{aligned}(11010) &= 1.(10000) + 1.(01000) + 0.(00100) \\ &\quad + 1.(00010) + 0.(00001) \\ &= (10000) + (01000) + (00010)\end{aligned}$$

(2.20) $S = \{(11010), (00111), (10101), (10001), (00010)\}$ also forms a basis for V_5. Express the vector (10111) as a linear combination of the vectors in S.

Let $\vec{v}_i \in S$ denote the basis vectors

Let $a_i \in F$. Then we try different combinations of the basis to find the vector (10111).

$\vec{v}_1$ (11010)	$\vec{v}_2$ (00111)	$\vec{v}_3$ (10101)	$\vec{v}_4$ (10001)	$\vec{v}_5$ (00010)	$\sum a_i \vec{v}_i$
0	0	0	1	1	(10011)
0	0	1	1	1	(00110)
0	0	1	1	0	(00101)
0	0	1	0	1	(10111)

$$(10111) = 0\cdot(11010) + 0\cdot(00111) + 1\cdot(10101) + 0\cdot(10001) + 1\cdot(00010)$$

$$= (10101) + (00010)$$

(2.22) List the possible orders taken on by the elements in the field GF(125) and determine the number of elements in the field that display each allowed order.

Since for an element $\beta \in GF(125)$,

$$\text{ord}(\beta) \mid (125-1) \quad =: \quad \text{ord}(\beta) \mid 124 .$$

The factors of 124 are :

2	124
2	62
31	31
	1

So the following numbers divides 124 with zero remainder

1, 2, 4, 31, 62, 124

$$\phi(t) = t \prod_{p \mid t} (1-p)$$

$$\phi(1) = 1$$

$$\phi(2) = (2-1) = 1$$

$$\phi(4) = \phi(2 \cdot 2) = 4\left(1 - \frac{1}{2}\right) = 2$$

$$\phi(31) = (31-1) = 30$$

$$\phi(63) = \phi(31\cdot 2) = \phi(31)\cdot\phi(2) = 30\cdot 1 = 30$$

$$\phi(124) = \phi(31\cdot 2\cdot 2) = 124\left(1-\frac{1}{31}\right)(1-2)$$

$$= 124\left(\frac{30}{31}\right)\left(\frac{1}{2}\right) = (2)(30) = 60$$

If we add all ϕ for the possible orders:

$$\Sigma\phi = \phi(1) + \phi(2) + \phi(4) + \phi(31) + \phi(63)$$

$$+ \phi(124)$$

$$= 1 + 1 + 2 + 30 + 30 + 60$$

$\Sigma\phi = 124$ =: number of nonzero elements in $GF(125)$.

(2.28) Express all of the nonzero elements of $GF(11)$ as powers of a single element in $GF(11)$.

We should find an element that is primitive in $GF(11)$.

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 11 + 5 = 5 \bmod 11$,

$2^5 = 32 = 2(11) + 10 = 10 \bmod 11$, $2^6 = 64 = 5(11) + 9 = 9 \bmod 11$,

$2^7 = 128 = 11(11) + 7 = 7 \bmod 11$, $2^8 = 256 = 23(11) + 3 = 3 \bmod 11$,

$2^9 = 512 = 46(11) + 6 = 6 \bmod 11$, $2^{10} = 1024 = 93(11) + 1 = 1 \bmod 11$

So $2^{10} = 1$, $\operatorname{ord}(2) = 10$.

This means 2 is a primitive element and we can write all elements of $GF(11)$ as some power of 2.

element	interms of 2^i
1	2^{10}
2	2^1

3	2^8
4	2^2
5	2^4
6	2^9
7	2^7
8	2^3
9	2^6
10	2^5

(2.34) Use the representation for GF(8) to compute the following:

We found in an example for a primitive polynomial $p(x) = x^3 + x + 1$, if α is a root, then

$\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$, then

Exponential representation	Polynomial representation
0	0
α	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^3 \cdot \alpha = (\alpha+1) \cdot \alpha = \alpha^2 + \alpha$
α^5	$\alpha^4 \cdot \alpha = (\alpha^2 + \alpha) \cdot \alpha = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
α^6	$\alpha^5 \cdot \alpha = (\alpha^2 + \alpha + 1) \cdot \alpha = \alpha^3 + \alpha^2 + \alpha$ $= \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$
$\alpha^7 = 1$	,

(a) $\alpha^4+\alpha^2+\alpha+1 =$

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

(b) $(\alpha^3+\alpha^2)\cdot(\alpha^6+\alpha^3) =$

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

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

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

$\alpha^4+\cancel{\alpha^3}+\cancel{\alpha^3}+\cancel{\alpha^2}+\cancel{\alpha^2}+\alpha =$

$\alpha^2+\cancel{\alpha}+\cancel{\alpha} = \alpha^2$

(c) $\alpha^6\cdot(\alpha^5+\alpha^4)+\alpha^2 =$

$(\alpha^2+1)\cdot(\cancel{\alpha^2}+\cancel{\alpha}+1+\cancel{\alpha^2}+\cancel{\alpha})+\alpha^2 =$

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

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

(d) $(\alpha^3x^2+\alpha x+1)(\alpha^5x^3+x+\alpha^2) =$

$\alpha^3x^2\cdot(\alpha^5x^3+x+\alpha^2)+\alpha x\cdot(\alpha^5x^3+x+\alpha^2)$

$+\alpha^5x^3+x+\alpha^2 =$

$\alpha^7\cdot\alpha\cdot x^5+\alpha^3x^3+\alpha^5x^2+\alpha^6x^4+\alpha x^2+\alpha^3x =$

$\alpha x^5+\alpha^6x^4+\alpha^3x^3+(\alpha^5+\alpha)x^2+\alpha^3x =$

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

$\alpha x^5+(\alpha^2+1)x^5+(\alpha+1)x^3+(\alpha^2+1)x^2+(\alpha+1)x =$

since $\alpha^2+1=\alpha^6$, $\alpha+1=\alpha^3$ we can also write it as

$\alpha x^5+\alpha^6x^5+\alpha^3x^3+\alpha^6x^2+\alpha^3x$

in GF(8)

Polynomials over Galois Fields :

3.1 Euclidean Domains and Euclid's Algorithm :

$GF(q)[x]$ forms a commutative ring with identity.

Recall that the ring is a collection of elements R with two binary operations "+" and "·" such that the following three properties hold:

1. R forms a commutative group under "+".
   The additive identity element is labeled "0".

2. The operation "·" is associative :
   for all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. The operation "·" is distributive over "+"

- A ring is a commutative ring if the operation "·" is commuative : for all $a, b \in R$, $a \cdot b = b \cdot a$
- A ring is a ring with identity if the operation "·" has an identity element, which is labeled "1"

Definition:

A metric is a function that assigns a size (or measure) to an element.

- A commutative ring with identity along with a metric makes the ring a Euclidean domain.

Definition: Euclidean Domains

A Euclidean domain is a set D with two binary operations "+" and "$\cdot$" that satisfy the following:

1. D forms an additive commutative ring with identity.
2. Cancelation property:
   if $a \cdot b = b \cdot c$ and $b \neq 0$, then $a = c$.
3. Every element $a \in D$ has an associated metric $g(a)$ such that:
   (a) for all nonzero $b \in D$, $g(a) \leq g(a \cdot b)$.
   (b) for all nonzero $a, b \in D$, $g(a) > g(b)$, there exist q and r such that: $a = qb + r$ where

either $r=0$ or $g(r) < g(b)$.

with q being called the quotient (ناتج القسمة)

and r the remainder (الباقي).

- Note: For the additive identity element 0, $g(0)$ is undefined.

- The Metric in Euclidean Domains:

(1) The ring of integers under addition and multiplication with metric $g(n)$ where n is an integer.

$$g(n) = |n| \quad : \text{the absolute value.}$$

(2) The ring of polynomials over a finite field with metric $g(f(x))$ where $f(x)$ is a polynomial.

$$g(f(x)) = \text{degree}(f(x)) : \text{the polynomial's degree}$$

- In a Euclidean domain D, let $a, b \in D$,

a is a divisor of b $(a|b)$ if there exists $c \in D$ such that $a \cdot c = b$.

Definition: Common Divisors

An element a is a common divisor of a collection of elements $\{b_1, b_2, b_3, \dots, b_n\}$ if $a|b_i$ for $i = 1, 2, 3, \dots, n$.

Definition: Greatest Common Divisors

If d is a common divisor of $\{b_1, b_2, b_3, \dots, b_n\}$, and all other common divisors are less than d, then d is the greatest common divisor (GCD) of $\{b_1, b_2, b_3, \dots, b_n\}$.

Example : GCD

(a) $GCD(168, 166) = 2$

$$\begin{array}{r|l} 2 & 168 \\ \hline 2 & 84 \\ 2 & 42 \\ 3 & 21 \\ 7 & 7 \\ & 1 \end{array} \qquad\qquad \begin{array}{r|l} 2 & 166 \\ \hline 83 & 83 \\ & 1 \end{array}$$

(b) $GCD(336, 54) = 6$

$$\begin{array}{r|l} 3 & 336 \\ \hline 2 & 112 \\ 2 & 56 \\ 2 & 28 \\ 2 & 14 \\ 7 & 7 \\ & 1 \end{array} \qquad\qquad \begin{array}{r|l} 2 & 54 \\ \hline 3 & 27 \\ 3 & 9 \\ 3 & 3 \\ & 1 \end{array}$$

Euclid's Algorithm: is a method to find the GCD of sets of elements in Euclidean domains.

The algorithm is as follows:

(1) Let $a, b \in D$ with $g(a) > g(b)$

(2) Let r_i with $i = -1, 0, 1, 2, \dots$

with $r_{-1} = a$ and $r_0 = b$.

(3) Repeat the following untill $r_i = 0$

define $r_i = r_{i-2} - q_i r_{i-1}$ with $g(r_i) < g(r_{i-1})$

if $r_i = 0$, then $r_{i-1} = GCD(a,b)$.

- Note: For $a, b, c \in D$,

$$GCD(a,b,c) = GCD\left(GCD(a,b), c\right)$$

Example: Euclid's Algorithm

(a) $GCD(168, 166)$

i	r_i	q_i
-1	168	–
0	166	–
1	2	1
2	0	83

$r_i = r_{i-2} - q_i r_{i-1}$

$r_1 = r_{-1} - q_1 r_0 = 168 - q_1(166)$
$= 168 - (1)(166) = 2$

$r_2 = r_0 - q_2 r_1 = 166 - q_2(2)$
$= 166 - (83)(2) = 0$

So $GCD(168, 166) = r_1 = 2$

Notice that: $GCD(168,166) = 2 = 168 - (1)(166)$

(b) $GCD(336, 54)$

i	r_i	q_i
-1	336	–
0	54	–
1	12	6
2	6	4
3	0	2

$r_i = r_{i-2} - q_i r_{i-1}$

$r_1 = r_{-1} - q_1 r_0 = 336 - q_1(54)$
$= 336 - 6(54) = 12$

$r_2 = r_0 - q_2 r_1 = 54 - q_2(12)$
$= 54 - 4(12) = 6$

$r_3 = r_1 - q_3 r_2 = 12 - q_3(6)$
$= 12 - (2)(6) = 0$

So $GCD(336, 54) = r_2 = 6$

Notice that: $GCD(336,54) = 6 = \overbrace{54 - 4(12)}^{r_2}$
$= 54 - 4[\overbrace{336 - 6(54)}^{r_1}]$
$= 54(25) + 336(-4)$

(c) $GCD(336, 108, 42)$

- $GCD(336, 108)$

i	r_i	q_i
-1	336	-
0	108	-
1	12	3
2	0	9

$r_i = r_{i-2} - q_i r_{i-1}$

$r_1 = r_{-1} - q_1 r_0 = 336 - q_1(108)$
$= 336 - (3)(108) = 12$

$r_2 = r_0 - q_2 r_1 = 108 - q_2(12)$
$= 108 - 9(12) = 0$

So $GCD(336, 108) = r_1 = 12$

Now $GCD(336, 108, 42) = GCD(GCD(336, 108), 42) = GCD(42, 12)$

- $GCD(42, 12)$

i	r_i	q_i
-1	42	-
0	12	-
1	6	3
2	0	2

$r_1 = r_{-1} - q_1 r_0 = 42 - q_1(12)$
$= 42 - (3)(12) = 6$

$r_2 = r_0 - q_2 r_1 = 12 - q_2(6)$
$= 12 - (2)(6) = 0$

$GCD(42, 12) = r_1 = 6$

So $GCD(336, 108, 42) = 6$

(d) $GCD(x^5+x^3+x+1,\ x^4+x^2+x+1)$ where the polynomials are from $GF(2)[x]$.

i	r_i	q_i
-1	x^5+x^3+x+1	—
0	x^4+x^2+x+1	—
1	x^2+1	x
2	$x+1$	x^2
3	0	x^2+1

$r_i = r_{i-2} - q_i r_{i-1}$

$$r_1 = r_{-1} - q_1 r_0 = x^5+x^3+x+1 - q_1(x^4+x^2+x+1)$$
$$= x^5+x^3+x+1 - x\cdot(x^4+x^2+x+1)$$
$$= x^5+x^3+x+1 - (x^5+x^3+x^2+x) = x^2+1$$

$$r_2 = r_0 - q_2 r_1 = x^4+x^2+x+1 - q_2(x^2+1)$$
$$= x^4+x^2+x+1 - x^2\cdot(x^2+1)$$
$$= x^4+x^2+x+1 - (x^4+x^2) = x+1$$

$$r_3 = r_1 - q_3 r_2 = x^2+1 - q_3(x+1)$$

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

$$= x^2+1 - \left(x^2 + (1+1)x + 1\right)$$

$$= x^2+1 - (x^2+1) = 0$$

$$\mathrm{GCD}\left(x^5+x^3+x+1,\ x^4+x^2+x+1\right) = r_2 = x+1$$

Note: $\mathrm{GCD}(a,b)$ can be written as a linear combination of a and b.

Theorem :

Let $B = \{b_1, b_2, b_3, \dots, b_n\} \subset D$ with $GCD(B) = d$, then $d = \sum_{i=1}^{n} \lambda_i b_i$ where $\{\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n\} \subset D$.

i.e. If $GCD(B) = d$, then d can be written as a linear combination of the elements of B.

- In the previous example, we were able to obtain the coefficients of the linear combination by working backwards in the steps. We can obtain them in a more direct method using the extended version of Euclid's algorithm.

The Extended Version of Euclid's Algorithm :

Using this method, we can find the GCD of sets of elements in Euclidean domains along with the coefficients of their linear combination to express the GCD.

The algorithm is as follows :

(1) Let $a, b \in D$ with $g(a) > g(b)$

(2) Let r_i, s_i, t_i with $i = -1, 0, 1, 2, \ldots$

with $r_{-1} = a \;,\; r_0 = b$

$s_{-1} = 1 \;,\; s_0 = 0$

$t_{-1} = 0 \;,\; t_0 = 1$

(3) Repeat the following untill $r_i = 0$

define $r_i = r_{i-2} - q_i r_{i-1}$ with $g(r_i) < g(r_{i-1})$

$s_i = s_{i-2} - q_i s_{i-1}$

$t_i = t_{i-2} - q_i t_{i-1}$

if $r_i = 0$, then $r_{i-1} = GCD(a, b)$ and

$r_{i-1} = s_{i-1} a + t_{i-1} b$.

(This provides the linear combination of a and b with the GCD(a,b) as the remainder).

- It is true for any i

$r_i = s_i a + t_i b$ with an r_i remainder.

- Since $r_i = s_i a + t_i b$ and $r_i = r_{i-2} - q_i r_{i-1}$,

then $r_i = r_{i-2} - q_i r_{i-1}$

$$= (s_{i-2} a + t_{i-2} b) - q_i (s_{i-1} a + t_{i-1} b)$$

$$r_i = [s_{i-2} - q_i s_{i-1}] a + [t_{i-2} - q_i t_{i-1}] b$$

also, $r_i = s_i a + t_i b$, then

$s_i = s_{i-2} - q_i s_{i-1}$ and $t_i = t_{i-2} - q_i t_{i-1}$

Example :

$$r_i = r_{i-2} - q_i r_{i-1}$$
$$s_i = s_{i-2} - q_i s_{i-1}$$
$$t_i = t_{i-2} - q_i t_{i-1}$$
$$r_i = s_i a + t_i b$$

(a) GCD(256, 108)

i	r_i	q_i	s_i	t_i
-1	256	—	1	0
0	108	—	0	1
1	40	2	1	-2
2	28	2	-2	5
3	12	1	3	-7
4	4	2	-8	19
5	0	3	27	-64

$256 = 256(1) + 108(0)$
$108 = 256(0) + 108(1)$
$40 = 256(1) + 108(-2)$
$28 = 256(-2) + 108(5)$
$12 = 256(3) + 108(-7)$
$4 = 256(-8) + 108(19)$
$0 = 256(27) + 108(-64)$

$r_1 = r_{-1} - q_1 r_0 = 256 - q_1 108 = 256 - (2)(108) = 40$
$s_1 = s_{-1} - q_1 s_0 = 1 - (2)(0) = 1$
$t_1 = t_{-1} - q_1 t_0 = 0 - (2)(1) = -2$

$r_2 = r_0 - q_2 r_1 = 108 - q_2 40 = 108 - (2)40 = 28$
$s_2 = s_0 - q_2 s_1 = 0 - (2)(1) = -2$
$t_2 = t_0 - q_2 t_1 = 1 - (2)(-2) = 5$

$r_3 = r_1 - q_3 r_2 = 40 - q_3 28 = 40 - (1)28 = 12$
$s_3 = s_1 - q_3 s_2 = 1 - (1)(-2) = 3$
$t_3 = t_1 - q_3 t_2 = -2 - (1)(5) = -7$

$r_4 = r_2 - q_4 r_3 = 28 - q_4 12 = 28 - 2(12) = 4$
$s_4 = s_2 - q_4 s_3 = -2 - (2)(3) = -8$
$t_4 = t_2 - q_4 t_3 = 5 - (2)(-7) = 19$

$r_5 = r_3 - q_5 r_4 = 12 - q_5 4 = 12 - (3)(4) = 0$
$s_5 = s_3 - q_5 s_4 = 3 - (3)(-8) = 27$
$t_5 = t_3 - q_5 t_4 = -7 - (3)(19) = -64$

$GCD(256, 108) = r_4 = 4$

and the linear combination of $GCD(256,108) = 4$ is

$$4 = 256(-8) + 108(19)$$

(b) GCD(336, 54)

i	r_i	q_i	s_i	t_i
-1	336	—	1	0
0	54	—	0	1
1	12	6	1	-6
2	6	4	-4	25
3	0	2	9	-56

$336 = 336(1) + 54(0)$
$54 = 336(0) + 54(1)$
$12 = 336(1) + 54(-6)$
$6 = 336(-4) + 54(25)$
$0 = 336(9) + 54(-56)$

$r_i = r_{i-2} - q_i r_{i-1}$
$s_i = s_{i-2} - q_i s_{i-1}$
$t_i = t_{i-2} - q_i t_{i-1}$
$r_i = s_i a + t_i b$

$r_1 = r_{-1} - q_1 r_0 = 336 - q_1 54 = 336 - 6(54) = 12$
$s_1 = s_{-1} - q_1 s_0 = 1 - (6)(0) = 1$
$t_1 = t_{-1} - q_1 t_0 = 0 - (6)(1) = -6$

$r_2 = r_0 - q_2 r_1 = 54 - q_2 12 = 54 - (4)(12) = 6$
$s_2 = s_0 - q_2 s_1 = 0 - (4)(1) = -4$
$t_2 = t_0 - q_2 t_1 = 1 - (4)(-6) = 25$

$r_3 = r_1 - q_3 r_2 = 12 - q_3 6 = 12 - (2)(6) = 0$
$s_3 = s_1 - q_3 s_2 = 1 - (2)(-4) = 9$
$t_3 = t_1 - q_3 t_2 = -6 - (2)(25) = -56$

$GCD(336, 54) = r_2 = 6$ and $6 = 336(-4) + 54(25)$

3.2 Minimal Polynomials and Conjugate Elements:

Definition: Minimal Polynomials

Let $\alpha \in GF(q^m)$. The minimal polynomial of α with respect to $GF(q)$ is the smallest-degree nonzero polynomial $p(x) \in GF(q)[x]$ such that $p(\alpha) = 0$.

. The properties of minimal polynomials are presented in the following theorem.

Theorem:

For each element $\alpha \in GF(q^m)$ there exists a unique monic polynomial $p(x) \in GF(q)[x]$ of minimal degree such that:

(1) $p(\alpha) = 0$

(2) $\text{degree}(p(x)) \leq m$

(3) If there exists a $f(x)$ with $f(\alpha) = 0$, then $f(x)$ is

a multiple of $p(x)$.

(4) $p(x)$ is irreducible in $GF(q)[x]$.

Note: Monic polynomial is a polynomial whose leading coefficient is 1.

i.e. a polynomial of degree n whose coefficient of x^n is 1.

- Note: primitive polynomials are minimal polynomials for primitive elements in a Galois field.

- For (3), $f(x)$ should be a multiple of $p(x)$, otherwise, there will exist another polynomial, say $r(x)$ such that $f(x) = p(x)\,q(x) + r(x)$ where $\text{degree}(r(x)) < \text{degree}(p(x))$ and this contradicts with the minimality of $p(x)$.

Thus, $f(x)$ should be a multiple of $p(x)$.

- Since $\alpha \in GF(q^m)$ is a root of $p(x) \in GF(q)[x]$, what are the other roots of $p(x)$?

3.2 Minimal Polynomials and Conjugate Elements:

Definition: Minimal Polynomials

Let $\alpha \in GF(q^m)$. The minimal polynomial of α with respect to $GF(q)$ is the smallest-degree nonzero polynomial $p(x) \in GF(q)[x]$ such that $p(\alpha) = 0$.

. The properties of minimal polynomials are presented in the following theorem.

Theorem:

For each element $\alpha \in GF(q^m)$ there exists a unique monic polynomial $p(x) \in GF(q)[x]$ of minimal degree such that:

(1) $p(\alpha) = 0$

(2) $\text{degree}(p(x)) \leq m$

(3) If there exists a $f(x)$ with $f(\alpha) = 0$, then $f(x)$ is

a multiple of $p(x)$.

(4) $p(x)$ is irreducible in $GF(q)[x]$.

Note: Monic polynomial is a polynomial whose leading coefficient is 1.

i.e. a polynomial of degree n whose coefficient of x^n is 1.

- Note: primitive polynomials are minimal polynomials for primitive elements in a Galois field.

- For (3), $f(x)$ should be a multiple of $p(x)$, otherwise, there will exist another polynomial, say $r(x)$ such that $f(x) = p(x)q(x) + r(x)$ where $\text{degree}(r(x)) < \text{degree}(p(x))$ and this contradicts with the minimality of $p(x)$.

Thus, $f(x)$ should be a multiple of $p(x)$.

- Since $\alpha \in GF(q^m)$ is a root of $p(x) \in GF(q)[x]$, what are the other roots of $p(x)$?

Definition: **Conjugates of Field Elements**

Let $\beta \in GF(q^m)$. The conjugates of β with respect to the subfield $GF(q)$ are the elements

$$\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \dots$$

- The conjugates of an element form a set called conjugacy class.

Theorem:

The conjugacy class of $\alpha \in GF(q^m)$ with respect to $GF(q)$ contains d elements, where $\alpha^{q^d} = \alpha$ and $d | m$.

Note: Since in $GF(q^m)$ the first element to repeat is $1 = \alpha^{(q^m - 1)}$, then $\alpha = \alpha^{q^m}$.

While in $GF(q)$ the first element to repeat is $\alpha = \alpha^{q^d}$.

Thus, $\alpha^{q^m} = \alpha^{q^d} = \alpha$

Since q is a prime or a power of a prime, $m > d$, and α^{q^d} is the first to repeat as α, then $d = GCD(m, d)$. Thus, d/m.

Example: Conjugacy Classes

(a) $\alpha \in GF(16)$, $ord(\alpha) = 3$. The conjugacy class of α with respect to $GF(2)$ is:

since $ord(\alpha) = 3$, then $\alpha^3 = 1$, then

$$\{\alpha, \alpha^2 = \alpha^2, \alpha^{2^2} = \alpha^4 = \alpha^3 \cdot \alpha = \alpha\} = \{\alpha, \alpha^2\}$$

(b) $\alpha \in GF(64)$, $ord(\alpha) = 63$. The conjugacy class of α with respect to $GF(4)$ is:

since $ord(\alpha) = 63$, then $\alpha^{63} = 1$, then

$$\{\alpha, \alpha^4, \alpha^{4^2} = \alpha^{16}, \alpha^{4^3} = \alpha^{64} = \alpha^{63} \cdot \alpha = 1\} = \{\alpha, \alpha^4, \alpha^{16}\}$$

(c) $\alpha \in GF(25)$, $ord(\alpha) = 6$. The conjugacy class of α with respect to $GF(5)$ is: $\alpha^6 = 1$

$$\{\alpha, \alpha^5, \alpha^{5^2} = \alpha^{25} = (\alpha^6)^4 \cdot \alpha = \alpha\} = \{\alpha, \alpha^5\}$$

Theorem:

Let $\alpha \in GF(q^m)$. Let $p(x)$ be the minimal polynomial of α with respect to $GF(q)$. The roots of $p(x)$ are exactly the conjugates of α with respect to $GF(q)$.

Note: Since all of the conjugates of α with respect to $GF(q)$ are roots of $p(x)$, then the coefficients of the minimal polynomial $p(x)$ are in the subfield $GF(q)$.

Example: The Minimal Polynomials of the Elements in GF(8) with Respect to GF(2):

If we use the primitive polynomial $p(x) = x^3 + x + 1$ and α as a root, using the below table:

Exponential representation	Polynomial representation
$\alpha^0 = 1$	1
α^1	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$
0	0

The conjugacy classes are as follows :

- $\{0\}$.
- $\{1\}$
- $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^4, \alpha^{2^3} = \alpha^8 = \alpha^7 \cdot \alpha = \alpha\} = \{\alpha, \alpha^2, \alpha^4\}$
- $\{\alpha^3, (\alpha^3)^{2^1} = \alpha^6, (\alpha^3)^{2^2} = (\alpha^3)^4 = \alpha^{12} = \alpha^7 \cdot \alpha^5 = \alpha^5,$
  $(\alpha^3)^{2^3} = (\alpha^3)^8 = \alpha^{24} = (\alpha^7)^3 \cdot \alpha^3 = \alpha^3\} = \{\alpha^3, \alpha^6, \alpha^5\}$

- The minimal polynomials computed from the conjugacy classes :

Conjugacy class	Minimal polynomial
$\{0\}$	$M_*(x) = (x-0) = x$
$\{1\}$	$M_0(x) = (x-1) = x+1$
$\{\alpha, \alpha^2, \alpha^4\}$	$M_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$
	$M_1(x) = x^3 + x + 1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$M_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$
	$M_3(x) = x^3 + x^2 + 1$

$$M_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$$
$$= \left(x^2 - (\alpha+\alpha^2)x + \alpha^3\right)(x-\alpha^4)$$
$$= (x^2 - \alpha^4 x + \alpha^3)(x-\alpha^4)$$
$$= x^3 - \alpha^4 x^2 + \alpha^3 x - \alpha^4 x^2 + \alpha x - 1$$
$$= x^3 + (\alpha^3+\alpha)x + 1$$
$$M_1(x) = x^3 + x + 1$$
$$M_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5)$$
$$= \left(x^2 - (\alpha^3+\alpha^6)x + \alpha^2\right)(x-\alpha^5)$$
$$= \left(x^2 - (\alpha+1+\alpha^2+1)x + \alpha^2\right)(x-\alpha^5)$$
$$= \left(x^2 - (\alpha^2+\alpha)x + \alpha^2\right)(x-\alpha^5)$$
$$= (x^2 + \alpha^4 x + \alpha^2)(x-\alpha^5)$$
$$= x^3 + \alpha^4 x^2 + \alpha^2 x + \alpha^5 x^2 + \alpha^2 x + 1$$
$$= x^3 + (\alpha^4+\alpha^5)x^2 + 1$$
$$= x^3 + (\alpha^2+\alpha+\alpha^2+\alpha+1)x^2 + 1$$
$$M_3(x) = x^3 + x^2 + 1$$

where the index of a minimal polynomial is the smallest logarithm to the base α of the roots of the polynomial.

Example: **The Minimal Polynomials of the Elements in GF(16) with respect to GF(4):**

Let α be a root of the primitive polynomial

$p(x) = x^4 + x + 1$.

Exponential representation	Polynomial representation
0	0
1	1
α	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$ since $\alpha^4+\alpha+1=0$
α^5	$\alpha^4.\alpha = (\alpha+1).\alpha = \alpha^2+\alpha$
α^6	$\alpha^5.\alpha = (\alpha^2+\alpha).\alpha = \alpha^3+\alpha^2$
α^7	$\alpha^4.\alpha^3 = (\alpha+1).\alpha^3 = \alpha^4+\alpha^3 = \alpha^3+\alpha+1$

$\alpha^8 \quad \alpha^4 \cdot \alpha^4 = (\alpha+1)\cdot(\alpha+1) = \alpha^2 + (1+1)\alpha + 1$

$= \alpha^2 + 1$

$\alpha^9 \quad \alpha^8 \cdot \alpha = (\alpha^2+1)\cdot\alpha = \alpha^3 + \alpha$

$\alpha^{10} \quad \alpha^9 \cdot \alpha = (\alpha^3+\alpha)\cdot\alpha = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$

$\alpha^{11} \quad \alpha^{10} \cdot \alpha = (\alpha^2+\alpha+1)\cdot\alpha = \alpha^3 + \alpha^2 + \alpha$

$\alpha^{12} \quad \alpha^{11} \cdot \alpha = (\alpha^3+\alpha^2+\alpha)\cdot\alpha = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^{13} \quad \alpha^{10} \cdot \alpha^3 = (\alpha^2+\alpha+1)\cdot\alpha^3 = \alpha^5 + \alpha^4 + \alpha^3$

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

$\alpha^{14} \quad \alpha^{13} \cdot \alpha = (\alpha^3+\alpha^2+1)\cdot\alpha = \alpha^4 + \alpha^3 + \alpha = \alpha + 1 + \alpha^3 + \alpha$

$= \alpha^3 + 1$

The coefficients of minimal polynomials will be in $GF(4)$, a subfield of $GF(16)$.

This subfield will have the elements in $GF(16)$ such that $\beta^4 = \beta \Rightarrow \beta^3 = 1 \Rightarrow (\alpha^i)^3 = 1 \Rightarrow 3i = 15$

$\Rightarrow i = 5$.

So the subfield is $\{0, 1, \alpha^5, \alpha^{10}, \alpha^{15} = 1\} = \{0, 1, \alpha^5, \alpha^{10}\}$

The conjugacy classes are :

$\boxed{\{0\}}$, $\boxed{\{1\}}$,

$\{\alpha, \alpha^4, \alpha^{4^2} = \alpha^{16} = \alpha^{15}.\alpha = \alpha\} = \boxed{\{\alpha, \alpha^4\}}$,

$\{\alpha^2, (\alpha^2)^4 = \alpha^8, (\alpha^2)^{4^2} = (\alpha^2)^{16} = \alpha^{32} = (\alpha^{15})^2.\alpha^2 = \alpha^2\} = \boxed{\{\alpha^2, \alpha^8\}}$,

$\{\alpha^3, (\alpha^3)^4 = \alpha^{12}, (\alpha^3)^{4^2} = (\alpha^3)^{16} = \alpha^{48} = (\alpha^{15})^3.\alpha^3 = \alpha^3\} = \boxed{\{\alpha^3, \alpha^{12}\}}$,

$\{\alpha^5, (\alpha^5)^4 = \alpha^{20} = \alpha^{15}.\alpha^5 = \alpha^5\} = \boxed{\{\alpha^5\}}$

$\{\alpha^6, (\alpha^6)^4 = \alpha^{24} = \alpha^{15}.\alpha^9 = \alpha^9, (\alpha^6)^{4^2} = (\alpha^6)^{16} = \alpha^{96} = \alpha^{90}.\alpha^6$

$= (\alpha^{15})^6.\alpha^6 = \alpha^6\} = \boxed{\{\alpha^6, \alpha^9\}}$

$\{\alpha^7, (\alpha^7)^4 = \alpha^{28} = \alpha^{15}.\alpha^{13} = \alpha^{13}, (\alpha^7)^{4^2} = (\alpha^7)^{16} = \alpha^{112} = \alpha^{105}.\alpha^7 =$

$(\alpha^{15})^7.\alpha^7 = \alpha^7\} = \boxed{\{\alpha^7, \alpha^{13}\}}$

$\{\alpha^{10}, (\alpha^{10})^4 = \alpha^{40} = \alpha^{30}.\alpha^{10} = \alpha^{10}\} = \boxed{\{\alpha^{10}\}}$

$\{\alpha^{11}, (\alpha^{11})^4 = \alpha^{44} = (\alpha^{15})^2.\alpha^{14} = \alpha^{14}, (\alpha^{11})^{4^2} = (\alpha^{11})^{16} = \alpha^{176} =$

$\alpha^{165}.\alpha^{11} = (\alpha^{15})^{11}.\alpha^{11} = \alpha^{11}\} = \boxed{\{\alpha^{11}, \alpha^{14}\}}$

Conjugacy Class	Minimal Polynomial
$\{0\}$	$M_*(x) = x$
$\{1\}$	$M_0(x) = x+1$
$\{\alpha, \alpha^4\}$	$M_1(x) = (x+\alpha)(x+\alpha^4)$ $= x^2 + (\alpha+\alpha^4)x + \alpha^5$ $= x^2 + (\alpha+\alpha+1)x + \alpha^5$ $M_1(x) = x^2 + x + \alpha^5$
$\{\alpha^2, \alpha^8\}$	$M_2(x) = (x+\alpha^2)(x+\alpha^8)$ $= x^2 + (\alpha^2+\alpha^8)x + \alpha^{10}$ $= x^2 + (\alpha^2+\alpha^2+1)x + \alpha^{10}$ $M_2(x) = x^2 + x + \alpha^{10}$
$\{\alpha^3, \alpha^{12}\}$	$M_3(x) = (x+\alpha^3)(x+\alpha^{12})$ $= x^2 + (\alpha^3+\alpha^{12})x + \alpha^{15}$ $= x^2 + (\alpha^3+\alpha^3+\alpha^2+\alpha+1)x + 1$ $= x^2 + (\alpha^2+\alpha+1)x + 1$ $M_3(x) = x^2 + \alpha^{10}x + 1$
$\{\alpha^5\}$	$M_5(x) = x + \alpha^5$
$\{\alpha^6, \alpha^9\}$	$M_6(x) = (x+\alpha^6)(x+\alpha^9)$ $= x^2 + (\alpha^6+\alpha^9)x + \alpha^{15}$ $= x^2 + (\alpha^3+\alpha^2+\alpha^3+\alpha)x + 1$ $= x^2 + (\alpha^2+\alpha)x + 1$ $M_6(x) = x^2 + \alpha^5x + 1$

$\{\alpha^7, \alpha^{13}\}$

$$M_7(x) = (x+\alpha^7)(x+\alpha^{13})$$
$$= x^2 + (\alpha^7 + \alpha^{13})x + \alpha^{20}$$
$$= x^2 + (\alpha^3+\alpha+1+\alpha^3+\alpha^2+1)x + \alpha^5$$
$$= x^2 + (\alpha^2+\alpha)x + \alpha^5$$
$$M_7(x) = x^2 + \alpha^5 x + \alpha^5$$

$\{\alpha^{10}\}$

$$M_{10}(x) = x + \alpha^{10}$$

$\{\alpha^{11}, \alpha^{14}\}$

$$M_{11}(x) = (x+\alpha^{11})(x+\alpha^{14})$$
$$= x^2 + (\alpha^{11}+\alpha^{14})x + \alpha^{25}$$
$$= x^2 + (\alpha^3+\alpha^2+\alpha+\alpha^3+1)x + \alpha^{10}$$
$$= x^2 + (\alpha^2+\alpha+1)x + \alpha^{10}$$
$$M_{11}(x) = x^2 + \alpha^{10}x + \alpha^{10}$$

- Appendix D contains a list of all the minimal polynomials with respect to GF(2) of the elements in the binary extension fields GF(4) through GF(1024).

3.3 Factoring $x^n - 1$:

Theorem :

The set of nonzero elements in $GF(q^m)$ form the complete set of roots of the expression $x^{(q^m-1)} - 1 = 0$.

Notes:

- Any element $\alpha \in GF(q^m)$ has an order $ord(\alpha)$ such that $ord(\alpha) \mid (q^m-1)$, where (q^m-1) is the number of non zero elements in $GF(q^m)$.
- Since for any element $\alpha^i \in GF(q^m)$, then $ord(\alpha^i) \mid (q^m-1)$. If α^i is a primitive element, then we can construct all (q^m-1) nonzero elements of $GF(q^m)$, if α^i is not primitive, then we can construct a subfield

in $GF(q^m)$, and it will have less elements than $GF(q^m)$ since its elements will repeat before all elements in $GF(q^m)$ are represented. That is, the element "1" will repeat as it is the first element to repeat with less elements in the subfield than (q^m-1).

This means that any element $\alpha^i \in GF(q^m)$ primitive or not primitive satisfies

$(\alpha^i)^n = \alpha^{q^m-1} = 1$, which is $x^{q^m-1} = 1$,

This is the same as $x^{q^m-1} - 1 = 0$.

Thus, any $\alpha^i \in GF(q^m)$ is a root of the polynomial $x^{q^m-1} - 1$. Since such polynomial has an order of (q^m-1), then all (q^m-1) nonzero elements are roots of $x^{q^m-1} - 1$. So the minimal polynomials with respect to $GF(q)$ of the nonzero elements in a given $GF(q^m)$ provides the complete factorization of $x^{q^m-1}-1$ as irreducible polynomials in the ring $GF(q)[x]$.

Example: Factoring $x^{q^m-1}-1$

From a previous example, the minimal polynomials of the elements in $GF(8)$ with respect to $GF(2)$ are:

Conjugacy class	Minimal polynomial
$\{0\}$	$M_*(x) = (x-0) = x$
$\{1\}$	$M_0(x) = (x-1) = x+1$
$\{\alpha, \alpha^2, \alpha^4\}$	$M_1(x) = x^3+x+1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$M_3(x) = x^3+x^2+1$

So $x^7-1 = (x+1)(x^3+x+1)(x^3+x^2+1)$

Notes :

- The number of conjugacy classes excluding the $\{0\}$ class equals the number of factors of a $x^{q^m-1}-1$ polynomial.
- The number of elements in a conjugacy class equals the degree of the minimal polynomial associated with such class.

- For the polynomial $x^{q^m-1}-1$ when $q^m-1=n$ is x^n-1. All the roots of $x^n-1=0$ are also called the n^{th} roots of unity since

$$x^n-1=0 \Rightarrow x^n=1 \Rightarrow x=(1)^{\frac{1}{n}} \Rightarrow x=\sqrt[n]{1}.$$

- To find an extention field of $GF(q)$ in which we may find n roots of unity to form a subfield with n distinct roots that satisfies $x^n-1=0$, the smallest extention field say $GF(q^m)$ is for a positive integer m where $n \mid (q^m-1)$. Here the elements of order n are called primitive n^{th} roots of unity. We will have $\phi(n)$ elements of order n in $GF(q^m)$.

Definition: The order of q modulo n:

The order of $q \bmod n$ is the smallest positive integer m such that $n \mid (q^m - 1)$.

i.e. If $\text{ord}(q \bmod n) = m$, then $GF(q^m)$ is the smallest extension field of $GF(q)$ in which we may find primitive n^{th} roots of unity.

Example: Primitive n^{th} Roots of Unity:

Find $GF(q^m)$, the smallest extention field of $GF(q)$ in which we may find primitive n^{th} roots of unity:

(a) the extention of $GF(2)$ with primitive 5^{th} roots of unity.

We need to find the smallest m such that

$$5 \mid 2^m - 1$$

for $m = 1$, $\text{REM}\left(\frac{2-1}{5}\right) = 1$

for $m=2$, $REM\left(\frac{2^2-1}{5}\right) = REM\left(\frac{3}{5}\right) = 3$

for $m=3$, $REM\left(\frac{2^3-1}{5}\right) = REM\left(\frac{7}{5}\right) = 2$

for $m=4$, $REM\left(\frac{2^4-1}{5}\right) = REM\left(\frac{15}{5}\right) = 0$

So $m=4$, then $GF(2^4) =: GF(16)$ is the smallest extention field of $GF(2)$ in which we may find primitive 5^{th} roots of unity.

This is as saying $ord(2 \bmod 5) = 4$. Since 4 is the smallest positive integer where where 2^4 equals the identity element under mod 5.

$2^1 \bmod 5 = 2$, $2^2 \bmod 5 = 4$,

$2^3 \bmod 5 = 8 \bmod 5 = 3$

$2^4 \bmod 5 = 16 \bmod 5 = 1 \bmod 5 \Rightarrow ord(2 \bmod 5) = 4$

$\Rightarrow GF(2^4) =: GF(16)$

(b) the extention of GF(5) with primitive 31^{st} roots of unity.

We need to find the smallest m such that

$$31 \mid 5^m - 1$$

for $m=1$, $REM\left(\frac{5-1}{31}\right) = 4$

for $m=2$, $REM\left(\frac{5^2-1}{31}\right) = REM\left(\frac{24}{31}\right) = 24$

for $m=3$, $REM\left(\frac{5^3-1}{31}\right) = REM\left(\frac{124}{31}\right) = 0$

So $m=3$, then $GF(5^3) =: GF(125)$ is the smallest extention field of GF(5) in which we may find primitive 31^{st} roots of unity.

Or we can find it from:

$5^1 \bmod 31 = 5$, $5^2 \bmod 31 = 25$,

$5^3 \bmod 31 = 125 \bmod 31 = 1 \bmod 31 \Rightarrow ord(5 \bmod 31) = 3$

$\Rightarrow GF(5^3) =: GF(125)$

(b) the extention of GF(3) with primitive 13^{th} roots of unity.

We need to find the smallest m such that

$$13 \mid 3^m - 1$$

for $m=1$, $REM\left(\frac{3^1-1}{13}\right) = 2$

for $m=2$, $REM\left(\frac{3^2-1}{13}\right) = 8$

for $m=3$, $REM\left(\frac{3^3-1}{13}\right) = REM\left(\frac{26}{13}\right) = 0$

So $m=3$, then $GF(3^3) =: GF(27)$ is the smallest extention field of GF(3) in which we may find primitive 13^{th} roots of unity.

Or we can find it from:

$3^1 \bmod 13 = 3$, $3^2 \bmod 13 = 9$,

$3^3 \bmod 13 = 27 \bmod 13 = 1 \bmod 13 \Rightarrow ord(3 \bmod 13) = 3$

$$\Rightarrow GF(3^3) =: GF(27)$$

Example: Factoring x^5-1 in $GF(4)[x]$:

We need to find the smallest extention field of $GF(4)$ in which we may find primitive 5^{th} roots of unity.

$4^1 \bmod 5 = 4$, $4^2 \bmod 5 = 16 \bmod 5 = 1 \bmod 5$

So $m = 2$, that is, $\operatorname{ord}(4 \bmod 5) = 2$.

So $GF(4^2) =: GF(16)$ is the smallest extention field where we can find 5^{th} roots of unity.

To choose a primitive 5^{th} root of unity, we need to choose an element $\beta \in GF(16)$ such that $\beta = (\alpha^i)^5 = 1 =: \alpha^{15}$

so, $5i = 15 \Rightarrow i = 3$

$\Rightarrow \operatorname{ord}(\alpha^3) = 5$.

Since $\beta \in GF(16)$ is a primitive 5^{th} root of unity, then $\beta^5 = 1 \Rightarrow (\alpha^3)^5 = 1$ since β is a root of $x^5 - 1$, $x^5 - 1 = 0$

$\Rightarrow \beta^5 - 1 = 0 \Rightarrow \beta^5 = 1$.

So $\{\beta, \beta^2, \beta^3, \beta^4, \beta^5 = 1\} =:$

$\{\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^3 = \alpha^9, (\alpha^3)^4 = \alpha^{12}, (\alpha^3)^5 = \alpha^{15} = 1\}$

$= \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15} = 1\}$

are the 5 distinct elements that are the primitive 5^{th} roots of unity.

The conjugacy classes other than the $\{0\}$ class are:

$\{1\}$,

$\{\beta, \beta^{4^1} = \beta^4, \beta^{4^2} = \beta^{16} = (\beta^5)^3 \cdot \beta = \beta\} = \{\beta, \beta^4\} =:$

$\{\alpha^3, (\alpha^3)^4 = \alpha^{12}\} = \{\alpha^3, \alpha^{12}\}$

$$\{\beta^2, (\beta^2)^{4^1} = \beta^8 = \beta^5 \cdot \beta^3 = \beta^3, (\beta^2)^{4^2} = (\beta^2)^{16} = (\beta^5)^6 \cdot \beta^2 = \beta^2\}$$

$$= \{\beta^2, \beta^3\} =: \{(\alpha^3)^2 = \alpha^6, (\alpha^3)^3 = \alpha^9\} = \{\alpha^6, \alpha^9\}$$

The operations are from the table found in the previous class, GF(16) with respect to GF(4) using $p(x) = x^4 + x + 1$.

Conjugacy Class	Associated Minimal Polynomial
$\{1\}$	$M_0(x) = x + 1$
$\{\beta, \beta^4\} =: \{\alpha^3, \alpha^{12}\}$	$M_3(x) = (x+\alpha^3)(x+\alpha^{12})$ $= x^2 + (\alpha^3+\alpha^{12})x + 1$ $= x^2 + (\alpha^3 + \alpha^3 + \alpha^2 + \alpha + 1)x + 1$ $M_3(x) = x^2 + \alpha^{10}x + 1$
$\{\beta^2, \beta^3\} =: \{\alpha^6, \alpha^9\}$	$M_6(x) = (x+\alpha^6)(x+\alpha^9)$ $= x^2 + (\alpha^6+\alpha^9)x + 1$ $= x^2 + (\alpha^3+\alpha^2+\alpha^3+\alpha)x + 1$ $M_6(x) = x^2 + \alpha^5 x + 1$

So the factoring of x^5+1 in the ring GF(4)[x]:

$$x^5 + 1 = (x+1)(x^2+\alpha^{10}x+1)(x^2+\alpha^5 x+1)$$

Definition : Cyclotomic Cosets

The cyclotomic cosets modulo n with respect to $GF(q)$ are a partitioning of the integers $\{0, 1, 2, \ldots, n-1\}$ into sets of the form

$$\{a, aq, aq^2, aq^3, \ldots, aq^{d-1}\}$$

i.e. The cyclotomic cosets modulo n with respect to $GF(q)$ contain the exponents of the n distinct powers of a primitive nth root of unity with respect to $GF(q)$. Each coset corresponds to a conjugacy class.

- Appendix C contains a list of the cyclotomic cosets modulo (2^m-1) for $m=2$ to $m=10$, with respect to $GF(2)$.

Example: Cyclotomic Cosets :

From a previous example we found the conjugacy classes of $GF(8)$ with respect to $GF(2)$ to find the factorization of x^7-1 as follows along with the corresponding cyclotomic cosets:

Conjugacy class	Cyclotomic coset	Minimal polynomial
$\{1\}$	$\{0\}$	$M_0(x) = x+1$
$\{\alpha, \alpha^2, \alpha^4\}$	$\{1, 2, 4\}$	$M_1(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$\{3, 5, 6\}$	$M_3(x) = (x+\alpha^3)(x+\alpha^5)(x+\alpha^6)$

3.4 Ideals in the Ring $GF(q)[x]/(x^n-1)$

In chapter 2, modulo m reduced the set of integers.
In Euclidean domains of polynomials, mod $f(x)$ reduced the set of polynomials.

The ring of polynomials $GF(q)[x]$ mod $f(x)$ can be denoted by $GF(q)[x]/f(x)$. This is a set of all polynomials obtained by taking the remainder of polynomials from $GF(q)[x]$ after dividing by $f(x)$.

i.e. $p(x) \in GF(q)[x]$, $REM\left(\frac{p(x)}{f(x)}\right) \in GF(q)[x]/f(x)$

Theorem:

If $p(x)$ is an irreducible polynomial in $GF(q)[x]$, then $GF(q)[x]/p(x)$ is a field.

- Equivalence classes of $GF(q)[x]/(x^n-1)$ are the set of polynomials of degree less than n. They are the remainder of polynomials from $GF(q)[x]$ after dividing by x^n-1. Each equivalence class is labeled with the smallest degree element.

Example: $GF(2)[x]/(x^3-1)$:

The equivalence classes are the remainder of polynomials from $GF(2)[x]$ after dividing by x^3-1, the list of remainders as equivalence classes are as follows.

Label	Equivalence classes
0	$\{0, x^3+1, x^4+x, x^5+x^2, x^6+x^3, \dots\}$
1	$\{1, x^3, x^4+x+1, x^5+x^2+1, x^6+x^3+1, \dots\}$
x	$\{x, x^3+x+1, x^4, x^5+x^2+x, x^6+x^3+x, \dots\}$
$x+1$	$\{x+1, x^3+x, x^4+1, x^5+x^2+x+1, x^6+x^3+x+1, \dots\}$
x^2	$\{x^2, x^3+x^2+1, x^4+x^2+x, x^5, x^6+x^3+x^2, \dots\}$
x^2+1	$\{x^2+1, x^3+x^2, x^4+x^2+x+1, x^5+1, x^6+x^3+x^2+1, \dots\}$

x^2+x $\{x^2+x, x^3+x^2+x+1, x^4+x^2, x^5+x, x^6+x^3+x^2+x, \dots\}$

x^2+x+1 $\{x^2+x+1, x^3+x^2+x, x^4+x^2+1, x^5+x+1, x^6+x^3+x^2+x+1, \dots\}$

- For a ring $GF(q)[x]/(x^n-1)$, if $q=2$, then we denote the ring $GF(2)[x]/(x^n+1) =: R_n$ which is the ring of binary polynomials of degree less than n.

Definition : Ideals

Let R be a ring, a nonempty subset $I \subseteq R$ is said to be an ideal if it satisfies the following:

(1) I forms a group under the addition operation in R

(2) For all $a \in I$ and for all $r \in R$, $a.r = b \in I$.

Definition : Principal Ideals

An ideal I contained in a ring R is said to be principal if there exists $g \in I$ such that every element $c \in I$ can be expressed as $c = m \cdot g$ for $m \in R$.

i.e. given g, we can generate I by the multiplication of elements in R with g.

- The element g is called the generator element.

Theorem : Ideals in $GF(q)[x]/(x^n-1)$

Let I be an ideal in $GF(q)[x]/(x^n-1)$. Then the following is true :

(1) There exists a unique monic polynomial $g(x) \in I$ of minimal degree.

(2) I is principal with generator $g(x)$.

(3) $g(x)$ divides x^n-1 in $GF(q)[x]$.

(i.e. if $g(x)h(x) = x^n - 1$, then $h(x) \in GF(q)[x]$)

Example: Principal Ideals in $GF(q)[x]/(x^n-1)$

(1) The ideals in $GF(2)[x]/(x^7-1)$:

from a previous example when we factorized

$$x^7+1 = (x+1)(x^3+x^2+1)(x^3+x+1)$$

The ideals contained in $GF(2)[x]/(x^7-1)$ are:

$\{0, (x+1)(x^3+x^2+1)(x^3+x+1), (x+1)(x^3+x^2+1), (x+1)(x^3+x+1),$
$(x^3+x^2+1)(x^3+x+1), (x+1), (x^3+x^2+1), (x^3+x+1)\}$

(2) The ideals in $GF(4)[x]/(x^5-1)$:

we found previously that $x^5+1 = (x+1)(x^2+\alpha^{10}x+1)(x^2+\alpha^5x+1)$

so the ideals contained in $GF(4)[x]/(x^5-1)$ are

$\{0, (x+1)(x^2+\alpha^{10}x+1)(x^2+\alpha^5x+1), (x+1)(x^2+\alpha^{10}x+1), (x+1)(x^2+\alpha^5x+1),$
$(x^2+\alpha^{10}x+1)(x^2+\alpha^5x+1), (x+1), (x^2+\alpha^{10}x+1), (x^2+\alpha^5x+1)\}$

Linear Block Codes

- Block codes introduce controlled amounts of redundancy into a transmitted data stream to provide the receiver with the ability to detect and possibly correct errors caused by the noise on the communication channel.

4.1 Block Error Control Codes :

Let C denote a block error control code, then C is a set of M code words, say

$$C = \{\vec{c}_0, \vec{c}_1, \vec{c}_2, \dots, \vec{c}_{M-1}\}.$$

Each code word has the form

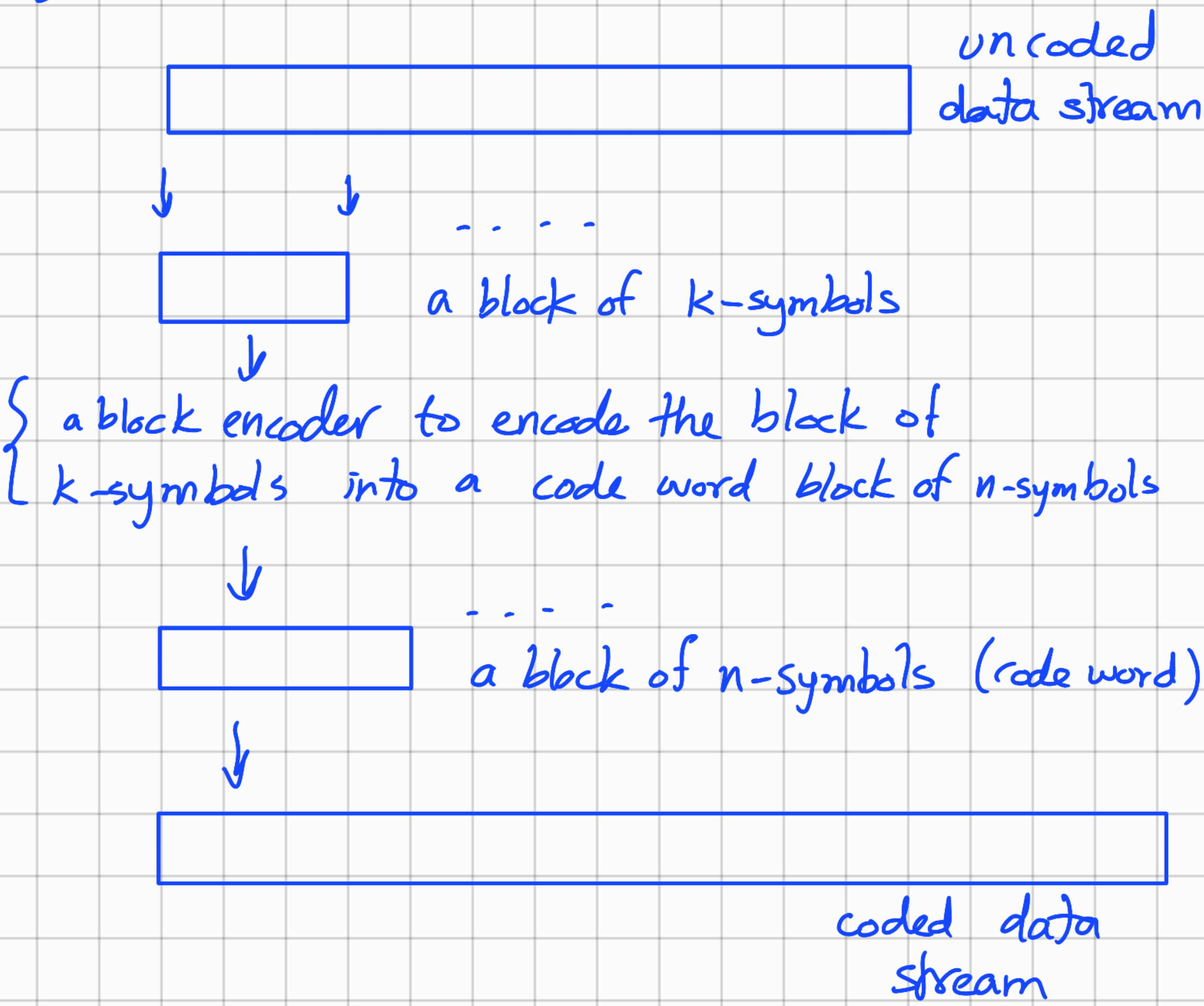
$$\vec{c}_i = (c_0, c_1, c_2, \dots, c_{n-1}).$$

If the coordinates take values from a $GF(q)$, then the code C is a q-ary.

The encoding process is as follows:

1. Breaking up the data stream into blocks
2. Mapping these blocks onto the code words in C.

- The mapping is usually one-to-one to ensure that the receiver can reverse the encoding process.



- If the symbols in the uncoded data stream can take any value from a $GF(q)$, then the collection of all possible k-symbol blocks form a k-tuples $\vec{m} = (m_0, m_1, \cdots, m_{k-1})$ which is a vector space over $GF(q)$. The number of possible k-symbol data vectors is q^k. If the number of possible code words for a block error control code C, denoted by M equals q^k, $M = q^k$, then the encoder breaks the data stream into k-symbol block, then each k-symbol block is mapped onto the code words in C.
- If $M \neq q^k$, i.e. M is not of this form, then the encoder works with blocks of varying length, and they are harder to implement.

- The encoder maps k-tuples over $GF(q)$ onto n-tuples over $GF(q)$. Both form a vector space over $GF(q)$. The first has q^k vectors, and the second has q^n vectors. So, only $M = q^k$ code words, thus, $q^n - M = q^n - q^k$ n-tuples patterns are invalid code words.
- The code C is said to contain redundancy if the number of valid code words is smaller than the number of possible n-symbol blocks.
- The redundancy r can be expressed as:

$$r = n - \log_q M$$

$$r = n - k \quad (\text{for } M = q^k)$$

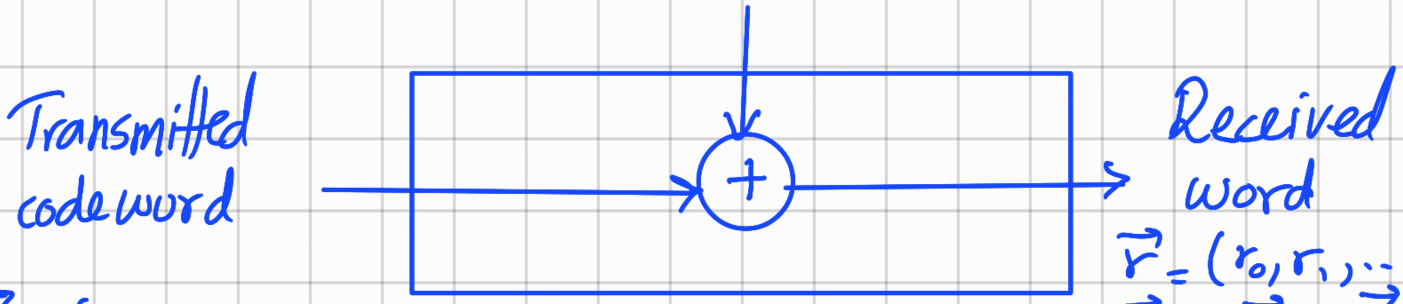
- Also, the redundancy r can be expressed in terms of the code rate R as:

$$R = \frac{\log_q M}{n}$$

$$R = \frac{k}{n} \quad (\text{for } M = q^k)$$

- Let the error corrupting a code word to be modeled as an additive noise from the communication channel added to the baseband transmitted code word as:

Error pattern $\vec{e} = (e_0, e_1, \ldots, e_{n-1})$



$\vec{c} = (c_0, c_1, \ldots, c_{n-1})$

Communication channel

$\vec{r} = (r_0, r_1, \ldots, r_{n-1})$

$\vec{r} = \vec{c} + \vec{e}$

$\vec{r} = (c_0 + e_0,\ c_1 + e_1,\ \ldots,\ c_{n-1} + e_{n-1})$

- In a binary channel, the error addition to the transmitted codeword is performed under mod 2.
- The error control decoder process at the receiver is as follows:

1. Usually the first step is error detection, which is to examine the received word and to determine if it is a code word or not. That is, to determine if errors are present in a received word or not.

An error pattern is undetectable if and only if it causes the received word to be a valid code word other than the one that was transmitted. So, for any given transmitted code word, there are $(M-1)$ other code words that may arrive at the receiver instead. Thus, there are (M-1) undetectable error patterns for any given transmitted code word.

2. The decoder can react to a detected error with one of the following responses:

(a) Request a retransmission of the word:
Automatic repeat request (ARQ) protocols is used in, for example, TCP/IP, IEEE 802.11 "WLAN", LAN, telegrams.

(b) Tag the word as being incorrect and pass it along to the data sink:
Muting is used when delay constraints do not allow for retransmission of the code word, so the incorrect received word will be set to a predetermined muted value instead of

correcting the error, it is used in, for example, voice communication.

(c) Attempt to correct the errors in the received word:

Forward error correction (FEC) uses the structure of the code to determine the most likely valid code word to have been sent given the incorrect received word.

A decoder error is made by the decoder if the decoder selects a code word other than the one transmitted. This decoder error is undetectable, while the initial error pattern was detected. The number of undetectable error patterns is less than the number of error patterns that causes decoder errors.

If the error control code is chosen carefully, then the most likely error patterns should cause the received word to be an invalid word, then the decoder can detect the presence of error, otherwise, the decoder will assume a correct word.

Usually on communication channels, the error patterns with a smaller number of nonzero coordinates are more likely to occur than error patterns with a larger number of nonzero coordinates.

Definition: **Code Word and Error Pattern Weight**

The weight of a code word or error pattern is the number of nonzero coordinates in the code word or error pattern.

- The weight of a code word $\vec{c}$ is denoted by $w(\vec{c})$

Example: **Weight**

(1) $w(1,0,0,1,1,0,1,1,1,1) = 7$

(2) $w(\alpha^3, \alpha^{29}, 0, 0, 1, \alpha^6, 0) = 4$

Definition: **Euclidean Distance**

For n-symbol blocks $\vec{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\vec{v} = (v_0, v_1, \ldots, v_{n-1})$. The Euclidean distance between two blocks $\vec{u}$ and $\vec{v}$ is

$$d_{Euclidean}(\vec{u}, \vec{v}) = \sqrt{(u_0 - v_0)^2 + (u_1 - v_1)^2 + \cdots + (u_{n-1} - v_{n-1})^2}$$

Definition : Hamming Distance

For n-symbol blocks $\vec{u} = (u_0, u_1, \dots, u_{n-1})$ and $\vec{v} = (v_0, v_1, \dots, v_{n-1})$. The Hamming distance between two blocks $\vec{u}$ and $\vec{v}$ is the number of coordinates in which the two blocks differ

$$d_{Hamming}(\vec{u}, \vec{v}) = d(\vec{u}, \vec{v}) = \left| \{ i \mid u_i \neq v_i, i = 0, 1, \dots, n-1 \} \right|$$

Definition : The Minimum Distance of a Block Code

The minimum distance of a block code C is the minimum Hamming distance between all distinct pairs of code words in C.

- A code with minimum distance d_{min} can detect all error patterns of weight less than d_{min}.
[i.e not equal to d_{min}, so less than or equal to $(d_{min} - 1)$].

- If the Hamming distance of the error pattern is d_{min} or more, then the error pattern causes the transmitted code word to look like another valid code word leading to an undetectable error.
- A maximum posterior decoder identifies the code word $\vec{c}_i$ that maximizes

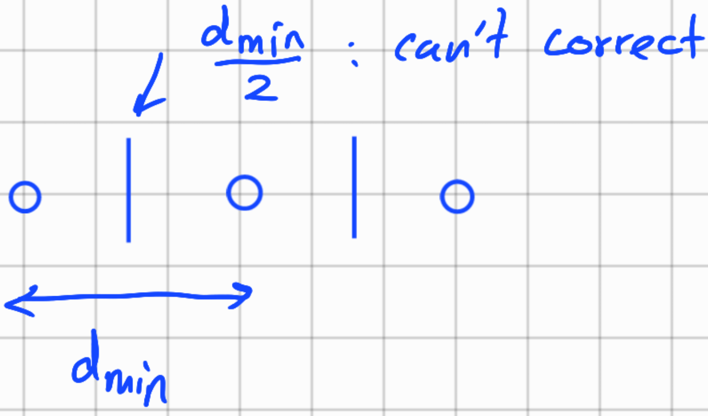
$$P\{\vec{c} = \vec{c}_i \mid \vec{r}\}$$

- A maximum likelihood decoder identifies the code word $\vec{c}_i$ that maximizes

$$P\{\vec{r} \mid \vec{c} = \vec{c}_i\}$$

- If the probability of transmission of any valid code word is assumed to be uniformly distributed, then the code word $\vec{c}_i$ that maximizes $P\{\vec{r} \mid \vec{c} = \vec{c}_i\}$ is the code word that minimizes $d(\vec{r}, \vec{c}_i) = w(\vec{e} = \vec{r} - \vec{c}_i)$. This is the code word that is closest in Hamming distance to the received word $\vec{r}$. Such decoder commits a decoder error when the received word $\vec{r}$ is closer to a wrong code word than to the correct code word. Since the valid code words are at least a distance d_{min} apart, then a decoder error is possible only if the error pattern has a weight greater than or equal to $d_{min}/2$.

- A code word with minimum distance d_{min} can correct all error patterns of weight less than or equal to $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$



Definition : Complete Decoders

A complete error correcting decoder is a decoder that, given a received word $\vec{r}$, selects as the transmitted code word $\vec{c}$ a code word that minimizes $d(\vec{r}, \vec{c})$.
(i.e. it always gives a decision)

- The complet decoder selects the code word that is closest to the received word regardless of the distance between the two since it is possible that there is more than one code word $\vec{c}$ that minimizes $d(\vec{r},\vec{c})$. In this case, the decoder chooses randomly from the possible code words.

Definition : Bounded - Distance Decoders

Given a received word $\vec{r}$, a t-error correcting bounded-distance decoder selects the code word $\vec{c}$ that minimizers $d(\vec{r},\vec{c})$ if and only if there exists $\vec{c}$ such that $d(\vec{r},\vec{c}) \leq t$. If no such $\vec{c}$ exists, then a decoder failure is declared.

$$\left(t \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor\right)$$

(i.e. it only gives a decision if $d(\vec{r},\vec{c}) \leq t$)

- For a complete decoder, an incorrect decision is a decoder error that is not detectable. For a bounded-distance decoder, a no decision is a decoder failure, which is detectable and can be resolved though a retransnission request.

Example: Binary Repetition Codes

(1) The length-four binary repetition code has two code words, (0000) and (1111).

It has $d_{min} = 4$. So it corrects error patterns of weights less than or equal to $\left\lfloor \frac{4-1}{2} \right\rfloor = \lfloor 1.5 \rfloor = 1$. So, weights zero and one. Then the complete decoder and the single error correcting bounded-distance decoder operate as follows:

Received word	Selected code word: Complete decoder	Selected code word: Bounded-distance decoder
(0000)	(0000)	(0000)
(0001)	(0000)	(0000)
(0010)	(0000)	(0000)
(0011)	(0000) or (1111)	decoder error declared
(0100)	(0000)	(0000)
(0101)	(0000) or (1111)	decoder error declared

(0110)	(0000) or (1111)	decoder error declared
(0111)	(1111)	(1111)
(1000)	(0000)	(0000)
(1001)	(0000) or (1111)	decoder error declared
(1010)	(0000) or (1111)	decoder error declared
(1011)	(1111)	(1111)
(1100)	(0000) or (1111)	decoder error declared
(1101)	(1111)	(1111)
(1110)	(1111)	(1111)
(1111)	(1111)	(1111)

(2) The length-three repetition code has two code words, (000) and (111).

It has $d_{min} = 3$, so it corrects error patterns of weights less than or equal to $\lfloor \frac{3-1}{2} \rfloor = 1$, so weights zero and one.

Then the complete decoder and the single error correcting bounded-distance decoder operate as follows:

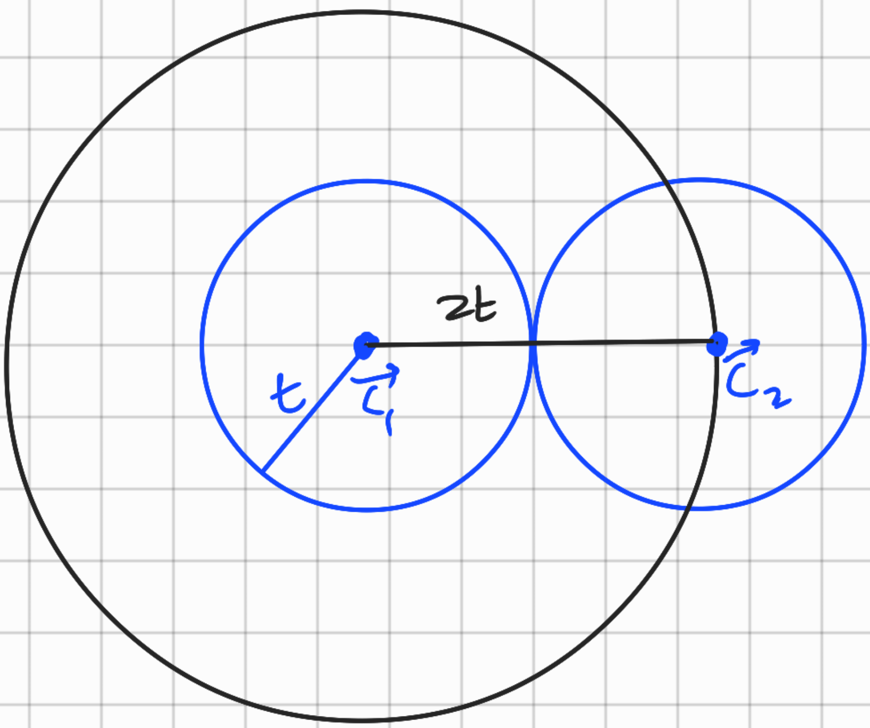
Received word	Selected code word	
	Complete decoder	Bounded-distance decoder
(000)	(000)	(000)
(001)	(000)	(000)
(010)	(000)	(000)
(011)	(111)	(111)
(100)	(000)	(000)
(101)	(111)	(111)
(110)	(111)	(111)
(111)	(111)	(111)

- To gain some usefull insights, consider the geometric interpretation of error correction.
- A Hamming sphere of radius t contains all possible received vectors that are at a Hamming distance less than or equal to t from a code word.
- The number of vectors in a Hamming sphere with radius t in an n-dimensional vector space over $GF(q)$ is denoted by $V_q(n,t)$ and

$$V_q(n,t) = \sum_{j=0}^{t} \binom{n}{k} (q-1)^j$$

where the number of vectors with Hamming distance j in an n-dimensional vector space over $GF(q)$ is $\binom{n}{j}(q-1)^j$.

- If a received vector $\vec{r}$ falls within a Hamming sphere, then the decoder selects the code word $\vec{c}$ at the center of the sphere.
- If a received vector $\vec{r}$ falls between the Hamming spheres, then the decoder declares a decoder failure if it is a bounded-distance decoder, or it selects at random one of the nearest code words if it is a complete decoder.



Theorem: The Hamming Bound

A t-error correcting q-ary code of length n must have redundancy r that satisfies

$$r \geq \log_q V_q(n,t)$$

Theorem: The Gilbert Bound

There exists a t-error correcting q-ary code of length n and redundancy r that satisfies

$$r \leq \log_q V_q(n,2t)$$

Definition: Perfect Codes

A block code is perfect if it satisfies the Hamming bound with equality.

(i.e. $r = \log_q V_q(n,t)$)

Theorem:

The number of code words in a perfect q-ary code must be of the form $M = q^k$ for some positive integer k.

- Here, perfect means that the code defines nonoverlapping Hamming spheres that perfectly fill an n-dimensional vector space.
- So, a perfect t-error correcting code with $q^k =: M$ code words of length n have parameters $\{q, n, k, t\}$ that satisfy

$$V_q(n,t) = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = \frac{q^n}{M} = q^{n-k}$$

- For error control codes, if we increase the length of the code, then the minimum distance d_{min} of the code must increase to maintain its reliability. Since for n symbols received, np symbols will be in error on average if a symbol is received in error with probability p. So, as n increases, d_{min} should increase to reduce the error probability.

4.2 Linear Block Codes

Definition: q-ary Linear Codes

Consider a block code C consisting of n-tuples $\{(c_0, c_1, \dots, c_{n-1})\}$ of symbols from $GF(q)$. C is a q-ary linear code if and only if C forms a vector subspace over $GF(q)$.

Definition: The Dimension of a Linear Code

The dimension of a linear code is the dimension of the corresponding vector space.

- An (n,k) code with symbols in $GF(q)$ is a linear code of length n and dimension k with a total of q^k code words of length n.

Linear codes properties

(1) The linear combination of any set of code words is a code word. Thus, the all-zero vector is a code word.

This property follows from a previous theorem that states that: Let $\vec{v}_1$ and $\vec{v}_2$ be an arbitrary pair of vectors in the vector space V over field F. S is a vector subspace of V if and only if any linear combination of $\vec{v}_1$ and $\vec{v}_2$ is also in S.

(2) The minimum distance of a linear code is equal to the weight of the lowest weight nonzero code word.

This property follows from the first property where for any two code words in a linear code, the Hamming distance between them is also a code word. Thus, the minimum distance is the weight of the minimum weight code word.

(3) The undetectable error patterns for a linear code are independent of the code word transmitted and always consist of the set of all nonzero code words.

This property follows from the fact that an undetectable error pattern causes the received word to be a valid code word, and since the error pattern is the difference between the transmitted word and the received word, so the error is also a code word.

. Let $\{\vec{g}_0, \vec{g}_1, \dots, \vec{g}_{k-1}\}$ be the basis of code words for the (n,k) q-ary code C. Then there exists a unique representation $\vec{c} = a_0\vec{g}_0 + a_1\vec{g}_1 + \dots + a_{k-1}\vec{g}_{k-1}$ for every code word $\vec{c} \in C$. Since every linear combination of the basis elements must be a code word, then there is a one-to-one mapping between the set of k-symbol blocks $(a_0, a_1, \dots, a_{k-1})$ over $GF(q)$ and the code words in C.

A matrix G is constructed by having as its rows the vectors in the basis. This matrix is the generator matrix for the code C.

- Let $\vec{m} = (m_0, m_1, \ldots, m_{k-1})$ be a q-ary block of uncoded data. Then

$$\vec{m}\,G = (m_0, m_1, \ldots, m_{k-1}) \begin{bmatrix} \vec{g}_0 \\ \vec{g}_1 \\ \vdots \\ \vec{g}_{k-1} \end{bmatrix}$$

$$= m_0 \vec{g}_0 + m_1 \vec{g}_1 + \cdots + m_{k-1} \vec{g}_{k-1} = \vec{c}$$

(each encoded data block is a linear combination of the basis).

- A q-ary code C of length n is a vector subspace embedded within the space of all n-tuples over $GF(q)$.

- The dual space of a linear code C is called the dual code of C and is denoted by $C^{\perp}$.

So, $C^{\perp}$ is an $(n-k)$ dimension subspace.

Let $\{\vec{h_0}, \vec{h_1}, \dots, \vec{h}_{n-k-1}\}$ be a basis for $C^{\perp}$.

A matrix H is constructed by having as its rows the vectors in the basis for $C^{\perp}$, this matrix is the parity-check matrix for the code C.

Theorem: The Parity-Check Theorem

A vector $\vec{c}$ is a code word in C if and only if $\vec{c}H^T = 0$.

(i.e. $\vec{c}H^T = (c_0, c_1, \dots, c_{n-1}) \begin{bmatrix} \vec{h_0} \\ \vec{h_1} \\ \vdots \\ \vec{h}_{n-k-1} \end{bmatrix}^T$

$$= (c_0, c_1, \dots, c_{n-1}) \left[\vec{h_0}^T \ \vec{h_1}^T \ \dots \ \vec{h}_{n-k-1}^T \right]$$

$$= \left[\vec{c}\cdot\vec{h}_0 \quad \vec{c}\cdot\vec{h}_1 \quad \cdots \quad \vec{c}\cdot\vec{h}_{n-k-1}\right]$$

$$= \left[0 \quad 0 \quad \cdots \quad 0\right]$$

$$= 0$$

- The generator and parity-check matrices for a linear block code reduce the encoding and error detection to matrix multiplication. So, there will be no need for a look-up table to be stored in the memory.

The problem of recovering the data block from a code word at the receiver can be greatly simplified through the use of systematic encoding. This is by embedding the data block without modification in the last k coordinates of the resulting code word.

This is obtained by using a systematic

generator matrix for an (n,k) code in the following form:

$$G = [P \mid I_k] \quad : \quad (k \times n)$$

So, when a data block in encoded using the systematic generator matrix

$$\vec{c} = \vec{m} G = \vec{m} [P \mid I_k]$$
$$= [\vec{m} P \mid \vec{m}]$$

(it is possible to use other than the lask k coordinates, here we will consider only this case).

The corresponding parity-check matrix for the above systematic generator matrix is as follows:

$$H = [I_{n-k} \mid -P^T] \quad : \quad ((n-k) \times n)$$

So, for a data block $\vec{m}$, the encoded block is

$$\vec{c} = \vec{m} G = \vec{m} [P | I_k]$$

then at the receiver, for error detection:

$$\vec{c} H^T = \vec{m} G H^T$$

where $G H^T = [P | I_k] [I_{n-k} | -P^T]^T$

$$= [P | I_k] \begin{bmatrix} I_{n-k} \\ -P \end{bmatrix}$$

$$= P I_{n-k} - I_k P$$

$$= P - P = 0$$

so, $\vec{m} G H^T = 0$.

Theorem:

Let C have parity check matrix H. The minimum distance of C is equal to the minimum nonzero number of columns in H for which a nontrivial linear combination sums to zero.

- Note: a nontrivial linear combination of symbols over GF(2) is a combination other than the sum of a column with itself.

Theorem: **Singleton Bound**

The minimum distance d_{min} for an (n,k) code is bounded by $d_{min} \leq n-k+1$.

- Note: An (n,k) code has an H matrix with $(n-k)$ linearly independent rows. For any matrix, the number of linearly independent rows equals to the number of linearly independent columns, this number is called the row rank or column rank.

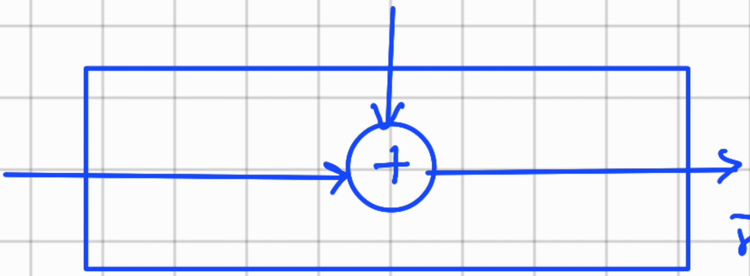
For the matrix H, it has $(n-k)$ linearly independent columns, thus, $(n-k+1)$ are linearly dependant. So, the minimum distance is bounded by $d_{min} = n-k+1$ according to the previous theorem.

4.3 Standard Array and Syndrome Table Decoding

Error pattern $\vec{e} = (e_0, e_1, \dots, e_{n-1})$

Transmitted codeword

$\vec{c} = (c_0, c_1, \dots, c_{n-1})$



Communication channel

Received word

$\vec{r} = (r_0, r_1, \dots, r_{n-1})$

$\vec{r} = \vec{c} + \vec{e}$

$\vec{r} = (c_0 + e_0,\ c_1 + e_1,\ \dots,\ c_{n-1} + e_{n-1})$

The received vector $\vec{r} = \vec{c} + \vec{e}$.

If lower-weight error patterns are more likely to occur than higher-weight error patterns, then the maximum likelihood decoder picks a code word $\vec{c}'$ such that $\vec{r} = \vec{c}' + \vec{e}'$, where $\vec{e}'$ has the smallest possible weight. A look-up table called standard array decoder is used for this decoding process.

A standard array decoder is constructed for an (n, k) linear q-ary code C as follows. Let the set V_n^q consist of all of the n-tuples over $GF(q)$. Then

(1) Remove from V_n^q (without replacement) all the code words in the code C. Write the code words in a single row starting with the all-zero code word.

(2) Select from the remaining n-tuples (without replacement) one of the patterns of lowest weight. Write this pattern in the column under the all-zero code word. Then add this pattern to each code word and write each sum under the respective code word. Remove the each sum from the set

of remaining n-tuples.

(3) Repeat step (2) until V_n^q is exhausted. Now the standard array is complete.

To decode a received word $\vec{r}$ using the standard array table, do the following:

(1) Locate the received word $\vec{r}$ in the table.

(2) The code word at the top of the column in which $\vec{r}$ is found is the maximum likelihood code word $\vec{c}$ associated with $\vec{r}$

(3) The error pattern most likely to have corrupted $\vec{r}$ is the pattern at the far left of the row on which $\vec{r}$ is located.

- Each row in the standard array table is a coset of C in V_n^q.

Example : Standard Array Decoder for a (7,3) Code

Let C be the (7,3) binary linear code with basis {(1000111), (0101011), (0011101)} and a generator matrix :

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

A standard array table for C is as follows:

TABLE 4-1. Standard Array for a (7,3) Linear Block Code

	0000000	1000111	0101011	0011101	1101100	1011010	0110110	1110001
	0000001	1000110	0101010	0011100	1101101	1011011	0110111	1110000
	0000010	1000101	0101001	0011111	1101110	1011000	0110100	1110011
	0000100	1000011	0101111	0011001	1101000	1011110	0110010	1110101
w=1	0001000	1001111	0100011	0010101	1100100	1010010	0111110	1111001
	0010000	1010111	0111011	0001101	1111100	1001010	0100110	1100001
	0100000	1100111	0001011	0111101	1001100	1111010	0010110	1010001
	1000000	0000111	1101011	1011101	0101100	0011010	1110110	0110001
	0000011	1000100	0101000	0011110	1101111	1011001	0110101	1110010
	0000110	1000001	0101101	**0011011**	1101010	1011100	0110000	1110111
	0001100	1001011	0100111	0010001	1100000 w=2	1010110	0111010	1111101
w=2 left	0011000	1011111	0110011	0000101	1110100	1000010	0101110	1101001
	0001010	1001101	0100001	0010111	1100110	1010000	0111100	1111011
	0010100	1010011	0111111	0001001	1111000	1001110	0100010	1100101
	0010010	1010101	0111001	0001111	1111110	1001000	0100100	1100011
	0111000	1111111	0010011	0100101	1010100	1100010	0001110	1001001

w=3 left

$1000111 + 0101011 = 1101100$ (5^{th} code word)

$1000111 + 0011101 = 1011010$ (6^{th} codeword)

$0101011 + 0011101 = 0110110$ (7^{th} codeword)

$1000111 + 0101011 + 0011101 = 1101100 + 0011101$

$= 1110001$ (8^{th} codeword)

If the received word $\vec{r} = 0011011$.

We look it up in the table (the underlined word).

The code word most likely to have been sent is the code word located at the top of the column in which $\vec{r}$ is located. It is 0011101.

So the error pattern most likely to have currupted $\vec{r}$ is the pattern at the far left of the row on which $\vec{r}$ is located. It is 0000110.

Example: Standard Array Decoder for a Perfect Code

The (5,1) repetition code has the following standard array:

00000	11111
00001	11110
00010	11101
00100	11011
01000	10111
10000	01111
00011	11100
00110	11001
01100	10011
11000	00111
10001	01110
10100	01011
01010	10101
00101	11010
10010	01101
01001	10110

The far left of the rows are the error patterns, they are all patterns with weights zero, one, and two. i.e. weights of $t \le \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{5-1}{2} \right\rfloor = 2$.

- A standard array table can be reduced by using the parity-check matrix H where $\vec{c}H^T = 0$. The reduced table is called the syndrome table. It will be reduced from q^n entries to q^{n-k} entry table.
- For a received word $\vec{r} = \vec{c} + \vec{e}$, the product of $\vec{r}H^T$ is called the syndrome vector $\vec{s}$ for the received vector $\vec{r}$.

Then,
$$\begin{aligned}
\vec{s} &= \vec{r}H^T \\
&= (\vec{c} + \vec{e})H^T \\
&= \vec{c}H^T + \vec{e}H^T \\
&= 0 + \vec{e}H^T \\
\vec{s} &= \vec{e}H^T
\end{aligned}$$

Thus, the syndrome vector $\vec{s}$ is independent of the transmitted code word $\vec{c}$, it only

depends on the error pattern $\vec{e}$.
So, in a standard array table, all received vectors in the same row have the same syndrome since the difference between each pair of vectors in the same row is a code word. However, the syndromes for vectors in different rows are not equal.
Thus, the entries in a standard array table that need to be stored are the error patterns (the headers of each row) and their syndromes to perform maximum likelihood decoding.

To decode using a syndrome table do the following:

(1) Compute the syndrome of a received vector.

(2) Look up the evaluated syndrome to determine the corresponding error pattern.

(3) Subtract the error pattern from the received word to get the code word.

Example: Syndrome Table Decoding

For the same code C in a previous example for a $(7,3)$ code. The G used was

$$G = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right]$$

So H is

$$H = \left[\begin{array}{ccc|cccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

To construct the syndrome table for $(7,3)$ code, take the error patterns written in the header of the standard array table the find each of their syndromes using $\vec{s} = \vec{e} H^T$

$$\vec{s} = \vec{e}\,H^T = \vec{e}\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

error pattern	syndrome
0000000	0000
0000001	0001
0000010	0010
0000100	0100
0001000	1000
0010000	1101
0100000	1011
1000000	0111
0000011	0011
0000110	0110
0001100	1100
0011000	0101
0001010	1010
0010100	1001
0010010	1111
0111000	1110

If $\vec{r} = (0011011)$,

$\vec{s} = \vec{r} H^T = 0110$,

so, $\vec{e} = 0000110$

Then the maximum likelihood transmitted code word is

$$\vec{c} = \vec{r} - \vec{e}$$

$$= (0011011) - (0000110)$$

$$\vec{c} = (0011101)$$

this is the same code word in the previous example when using the standard array table.

4.4 The Weight Distribution of Block Codes

Definition: **The Weight Distribution of a Block Code**

The weight distribution of an (n,k) code C is a series of coefficients $A_0, A_1, \ldots, A_n$, where A_i is the number of code words in C of weight i.

- The weight distribution $\{A_0, A_1, \ldots, A_n\}$ for a code is usually written as a polynomial $A(x) = A_0 + A_1 x + A_2 x^2 + \cdots + A_n x^n$. This representation is called the **weight enumerator**.
- In many cases the weight enumerator for the dual of a code is easier to find than the code itself.

Theorem: **The MacWilliams Identity**

Let $A(x)$ and $B(x)$ be the weight enumerators for an (n,k) code C and its $(n,n-k)$ dual code $C^\perp$, respectively. $A(x)$ and $B(x)$ are related by the following identity.

$$B(x) = 2^{-k}(1+x)^n A\left(\frac{1-x}{1+x}\right)$$

4.5 The Hamming Codes

For the family of binary Hamming codes, the performance parameters are expressed as a function of a single integer m, where $m \geq 2$.

Number of parity symbols : $m = n - k$

Code length : $n = 2^m - 1$

Number of information symbols : $k = n - m = 2^m - m - 1$

Error correcting capability : $t = 1$

The parity-check matrices for a binary Hamming code are easy to construct, then the corresponding generator matrix can be found. For a length $n = 2^m - 1$ Hamming code, the columns of the H matrix consist of all nonzero binary m-tuples. Each ordering of the columns gives a different (n, m) Hamming code.

In general, the Hamming codes have minimum distance $d_{min} = 3$, so $t = 1$ making it a single-error-correcting code. It is also a perfect code since $r = m = n-k$.

Hamming codes can be decoded using a syndrome table. Since these codes are single-error-correcting codes, the syndrome table has a simple relation to the parity-check matrix. Since

$$\vec{s} = \vec{r} H^T = \vec{e} H^T = \vec{e} \begin{bmatrix} \vec{h}_0 \\ \vec{h}_1 \\ \vdots \\ \vec{h}_{n-k-1} \end{bmatrix}^T$$

$$\vec{s} = \vec{e} \left[\vec{h}_0^T \ \vec{h}_1^T \ \dots \ \vec{h}_{n-k-1}^T \right]$$

and $\vec{e}$ is an error pattern with a single one in its j^{th} coordinate position, then $\vec{s}$ will be the j^{th} row of H^T, which is the j^{th} column of H.

Hamming Code Decoding Algorithm :

(1) Compute the syndrome $\vec{s}$ for the received word $\vec{r}$. If $\vec{s}=0$, then $\vec{r}$ is a valid code word so go to step (4).

(2) Determine the j^{th} column of H that equals the computed syndrome (or the j^{th} row of H^T).

(3) Complement the j^{th} bit in the received word $\vec{r}$.

(4) Output the resulting code word and stop.

- The weight enumerator for (n,k) binary Hamming codes is :

$$A(x) = \frac{1}{n+1}\left((1+x)^n + n(1-x)(1-x^2)^{\left(\frac{n-1}{2}\right)}\right)$$

Example: The (15, 11) Hamming Code

To construct one of the (15, 11) Hamming codes, we can choose the following H matrix and we design it to be a systematic code.

$$H = \left[\begin{array}{cccc|ccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}\right]$$

I_4 matrix

$\Rightarrow -P^T$

the columns are nonzero 4-tuples other than the 1st 4 columns already written in the identity matrix I_4

Also, since $n = 15$ and $k = 11$, then $m = 15 - 11 = 4$, and we will have $2^4 - 1 = 15$ nonzero 4-tuples as the number of columns in the H matrix.

For this H matrix, we can find its corresponding G matrix as follows:

$$G = \left[\begin{array}{cccc|ccccccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right]$$

P

I_{11} : this will ensure that the last 11 bits of a code word is always the message bits.

It is clear that $d_{min} = 3$, since the minimum number of nontrivial (distinct) linear combination sums of columns in H is 3.

So, $t \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$

so it is a single-error-correcting code.

Consider the following received words to decode:

(1) $\vec{r}_1 = (1110001000000010) =: (r_0, r_1, \dots, r_{15})$

(2) $\vec{r}_2 = (1001000010000001)$ 〃

(3) $\vec{r}_3 = (0001000000000011)$ 〃

Since $H = \left[\begin{array}{cccc|ccccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$

$$\vec{s} = \vec{r} H^T = \vec{r} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

0th row

15th row

$$\begin{array}{ccc} \vec{r}_1 & \vec{r}_2 & \vec{r}_3 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}$$

(1) $\vec{r}_1 = (111000100000010)$

$\vec{S}_1 = [1,1,1,0,0,0,1,0,0,0,0,0,0,1,0]\, H^T$

$= [2(1) \bmod 2,\ 3(1) \bmod 2,\ 3(1) \bmod 2,\ 1 \bmod 2]$

$\vec{S}_1 = [0,1,1,1]$

$\vec{S}_1 = (0111)$

So an error occured in the 6^{th} location of $\vec{r}_1$

so $\vec{c}_1 = [1,1,1,0,0,0,0,0,0,0,0,0,0,1,0]$

$\vec{c}_1 = (111000000000010)$

(2) $\vec{r}_2 = (100100001000001)$

$\vec{S}_2 = [3(1) \bmod 2,\ 1 \bmod 2,\ 1 \bmod 2,\ 3 \bmod 2]$

$= [1,1,1,1]$

$\vec{S}_2 = (1111)$

So an error occured in the 15^{th} location of $\vec{r}_2$

so $\vec{c}_2 = (100100001000000)$

(3) $\vec{r}_3 = (000100000000011)$

$\vec{S}_3 = [2 \bmod 2, 2 \bmod 2, 2 \bmod 2, 2 \bmod 2]$

$= [0, 0, 0, 0]$

$\vec{S}_3 = (0000)$

so no error occured in $\vec{r}_3$

so $\vec{c}_3 = \vec{r}_3 = (000100000000011)$