ECE 575

Coding Theory

A-321

Groups - A Group $(S, \otimes)$ is a set together with a binary operation $\otimes$ on S such that

1) Closure $a, b \in S \rightarrow a \otimes b \in S$

2) The operator is associative:

$a, b, c \in S, \quad (a \otimes b) \otimes c = a \otimes (b \otimes c)$

3) There is an element $e \in S$ called the identity element such that $a \otimes e = e \otimes a = a$ for all $a \in S$

4) For every $a \in S$, there is an element $b \in S$ known as the inverse of a such that

$a \otimes b = e \rightarrow b = a^{-1}$

The set with operation $\otimes$ satisfying all the above properties is called a group

5) A group $(S, \otimes)$ is commutative, if for every $a, b \in S \quad a \otimes b = b \otimes a$

- A group that is commutative with an additive like operator is said to be an Abelian group

(2)

Ex:

The set $(\mathbb{Z}, +)$, which is the set of integers under addition, forms a group.

if $a, b, c \in \mathbb{Z}$

1) $a, b \in \mathbb{Z}$ $a+b \in \mathbb{Z}$ → closure

2) $(a+b)+c = a+(b+c)$ → associative

3) $a+0=0+a=a$ → 0 is the identity element

4) $a+b=0$ → $b=-a$ → every element has an inverse

5) Since $a+b=b+a$

The group is also commutative (Abelian group)

Ex:

$S=\{0,1,2,3,4\}$ → set

$\oplus$ → modulo 5 addition, i.e. $\oplus = \oplus$

$(S, \oplus)$ → form a group

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From table

$a, b, c \in S$

1) $a, b \in S$ $a \oplus b \in S$ closure

2) Associative $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

3) Identity element is 0

4) Every element has an inverse $4^{-1}=1$

(3)

Commutative property also holds.

As with sets, groups can be finite or infinite, and the number of elements within a finite group is known of the order of the group, and denoted by $|S|$

Ex:

$S = \{1, 2, 3\}$ $\otimes \rightarrow$ mod 4

$\otimes$	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

$(S, \otimes) \rightarrow$ is not a group

$0 \notin S$ closure is not satisfied

Ex:

$S = \{1, 2, 3, 4\}$ $\otimes \rightarrow$ mod 5 addition

$(S, \otimes) \rightarrow$ not a group

$\oplus$	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

$0 \notin S \rightarrow$ closure is not satisfied.

(4)

Ex: $S = \{1, 2, 3\}$ $\otimes \rightarrow$ mod 4 multiplication

$\otimes$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Element 2 does not has an inverse

$(S, \otimes) \rightarrow$ not a group

Hence:

$S = \{0, 1, \ldots m-1\}$ $\otimes \rightarrow$ mod m addition

$(S, \otimes) \rightarrow$ form a group

$S = \{1, \ldots m-1\}$ $\otimes \rightarrow$ mod m addition

$(S, \otimes) \rightarrow$ not a group

$S = \{1, 2, \ldots m-1\}$ $\otimes \rightarrow$ mod m multiplication

$(S, \otimes) \rightarrow$ is a group
if m is a prime number,
otherwise not a group

Ex: $S = \{1, 2, \ldots 15\}$ $\otimes \rightarrow$ mod 16 multiplication

$S = \{1, 2, \ldots m-1\}$ $m = 16$

Since m is not a prime number
$(S, \otimes)$ is not a group

(5)

Subgroups

A subgroup $(S_g, \otimes)$ of a group $(S, \otimes)$ is a group formed from a subset of elements in a group S with the same operation.

Ex:

$S = \{0, 1, 2, 3, 4, 5\}$, $\otimes \rightarrow$ mod 6 addition

Let $S_g = \{0, 2, 4\}$ $\otimes \rightarrow$ mod 6 addition

$(S_g, \otimes) \rightarrow$ forms a group

S_g is a subgroup of S.

Let $H = \{1, 2 \ldots 5\}$ $\otimes \rightarrow$ mod 6 addition

$(H, \otimes) \rightarrow$ not a subgroup

Note: Every subset of S may not form a group with $\otimes$ operation.

Cyclic Groups and the Order of an element

$(S, \otimes)$ → a group

define $a^n = \underbrace{a \otimes a \otimes \cdots a}_{n \text{ times}}$ $\qquad \bar{a}^n = \underbrace{(\bar{a}^1) \otimes (\bar{a}^1) \otimes \cdots \otimes \bar{a}^1}_{n \text{ times}}$

Defn: $a \in S$ the set $\{a^n \mid n \in \mathbb{Z}\}$ generates a subgroup of G called the cyclic subgroup.

$a \rightarrow$ the generator of the subgroup

Defn: If every element of a group can be generated by a single element, the group is said to be cyclic

Ex: $S = \{0, 1, 2, 3, 4\}$ $\otimes \rightarrow$ mod 5 addition

denoted as $(\mathbb{Z}_5, \oplus)$

$(S, \otimes) \rightarrow$ is a group

(7)

$2 \in S$ using 2 we can generate all the other group elements

$2+2=4$

$2+2+2=1$

$2+2+2+2=3$

$2+2+2+2+2=0$.

mod 5 addition.

$\rightarrow \{0,1,3,4\}$ & other elements.

Hence $(S,\emptyset)$ is a cyclic group

Using element 3

$3+3=1$

$3+3+3=4$

$3+3+3+3=2$

$3+3+3+3+3=0$

$\rightarrow \{0,1,2,4\}$ & other elements.

Defn: $(S,\emptyset) \rightarrow$ a group

$a \in S$ the smallest n such that

a^n is equal to the identity in S is said to be the order of a. If no such n exists, a is of infinite order.

(8)

Cosets: Let H be a subgroup of $(S, *)$

$a \in S$. The left coset of H,

$a * H$, is the set $\{a * h \mid h \in H\}$

The right coset of H is

$$H * a = \{h * a \mid h \in H\}$$

In a commutative group, the left and right cosets are the same.

Ex:

Let $S = \mathbb{Z}$ $\quad * \to +$

$(\mathbb{Z}, +) \to$ is a group

Let $S_0 = 3\mathbb{Z} \to S_0 = \{\ldots -6, -3, 0, 3, 6, \ldots\}$

S_0 is a subgroup of S.

Cosets can be formed of

$$S_1 = S_0 + 1 = \{\ldots -5, -2, 1, 4, 7, \ldots\}$$

$$S_2 = S_0 + 2 = \{\ldots -5, -2, 1, 4, 7, \ldots\}$$

Note that S_1 & S_2 are not groups (no identity element

(9) $S = S_0 \cup S_1 \cup S_2$

Lemma: Every coset of H in a group S has the same number of elements.

Lagrange Theorem:
Let S be a group of finite order and let H be a subgroup of S. Then the order of H divides the order of S. That is, $|H|$ divides $|S|$

$|H| \rightarrow$ number of elements in H.

Proof: The set of cosets partition S into disjoint sets, each of which has the same number of elements, $|H|$. These disjoint sets completely cover S. So the number of elements in S must be a multiple of $|H|$.

Ex: $S = \{0,1,2,3,4,5\}$ $\otimes \rightarrow$ mod 6 addition

$(S, \otimes) \rightarrow$ group

$H = \{0,2,4\}$ $\otimes \rightarrow$ mod 6 addition

$(H, \otimes) \rightarrow$ is a subgroup of S

(10)

$H = \{0, 2, 4\}$

$H_1 = H+1 \longrightarrow \{1, 3, 5\}$ ⟶ same take only one

$H_2 = H+2 \longrightarrow \{2, 4, 0\}$

$H_3 = H+3 \longrightarrow \{3, 5, 1\}$

$H = \{0, 2, 4\}$ $H_1 = \{1, 3, 5\}$ $H_2 = \{2, 4, 0\}$

↳ same of H omit it.

$S = H \cup H_1$

↳ subgroup ↘ coset

Ex: $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ⌀ mod 10 addition.

$H = \{0, 5\}$ ⌀ → mod 10 addition

$(H, ⌀)$ → subgroup

$H_1 = H+1 \longrightarrow H_1 = \{1, 6\}$

$H_2 = H+2 \longrightarrow H_2 = \{2, 7\}$ → cosets

$H_3 = H+3 \longrightarrow H_3 = \{3, 8\}$

$H_4 = H+4 \longrightarrow H_4 = \{4, 9\}$

$S = H \cup H_1 \cup H_2 \cup H_3 \cup H_4$

(10A)

Ex: $S = \{1, 2, 3, 4, 5, 6\}$

$\otimes \rightarrow$ mod 7 multiplication

$S_g \rightarrow$ subgroup

Find a S_g and determine all the cosets

S/n:

$S_g = \{1, 2, 4\} \rightarrow$ subgroup

$H_3 = S_g \otimes 3 \rightarrow H_3 = \{3, 6, 5\}$ ✓

$H_2 = S_g \otimes 2 \rightarrow H_2 = \{2, 4, 1\}$ ×

$S = S_g \cup H_3 \rightarrow \{1, 2, 4\} \cup \{3, 5, 6\}$

Ex: Propose an infinite group

determine a subgroup

and find all the cosets

Fields:

S → a set

× → an operation defined on set S

+ → another operation defined on set S

① (S, ×) form a commutative group

② (S, +) form a commutative group

③ a, b, c ∈ S

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

× operation is distributive over + operation

If ①, ②, and ③ are satisfied, then we say that (S, ×, +) form a field

OR (S, ×, +) is a field

Fields can be finite or infinite

Ex^os

$F_2 = \{0, 1\}$

+ → mod 2 addition

× → multiplication

Is F_2 a field?

$(F_2, +)$ → a commutative group

S/n^os

+	0	1
0	0	1
1	1	0

- closure
- associative
- identity element
- inverse element
- commutative

(12)

×	0	1
0	0	0
1	0	1

$(F_2, \times)$ → a commutative group

- closure
- associative
- identity element 1
- inverse element $1 \cdot 1 = 1$
- commutative $1 \cdot 0 = 0 \cdot 1$

× is distributive over +

$1 \times (0+1) = 1 \times 0 + 1 \times 1$

$1 = 1$ ✓

Hence $(F_2, \times, +)$ is a field

OR F_2 is a field in short

F_2 is usually called Galois field or binary field and is indicated by GF(2)

Ex: $S = \{0,1,2,3,4\}$ × → mod 5 multiplication
+ → mod 5 addition

$(S, \times)$ → a commutative group

$(S, +)$ → a " "

× is distributive over +

Hence S is a field.

(13) Ex°: $S = \{0, \mp1, \mp2, \mp3, \dots\}$ the set of integers

$\times \rightarrow$ multiplication

$+ \rightarrow$ addition

$(S, +) \rightarrow$ a commutative group

$(S, \times) \rightarrow$ is not a commutative group (every element does not have an inverse)

S is not a field.

Ex°: $S = \{$Real numbers$\}$

$\times \rightarrow$ classical multiplication

$+ \rightarrow$ " addition

$(S, \times) \rightarrow$ a commutative group

$(S, +) \rightarrow$ " " "

$a, b, c \in S \qquad a \times (b + c) = a \times b + a \times c$ ✓

Then S is a field

Ex°: $S = \{0, 1, 2, 3\}$ $\times \rightarrow$ mod 4 multiplication

$+ \rightarrow$ mod 4 addition

$(S, +) \rightarrow$ a commutative group S is

$(S - \{0\}, \times) \rightarrow$ is not a commutative group not a field

(14)

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

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

→ 2 does not has an inverse

Fields can be constructed by taking modulo-m addition & multiplication over the set $\{0, 1, \ldots m-1\}$ where m is a prime number. Those fields are known as prime fields.

Ex: Construct the prime field under modulo-7 arithmetic

Soln: $S = \{0, 1, 2, 3, 4, 5, 6\}$

$\times \rightarrow$ mod 7 multiplication

$+ \rightarrow$ mod 7 addition

$(S, +)$ → form a commutative group

$(S - \{0\}, \times)$ → form a commutative group

$(S, \times, +)$ → a prime field

addition

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

multiplication

x	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

Vector Spaces

Vector → a collection of objects (numbers)

($\vec{v}$)

Set of vectors $\overline{V} = \{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_N\}$

$\overline{V}$ → a set; $\vec{v}_1, \vec{v}_2, \ldots \vec{v}_N$ → vectors

Given a field F and a vector set $\overline{V}$

with $+$ → vector addition

$\cdot$ → scalar multiplication

$\overline{V}$ is a vector space if

① $(\overline{V}, +)$ → form a commutative group

② For every $a, b \in F$ & $\vec{v}$ & $\vec{w} \in V$

$a\vec{v} + b\vec{w} \in \overline{V}$, i.e, closure

③ $a, b \in F$ $\vec{u}, \vec{v} \in \overline{V}$

$(a+b)\vec{v} = a\vec{v} + b\vec{v}$ & $a(\vec{u} + \vec{v}) = a\vec{u} + b\vec{v}$

④ The operation $\cdot$ is associative

$(a.b).\vec{v} = a.(b.\vec{v})$ for $\forall\, a, b \in F$ & $\vec{v} \in \overline{V}$

The vectors that we are interested in are ordered sequences represented by

$$\bar{u} = (u_0 \; u_1 \; \cdots \; u_{n-1})$$

An ordered sequence with n elements is also called n-tuple.

Vector addition

Given two n-tuples $\bar{u}$ & $\bar{w}$

$$\bar{u} = (u_0 \; u_1 \; \cdots \; u_{n-1}) \qquad \bar{w} = (w_0 \; w_1 \; \cdots \; w_{n-1})$$

$$\bar{u} + \bar{w} = (u_0 + w_0 \quad u_1 + w_1 \quad \cdots \quad u_{n-1} + w_{n-1})$$

Scalar multiplications

$a \in F \rightarrow$ field

$$\bar{u} = (u_0 \cdots u_{n-1})$$

$$a \cdot \bar{u} = (a u_0 \quad a u_1 \cdots a u_{n-1})$$

Linear Combinations

Let $\bar{v}_1, \bar{v}_2, \ldots \bar{v}_k$ be vectors in a vector space $\bar{V}$ and let $a_1, a_2 \ldots a_k$ be scalars in a field F

The operation

$$a_1\bar{v}_1 + a_2\bar{v}_2 + \ldots + a_k\bar{v}_k$$

is said to be a linear combination of the vectors.

The linear combination can be obtained from the products

$$[a_1 \; a_2 \ldots a_k]\begin{bmatrix}\bar{v}_1 \\ \bar{v}_2 \\ \vdots \\ \bar{v}_k\end{bmatrix}$$

$$[\bar{v}_1 \; \bar{v}_2 \ldots \bar{v}_k]\begin{bmatrix}a_1 \\ a_2 \\ \vdots \\ a_k\end{bmatrix}$$

Linear Independence & Dependence

The vectors $\bar{v}_1, \bar{v}_2 \ldots \bar{v}_k$ are linearly independent if $a_1\bar{v}_1 + a_2\bar{v}_2 + \ldots + a_k\bar{v}_k = 0$ is satisfied for only $a_1 = a_2 = \ldots = a_k = 0$

If there exists a nonzero a_i value then the vectors $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_k$ are said to be linearly dependent.

(18)

Ex3 Determine whether the following sets of vectors are linearly dependent or independent

a) $\overline{v_1} = (3 \quad -8 \quad 5)$ $\overline{v_2} = (-2 \quad 2 \quad 14)$

$\overline{v_3} = (-1 \quad 6 \quad -19)$

b) $\overline{w_1} = (-2 \quad 0 \quad 0)$ $\overline{w_2} = (0 \quad 7 \quad 0)$

$\overline{w_3} = (0 \quad 0 \quad 9)$

Sln3

$$a_1\overline{v_1} + a_2\overline{v_2} + a_3\overline{v_3} = (3a_1 - 2a_2 - a_3 \quad -8a_1 + 2a_2 + 6a_3 \quad 5a_1 + 14a_2 - 19a_3)$$

a)

If $a_1 = a_2 = a_3 = 1$

we get $(0 \; 0 \; 0)$

and therefore the vectors are linearly dependent.

b) $a_1\overline{w_1} + a_2\overline{w_2} + a_3\overline{w_3} = (-2a_1 \quad 7a_2 \quad 9a_3)$

The only way $(-2a_1 \quad 7a_2 \quad 9a_3)$ equals $(0\,0\,0)$

is if $a_1 = a_2 = a_3 = 0$.

So the vectors are linearly dependent.

Basis Vectors

- Within a vector space there always exists at least one set of linearly independent vectors from which all other vectors can be generated.

These are known as basis vectors and a set of basis vectors is referred to as a basis for the vector space. Each vector within the vector space can be uniquely expressed as a linear combination of the basis vectors.

- The basis vectors are said to span the vector space.
- The number of vectors within the basis is called the dimension of the vector space.
- In an m-dimensional space any set of m linearly independent vectors span the vector space and is therefore a basis for the space.

Standard Basis

For m-dimensional vector space the vectors $\underline{b}_1 = (1\,0\,.\,0)$ $\underline{b}_2 = (0\,1\,.\,.\,0)$

$\underline{b}_m = (0\,.\,0\,.\,.\,.\,1)$ are referred to as the standard basis.

Subspaces

In a vector space, subsets of vectors exist that have all the characteristics of a vector space under vector addition and scalar multiplication, in which case the subset of vectors is known as a vector subspace or subspace

Defn: Let $\underline{V}$ be a vector space over a scalar field F, and let $\underline{W} \subset \underline{V}$. For $\forall \underline{w}_1, \underline{w}_2 \in \underline{W}$ and $\forall a, b \in F$, $a\underline{w}_1 + b\underline{w}_2 \in \underline{W}$ then $\underline{W}$ is called a vector subspace (or simply a subspace) of $\underline{V}$.

Inner Product (Dot product)

Let $\bar{u} = (u_0\ u_1 \dots u_{n-1})$ $\bar{v} = (v_0 \dots v_{n-1})$

$$\bar{u} \cdot \bar{v} = \sum_{i=0}^{n-1} u_i v_i$$

Orthogonality

Two vectors $\bar{u}$ & $\bar{v}$ are said to be orthogonal if $\bar{u} \cdot \bar{v} = 0$. When $\bar{u}$ & $\bar{v}$ are orthogonal this is denoted as $\bar{u} \perp \bar{v}$

Dual Spaces

Let $\underline{W}$ be a subspace of $\underline{V}$

The dual space of $\underline{W}$ is $\underline{W}_d$ such that

$\forall\ \bar{w} \in \underline{W}$ & $\forall\ \bar{w}_d \in \underline{W}_d$

$$\bar{w} \cdot \bar{w}_d = 0$$

$$\dim(\underline{W}_d) = \dim(\underline{V}) - \dim(\underline{W})$$

$$\downarrow$$

$$\dim(\underline{W}_d) = n - k$$

Cross Products

$\bar{u} = (u_x\ u_y\ u_z)$ $\quad \bar{v} = (v_x\ v_y\ v_z)$

$$\bar{u} = u_x \bar{a}_x + u_y \bar{a}_y + u_z \bar{a}_z$$

$$\bar{v} = v_x \bar{a}_x + v_y \bar{a}_y + v_z \bar{a}_z$$

$$\bar{u} \times \bar{v} = \begin{vmatrix} \bar{a}_x & \bar{a}_y & \bar{a}_z \\ u_x & u_y & u_z \\ v_x & v_y & v_z \end{vmatrix} = (u_y v_z - u_z v_y)\vec{a_x} + (u_z v_x - u_x v_z)\vec{a_y} + (u_x v_y - u_y v_x)\bar{a}_z$$

(22)

Ex: A basis is given

$B=\{(011),(101)\}$ $F_2=\{0,1\}$

Find the vector space generated by this basis.

Matrices:

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \qquad A=\begin{bmatrix} \bar{v}_1 \\ \bar{v}_2 \\ \vdots \\ \bar{v}_n \end{bmatrix}$$

- The set of linear combinations of the row vectors $\bar{v}_i$ form a vector space and referred to as the row space of the matrix A.
- Similarly column space is also defined.
- The dimensions of the column & row vector spaces known as the column rank and row rank respectively are the same and are referred to as the rank of the matrix

Elementary Row Operations

a) Interchanging rows

b) multiplying a row by a non-zero scalar

c) Adding a multiple of one row to another row.

Elementary row operations does not affect the row space.

Ex:

$$A=\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

row1 $\leftarrow$ row1 + row3 $\quad A_1=\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$

row2 $\longleftrightarrow$ row3 $\quad A_2=\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$

A & A_2 have the same row space

Theorem: Let V be a n-dimensional vector space defined over a scalar field with a finite number of elements q in it. Then the number of elements in V is $|V|=q^n$

Ex 3

$S = \{0, 1, 2, 3\}$

$+ \longrightarrow$ mod 4 addition

$\cdot \longrightarrow$ mod 4 multiplication

$(S, +, \cdot) \longrightarrow$ is it a field or not ?

do it by yourself.

Linear Block Codes as Vector Spaces: