EE653 - Coding Theory

Lecture 2: Background on Abstract Algebra

Dr. Duy Nguyen

January 18, 2017

San Diego State University

Leadership Starts Here

Outline

Definitions

Definition 1

A **binary operation** $*$ *on a set* G *is a rule that for each* $a \in G, b \in G$ *assigns* $c = a * b$*, such that* $c \in G$*.*

Definition 2

A **group** *consists of a set* G *and a binary operation* $*$ *with the following properties:*

1. *Associativity:* $(a * b) * c = a * (b * c)$ *for* $a, b, c \in G$*.*
2. *Existence of Identity: There exists* $e \in G$ *such that* $a * e = e * a = a$*, for all* $a \in G$*.*
3. *Existence of Inverse: For each* $a \in G$*, there exists a unique element* $a^{-1} \in G$ *such that* $a * a^{-1} = a^{-1} * a = e$*.*

Properties of Groups

Theorem 1

The identity element is unique.

Proof?

Theorem 2

The inverse of an element a in group is unique.

Proof?

Definitions

Definition 3

A group is said to be **commutative** *or* **abelian** *if also satisfies:*
Commutativity: For all $a, b \in G, a * b = b * a$.

- If a group is commutative, then the group operation is often represented as "$+$"
- Examples of groups:
  - The set of integers forms a commutative group under addition.
  - The set of integers does **not** form a group under multiplication. Why?
  - The set of rational numbers excluding zero forms a group under multiplication.
  - The set of $(n \times n)$ matrices with real elements forms a commutative group under matrix addition

Definitions

Definition 4

The **order** *or* **cardinality** *of a group is the number of elements in the group.*

Definition 5

If the order or a group is finite, the group is a **finite group**. *Otherwise, it is an* **infinite group**.

Finite groups using modulo arithmetic

- In ECC, we are concerned with finite groups.
- Construction of finite groups using modulo arithmetic on integers:
  - The result of **addition modulo** m of $a, b \in G$ is the remainder, c, of $a + b$ divided by m, where $0 \leq c \leq m - 1$:

    $$a + b = k \cdot m + c,$$

    where k is the largest integer such that

    $$k \cdot m < (a + b).$$

  - Modulo addition can be expressed in several ways. We will start with a more-descriptive form than in the text:

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

Construction of Groups Using Modulo Addition

- Define G by $G = \{0, 1, 2, \ldots, m-1\}$
- Define $c = a \boxplus b$ by $a + b \equiv c \bmod m$
- Then $(G, \boxplus)$ is a group:
  - $a \boxplus b$ is an integer between 0 and $m-1$, so G is closed under $\boxplus$
  - $\boxplus$ is associative
  - Identity element under $\boxplus$ is zero $a \boxplus 0 = a$, $a \boxplus b = a \Rightarrow b = km$, but $b = km \Rightarrow b = 0$ (identity is unique)
  - For a in G, $m - a$ is also in G. Let $c = a \boxplus m - a$. Then

$$a + m - a \equiv c \bmod m$$
$$m \equiv c \bmod m$$
$$\Rightarrow m = k \cdot m + c \Rightarrow c = 0$$

    (Inverses are in G.)
  - This defines an *additive group* over the integers $\bmod\ m$

Construction of Groups Using Modulo Multiplication

- Suppose we select a prime number p, and let $G = \{1, 2, \ldots, p-1\}$.
- Define $\boxdot$ by $c = a \boxdot b$ if $a \cdot b \equiv c \bmod p$.
- $(G, \boxdot)$ is then a group of order $p-1$

Claim: $(G, \boxdot)$ is a group of order $p-1$

- Associativity
- Identity: clearly $a \boxdot 1 = a$
- Inverse: Let $i \in G$ be an element for which we want to find an inverse by Euclid's Theorem, $\exists\ a, b$ such that

$$a \cdot i + b \cdot p = 1$$

and a, p are relatively prime. We then have $a \cdot i = -b \cdot p + 1$. What next?

Subgroup

Definition 6

Subgroup: *If H is a nonempty subset of G and H is closed under $*$ and satisfies all the conditions of a group, then H is a subgroup of G.*

Example: G: rational numbers under real addition. H: integers under real addition

Theorem 3

Let G be a group under binary operation $*$. Let H be a non-empty subset of G. Then H is a subgroup of G if the following conditions hold:

- *H is closed under $*$*
- *For any element a in H, the inverse of a is also in H.*

Proof?

Coset

Definition 7

Let H be a subgroup of G with binary operation $*$. Let a be an element of G. Then the set of elements $a * H \triangleq \{a * h : h \in H\}$ is called a left coset of H; the set of elements $H * a \triangleq \{h * a : h \in H\}$ is called a right coset of H.

For a commutative group, left and right cosets are identical. Hereafter, we just call them cosets.

Theorem 4

Let H be a subgroup of a group G under binary operation $*$. No two elements in a coset of H are identical.

Theorem 5

Let H be a subgroup of a group G under binary operation $*$. No two elements in two different cosets of H are identical.

Definitions: Rings

Definition 8

*A **ring** is a collection of elements R with two binary operations, usually denoted "$+$" and "$\cdot$" with the following properties:*

1. $(R, +)$ **is a commutative group**. *The additive identity is labeled "0".*
2. $\cdot$ **is Associative:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $\cdot$ **Distributes over** $+$.

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

Definitions: Rings

Definition 9

A ring is a commutative ring if $\cdot$ *is commutative:* $a \cdot b = b \cdot a$.

Definition 10

A ring is a ring with identity if $\cdot$ *has an identity, which is labeled "1".*

Outline

Definitions: Fields

Definition 11

*A **field** is a commutative ring with identity in which every element has an inverse under $\cdot$.*

- Essentially, a field is:
  - a set of elements F
  - with two binary operations $+$ (addition) and $\cdot$ (multiplication).
  - "$+$","$\cdot$", and inverses can be used to do *addition, subtraction, multiplication*, and *division* without leaving the set.

Definitions: Fields

Definition 12

Formal definition: A **field** *consists of a set F and two binary operations $+$ and $\cdot$ that satisfy the following properties:*

1. *F forms a commutative group under addition $(+)$. The additive identity is labeled "0".*
2. *$F - \{0\}$ forms a commutative group under multiplication $(\cdot)$. The multiplicative identity is labeled "1".*
3. *The operation "$\cdot$" distributes over $+$:*

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

Fields: Examples

Examples of Fields

- The rational numbers
- The integers do not form a field because they do not form a group under "$\cdot$". (There are no multiplicative inverses.)
- The real numbers
- The complex numbers

Observe that they are all infinite fields.

Properties of Fields

- **Property I.** For every element a in a field, $a \cdot 0 = 0 \cdot a = 0$.
  Proof?

- **Property II.** For any two nonzero elements a and b in the field, $a \cdot b \neq 0$.
  Proof: The nonzero elements are closed under $\cdot$.

- **Property III.** If $a \cdot b = 0$ and $a \neq 0$, then $b = 0$.
  Proof: From Property II.

- **Property IV.** For $a \neq 0$, $a \cdot b = a \cdot c$ implies $b = c$.
  Proof: Multiply each side by a^{-1}.

Finite Fields

- Finite fields are more commonly known as **Galois Fields** after their discoverer
- A Galois field with p members is denoted **GF(p)**
- Every field must have at least 2 elements:
  - the additive identity '0', and
  - the multiplicative identity '1'

Binary Fields

- There exists a finite field with 2 elements: the **binary field**, denoted **GF(2)**
  - $F = \{0, 1\}$
  - $+$ defined as modulo–2 addition

$+$	0	1
0	0	1
1	1	0

  - $\cdot$ defined as modulo–2 multiplication

$\cdot$	0	1
0	0	0
1	0	1

  - It is easy to verify that $\cdot$ distributes of $+$ by trying each of the 8 possible combinations

$GF(p)$

Given a prime number p, the integers $\{0, 1, 2, \ldots, p-1\}$ form a field under modulo p addition and multiplication.

- $\{0, 1, \ldots, p-1\}$ is a commutative group under mod p addition
- $\{1, \ldots, p-1\}$ is a commutative group under mod p multiplication
- modulo multiplication distributes over modulo addition

Examples of $GF(3)$

- The next smallest group after **GF(2)** is **GF(3)**, $F = \{0, 1, 2\}$
  - $+$ defined by

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

  - $\cdot$ defined by

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

Constructions of Finite Fields

- Modulo arithmetic can be used to construct fields of size p, where p is prime.
- Modulo arithmetic **cannot** be used to construct fields of size p if p is not prime.
- Finite fields **GF(q)** do not exist for all q.
- However, finite fields **GF(q)** do exist if $q = p^m$, where p is prime and $m > 1$.
- GF(p^m) is called an extension field of GF(p) because it is constructed as a vector space over **GF(q)**.

Subtraction and Division in Fields

- Subtraction over the field: to subtract b from a, find the additive inverse of b (call it $-b$) and add it to a:

$$a - b = a + (-b)\,.$$

- Division over the field can be defined in the same way: to divide a by b, first find the multiplicative inverse of b (call it $b - 1$), and multiply it by a:

$$a/b = a \cdot b^{-1}.$$

Outline

Definition: Vector Space

Definition 13

A vector space consists of:

- V, *a set of elements called vectors;*
- F, *a field of elements called scalars;*
- $+$, *a binary operator on* $V \ni \forall \underline{v}_1, \underline{v}_2 \in V$, $\underline{v}_1 + \underline{v}_2 = \underline{v} \in V$, *called vector addition;*
- $\cdot$, *a binary operator on* F *and* V *if* $a \in F$, $\underline{v} \in V$, $a \cdot \underline{v} = \underline{w} \in V$ *called scalar multiplication;*

that satisfy the five properties below.

Properties of Vector Spaces

(i) V is a commutative group under $+$

(ii) $\forall a \in F$, $\underline{v} \in V$, $a \cdot \underline{v} \in V$

(closed under scalar multiplication)

(iii) $\forall \underline{u}, \underline{v} \in V$ and $a, b \in F$

$$a \cdot (\underline{u} + \underline{v}) = a \cdot \underline{u} + a \cdot \underline{v}$$
$$(a + b) \cdot \underline{v} = a \cdot \underline{v} + b \cdot \underline{v}$$

($\cdot$ distributes over $+$)

(iv) $\forall \underline{v} \in V$, $a, b \in F$,

$$(a \cdot b) \cdot \underline{v} = a \cdot (b \cdot \underline{v})$$

($\cdot$ is associative)

(v) The multiplier identity $1 \in F$ is the identity for scalar multiplication

$$1 \cdot \underline{v} = \underline{v}.$$

Properties of Vector Spaces

The additive identity of V is denoted by $\underline{0}$.
Additional Properties:

I) $0 \cdot \underline{v} = 0 \ \forall v \in V$

II) $c \cdot \underline{0} = \underline{0}$

III) $(-c) \cdot \underline{v} = c \cdot (-\underline{v}) = -(c \cdot \underline{v})$

Common Vector Spaces

- n-tuples $(\underline{v}) = (v_0, v_1, \ldots, v_{n-11})$
  - each $v_i \in F$

- $+$ defined by $\underline{u} = (u_0, u_1, \ldots, u_{n-1})$ then $u + v = (u_0 + v_0, u_1 + v_1, \ldots, u_{n-1} + v_{n-11})$

- $\cdot$ defined by $a \in F$, $a \cdot \underline{v} = (av_0, av_1, \ldots, av_{n-1})$

We will focus on $F = GF(2)$ or $GF(2^m)$.

Linear Combinations

Definition 14

Let $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n \in V$ *and* $a_1, a_2, \ldots, a_n \in F$. *Then* $a_1\underline{v}_1 + a_2\underline{v}_2 + \cdots + a_n\underline{v}_n \in V$ *is a linear combination of* $v_1, v_2, \ldots, v_n$.

Definition 15

If $G = \{\underline{v}_0, \underline{v}_1, \cdots, \underline{v}_n\}$ *is a collection of vectors* $\ni$ *the linear combinations of vectors in* G *is all vectors in a vector space* V, *then* G *is a spanning set for* V

Example

Let V_n denote the vector space of n–tuples whose elements $\in GF(2)$

$$V_4 = \begin{array}{cccc} (0000) & (0001) & (0010) & (0011) \\ (0100) & (0101) & (0110) & (0111) \\ (1000) & (1001) & (1010) & (1011) \\ (1100) & (1101) & (1110) & (1111) \end{array}$$

Then $G = \{(1000), (0110), (1100), (1001), (0011)\}$ is a spanning set for V (G spans V).

Note: The vectors in G are *linearly dependent*.

Linearly Independent

Definition 16

- *A set of vectors $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_k$ in a vector space V over a field F are linearly dependent if $\exists a_1, a_2, \ldots, a_k \in F$ $\ni a_1\underline{v}_1 + a_2\underline{v}_2 + \cdots + a_k\underline{v}_k = \underline{0}$, and at least one $a_i \neq 0$.*
- *Otherwise $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_k$ are linearly dependent.*

Ex:(cont) The vectors in G are linearly dependent because (for example)

$$(0110) + (1100) + (0011) = (1001)$$

(i.e., the sum of these four is $\underline{0}$) *Vectors are linearly dependent if one can be expressed as the linear combination of the others.* We can delete (1001) from G and still have a spanning set for V. However, we cannot delete any more vectors and still have a spanning set for V.

Definitions

Definition 17

A spanning set for V is a basis for V if it has minimum cardinality.

Example: Bases for V_4 Clearly $\{(1000),(0110),(1100),(0011)\}$ is a basis for V_4.
A common basis for V_n is the *canonical basis*.
Example: Canonical basis for V_4: $\{(1000),(0100),(0010),(0001)\}$

Definition 18

The dimension of a vector space V, written $\dim(V)$, is the cardinality of a basis for V.

Definitions

Theorem 6

Let $\{v_0, v_1, \dots, v_{k-1}\}$ be a basis for a vector space V. For every $\underline{v} \in V$, there is a unique representation

$$\underline{v} = a_0\underline{v}_0 + a_1\underline{v}_1 + \cdots + a_{k-1}\underline{v}_{k-1}. \quad (1)$$

Definitions

Definition 19

If V is a vector space over a field F and $S \subset V$ is also a vector space over F, then S is a subspace of V.

Theorem 7

(Theorem 2.18) Let $S \subset V$, $S \neq \emptyset$ then S is a subspace of V if:
i) $\forall \underline{u}, \underline{v} \in S$, $\underline{u} + \underline{v} \in S$.
ii) $\forall a \in F, \underline{u} \in S$, $a \cdot \underline{u} \in S$

Theorem 8

(Theorem 2.19) Let $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k \in V$ over F. The set of all linear combinations of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$ forms a vector subspace of V.

Inner Product

Definition 20

Let $\underline{u}, \underline{v} \in V$, a vector space of n–tuples over a field F. Then the inner (or dot) product of $\underline{u}$ and $\underline{v}$ is

$$\begin{aligned} \underline{u} \cdot \underline{v} &= u_0 v_0 + u_1 v_1 + \cdots + u_{n-1} v_{n-1} \\ &= \sum_{i=0}^{n-1} u_i v_i, \end{aligned}$$

which is a scalar.

Properties of Inner Product

(i) Commutativity $\Rightarrow \underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$

(ii) Associativity $\Rightarrow (a \cdot \underline{u}) \cdot \underline{v} = a \cdot (\underline{u} \cdot \underline{v})$

(iii) Distributivity over $+ \Rightarrow \underline{u} \cdot (\underline{v} + \underline{w}) = \underline{u} \cdot \underline{v} + \underline{u} \cdot \underline{w}$

Definition 21

If $\underline{u}, \underline{v} \in V$ (a vector space), and $\underline{u} \cdot \underline{v} = 0$, then $\underline{u}$ and $\underline{v}$ are orthogonal.

Null Space

Definition 22

- *Let* S *be a* $\dim k$ *subspace of* V_n. *Let* S_d *be all vectors in* $V_n \ni$ *if* $\underline{u} \in S$, $\underline{v} \in S_d$, $\underline{u} \cdot \underline{v} = 0$.
- *Then* S_d *is also a subspace of* V_n, *and* S_d *is called the null space or dual space of* S.

Null Space

Proof that S_d is a subspace of V_n: S_d is nonempty, since
$\underline{0} \cdot \underline{u} = 0$, $\forall \underline{u} \in V_n \Rightarrow \underline{0} \in S_d$.
Suppose $\underline{v} \in S_d$,$\underline{w} \in S_d$. Then $\underline{v} \cdot \underline{u} = 0$ and $\underline{w} \cdot \underline{u} = 0 \forall \underline{u} \in S$

(i) $(v + w) \cdot u = (v \cdot u) + (w \cdot u) = 0$
$\Rightarrow \underline{v} + \underline{w} \in S_d$

(ii) For any $a \in F$, $(a \cdot \underline{w}) \cdot \underline{u} = a \cdot (\underline{w} \cdot \underline{u}) = a \cdot 0 = 0$
$\Rightarrow a \cdot \underline{w} \in S_d$

(i) $\&$ (ii) $\Rightarrow$ any linear combination of vectors in S_d is in S_d.
$\Rightarrow S_d$ is a subspace of V.

Null Space

Theorem 9

The dimension theorem: Let S be a finite dimensional vector subspace of V and let S_d be the corresponding dual space. Then

$$\dim(S) + \dim(S_d) = \dim(V).$$

Matrices over GF(Q)/GF(2)

$k \times n$ matrix over $GF(q)$

- k rows
- n columns
- $g_{i,j} \in GF(q)$

$$\underline{G} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

$\underline{G}$ is also abbreviated as $[g_{ij}]$.

Matrices over GF(Q)/GF(2)

Let $\underline{g}_i$ denotes the vector of the i^{th} row

$$g_i = \begin{bmatrix} g_{i0} & g_{i1} & \cdots & g_{i,n-1} \end{bmatrix} \tag{2}$$

Then,

$$\underline{G} = \begin{bmatrix} \underline{g}_0 \\ \underline{g}_1 \\ \vdots \\ \underline{g}_{k-1} \end{bmatrix} \tag{3}$$

Matrices over GF(Q)/GF(2)

If the k rows $\underline{g}_0, \ldots, \underline{g}_{k-1}$ are linearly independent, then:

- There are q^k linear combination of the $\underline{g}_i$
- These q^k vectors form a k–dimensional vector space over the n–tuples over $GF(q)$, called the *row space* of $\underline{G}$.

Matrices over GF(Q)/GF(2)

Any matrix G may be transformed by elementary row operations (swapping rows, adding rows) into a matrix G' that has the same row space.

If S is the row space of $\underline{G}_{n\times n}$, then the null space S_d has dim $n-k$.

Let $\underline{h}_0, \underline{h}_1, \ldots, \underline{h}_{n-k-1}$ denotes $n-k$ linearly independent vectors in S_d and

$$\underline{H} = \begin{bmatrix} \underline{h}_0 \\ \underline{h}_1 \\ \vdots \\ \underline{h}_{n-k-1} \end{bmatrix} \tag{4}$$

Then the row space of $\underline{H}$ is S_d.

The row space of $\underline{G}$ is the null space of $\underline{H}$, and vice versa.

More Matrix Operations

Matrix addition and multiplication is as expected:
Addition is componentwise for 2 matrices of the same size:

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}] \tag{5}$$

Multiplication of a $k \times n$ matrix A by an $n \times l$ matrix B yields a $k \times l$ matrix C.

$$c_{ij} = \underline{a}_i \cdot \underline{b}_j \tag{6}$$

where
$\underline{a}_i$ is the i^{th} row of A
$\underline{b}_j$ is the j^{th} column of B.

$$c_{ij} = \sum_{t=0}^{n-1} a_{it} b_{tj} \tag{7}$$

More Matrix Operations

$\underline{G}^T$ = transpose of $\underline{G} = n \times k$ matrix whose columns are the rows of $\underline{G}$.

$\underline{I}_k = k \times k$ Identity matrix $= \begin{cases} 1 & \text{in } (i,i) \text{ positions} \\ 0 & \text{elsewhere} \end{cases}$

Example:

$$\underline{I}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Submatrix of $\underline{G}$ = matrix created by removing rows and/or columns from $\underline{G}$.