MAT4006: Introduction to Coding Theory

Lecture 03: Error Correction, Groups, Rings, Fields

Instructor: Zitan Chen
Scribe: Siqi Yao

Spring 2025

1 Error Correction

Definition 1.1 (Error Correction)

Let ν be a positive integer. We say a code $C \subseteq A^n$ can correct ν errors if there exists a decoder $\mathcal{D} : A^n \to C$ such that for any $x \in C$ and $y \in A^n$ with $d(x, y) \leq \nu$, one has $\mathcal{D}(y) = x$.

Theorem 1.1

A code $C \subseteq A^n$ can correct ν errors if $d(C) \geq 2\nu + 1$.

Proof. Let $x \in C$ and $y \in A^n$ be such that $d(x, y) \leq \nu$.

Let $x' \in C$, with $x' \neq x$. Then

$$d(x, x') \geq d(C) \geq 2\nu + 1.$$

By the triangle inequality,

$$d(x, x') \leq d(x, y) + d(y, x') \leq \nu + d(x', y),$$

so

$$2\nu + 1 \leq d(x, x') \leq \nu + d(x', y) \Rightarrow \nu + 1 \leq d(x', y).$$

Hence,

$$d(x, y) < d(x', y) \quad \text{for all } x' \in C,\ x' \neq x.$$

Using the *minimum distance decoder*, we will decode y to x, thus correcting the errors. □

Theorem 1.2

If a code $C \subseteq A^n$ can correct ν errors, then $d(C) \geq 2\nu + 1$.

Proof. Let $x \in C$ be the transmitted codeword.

There exists $x' \in C$ such that $d(x, x') = d(C)$.

Suppose $d(C) \leq 2\nu$, we will construct $y \in A^n$ such that $d(x', y) \leq d(x, y)$, meaning we cannot decode y uniquely to x.

Let $I \subseteq \{1, \ldots, n\}$ be the set of positions where x and x' differ:

$$I = \{i \mid x_i \neq x'_i\}, \quad \text{so that } |I| = d(x, x').$$

Let $J \subset I$ with $|J| = \left\lfloor \frac{d(x,x')}{2} \right\rfloor$.
Define the received word $y = (y_1, \ldots, y_n)$ as:

$$y_i = \begin{cases} x_i, & i \in J, \\ x'_i, & i \in \{1, \ldots, n\} \setminus J. \end{cases}$$

A concrete example:

$$\begin{aligned} x &= (x_1, \ldots, x_n) = & 000\underline{11}111 \\ x' &= (x'_1, \ldots, x'_n) = & 00000\underline{000} \\ y &= (y_1, \ldots, y_n) = & 000\underline{11000} \end{aligned}$$

The blue part corresponds to set J while the green part corresponds to set I.
Then,

$$d(y, x) = |I \setminus J| = \left\lceil \frac{d(x, x')}{2} \right\rceil, \quad d(y, x') = |J| = \left\lfloor \frac{d(x, x')}{2} \right\rfloor.$$

Hence, $d(y, x) \geq d(y, x')$ and

$$d(x, y) = \left\lceil \frac{d(x, x')}{2} \right\rceil \leq \nu.$$

So y is within ν of x but closer to another codeword x', making correct decoding to x impossible. □

2 Groups

Definition 2.1 (Group)

A group is a nonempty set G with a binary operation "$\cdot$" satisfying the following axioms:

1. **Closure:** For every $a, b \in G$, we have $a \cdot b \in G$.
2. **Associativity:** For every $a, b, c \in G$, we have

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

3. **Identity element:** There exists an element $1 \in G$ such that

$$1 \cdot a = a \cdot 1 = a \quad \text{for every } a \in G.$$

4. **Inverse element:** For each $a \in G$, there exists an element $a^{-1} \in G$ such that

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

If these properties are satisfied, we say that $(G, \cdot)$ is a group, or simply that G is a group.

Note:

1. If the binary operation is multiplication, then the group doesn't contain 0.
2. If only axiom 1, 2 is satisfied, then the set is called a **semigroup**.
3. If only axiom 1, 2, 3 is satisfied, then the set is called a **monoid**.

Definition 2.2 (Abelian Group)

A group is called **commutative** or **abelian** if

$$a \cdot b = b \cdot a \quad \text{for every } a, b \in G.$$

Power

For an element $a \in G$ and a positive integer n, the notation

$$a^n$$

stands for

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}.$$

Also define

$$a^{-n} \quad \text{as the power } (a^{-1})^n, \text{ and} \quad a^0 = 1 \in G.$$

Two main notational conventions for groups:

Group Type	Operation	Identity	Power	Inverse	Remark
Multiplicative Group	$\cdot$	1	a^n	a^{-1}	$ab = a \cdot b$
Additive Group	$+$	0	na	$-a$	$a - b = a + (-b)$

Examples

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

Let

$$n\mathbb{Z} = \{ni \mid i \in \mathbb{Z}\} \triangleq (n).$$

Then

$$(n\mathbb{Z}, +) \text{ is a group.}$$

3 Rings

Definition 3.1 (Ring)

A ring is a nonempty set R with two binary operations $\cdot$ and $+$ satisfying:

1. $(R, +)$ is an abelian group.
2. **Associativity of $\cdot$:** For every $a, b, c \in R$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$
3. **Distributivity:** For every $a, b, c \in R$,
$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{and} \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$
I.e., multiplication is distributive with respect to addition.
4. **Closure under multiplication:** For every $a, b \in R$, $a \cdot b \in R$.

Conventions

When writing expressions, the multiplication $\cdot$ takes precedence over the addition $+$.

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

and

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

The identity element with respect to $+$ is called the **zero element**.

Definition 3.2 (Ring with Identity)

A ring with identity is a ring R in which the multiplication operation $\cdot$ has an identity element, i.e., there exists $1 \in R$ such that

$$1 \cdot a = a \cdot 1 = a \quad \text{for every } a \in R.$$

Definition 3.3 (Commutative Ring)

A commutative ring is a ring in which the multiplication operation $\cdot$ is commutative, i.e.,

$$a \cdot b = b \cdot a \quad \text{for every } a, b \in R.$$

4 Fields

Definition 4.1 (Field)

A field is a commutative ring in which the nonzero elements $F^* := F \setminus \{0\}$ form a group with respect to multiplication.
Note: This implies F^* has the *multiplicative inverse*

Lemma 4.1

Let F be a field and $a, b \in F$. Then:

(i) $0 \cdot a = 0$

(ii) $ab = 0$ implies $a = 0$ or $b = 0$

(iii) $(-1) \cdot a = -a$

Proof. (i) $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$

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

(ii) Given $ab = 0$, if $a \neq 0$, then

$$a^{-1} \cdot ab = a^{-1} \cdot 0 = 0 \cdot a^{-1} = 0,$$

$$\Rightarrow 1 \cdot b = 0, b = 0$$

Similarly, if $b \neq 0$, we have $a = 0$.

(iii) $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0$

$$\Rightarrow (-1) \cdot a = -a.$$

$\square$

Examples

- $(\mathbb{Z}, +, \cdot)$ is a ring, called the ring of integers, **not a field**.
- $(\mathbb{Z}^*, \cdot)$ is not a group.
- $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are fields.

Remark

A field containing finite elements is called a **finite field**.