The Roadmap from Polynomials to Quantum-safe Cryptosystems

A perspective from discrete mathematics (Part 1/4)

Chunlei Li (University of Bergen, Norway)

INCP2-2024/10213 on
Mathematical Theory of Data Transmission and Data Encryption
Oct. 6-10, 2025, Tromsø
Fall school on Geometry in Cryptography and Communication

Outline[1]

1. Algebra Structures
2. Finite Fields
3. Linear Block Codes
4. Cyclic and Quasi-Cyclic Codes

[1] The materials in this lecture can be found from [1, 2]

Algebra Structures

Algebra Structures

Algebraic Structure $(S, \odot)$

A set S with certain arithmetic operations "$\odot$"

$$\begin{aligned} S \times S &\to S \\ (x_i, x_j) &\mapsto x_i \odot x_j \end{aligned}$$

satisfying certain laws.

Group $(G, \otimes)$

A set G with an arithmetic operation $\otimes$ on elements in G satisfying the following four laws:

- **closure**: $x \otimes y \in G$ for any $x, y \in G$;
- **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **identity element**: $\exists\, I \in G$ such that $x \otimes I = I \otimes x = x$;
- **inverse element**: $\exists\, y \in G$ such that $x \otimes y = y \otimes x = I$.

G is a **cyclic group** if $G = \langle g \rangle = \{I, g, g^2, \cdots, \}$, where g is called a **generator** of G;

Algebra Structures - Group

Group $(G, \otimes)$

A set G with an arithmetic operation $\otimes$ on elements in G satisfying the following four laws:

- **closure**: $x \otimes y \in G$ for any $x, y \in G$;
- **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **identity element**: $\exists\, I \in G$ such that $x \otimes I = I \otimes x = x$;
- **inverse element**: $\exists\, y \in G$ such that $x \otimes y = y \otimes x = I$.

G is a **cyclic group** if $G = \langle g \rangle = \{I, g, g^2, \cdots, \}$, where g is called a **generator** of G;

Ex. 1: Which is a group?

- $(\{0, 1, 2, 3\}, +)$, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$;

Ring $(R, \otimes, \oplus)$

A set R with two arithmetic operations $\otimes$ and $\oplus$ on elements in G satisfying the following laws:

- $(R, \oplus)$ is a group and $x \oplus y = y \oplus x$ (Abelian Group)
- for multiplication $\otimes$:
  - **closure**: $x \otimes y \in R$;
  - **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **distributive**: $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Ring $(R, \otimes, \oplus)$

A set R with two arithmetic operations $\otimes$ and $\oplus$ on elements in G satisfying the following laws:

- $(R, \oplus)$ is a group and $x \oplus y = y \oplus x$ (Abelian Group)
- for multiplication $\otimes$:
  - **closure**: $x \otimes y \in R$;
  - **associative**: $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- **distributive**: $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Example (Rings we have learned)

- Integer Ring $(\mathbb{Z}, +, \times)$;
- Polynomial Ring $(P, +, \otimes)$ with $P = \{\sum_i a_i x^i : a_i \in \mathbb{Z}\}$;

Algebra Structures - Field

Field $(F, \otimes, \oplus)$

A set F with two arithmetic operations $\otimes$ and $\oplus$ on elements in F satisfying the following laws:

- $(R, \oplus)$ is an Abelian group;
- $(R \setminus \{0\}, \otimes)$ is also an Abelian group;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Algebra Structures - Field

Field $(F, \otimes, \oplus)$

A set F with two arithmetic operations $\otimes$ and $\oplus$ on elements in F satisfying the following laws:

- $(R, \oplus)$ is an Abelian group;
- $(R \setminus \{0\}, \otimes)$ is also an Abelian group;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

Example

- Is $(\mathbb{Z}, +, \times)$ or $(\mathbb{Z}_n, +, \times)$ a field?
- Number Fields: $(\mathbb{R}, +, \times)$ (Infinite number of elements)

Ex. 2

Give a few more examples of fields

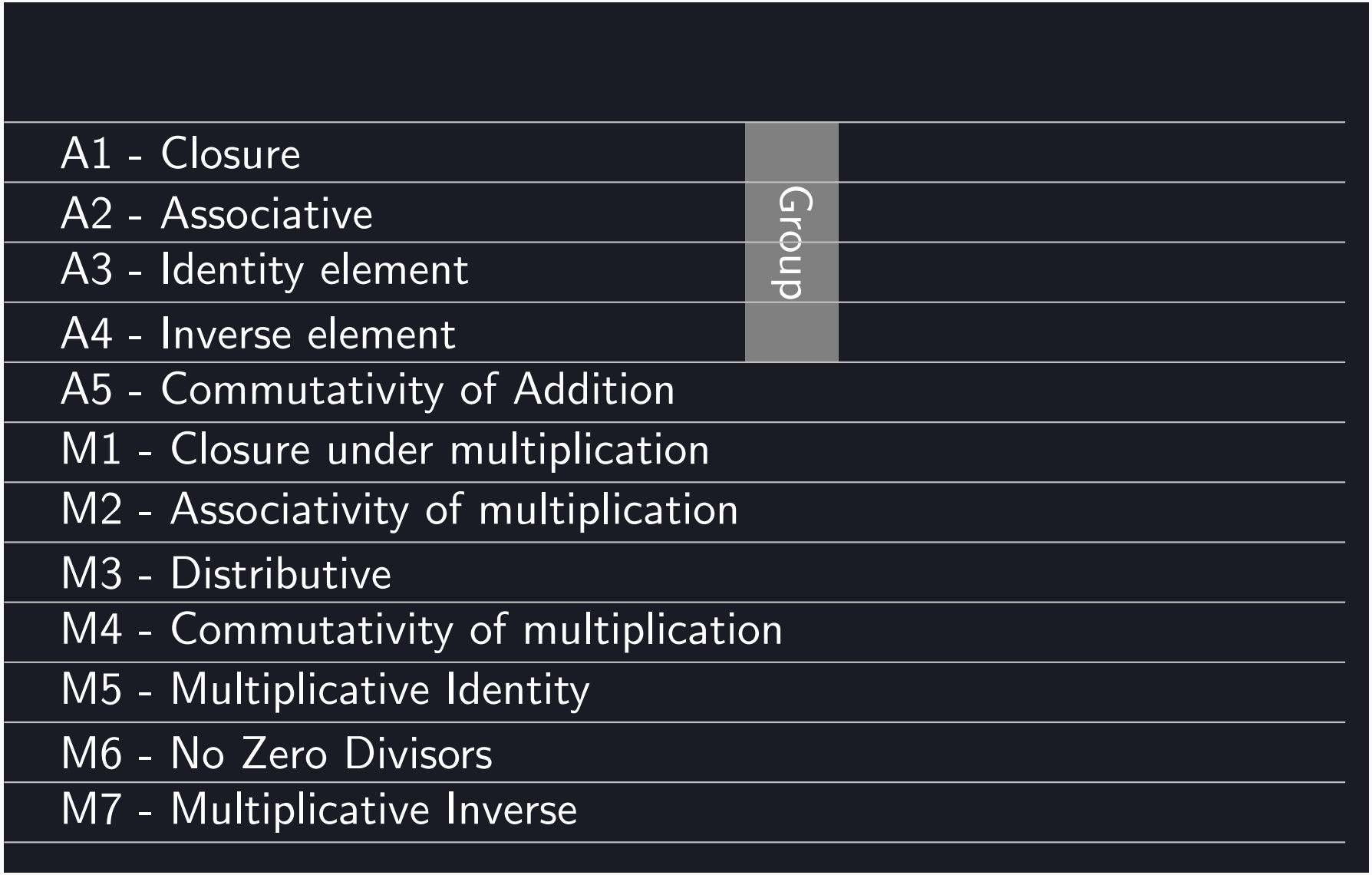
Example

- Is $(\mathbb{Z}, +, \times)$ or $(\mathbb{Z}_n, +, \times)$ a field?
- Number Fields: $(\mathbb{R}, +, \times)$ (Infinite number of elements)

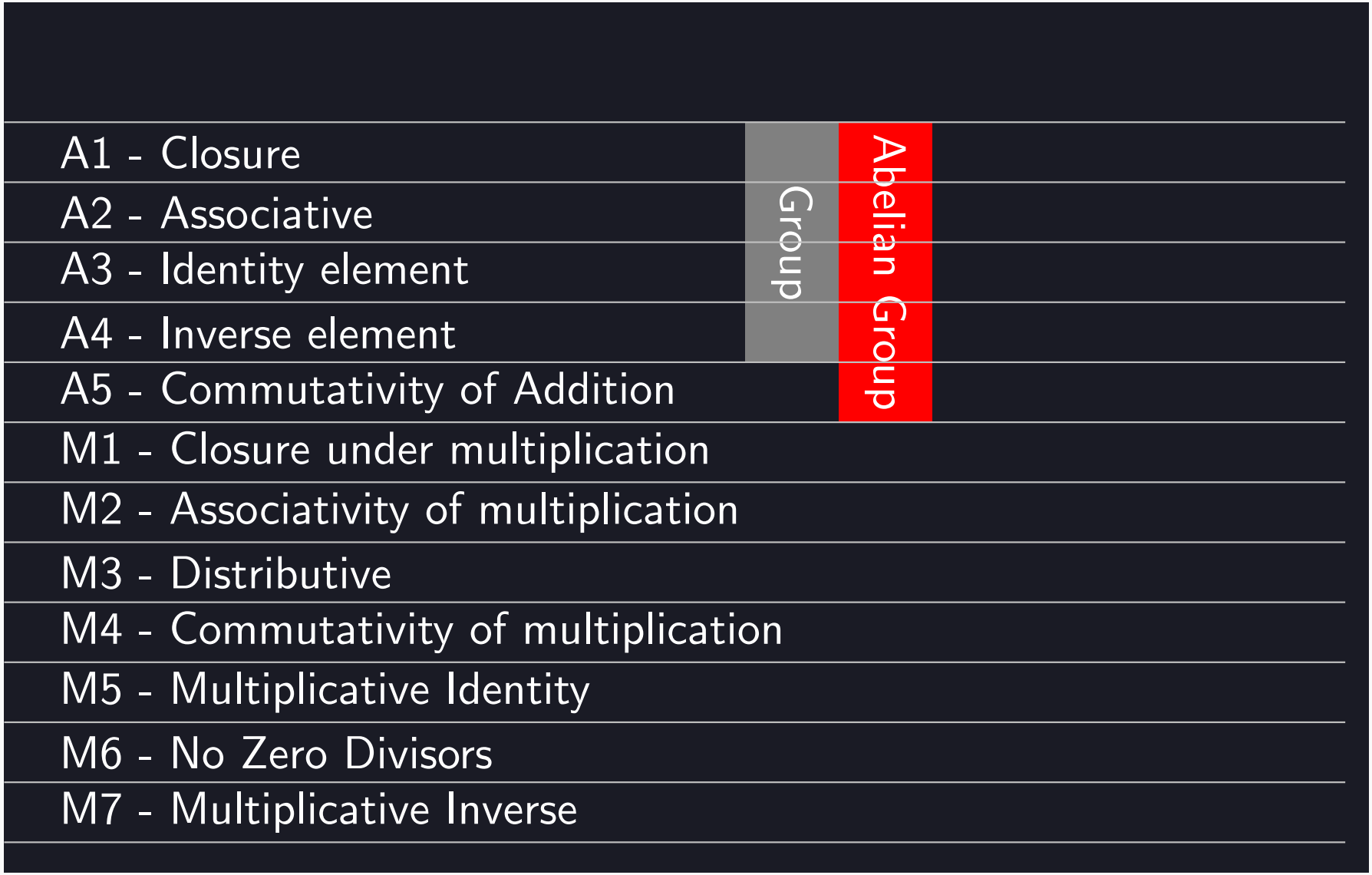
Ex. 2

Give a few more examples of fields

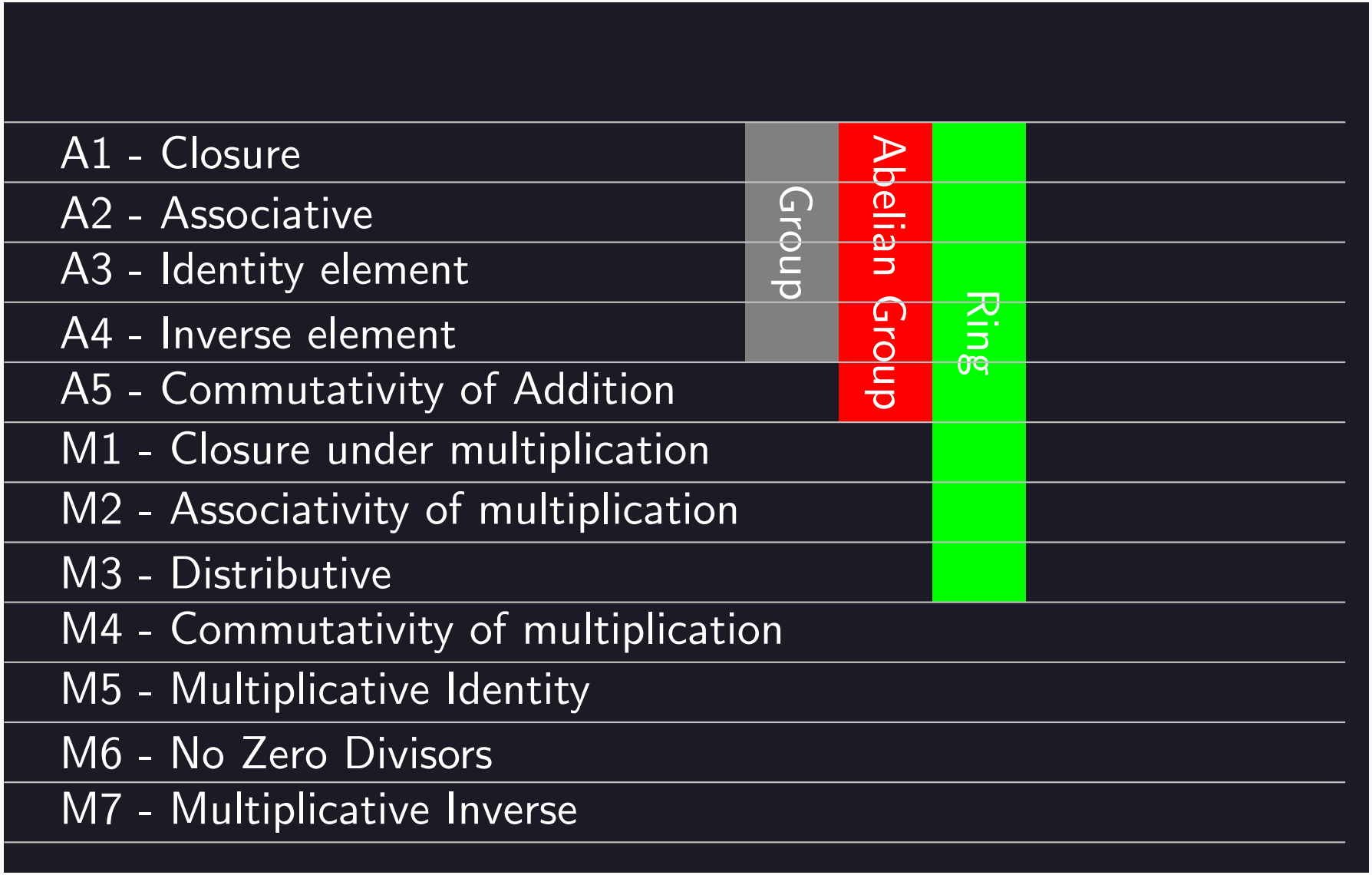
Algebra Structures Hierarchy - Group, Ring, Field



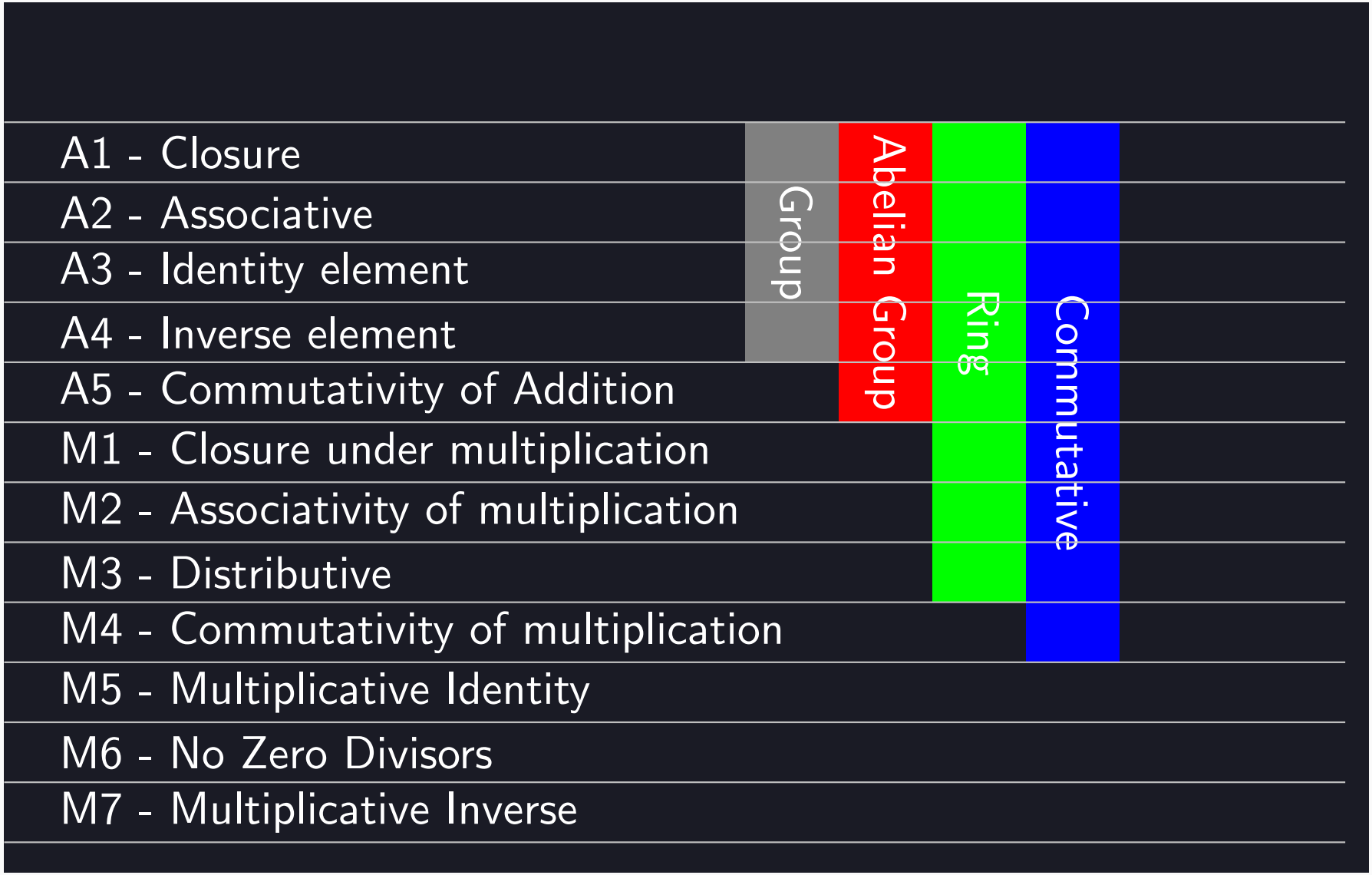
Algebra Structures Hierarchy - Group, Ring, Field



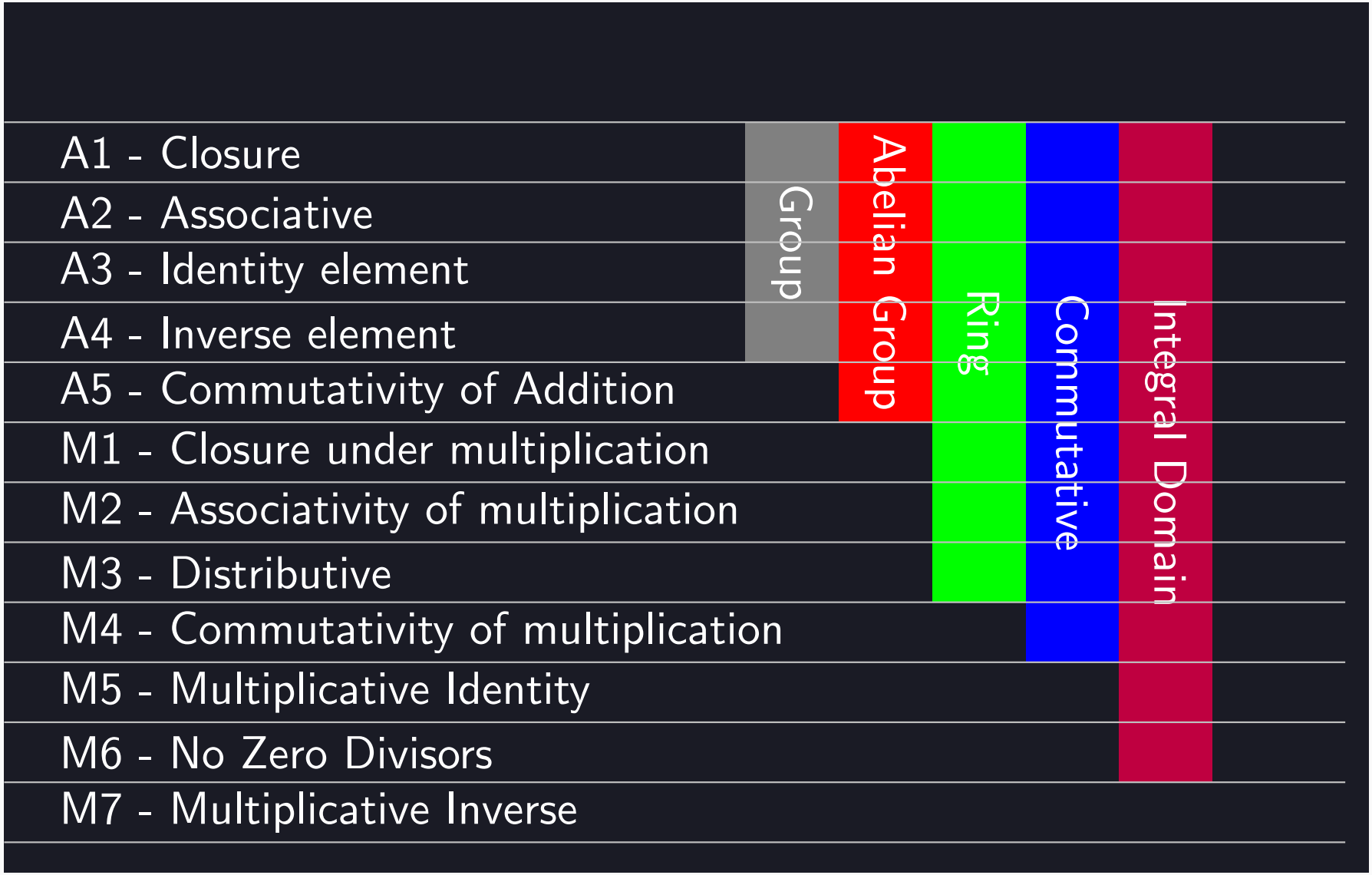
Algebra Structures Hierarchy - Group, Ring, Field



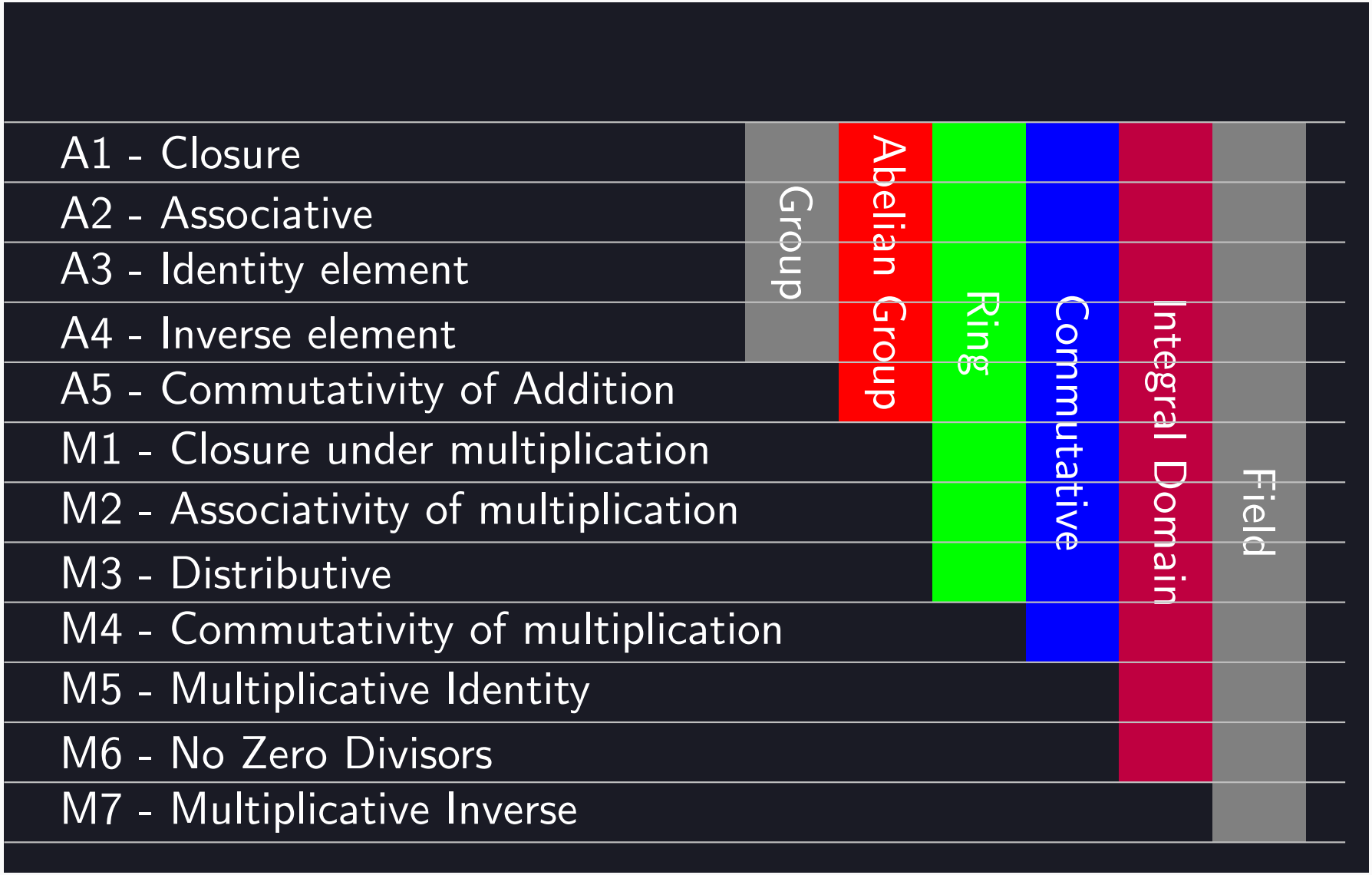
Algebra Structures Hierarchy - Group, Ring, Field



Algebra Structures Hierarchy - Group, Ring, Field



Algebra Structures Hierarchy - Group, Ring, Field



Finite Fields

Finite Fields $\mathbb{F}_{p^n}$

Existence of Finite Fields

Finite fields exist iff. they contain p^n elements for a prime p.

Construction of Finite Fields

- $n = 1$, $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ with $(+, \times)$ is a field;
  - $(\mathbb{Z}_p, +)$ is an abelian group;
  - $(\mathbb{Z}_p, \times)$ is also an abelian group:
    $\forall\ x \in \mathbb{Z}_p^*, \exists\ y \in \mathbb{Z}_p^*$ s.t. $xy \equiv 1 \mod p$ since $(x, p) = 1$
- The binary case $p = 2$ is of particular interest
  - the addition in $GF(2) = \{0, 1\}$ is the logic XOR

Finite Fields $\mathbb{F}_{p^n}$

- Integer Ring $(\mathbb{Z}, +, \times)$
  - prime $p \in \mathbb{Z}$: divisible only by 1 and itself;
  - $a \equiv b \mod p$ iff. $p|(a - b)$
  - The ring $\mathbb{Z}$ modulo a prime p yields $\mathbb{F}_p$;

Finite Fields $\mathbb{F}_{p^n}$

- Integer Ring $(\mathbb{Z}, +, \times)$
  - prime $p \in \mathbb{Z}$: divisible only by 1 and itself;
  - $a \equiv b \mod p$ iff. $p|(a-b)$
  - The ring $\mathbb{Z}$ modulo a prime p yields $\mathbb{F}_p$;
- Poly. Ring $(\mathbb{Z}_p[x], +, \times)$, $\mathbb{Z}_p[x] = \{\sum_i a_i x^i : a_i \in \mathbb{Z}_p\}$
  - irreducible poly. $f(x)$: "prime" in $\mathbb{Z}_p[x]$;
  - $g_1(x) \equiv g_2(x) \mod f(x)$ iff. $f(x)|(g_1(x) - g_2(x))$
  - $\mathbb{Z}_p[x]$ modulo an irreducible poly $f(x)$ of degree n yields $\mathbb{F}_{p^n}$

Unique Representation

Let $f(x)$ be an irreducible poly. of degree n in $\mathbb{F}_p[x]$.

$$\mathbb{F}_{p^n} := \mathbb{F}_p[x] \Big/ (f(x)) = \left\{ \sum_{i=0}^{n-1} a_i x^i,\ a_i \in \mathbb{F}_p \right\}$$

- $a(x) \oplus b(x) = \sum_{i=0}^{n-1} (a_i \oplus b_i) x^i = c(x) = \sum_{i=0}^{n-1} c_i x^i$
- $a(x) \otimes b(x) = a(x)b(x) \bmod f(x) = c(x) = \sum_{i=0}^{n-1} c_i x^i$

$a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longleftrightarrow a = (a_{n-1}, \cdots, a_1, a_0)$

- $a \oplus b \leftrightarrow a(x) \oplus b(x) = c(x) \leftrightarrow c = (c_0, \cdots, c_{n-1})$
- $a \otimes b \leftrightarrow a(x) \otimes b(x) = c(x) \leftrightarrow c = (c_0, \cdots, c_{n-1})$

Finite Fields $\mathbb{F}_{2^3}$

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

(a) Addition

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(b) Multiplication

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Finite Fields $\mathbb{F}_{2^4}$

C

Ex. : Complete the following arithmetic

- $(1,0,0,1) \otimes (1,1,0,0)$; $(1,0,1,1) \otimes (1,0,0,1)$;

Properties of Finite Fields

For a finite field $\mathbb{F}_{p^n}$ generated from a primitive poly. $f(x)$ of degree n and a root α, we have

- $\mathbb{F}_{p^n}^*$ is a cyclic multiplicative group generated by α
- the factorization

$$x^{p^n} - x = \prod_{\beta \in \mathbb{F}_{p^n}} (x - \beta) = x \prod_{j=0}^{p^n - 2} (x - \alpha^j)$$

- all linear maps from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ are given by the trace function $\mathrm{Tr}(ax)$ with $a \in \mathbb{F}_{p^n}$, where

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

Ex. 4

Prove that $\mathrm{Tr}(\beta)$ belongs to $\mathbb{F}_p$ for any $\beta \in \mathbb{F}_{p^n}$

Linear Block Codes

Vector Space

Suppose $\mathbb{F}$ is a field with addition $+$ and multiplication $\cdot$

Vector Space over $\mathbb{F}$

Suppose $\mathbb{F}^n$ is the set of all n-tuples over $\mathbb{F}$, i.e.,

$$\mathbb{F}^n = \{x = (x_0, x_1, \ldots, x_{n-1}) | x_i \in \mathbb{F},\ 1 \leq i \leq n\}.$$

Then $\mathbb{F}^n$ forms a vector space $V = (\mathbb{F}^n, +, \mathbb{F})$, which, for any $x, y \in \mathbb{F}^n$ and $c \in \mathbb{F}$, satisfies

- $x + y = (x_0 + y_0, x_1 + y_1, \ldots, x_{n-1} + y_{n-1}) \in \mathbb{F}^n$
- $c \cdot x = (cx_0, cx_1, \ldots, cx_{n-1}) \in \mathbb{F}^n$

A vector space over $V = (\mathbb{F}^n, +, \mathbb{F})$ is an additive group allowing for scalar product

Basis

A group of n elements $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}^n$ is called a basis of $\mathbb{F}^n$ if they are linearly independent over $\mathbb{F}$. Moreover,

$$\mathbb{F}^n = \left\{ \sum_{i=1}^{n} c_i \alpha_i \mid c_1, \ldots, c_n \in \mathbb{F} \right\}$$

Subsapce

For a vector space $V = (\mathbb{F}^n, +, \mathbb{F})$, a subset $S \subseteq V$ is a linear subspace of V if for any $x, y \in S$ and $c \in \mathbb{F}$,

- $x + y \in S$ and $c \cdot x \in S$

If S can be generated by k linearly independent $\alpha_1, \ldots, \alpha_k$ as

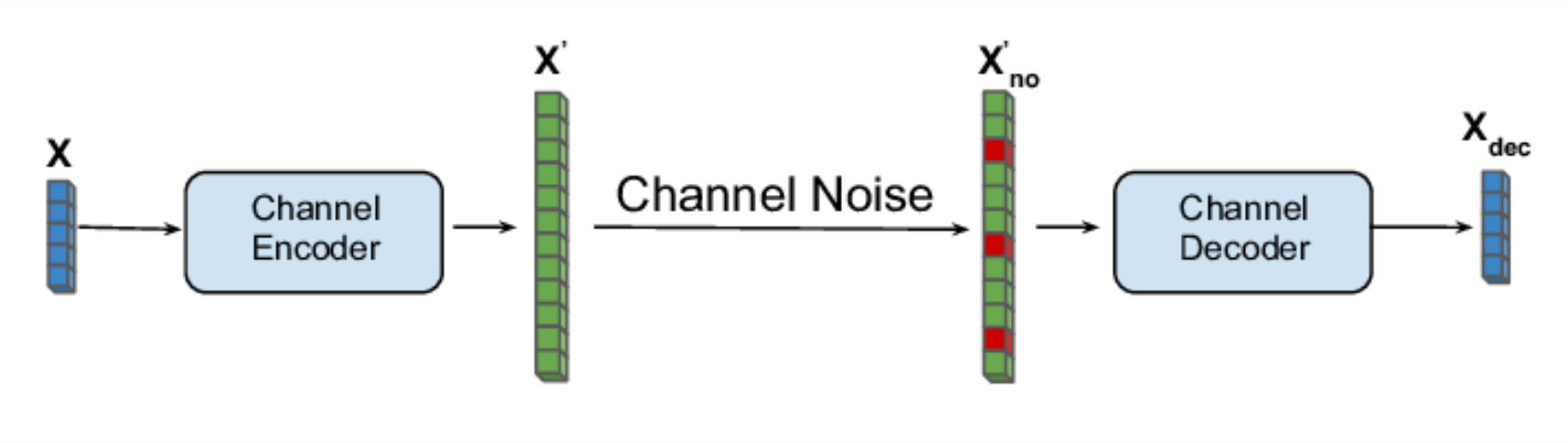
$$S = \left\{ \sum_{i=1}^{k} c_i \alpha_i \mid c_1, \ldots, c_n \in \mathbb{F} \right\},$$

then S has dimension k with a basis $\alpha_1, \ldots, \alpha_k$.

We are mainly interested in $\mathbb{F}$ as finite fields $\mathbb{F}_q$ in the context of coding theory and cryptography.

Linear Codes for Error Correction

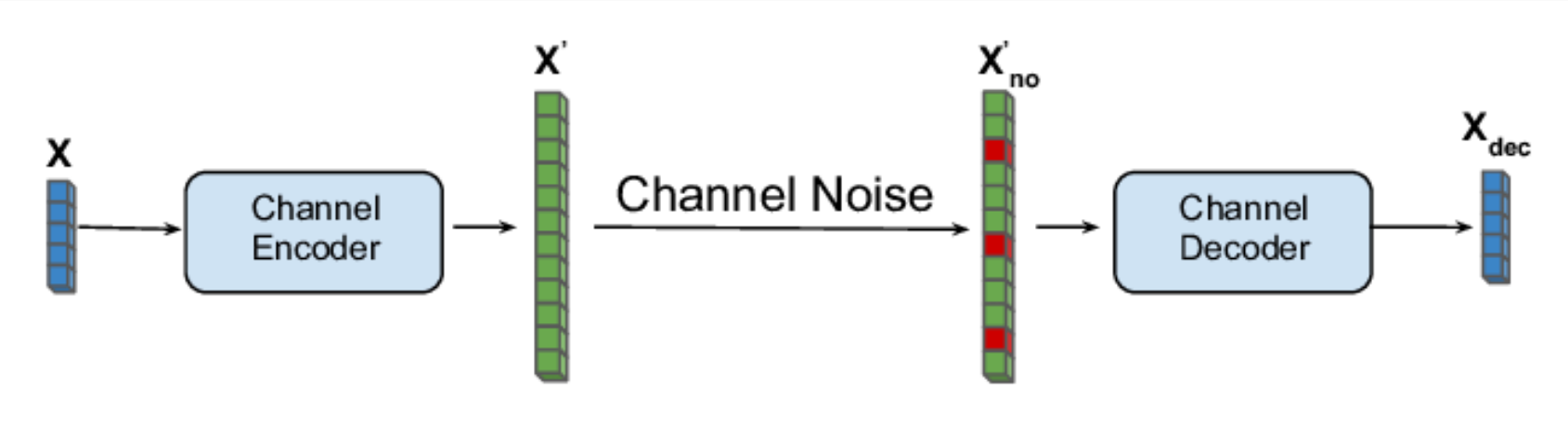
When the vector space $\mathbb{F}_q^n$ is equipped with a certain metric of distance, it brings error-correcting capability.



- **Encoder**: message of length $k \Rightarrow$ codeword of length n
- **Decoder:**
  - receive a noisy word: transmitted codeword + noise
  - identify the transmitted codeword by the maximum likelihood (ML) strategy, which often reduces to nearest neighbor or majority voting

Linear Codes for Error Correction

When the vector space $\mathbb{F}_q^n$ is equipped with a certain metric of distance, it brings error-correcting capability.



- **Encoder**: message of length $k \Rightarrow$ codeword of length n
- **Decoder:**
  - receive a noisy word: transmitted codeword + noise
  - identify the transmitted codeword by the maximum likelihood (ML) strategy, which often reduces to nearest neighbor or majority voting

Linear Codes with the Hamming metric

The **Hamming weight** of $x \in \mathbb{F}_q^n$ is

$$wt(x) = |\{1 \leq i \leq n : x_i \neq 0\}|.$$

The Hamming distance between $x, y \in \mathbb{F}_q^n$ is defined as

$$d(x, y) = wt(x - y).$$

Linear Codes

An $[n, k, d]_q$ linear code C is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with

- dimension k
- minimum distance/weight d, namely,

$$\min_{c_1 \neq c_2 \in C} d(x, y) = \min_{0 \neq c \in C} wt(c) = d.$$

Generator and Parity-Check Matrices

Generator Matrix

Given an $[n, k]$ linear code C, its generator matrix is a $k \times n$ matrix whose k rows form a basis of C

- each basis of C yields a genertor matrix of C
- each codeword $c = mG$ for some message $m \in \mathbb{F}_q^k$

Parity-Check Matrix

An $[n, k]$ linear code C can be seen as a solution space of a system of linear equations $xH^\intercal = 0$, where H is an $(n-k) \times n$ matrix with rank $n-k$, and is called the parity-check matrix of C

- $cH^\intercal = 0$ for any $c \in C$;
- $GH^\intercal = 0_{k \times (n-k)}$ since $cH^\intercal = mGH^\intercal = 0$ for any $m \in \mathbb{F}_q^k$

Systematic Generator and Parity-Check Matrix

For an $[n, k]$ linear code C, all generator matrix can be reduced to a **systematic generator matrix** of the form

$$G = [I_k | P]$$

Correpondingly, the **systematic parity-check matrix** of C has the form

$$H = [-P^{\mathsf{T}} | I_{(n-k)}]$$

where I_t is the $t \times t$ identity matrix

It is clear that

$$GH^{\mathsf{T}} = [I_k, P_{k\times(n-k)}] \cdot [-P^{\mathsf{T}}, I_{(n-k)\times(n-k)}]^{\mathsf{T}} = \mathbf{0}$$

Example. Find the systematic genertor matrix and parity-check matrix for

$$\begin{aligned} C = \{&0000000, 1111111, 1000101, 1100010, \\ &0110001, 1011000, 0101100, 0010110, \\ &0001011, 0111010, 0011101, 1001110, \\ &0100111, 1010011, 1101001, 1110100\} \end{aligned}$$

Dual Codes

For an $[n, k, d]_q$ linear code, its dual code is defined as follows:

$$C^{\perp} = \{x \in \mathbb{F}_q^n | x \cdot c = \sum_{i=1}^{n} x_i c_i = 0\}.$$

Properties of Dual Code

- $C^{\perp}$ has dimension $n - k$
- a generator matrix of $C^{\perp}$ is a parity-check of C, i.e.,

$$C^{\perp} = \{mH | m \in \mathbb{F}_q^{n-k}, H \text{ is a parity-check matrix of } C\}$$

- a parity-check matrix of $C^{\perp}$ is a generator of C

Advantages of Linear Codes

- more efficient to compute the minimum distance
- easy to encode messages with generator matrices
- could allow for efficient decoding

Encoding for Linear Codes

Given a generator matrix G of an $[n, k]$ linear code, the encoding process is given by

$$m \mapsto m \cdot G, \qquad \text{for any m} \in \mathbb{F}_q^k$$

E.g.: the binary $(7, 4, 3)$ Hamming code with generator matrix

$$G = \begin{bmatrix} 1000110 \\ 0100101 \\ 0010011 \\ 0001111 \end{bmatrix}$$

A message 0110 encoded as 0110110

Decoding for Linear Codes

Given a received word $r = c + e$, try to recover the original codeword c.

Nearest Neighbor Decoding

Given a received word y, find a codeword $c \in C$ closest to y:

$$\hat{c} = \operatorname{argmin}_{c \in C} d(c, y)$$

- a naive method: test all codewords $c \in C$, complexity $O(q^k)$

Let's try harder ...

Partition of $\mathbb{F}_q^n$

Given an $[n, k]_q$ linear code C with parity-check matrix H, the whole vector space $\mathbb{F}_q^n$ can be partitioned w.r.t H:

- $cH^\intercal = 0$ for any $c \in C$
- $xH^\intercal = yH^\intercal$ iff $x - y \in C$
- the standard array

$$\mathbb{F}_q^n = C \sqcup (a_2 + C) \sqcup \cdots \sqcup (a_{q^{n-k}} + C)$$

where $a + C = \{a + c : c \in C\}$ is called a coset of C

Example: For a $(7, 3)$ code, a generator matrix is

$$G = \left[\begin{array}{ccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

The codewords for this code are

row 1	0000000	0111100	1011010	1100110	1101001	1010101	0110011	0001111

Table 3.1: The Standard Array for a Code

Row 1	0000000	0111100	1011010	1100110	1101001	1010101	**0110011**	0001111
Row 2	1000000	1111100	0011010	0100110	0101001	0010101	1110011	1001111
Row 3	0100000	0011100	1111010	1000110	1001001	1110101	0010011	0101111
Row 4	0010000	0101100	1001010	1110110	1111001	1000101	0100011	0011111
Row 5	0001000	0110100	1010010	1101110	1100001	1011101	0111011	0000111
Row 6	0000100	0111000	1011110	1100010	1101101	1010001	0110111	0001011
Row 7	0000010	0111110	1011000	1100100	1101011	1010111	0110001	0001101
Row 8	0000001	0111101	1011011	1100111	1101000	1010100	0110010	0001110
Row 9	1100000	1011100	0111010	0000110	0001001	0110101	1010011	1101111
Row 10	1010000	1101100	0001010	0110110	0111001	0000101	1100011	1011111
Row 11	0110000	0001100	1101010	1010110	1011001	1100101	0000011	0111111
Row 12	1001000	1110100	0010010	0101110	0100001	0011101	1111011	1000111
Row 13	**0101000**	0010100	1110010	1001110	1000001	1111101	**0011011**	0100111
Row 14	0011000	0100100	1000010	1111110	1110001	1001101	0101011	0010111
Row 15	1000100	1111000	0011110	0100010	0101101	0010001	1110111	1001011
Row 16	1110000	1001100	0101010	0010110	0011001	0100101	1000011	1111111

- each row is a coset of C
- the leading entry with smallest weight in each row is call the coset leader
- For any $r \in \mathbb{F}_q^n$, if $r \in e + C$, then $rH^\mathsf{T} = eH^\mathsf{T} = s$

Bounded-distance Decoding based on syndrome

Given a received word $y = c + e$, calculte the **syndrome**

$$s = yH^{\mathsf{T}} = cH^{\mathsf{T}} + eH^{\mathsf{T}} = eH^{\mathsf{T}}$$

- make a syndrome table of e, eH^{T} for all errors e with

$$wt(e) = t \leq \lfloor \frac{d-1}{2} \rfloor$$

- for y, find a match in the table such that $yH^{\mathsf{T}} = eH^{\mathsf{T}}$
- guess the codeword $\hat{c} = y - e$ and check $\hat{c}H^{\mathsf{T}} = 0$?

Example: the binary $(7, 4, 3)$ Hamming code with parity-check matrix

$$H = \begin{bmatrix} 1101100 \\ 1011010 \\ 0111001 \end{bmatrix}$$

A one-time look-up table:

e	100000	0100000	0010000	0001000	0000100	0000010	000001
eH^T	110	101	011	111	100	010	001

Suppose the received word $y = 1100100$ (from $c = 1101100$ with 1 bit error). The receiver compute

$$Hy^\mathsf{T} = (1100100) \begin{bmatrix} 1101100 \\ 1011010 \\ 0111001 \end{bmatrix}^\mathsf{T} = (111).$$

This matches with the error $e = 0001000$. Then the decoded word is $c' = y + e = 1101100$. DONE!

Ex. 4: Decode the following words

- 0111101, 1110110, 0011011

Table 3.1: The Standard Array for a Code

Row 1	0000000	0111100	1011010	1100110	1101001	1010101	**0110011**	0001111
Row 2	1000000	1111100	0011010	0100110	0101001	0010101	1110011	1001111
Row 3	0100000	0011100	1111010	1000110	1001001	1110101	0010011	0101111
Row 4	0010000	0101100	1001010	1110110	1111001	1000101	0100011	0011111
Row 5	0001000	0110100	1010010	1101110	1100001	1011101	0111011	0000111
Row 6	0000100	0111000	1011110	1100010	1101101	1010001	0110111	0001011
Row 7	0000010	0111110	1011000	1100100	1101011	1010111	0110001	0001101
Row 8	0000001	0111101	1011011	1100111	1101000	1010100	0110010	0001110
Row 9	1100000	1011100	0111010	0000110	0001001	0110101	1010011	1101111
Row 10	1010000	1101100	0001010	0110110	0111001	0000101	1100011	1011111
Row 11	0110000	0001100	1101010	1010110	1011001	1100101	0000011	0111111
Row 12	1001000	1110100	0010010	0101110	0100001	0011101	1111011	1000111
Row 13	**0101000**	0010100	1110010	1001110	1000001	1111101	**0011011**	0100111
Row 14	0011000	0100100	1000010	1111110	1110001	1001101	0101011	0010111
Row 15	1000100	1111000	0011110	0100010	0101101	0010001	1110111	1001011
Row 16	1110000	1001100	0101010	0010110	0011001	0100101	1000011	1111111

Question

Given the standard array of C, can we decode errors e with Hamming weight beyond one?

The Main Problem in Coding Theory

A good $[n, k, d]_q$ linear code should have

- large code rate k/n, and
- large relative distance d/n

Main Problem

- to optimize one of n, k, d for given values of the other two
- to design efficient decoding algorithms

How to construct good codes?

- a nontrivial research topic
- **primary/direct constructions:** from special objects in algebra, combinatorics, geometry, etc.
- **secondary constructions:** manipulate good linear codes, e.g.
  - extending: adding a parity symbol to each codeword
  - truncating: removing symbols in fixed positions of all codewords
  - concatenating

Concatenated Codes

The concatenated code $C = C_1 * C_2$ is a q-ary code given by

$$C = \{(c_{\alpha_1}, \ldots, c_{\alpha_{n_2}}) \,|\, c_{\alpha_i} \in C_1, (\alpha_1, \ldots, \alpha_{n_2}) \in C_2\}$$

where

- C_1 is an (n_1, M_1, d_1) q-ary code (inner code)
- C_2 is an (n_2, M_2, d_2) M_1-ary code (outer code)
- there exists a 1-to-1 correspondence between the alphabet of size M_1 used in C_2 and codewords in C_1 (e.g., C_1 is a $[8, 4]_2$ code and C_2 is a code over $\mathbb{F}_{2^8}$)

The code C has parameters $(n_1 n_2, M_2, \geq d_1 d_2)$.

Cyclic and Quasi-Cyclic Codes

Brief Introduction

- Cyclic codes are in the center of interest of coding theory
- Cyclic codes of relatively small length have good parameters
- In the list cyclic codes of length 63 there are 51 codes that have the largest known minimum distance for a given dimension
- Binary cyclic codes are better than the GV bound for lengths up to 1023
- Rich combinatorics is involved in the determination of the parameters of cyclic codes

Cyclic Shift

The **cyclic shift** of a word $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^n$ is defined by

$$\sigma(c) = (c_{n-1}, c_0, \cdots, c_{n-2}).$$

The cyclic shift defines a linear map $\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The i -fold composition $\sigma^i = \sigma \circ \cdots \circ \sigma$ is the i-fold forward shift

Cyclic Codes

An $\mathbb{F}_q$-linear code C of length n is called **cyclic** if

$$\sigma(c) \in C \text{ for any } c \in C.$$

In other words, cyclic codes are invariant under σ^i for all $i \geq 0$

Example - 1

Consider the binary $[7, 4, 3]$ Hamming code C with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The codewords are

$$0000000, 1000110, 0100101, 1100011,$$
$$0010011, 1010101, 0110110, 1110000,$$
$$0001111, 1001001, 0101010, 1101100,$$
$$0011100, 1011010, 0111001, 1111111$$

The 3rd row's shift 0100110 is not in C. Hence the Hamming code is not cyclic.

Example - 1 (cont)

After a permutation of the columns (1265734) and a row operation of G we get the generator matrix G' of the code C':

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

In this case, every row of G' is a circular shift of the first row.

Note: C is not cyclic, but its equivalence C' is a cyclic code

Dual code

The dual of a cyclic code is again cyclic

Proof. Let C be a cyclic code. Then $\sigma(c) \in C$ for all $c \in C$. So

$$\sigma^{n-1}(c) = (c_1, \cdots, c_{n-1}, c_0) \in C.$$

Let $x \in C^{\perp}$. Then the inner product of x and any codeword in C is zero. Thus,

$$\begin{aligned} \langle \sigma(x), c \rangle &= x_{n-1}c_0 + x_0c_1 + \cdots + x_{n-2}c_{n-1} \\ &= x_0c_1 + \cdots + x_{n-2}c_{n-1} + x_{n-1}c_0 \\ &= \langle x, \sigma^{n-1}(c) \rangle = 0. \end{aligned}$$

That is, the inner product of $\sigma(x)$ and any $c \in C$ is zero. Thus, $\sigma(x) \in C^{\perp}$.

Dual code

The dual of a cyclic code is again cyclic

Proof. Let C be a cyclic code. Then $\sigma(c) \in C$ for all $c \in C$. So

$$\sigma^{n-1}(c) = (c_1, \cdots, c_{n-1}, c_0) \in C.$$

Let $x \in C^{\perp}$. Then the inner product of x and any codeword in C is zero. Thus,

$$\begin{aligned} \langle \sigma(x), c \rangle &= x_{n-1}c_0 + x_0c_1 + \cdots + x_{n-2}c_{n-1} \\ &= x_0c_1 + \cdots + x_{n-2}c_{n-1} + x_{n-1}c_0 \\ &= \langle x, \sigma^{n-1}(c) \rangle = 0. \end{aligned}$$

That is, the inner product of $\sigma(x)$ and any $c \in C$ is zero. Thus, $\sigma(x) \in C^{\perp}$.

Polynomial Ring $\mathbb{R}_{q^n}$

Take $u(x) = x^n - 1$ and define the quotient ring

$$\mathbb{R}_{q^n} = \mathbb{F}_q[x]/(u(x)) = \left\{ \sum_{i=0}^{n-1} a_i \mathbf{x}^i \mid a_i \in \mathbb{F}_q \right\}$$

where $\mathbf{x}^n = 1$.

From $\mathbf{x}^n = 1$, we see that

$$\mathbf{x}(a_0 + a_1\mathbf{x} + \cdots + a_{n-1}\mathbf{x}^{n-1}) = a_{n-1} + a_0\mathbf{x} + \cdots + a_{n-2}\mathbf{x}^{n-2}$$

Correspondence between $\mathbb{F}_q^n$ and $\mathbb{R}_{q^n}$

Consider the map $\phi : \mathbb{F}_q^n \to \mathbb{R}_{q^n}$ defined by

$$\phi(a) = \phi(c_0, c_1, \cdots, c_{n-1}) = c_0\mathbf{1} + c_1\mathbf{x} + \cdots + c_{n-1}\mathbf{x}^{n-1} = c(\mathbf{x}).$$

Then ϕ is an 1-to-1 one mapping that satisfies

$$\phi(\alpha c_1 + \beta c_2) = \alpha\phi(c_1) + \beta\phi(c_2)$$

Cyclic $[7, 4, 3]$ Hamming code - 1

Consider the $[7, 4, 3]$ linear code C' with the generator polynomial

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

The row corresponds to

$$\begin{aligned} g'_1(x) &= 1 + \mathbf{x}^4 + \mathbf{x}^5 \\ g'_2(x) &= \mathbf{x} + \mathbf{x}^5 + \mathbf{x}^6 \\ g'_3(x) &= \mathbf{x}^2 + \mathbf{x}^4 + \mathbf{x}^5 + \mathbf{x}^6 \\ g'_4(x) &= \mathbf{x}^3 + \mathbf{x}^4 + \mathbf{x}^6 \end{aligned}$$

Examples of Rings

- the integer ring $\mathbb{Z}$;
- the polynomial ring $\mathbb{Z}[x] = \{\sum_i a_i x^i \mid a_i \in \mathbb{Z}\}$

Examples of Ideals

- the set $n\mathbb{Z} = \{yn \mid y \in \mathbb{Z}\}$;
- the set

$$\langle g(x) \rangle = \{a(x)g(x) \mid a(x) \in \mathbb{Z}[x]\}$$

Proposition

Cyclic codes in $\mathbb{F}_q^n$ correspond 1-to-1 to **ideals** in $\mathbb{R}_{q^n}$ by

$$(c_0, c_1, \cdots, c_{n-1}) \leftrightarrow c_0\mathbf{1} + c_1\mathbf{x} + \cdots + c_{n-1}\mathbf{x}^{n-1}$$

Ideals in $\mathbb{R}_{q^n}$

For the quotient ring

$$\mathbb{R}_{q^n} = \mathbb{F}_q[x]/(u(x)) = \left\{ \sum_{i=0}^{n-1} a_i \mathbf{x}^i \mid a_i \in \mathbb{F}_q \right\}$$

its ideal can be given by certain polynomial $p(\mathbf{x}) \in \mathbb{R}_{q^n}$ as

$$\langle p(\mathbf{x}) \rangle = \{ p(\mathbf{x}) a(\mathbf{x}) \, : \, a(\mathbf{x}) \in \mathbb{R}_{q^n} \}$$

indicating that for any $c(\mathbf{x}) \in \langle p(\mathbf{x}) \rangle$, one has

$$c(x) = a(x)p(x) + b(x)(x^n - 1).$$

Assume $g(x) = \gcd(p(x), x^n - 1) \in \mathbb{R}_{q^n}$. It is clear that

- for any $c(x) \in \langle p(x) \rangle$, $g(x) | c(x)$
- $g(x)$ is the polynomial in $\langle p(x) \rangle$ that has the minimal degree

Generator Polynomial - Property

Proposition

Let C be a linear cyclic code of length n over $\mathbb{F}_q$ and $g(x)$ be the generator polynomial of C, namely, $C = \langle g(x) \rangle$. Then

- $g(x)$ is monic and $g(x) | x^n - 1$;
- a polynomial $c(x)$ belongs to C if and only if $g(x) | c(x)$

Generator matrix of cyclic codes

Given a cyclic code C of length n with generator polynomial

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k-1} x^{n-k-1} + x^{n-k},$$

its generator matrix is given by

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 1 & & & & \\ & g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 1 & & & \\ & & g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 1 & & \\ & & & \ddots & \ddots & & \ddots & & \ddots & \\ & & & & g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 1 \end{pmatrix}_{k \times n}$$

Parity-check Polynomial

Given a cyclic code C of length n with generator polynomial

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k-1} x^{n-k-1} + x^{n-k},$$

its parity-check polynomial is defined as

$$h(x) = (x^n - 1)/g(x).$$

- A codeword $c(x)$ in C if and only if

$$c(x)h(x) \equiv 0 \mod (x^n - 1).$$

Relating $h(x)$ and $C^{\perp}$

Let $h(x) = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + h_k x^k$ (with $h_k = 1$) be a parity-check polynomial for a code C. Then a parity-check matrix of C is

$$H = \begin{pmatrix} 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & & & \\ & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & & \\ & & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & \\ & & & & \ddots & \ddots & & \ddots & \ddots & \\ & & & & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 \end{pmatrix}$$

Ex. 5

Verify that the matrix H defined above indeed satisfies $GH^{\mathsf{T}} = \mathbf{0}$ for the generator matrix G derived from the generator polynomial $g(x)$ of a cyclic code C.

Quasi-Cyclic Codes

One direction of generalizing cyclic codes:

Definition

A linear block code C of length $n = m\ell$ over a finite field $\mathbb{F}_q$ is called a quasi-cyclic code of index l if

$$c = (c_0, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow c' = (c_{n-\ell}, \ldots, c_0, \ldots, c_{n-\ell-1}) \in \mathcal{C}$$

When $\ell = 1$ a quasi-cyclic code reduces to a cyclic code

Example: The binary $[6, 3]$ code with generator matrix

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

is a quasi-cyclic code with $\ell = 2$.

To ease the visualization we can write the shifts as blocks,

$$G = \begin{bmatrix} 11 & 01 & 00 \\ 00 & 11 & 01 \\ 01 & 00 & 11 \end{bmatrix}$$

For the previous code, if we group columns $1, 3, 5$ and $2, 4, 6$, we get a matrix of the form

$$\begin{bmatrix} 100 & 110 \\ 010 & 011 \\ 001 & 101 \end{bmatrix}$$

We see that this matrix consists of two submatrices, and both are a 3×3 circulant matrix.

In general, one can permutate the generator matrix of a quasi-cyclic code to get a generator matrix consisting of ℓ circulant submatrices: $G = [G_0, G_1, \ldots, G_{\ell-1}]$ where each G_i is given by

$$G_i = rot(g_0, g_1, \ldots, g_{m-1}) = \begin{bmatrix} g_0 & g_1 & \cdots & g_{m-1} \\ g_{m-1} & g_0 & \cdots & g_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_0 \end{bmatrix}$$

Equivalent Definition

A linear block code with a generator matrix G of the above form is a quasi-cyclic code.

Likewise, a quasi-cyclic code has a parity-check matrix of the form

$$H = [H_0, H_1, \ldots, H_{\ell-1}]$$

where H_j is a circulant matrix.

In particular, we will consider a special type of quasi-cyclic codes.

Systematic Quasi-Cyclic Codes

A systematic quasi-cyclic $[m\ell, m]$ code of index ℓ and code rate $1/\ell$ is a quasi-cyclic code with an $(\ell-1)m \times \ell m$ parity-check matrix of the form:

$$H = \begin{bmatrix} I_m & 0 & \cdots & 0 & H_0 \\ 0 & I_m & & & H_1 \\ & & \ddots & & \vdots \\ 0 & & \cdots & I_m & H_{\ell-2} \end{bmatrix}$$

where $H_0, H_1, \ldots, H_{\ell-2}$ are circulant matrices

References i

F. MacWilliams and N. Sloane.

The Theory of Error-Correcting Codes.

North-holland Publishing Company, 2nd edition, 1978.

T. K. Moon.

Error Correction Coding: Mathematical Methods and Algorithms.

John Wiley & Sons, 2nd edition, 2020.