Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 16
March 14, 2023

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_{\Sigma}$ code exist?

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_{\Sigma}$ code exist?

Field A field is given by a triple $(S, +, \cdot)$, where S is a set of elements and $+, \cdot$ are functions from $S \times S$ to S with the following properties:

1. $(S, +)$ form a commutative group with identity element denoted by $0 \in S$

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_\Sigma$ code exist?

Field A field is given by a triple $(S, +, \cdot)$, where S is a set of elements and $+, \cdot$ are functions from $S \times S$ to S with the following properties:

1. $(S, +)$ form a commutative group with identity element denoted by $0 \in S$
2. $(S \setminus \{0\}, \cdot)$ form a commutative group with identity element $1 \in S \setminus \{0\}$

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_\Sigma$ code exist?

Field A field is given by a triple $(S, +, \cdot)$, where S is a set of elements and $+, \cdot$ are functions from $S \times S$ to S with the following properties:

1. $(S, +)$ form a commutative group with identity element denoted by $0 \in S$
2. $(S \setminus \{0\}, \cdot)$ form a commutative group with identity element $1 \in S \setminus \{0\}$
3. $a \cdot (b + c) = a \cdot b + a \cdot c,\ a, b, c \in S$

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_\Sigma$ code exist?

Field A field is given by a triple $(S, +, \cdot)$, where S is a set of elements and $+, \cdot$ are functions from $S \times S$ to S with the following properties:

1. $(S, +)$ form a commutative group with identity element denoted by $0 \in S$
2. $(S \setminus \{0\}, \cdot)$ form a commutative group with identity element $1 \in S \setminus \{0\}$
3. $a \cdot (b + c) = a \cdot b + a \cdot c,\ a, b, c \in S$

Note that $\Sigma = \{0, 1\}$ is a field with modulo 2 addition and multiplication. In general, a field with finite elements is called a finite field.

Codes

Question Given $n, k, d_{\min}, \Sigma$, does an $(n, k, d_{\min})_\Sigma$ code exist?

Field A field is given by a triple $(S, +, \cdot)$, where S is a set of elements and $+, \cdot$ are functions from $S \times S$ to S with the following properties:

1. $(S, +)$ form a commutative group with identity element denoted by $0 \in S$
2. $(S \setminus \{0\}, \cdot)$ form a commutative group with identity element $1 \in S \setminus \{0\}$
3. $a \cdot (b + c) = a \cdot b + a \cdot c,\ a, b, c \in S$

Note that $\Sigma = \{0, 1\}$ is a field with modulo 2 addition and multiplication. In general, a field with finite elements is called a finite field.

Order of finite fields Every finite field has order p^s for some prime p and integer $s \geq 1$. Conversely for every prime p and integer $s \geq 1$ there exists a filed of order p^s (unique up to isomorphism)

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Sphere Given $x \in F_q^n$, we define the sphere or the ball of radius ϵ around x as

$$B_\epsilon(x) = \left\{ y \in F_q^n : d(x, y) \leq \epsilon \right\}.$$

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Sphere Given $x \in F_q^n$, we define the sphere or the ball of radius ϵ around x as

$$B_\epsilon(x) = \left\{ y \in F_q^n : d(x, y) \leq \epsilon \right\}.$$

Volume $V_q(n, \epsilon) = |B_\epsilon(x)|$ is called the volume or size of the ball

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Sphere Given $x \in F_q^n$, we define the sphere or the ball of radius ϵ around x as

$$B_\epsilon(x) = \left\{ y \in F_q^n : d(x, y) \leq \epsilon \right\}.$$

Volume $V_q(n, \epsilon) = |B_\epsilon(x)|$ is called the volume or size of the ball

Proposition $V_q(n, \epsilon) = \sum_{i=0}^{\epsilon} \binom{n}{i} (q-i)^i$

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Sphere Given $x \in F_q^n$, we define the sphere or the ball of radius ϵ around x as

$$B_\epsilon(x) = \left\{ y \in F_q^n : d(x, y) \leq \epsilon \right\}.$$

Volume $V_q(n, \epsilon) = |B_\epsilon(x)|$ is called the volume or size of the ball

Proposition $V_q(n, \epsilon) = \sum_{i=0}^{\epsilon} \binom{n}{i} (q-i)^i$

Proof: Count the number of words which are at a distance exactly i from x. There are $\binom{n}{i}$ ways to choose the i positions that will be different and for each of these positions there are $q-1$ choices for which symbol will be in that position

Code

Notation For every prime power q a field with q elements will be denoted as F_q or F_{p^s}

Sphere Given $x \in F_q^n$, we define the sphere or the ball of radius ϵ around x as

$$B_\epsilon(x) = \left\{ y \in F_q^n : d(x, y) \leq \epsilon \right\}.$$

Volume $V_q(n, \epsilon) = |B_\epsilon(x)|$ is called the volume or size of the ball

Proposition $V_q(n, \epsilon) = \sum_{i=0}^{\epsilon} \binom{n}{i} (q-i)^i$

Proof: Count the number of words which are at a distance exactly i from x. There are $\binom{n}{i}$ ways to choose the i positions that will be different and for each of these positions there are $q-1$ choices for which symbol will be in that position

Notation Let $A(n, d)$ denote the maximum number of codewords in a code of length n with minimum distance d

Code

Sphere packing bound $A(n,d) \leq \frac{q^n}{V_q\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}$

Code

Sphere packing bound $A(n,d) \leq \frac{q^n}{V_q\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}$

Proof: Let C be a code of length n and minimum distance d. By assumption we can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, so the spheres of radius $\lfloor \frac{d-1}{2} \rfloor$ around each codeword are disjoint. Then the union of the sizes of these spheres is $|C|\ V_q(n, \lfloor \frac{d-1}{2} \rfloor)$.

Code

Sphere packing bound $A(n,d) \leq \frac{q^n}{V_q\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}$

Proof: Let C be a code of length n and minimum distance d. By assumption we can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, so the spheres of radius $\lfloor \frac{d-1}{2} \rfloor$ around each codeword are disjoint. Then the union of the sizes of these spheres is $|C|\ V_q(n, \lfloor \frac{d-1}{2} \rfloor)$.
m

Gilbert bound $A(n,d) \geq \frac{q^n}{V_q(n,d-1)}$

Code

Sphere packing bound $A(n,d) \leq \frac{q^n}{V_q\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}$

Proof: Let C be a code of length n and minimum distance d. By assumption we can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, so the spheres of radius $\lfloor \frac{d-1}{2} \rfloor$ around each codeword are disjoint. Then the union of the sizes of these spheres is $|C|\ V_q(n, \lfloor \frac{d-1}{2} \rfloor)$.
m

Gilbert bound $A(n,d) \geq \frac{q^n}{V_q(n,d-1)}$

Proof: Let C be a length n minimum distance d code with M codewords, where M is the maximal among all such codes. No word in F_q^n in distance at least d from every codeword because then we could add it to C and get a length n minimum distance d code with $M+1$ words. Therefore if we put a ball of radius $d-1$ around each codeword in C, we must cover all of F_q^n

Code

Another way to define perfect code When the equality holds in the above proposition i.e. $|C| = \frac{q^n}{V_q\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}$ then C is called a perfect $\lfloor \frac{d-1}{2} \rfloor$-error correcting code

Code

Observation

$\rightarrow$ Let $i \in \{1, 2\}$, let C_i be an $[n_i, k_i, d_i]$ code. Then

$$C_1 \oplus C_2 = \{(c_1, c_2) : c_1 \in C_1, c_2 \in C_2\}$$

is an $[n_1 + n_2, k_1 + k_2, \min(d_1, d_2)]$ linear code

Code

Observation

$\rightarrow$ Let $i \in \{1, 2\}$, let C_i be an $[n_i, k_i, d_i]$ code. Then

$$C_1 \oplus C_2 = \{(c_1, c_2) : c_1 \in C_1, c_2 \in C_2\}$$

is an $[n_1 + n_2, k_1 + k_2, \min(d_1, d_2)]$ linear code

$\rightarrow$ If G_i is a generator matrix of C_i, and H_i is the corresponding parity-check matrix then $C_1 \oplus C_2$ has generator matrix and parity-check matrix as

$$\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \text{ and } \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}$$

Code

$\rightarrow$ Let C_1, C_2 be linear codes with parameters $[n, k_i, d_i]$. Then let

$$C = \{(u, u + v) : u \in C_1, v \in C_2\}$$

is a $[2n, k_1 + k_2, \min(2d_1, d_2)]$ code

Code

→ Let C_1, C_2 be linear codes with parameters $[n, k_i, d_i]$. Then let

$$C = \{(u, u + v) : u \in C_1, v \in C_2\}$$

is a $[2n, k_1 + k_2, \min(2d_1, d_2)]$ code

→ If C_i has generator matrix G_i and parity-check matrix H_i then the generator matrix and parity-check matrix of C are given by

$$\begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix} \text{ and } \begin{bmatrix} H_1 & 0 \\ -H_2 & H_2 \end{bmatrix}$$

respectively

Code

→ Let C_1, C_2 be linear codes with parameters $[n, k_i, d_i]$. Then let

$$C = \{(u, u + v) : u \in C_1, v \in C_2\}$$

is a $[2n, k_1 + k_2, \min(2d_1, d_2)]$ code

→ If C_i has generator matrix G_i and parity-check matrix H_i then the generator matrix and parity-check matrix of C are given by

$$\begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix} \text{ and } \begin{bmatrix} H_1 & 0 \\ -H_2 & H_2 \end{bmatrix}$$

respectively

→ The subset of $\{0, 1\}^n$ consisting of two words $(0, 0, \ldots, 0)$ and $(1, 1, \ldots, 1)$ is called the binary repetition code of length n

Codes

Polynomial Let F_q be a finite field with q elements. Then a function

$$F(X) = \sum_{i=0}^{d} f_i X^i$$

for some positive integer d, with coefficients $f_i \in F_q$, and $f_d \neq 0$. For example, $2X^3 + X^2 + 5X + 6$ is a polynomial over F_q.

Codes

Polynomial Let F_q be a finite field with q elements. Then a function

$$F(X) = \sum_{i=0}^{d} f_i X^i$$

for some positive integer d, with coefficients $f_i \in F_q$, and $f_d \neq 0$. For example, $2X^3 + X^2 + 5X + 6$ is a polynomial over F_q. f_d is called the degree of $F(X)$.

Codes

Polynomial Let F_q be a finite field with q elements. Then a function

$$F(X) = \sum_{i=0}^{d} f_i X^i$$

for some positive integer d, with coefficients $f_i \in F_q$, and $f_d \neq 0$. For example, $2X^3 + X^2 + 5X + 6$ is a polynomial over F_q. f_d is called the degree of $F(X)$.

Operations

Addition: $F(X) + G(X) = \sum_{i=0}^{\max(\deg(F),\deg(G))} (f_i + g_i)X^i$

Codes

Polynomial Let F_q be a finite field with q elements. Then a function

$$F(X) = \sum_{i=0}^{d} f_i X^i$$

for some positive integer d, with coefficients $f_i \in F_q$, and $f_d \neq 0$. For example, $2X^3 + X^2 + 5X + 6$ is a polynomial over F_q. f_d is called the degree of $F(X)$.

Operations

Addition: $F(X) + G(X) = \sum_{i=0}^{\max(\deg(F),\deg(G))} (f_i + g_i) X^i$

Multiplication:

$$F(X) \cdot G(X) = \sum_{i=0}^{\deg(F)+\deg(G)} \left(\sum_{j=0}^{\min(i,\deg(F))} f_j \cdot g_{i-j} \right) X^i$$

Code

root $\alpha \in F_q$ is a root of a polynomial $F(X)$, if $F(\alpha) = 0$. For example, 1 is a root of $1 + X^2$ over F_2

Code

root $\alpha \in F_q$ is a root of a polynomial $F(X)$, if $F(\alpha) = 0$. For example, 1 is a root of $1 + X^2$ over F_2

irreducible A polynomial $F(X)$ is called irreducible if for every $G_1(X), G_2(X)$ such that $F(X) = G_1(X)G_2(X)$, we have $\min(\deg(G_1), \deg(G_2)) = 0$

Code

root $\alpha \in F_q$ is a root of a polynomial $F(X)$, if $F(\alpha) = 0$. For example, 1 is a root of $1 + X^2$ over F_2

irreducible A polynomial $F(X)$ is called irreducible if for every $G_1(X), G_2(X)$ such that $F(X) = G_1(X)G_2(X)$, we have $\min(\deg(G_1), \deg(G_2)) = 0$

For example, $1 + X^2$ is not-irreducible over F_2, since $(1 + X)(1 + X) = 1 + X^2$

Code

root $\alpha \in F_q$ is a root of a polynomial $F(X)$, if $F(\alpha) = 0$. For example, 1 is a root of $1 + X^2$ over F_2

irreducible A polynomial $F(X)$ is called irreducible if for every $G_1(X), G_2(X)$ such that $F(X) = G_1(X)G_2(X)$, we have $\min(\deg(G_1), \deg(G_2)) = 0$

For example, $1 + X^2$ is not-irreducible over F_2, since $(1 + X)(1 + X) = 1 + X^2$

$1 + X + X^2$ is irreducible of degree 2 over F_2 (is it the only one!!)

Code

root $\alpha \in F_q$ is a root of a polynomial $F(X)$, if $F(\alpha) = 0$. For example, 1 is a root of $1 + X^2$ over F_2

irreducible A polynomial $F(X)$ is called irreducible if for every $G_1(X), G_2(X)$ such that $F(X) = G_1(X)G_2(X)$, we have $\min(\deg(G_1), \deg(G_2)) = 0$

For example, $1 + X^2$ is not-irreducible over F_2, since $(1 + X)(1 + X) = 1 + X^2$

$1 + X + X^2$ is irreducible of degree 2 over F_2 (is it the only one!!)

Caution: if a polynomial $E(X) \in F_q[X]$ has no root in F_q. it does not mean that $E(X)$ is irreducible. For example, $(1 + X + X^2)^2$ over F_2 does not have any root in F_2 but it is obviously is not irreducible

Code

Theorem Let $E(X)$ be an irreducible polynomial with degree at least 2 over F_p, p is prime. Then the set of polynomials in $F_p[X]$ modulo $E(X)$, denoted by $F_p[X]/E(X)$, is a field (Question What should be the order of this field?)

Code

Theorem Let $E(X)$ be an irreducible polynomial with degree at least 2 over F_p, p is prime. Then the set of polynomials in $F_p[X]$ modulo $E(X)$, denoted by $F_p[X]/E(X)$, is a field (Question What should be the order of this field?)

Observation

$\rightarrow$ Polynomials in $F_p[X]$ are of degree at most $s-1$. There are p^s such polynomials

Code

Theorem Let $E(X)$ be an irreducible polynomial with degree at least 2 over F_p, p is prime. Then the set of polynomials in $F_p[X]$ modulo $E(X)$, denoted by $F_p[X]/E(X)$, is a field (Question What should be the order of this field?)

Observation

- $\rightarrow$ Polynomials in $F_p[X]$ are of degree at most $s-1$. There are p^s such polynomials
- $\rightarrow$ Addition: $(F(X)+G(X))\text{mod}E(X) = F(X)\text{mod}E(X)+G(X)\text{mod}E(X) = F(X)+G(X)$

Code

Theorem Let $E(X)$ be an irreducible polynomial with degree at least 2 over F_p, p is prime. Then the set of polynomials in $F_p[X]$ modulo $E(X)$, denoted by $F_p[X]/E(X)$, is a field (Question What should be the order of this field?)

Observation

- $\rightarrow$ Polynomials in $F_p[X]$ are of degree at most $s-1$. There are p^s such polynomials
- $\rightarrow$ Addition: $(F(X)+G(X))\text{mod}E(X) = F(X)\text{mod}E(X)+G(X)\text{mod}E(X) = F(X)+G(X)$
- $\rightarrow$ Multiplication: $(F(X)\cdot G(X))\text{mod}E(X)$ is the unique polynomial $R(X)$ with degree at most $s-1$ such that for some $A(X)$, $R(X)+A(X)E(X) = F(X)\cdot G(X)$

Code

Theorem Let $E(X)$ be an irreducible polynomial with degree at least 2 over F_p, p is prime. Then the set of polynomials in $F_p[X]$ modulo $E(X)$, denoted by $F_p[X]/E(X)$, is a field (Question What should be the order of this field?)

Observation

- $\rightarrow$ Polynomials in $F_p[X]$ are of degree at most $s-1$. There are p^s such polynomials
- $\rightarrow$ Addition: $(F(X)+G(X))\text{mod}E(X) = F(X)\text{mod}E(X) + G(X)\text{mod}E(X) = F(X)+G(X)$
- $\rightarrow$ Multiplication: $(F(X)\cdot G(X))\text{mod}E(X)$ is the unique polynomial $R(X)$ with degree at most $s-1$ such that for some $A(X)$, $R(X)+A(X)E(X) = F(X)\cdot G(X)$

For example, for $p=2$ and $E(X) = 1+X+X^2$, $F_2[X]/(1+X+X^2)$ has its elements $0, 1, X, 1+X$.

Code

Question Does there exist irreducible polynomials of every degree?

Code

Question Does there exist irreducible polynomials of every degree?

(Binary) Cyclic codes

Code

Question Does there exist irreducible polynomials of every degree?

(Binary) Cyclic codes

Cyclic shift Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$. Define

$$\mathbf{v}^{(1)} = (v_{n-1}, v_0, \ldots, v_{n-2})$$

is called a cyclic shift of $\mathbf{v}$.

Code

Question Does there exist irreducible polynomials of every degree?

(Binary) Cyclic codes

Cyclic shift Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$. Define

$$\mathbf{v}^{(1)} = (v_{n-1}, v_0, \ldots, v_{n-2})$$

is called a cyclic shift of $\mathbf{v}$.If the entries of $\mathbf{v}$ are cyclically shifted i places to the right, the resulting n-tuple is

$$\mathbf{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1})$$

Code

Question Does there exist irreducible polynomials of every degree?

(Binary) Cyclic codes

Cyclic shift Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$. Define

$$\mathbf{v}^{(1)} = (v_{n-1}, v_0, \ldots, v_{n-2})$$

is called a cyclic shift of $\mathbf{v}$.If the entries of $\mathbf{v}$ are cyclically shifted i places to the right, the resulting n-tuple is

$$\mathbf{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1})$$

An (n, k) linear code C is called a cyclic code if every cyclic shift of a codeword in C is also a codeword in C

Code

Algebraic properties of cyclic codes Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be a codeword. Then define

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \ldots + v_{n-1} X^{n-1}$$

$\rightarrow$ Each codeword corresponds to a polynomial of degree $n-1$ or less

Code

Algebraic properties of cyclic codes Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be a codeword. Then define

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \ldots + v_{n-1} X^{n-1}$$

$\rightarrow$ Each codeword corresponds to a polynomial of degree $n-1$ or less

$\rightarrow$ The correspondence $\mathbf{v} \leftrightarrow \mathbf{v}(X)$ is one-to-one

Code

Algebraic properties of cyclic codes Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be a codeword. Then define

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \ldots + v_{n-1} X^{n-1}$$

$\rightarrow$ Each codeword corresponds to a polynomial of degree $n-1$ or less

$\rightarrow$ The correspondence $\mathbf{v} \leftrightarrow \mathbf{v}(X)$ is one-to-one

$\rightarrow$ $\mathbf{v}(X)$ is called the code polynomial of $\mathbf{v}$

Code

$\rightarrow$ Then

$$\mathbf{v}^{(i)} = v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_0 X^i + v_1 X^{i+1} + \ldots + v_{n-i-1}X^{n-1}$$

Code

→ Then

$$\mathbf{v}^{(i)} = v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_0 X^i + v_1 X^{i+1} + \ldots + v_{n-i-1}X^{n-1}$$

→ Further

$$\begin{aligned} X^i \mathbf{v}(X) &= v_o X^i + v_1 X^{i+1} + \ldots + v_{n-i-1}X^{n-1} + \ldots \\ &\quad + v_{n-1}X^{n+i-1} \\ &= v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_0 X^i + \ldots \\ &\quad + v_{n-i-1}X^{n-1} + v_{n-i}(X^n + 1) + v_{n-i+1}X(X^n + 1) + \ldots \\ &\quad + v_{n-1}X^{i-1}(X^n + 1) \\ &= q(X)(X^n + 1) + \mathbf{v}^{(i)}(X) \end{aligned}$$

Code

→ Then

$$\mathbf{v}^{(i)} = v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_0 X^i + v_1 X^{i+1} + \ldots + v_{n-i-1}X^{n-1}$$

→ Further

$$\begin{aligned} X^i \mathbf{v}(X) &= v_o X^i + v_1 X^{i+1} + \ldots + v_{n-i-1}X^{n-1} + \ldots \\ &\quad + v_{n-1}X^{n+i-1} \\ &= v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_0 X^i + \ldots \\ &\quad + v_{n-i-1}X^{n-1} + v_{n-i}(X^n + 1) + v_{n-i+1}X(X^n + 1) + \ldots \\ &\quad + v_{n-1}X^{i-1}(X^n + 1) \\ &= q(X)(X^n + 1) + \mathbf{v}^{(i)}(X) \end{aligned}$$

→ Thus $\mathbf{v}^{(i)}(X)$ is the remainder resulting from dividing the polynomial $X^i \mathbf{v}(X)$ by $X^n + 1$

Code

In general, for finite fields of order q,

$\rightarrow$ $F_q[X] = \{a_0 + a_1X + \ldots + a_nX^n : n \in \mathbb{N}, a_i \in F_q\}$ is called the polynomial ring

Code

In general, for finite fields of order q,

$\rightarrow$ $F_q[X] = \{a_0 + a_1X + \ldots + a_nX^n : n \in \mathbb{N}, a_i \in F_q\}$ is called the polynomial ring

$\rightarrow$ The multiples of $X^n - 1$ form a principal ideal in $F_q[X]$

Code

In general, for finite fields of order q,

$\rightarrow$ $F_q[X] = \{a_0 + a_1X + \ldots + a_nX^n : n \in \mathbb{N}, a_i \in F_q\}$ is called the polynomial ring

$\rightarrow$ The multiples of $X^n - 1$ form a principal ideal in $F_q[X]$

$\rightarrow$ The residue class ring $F_q[x]/(X^n - 1)$ has the set of polynomials

$$\{a_0 + a_1X + \ldots + a_{n-1}X^{n-1} : a_i \in F_q, 0 \leq i < n\}$$

Code

In general, for finite fields of order q,

$\rightarrow$ $F_q[X] = \{a_0 + a_1X + \ldots + a_nX^n : n \in \mathbb{N}, a_i \in F_q\}$ is called the polynomial ring

$\rightarrow$ The multiples of $X^n - 1$ form a principal ideal in $F_q[X]$

$\rightarrow$ The residue class ring $F_q[x]/(X^n - 1)$ has the set of polynomials

$$\{a_0 + a_1X + \ldots + a_{n-1}X^{n-1} : a_i \in F_q, 0 \leq i < n\}$$

$\rightarrow$ Clearly F_q^n is isomorphic to this ring

$$(a_0, a_1, \ldots, a_{n-1}) \in F_q^n \leftrightarrow a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in F_q[X]/(X^n - 1),$$

note that the multiplicative structure is defined by multiplications $\mathrm{mod}(x^n - 1)$

Code

In general, for finite fields of order q,

$\rightarrow$ $F_q[X] = \{a_0 + a_1X + \ldots + a_nX^n : n \in \mathbb{N}, a_i \in F_q\}$ is called the polynomial ring

$\rightarrow$ The multiples of $X^n - 1$ form a principal ideal in $F_q[X]$

$\rightarrow$ The residue class ring $F_q[x]/(X^n - 1)$ has the set of polynomials

$$\{a_0 + a_1X + \ldots + a_{n-1}X^{n-1} : a_i \in F_q, 0 \leq i < n\}$$

$\rightarrow$ Clearly F_q^n is isomorphic to this ring

$$(a_0, a_1, \ldots, a_{n-1}) \in F_q^n \leftrightarrow a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in F_q[X]/(X^n - 1),$$

note that the multiplicative structure is defined by multiplications $\mod(x^n - 1)$

Conclusion Interpret a linear code as a subset of $F_q[X]/(X^n - 1)$

Code

Theorem A linear code C in F_q^n is cyclic if and only if C is an ideal in $F_q/(X^n - 1)$

Code

Theorem A linear code C in F_q^n is cyclic if and only if C is an ideal in $F_q/(X^n - 1)$

Proof If C is an ideal in $F_q[X]/(X^n - 1)$ and $\mathbf{v}(X) = v_0 + v_1X + \ldots + v_{n-1}X^{n-1}$ is any codeword, then $X\mathbf{v}(X)$ is also a codeword i.e.

$$(v_{n-1}, v_0, v_1, \ldots, v_{n-2}) \in C$$

Code

Theorem A linear code C in F_q^n is cyclic if and only if C is an ideal in $F_q/(X^n-1)$

Proof If C is an ideal in $F_q[X]/(X^n-1)$ and $\mathbf{v}(X) = v_0 + v_1X + \ldots + v_{n-1}X^{n-1}$ is any codeword, then $X\mathbf{v}(X)$ is also a codeword i.e.

$$(v_{n-1}, v_0, v_1, \ldots, v_{n-2}) \in C$$

Conversely, if C is cyclic, then for every codeword $\mathbf{v}(X)$ the word $X\mathbf{v}(X)$ is also in C. Therefore $X^i\mathbf{v}(X)$ is in C for every i, and since C is linear $\mathbf{u}(X)\mathbf{v}(X)$ is in C for every polynomial $\mathbf{u}(X)$. Hence C is an ideal.

Code

Theorem A linear code C in F_q^n is cyclic if and only if C is an ideal in $F_q/(X^n-1)$

Proof If C is an ideal in $F_q[X]/(X^n-1)$ and $\mathbf{v}(X) = v_0 + v_1X + \ldots + v_{n-1}X^{n-1}$ is any codeword, then $X\mathbf{v}(X)$ is also a codeword i.e.

$$(v_{n-1}, v_0, v_1, \ldots, v_{n-2}) \in C$$

Conversely, if C is cyclic, then for every codeword $\mathbf{v}(X)$ the word $X\mathbf{v}(X)$ is also in C. Therefore $X^i\mathbf{v}(X)$ is in C for every i, and since C is linear $\mathbf{u}(X)\mathbf{v}(X)$ is in C for every polynomial $\mathbf{u}(X)$. Hence C is an ideal.

Convention As mentioned above we consider cyclic codes of length n over F_q with $\gcd(n, q) = 1$.

Code

$\rightarrow$ Since $F_q/(X^n - 1)$ is a principal ideal ring, every cyclic code C consists of the multiples of a polynomial $g(X)$ which is the monic polynomial of lowest degree in the ideal

Code

$\rightarrow$ Since $F_q/(X^n - 1)$ is a principal ideal ring, every cyclic code C consists of the multiples of a polynomial $g(X)$ which is the monic polynomial of lowest degree in the ideal

$\rightarrow$ The polynomial $g(X)$ is called the generator polynomial of the cyclic code

Code

- $\rightarrow$ Since $F_q/(X^n - 1)$ is a principal ideal ring, every cyclic code C consists of the multiples of a polynomial $g(X)$ which is the monic polynomial of lowest degree in the ideal
- $\rightarrow$ The polynomial $g(X)$ is called the generator polynomial of the cyclic code
- $\rightarrow$ The generator polynomial is a divisor of $X^n - 1$

Code

- $\rightarrow$ Since $F_q/(X^n - 1)$ is a principal ideal ring, every cyclic code C consists of the multiples of a polynomial $g(X)$ which is the monic polynomial of lowest degree in the ideal
- $\rightarrow$ The polynomial $g(X)$ is called the generator polynomial of the cyclic code
- $\rightarrow$ The generator polynomial is a divisor of $X^n - 1$
- $\rightarrow$ Let $X^n - 1 = f_1(X)f_2(X)\dots f_t(X)$ be the decomposition of $X^n - 1$ into irreducible factors (each of which are different!! why?)

Code

- $\rightarrow$ Since $F_q/(X^n - 1)$ is a principal ideal ring, every cyclic code C consists of the multiples of a polynomial $g(X)$ which is the monic polynomial of lowest degree in the ideal
- $\rightarrow$ The polynomial $g(X)$ is called the generator polynomial of the cyclic code
- $\rightarrow$ The generator polynomial is a divisor of $X^n - 1$
- $\rightarrow$ Let $X^n - 1 = f_1(X)f_2(X)\dots f_t(X)$ be the decomposition of $X^n - 1$ into irreducible factors (each of which are different!! why?)
- $\rightarrow$ Cyclic codes of length n is formed by picking one of the 2^t factors of $X^n - 1$ as a generator polynomial $g(X)$ and defining the corresponding code to be the set of multiples of $g(X)$ mod$(X^n - 1)$

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$\rightarrow$ There are 8 cyclic codes of length 7

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$\rightarrow$ There are 8 cyclic codes of length 7

$\rightarrow$ One has $\mathbf{0}$ as the only codeword and one contains all possible

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$\rightarrow$ There are 8 cyclic codes of length 7

$\rightarrow$ One has $\mathbf{0}$ as the only codeword and one contains all possible

$\rightarrow$ The code with generator $X - 1$ contains all words of even weight

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$\rightarrow$ There are 8 cyclic codes of length 7

$\rightarrow$ One has $\mathbf{0}$ as the only codeword and one contains all possible

$\rightarrow$ The code with generator $X - 1$ contains all words of even weight

$\rightarrow$ Then $[7, 1]$ cyclic code has $\mathbf{0}$ and $\mathbf{1}$ as codewords

Code

Example Over F_2 :

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$\rightarrow$ There are 8 cyclic codes of length 7

$\rightarrow$ One has $\mathbf{0}$ as the only codeword and one contains all possible

$\rightarrow$ The code with generator $X - 1$ contains all words of even weight

$\rightarrow$ Then $[7, 1]$ cyclic code has $\mathbf{0}$ and $\mathbf{1}$ as codewords

$\rightarrow$ The remaining four codes have dimension $3, 3, 4, 4$ respectively. For example, $g(X) = (X - 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$ generates a $[7, 3]$ cyclic code