

CYCLIC CODES

→ definition

→ polynomials over finite fields

→ cyclic code characterization

Cyclic codes definition

$C \subseteq \{0, \dots, q-1\}^n$ is cyclic if

1.) $\forall x, y \in C \quad x + y \in C$

2.) $\forall x \in C \quad a \cdot x \in C$



3.) $\forall x \in (x_0, \dots, x_{n-1}) \in C$

$\Downarrow \Uparrow$
 $(x_{n-1}, x_0, x_1, \dots, x_{n-2})$

EX.3.1 Are the following codes cyclic?

a.) $\{0000, 1212, 2121\} \subseteq (\mathbb{F}_3)^4 \quad (\{0, 1, 2\}, (x, \cdot) \pmod 3)$

LINEARITY ✓

$(1212) + (2121) = (3333) = (0000)$

$2 \cdot (1212) = (2424) = (2121) \quad \checkmark$

$\curvearrowright 2121 \approx 1212 \quad \checkmark$

b.) $C_3 = \{x_0 x_1 x_2 x_3 x_4 \in \{0, 1, 2\}^5 \mid x_0 + x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 3\}$

↑ ↑ ↑ ↑ ↑

$$b) C_3 = \{x_0 x_1 x_2 x_3 x_4 \in \{0,1,2\} \mid x_0 + x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod{3}\}$$

$$\begin{array}{cccccc} \uparrow & \uparrow & \uparrow & \uparrow & \downarrow & \\ 3 & 3 & 3 & 3 & \approx 3 & \text{codewords} \end{array}$$

$$x = (x_0 \dots x_4) \in C$$

$$y = (y_0 \dots y_4)$$

$$\sum_{i=0}^4 x_i \equiv 0 \pmod{3} \quad \sum_{i=0}^4 y_i \equiv 0 \pmod{3}$$

$$I. x + y \in C$$

$$x + y = (x_0 + y_0, x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)$$

$$\sum_{i=0}^4 x_i + y_i \equiv \sum_{i=0}^4 x_i + \sum_{i=0}^4 y_i = 0 + 0 = 0 \pmod{3}$$

$$II. \text{ for each } c \in \mathbb{F}_3 \quad \forall x \in C$$

$$c \cdot x \in C$$

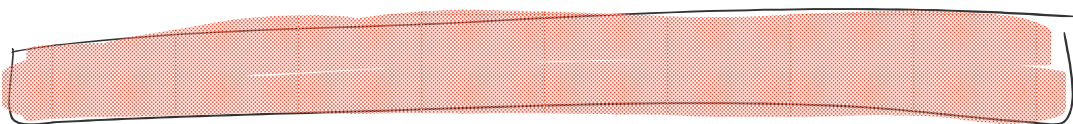
$$c \cdot x = (c \cdot x_0, c \cdot x_1, c \cdot x_2, c \cdot x_3, c \cdot x_4)$$

$$\sum_{i=0}^4 c \cdot x_i \equiv c \cdot \sum_{i=0}^4 x_i = c \cdot 0 = 0 \pmod{3}$$

$$III. \text{ if } (x_0, \dots, x_4) \in C \text{ is also } (x_4, x_0, \dots, x_3) \in C$$

$$(x_0 + x_1 + x_2 + x_3 + x_4) = 0 \Rightarrow (x_4 + x_0 + x_1 + x_2 + x_3) = 0$$

✓



$$C \in \mathbb{F}_q^n$$

$$(c_0, c_1, \dots, c_{n-1}) \in \{0, \dots, q-1\}^n \text{ set of all polynomials over } \mathbb{F}_q$$

$$\Downarrow$$

$$(c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}) \in \mathbb{F}_q[x]$$

Rings $(S = \{0, \dots, n-1\}, +, \cdot)$ n -prime
 $+, \cdot \pmod n$

1.) $(S, +)$ is a commutative group

- > addition is associative $(a+b)+c = a+(b+c)$
- > $a+b = b+a$ (addition is commutative)
- > there is a neutral element '0' s.t. $a+0 = a$
- > for each a , there is an additive inverse $1-a$ s.t. $a+(-a) = 0$

2.) -> multiplication is associative $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

-> there is a neutral element '1' s.t. $a \cdot 1 = a$

-> ' \cdot ' is distributive toward ' $+$ ' (left distributive)

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

RING \nrightarrow

+ FIELD AXIOM

-> for each $a \neq 0$ there is an inverse a^{-1}

$$\text{s.t. } a \cdot a^{-1} = 1.$$

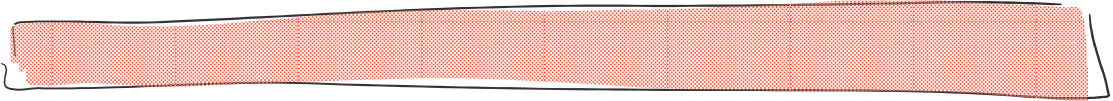
-> $\{0, 1, 2, 3\} \pmod 4$

2^{-1} does not exist

$\{0, 2, 0, 2\}$

$(\{0, \dots, n-1\}, +, \cdot \pmod n) \rightsquigarrow$ is generally a ring not a field.

if n is a prime \uparrow is a field



Finite fields exist for any number of elements p^k , where p is a prime.

$\mathbb{F}[x]$ - set of all polynomials defined over a finite field \mathbb{F} .

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \quad a_i \in \mathbb{F} \quad f(x) \approx (a_0, a_1, \dots)$$

$\mathbb{F}_2[x]$ examples

$$1+x \quad \deg(x+1) = 1$$

$$1+x+x^3+x^7 \quad \deg(1+x+x^3+x^7) = 7$$

$$1+x+x^2+\frac{1}{2}x^3 = 1+x+x^2 \quad \deg(1+x+x^2) = 2$$

$\deg(f(x))$ is it's highest exponent



Division of polynomials

Example:

$$x^7 - 1 : x^3 + x^2 + 1$$

a_0 in \mathbb{F}_2

$$\begin{array}{r} x^7 + 1 \\ \underline{-(x^3 + x^2 + 1)} \\ x^4 + x^2 + x \\ \underline{-(x^4 + x^3 + x^2 + 1)} \\ -x^3 + x^2 + x \\ \underline{-(x^3 + x^2 + 1)} \\ x \end{array}$$

$$\begin{array}{l} b_1 \text{ in } \mathbb{F}_3 \approx (0, 1, 2) \approx (0, 1, -1) \\ x^7 - 1 : x^3 + x^2 + 1 = x^4 - x^3 + x^2 + x \\ \underline{-(x^3 + x^2 + 1)} \\ -x^4 + x^3 + x^2 + x - 1 \\ \underline{-(x^4 + x^3 + x^2 + 1)} \\ -2x^3 + x^2 + x - 2 \end{array}$$

$$\begin{array}{r} \overline{7 \quad -6 \quad -4} \\ \overline{X^7 + X^6 + X^4} \\ \underline{X^7 - X^6 - X^4 + 1} \\ X^6 + X^4 + 1 \\ \underline{-(X^6 + X^5 + X^3)} \\ X^5 + X^4 + X^3 + 1 \\ \underline{-(X^5 + X^4 + X^2)} \\ X^3 + X^2 + 1 \end{array}$$

$$\begin{array}{r} \overline{X^7 + X^6 + X^4} \\ \underline{-X^6 - X^5 - 1} \\ \hline \overline{-(X^6 - X^5 - X^3)} \\ \underline{X^5 - X^4 + X^3 - 1} \\ \hline \overline{-(X^5 + X^4 + X^2)} \\ \underline{X^4 + X^3 - X^2 - 1} \\ \hline \overline{-(X^4 + X^3 + X)} \\ \underline{-X^3 - X - 1} \end{array}$$

$$X^7 - 1 = (X^3 + X^2 + 1)(X^4 - X^3 + X - 1)$$

$f(x) = q(x) \cdot h(x) + r(x)$
 $\deg(r(x)) < \deg(h(x))$

$\left. \begin{array}{l} \text{polynomials can be divided} \\ \text{with a remainder} \end{array} \right\}$

$\mathbb{F}[x]/f(x) \rightsquigarrow$ all remainders after division by $f(x)$

Example

$\mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\}$

$(\text{mod } x^2+x+1) \quad x^2+x+1 = 1$
 $x^2+x+1 - (x^2+x+1) = 0$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

+	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

φ
Commutative group

$$x(x+1) = x^2+x : x^2+x+1 = 1$$

\mathbb{F} all ring axioms and a field axiom

If all ring axioms
and a field axiom
hold.

$\left(\{0, 1, x, x+1\}, \cdot, + \text{ mod } x^2+x+1 \right)$ is a Field!

Primitive polynomials

A primitive polynomial over \mathbb{F}_q cannot be written as a product of two other polynomials.

$\mathbb{F}_q[x]/f(x)$ is a field iff $f(x)$ is primitive

(x^2+x+1) is primitive over \mathbb{F}_2

$x \cdot x = x^2 \neq x^2+x+1$
 $x(x+1) = x^2+x \neq x^2+x+1$
 $(x+1)(x+1) = x^2+1 \neq x^2+x+1$ \rightarrow Q.E.D
 x^2+x+1 is primitive

$R_n = \mathbb{F}_2[x]/x^n-1$ = all polynomials with $\text{deg} < n$
together with multiplication
and addition "mod x^n-1 "

\approx All strings of length n

MULTIPLICATION BY x

$$f(x) \in R_n = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \approx (a_0 \dots a_{n-1})$$

$$x \circ f(x) = a_0x + a_1x^2 + \dots + a_{n-1}x^n = (a_{n-1}) + a_0x + \dots + a_{n-2}x^{n-1}$$

$$\approx (a_{n-1} a_0 \dots a_{n-1})$$

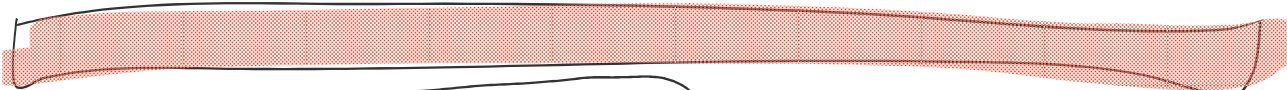
⤴

$$a_{n-1}x^n + \dots + a_1x^2 + a_0x : x^n - 1 = a_{n-1}$$

$$-(a_{n-1}x^n - a_{n-1})$$

$$a_{n-2}x^{n-1} + a_{n-3}x^{n-2} + \dots + a_1x^2 + a_0x + a_{n-1}$$

⤴



Ideals $\boxed{I \subseteq \mathbb{F}[x]/(x^n-1)}$ a subset of polynomials
 closed under multiplication.

$$\langle g(x) \rangle = \{ g(x) \cdot h(x) \mid h(x) \in \mathbb{F}[x]/(x^n-1) \}$$

$$\mathbb{F}_2[x]/(x^3-1) = \{ 0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^2+x \} \leftarrow$$

$$\langle x+1 \rangle = \{ 0, x+1, x^2+x, x^2+1 \}$$

$$\{ 000, 110, 011, 101 \}$$

$$(x+1) \cdot x^2 = x^3 + x^2 = x^3 - 1$$

$$- (x^3 - 1) = 1$$

$$\hline x^2 - 1 = x^2 + 1$$

$$\langle x^2+1 \rangle = \{ h(x) \cdot x^2+1 \mid h(x) \in \mathbb{R}_n \}$$

$$(x^2+1) = x^2 \cdot (x+1)$$

$$\langle x^2+1 \rangle = \{ h(x) \cdot x^2 \cdot x+1 \mid h(x) \in \mathbb{R}_n \}$$

$$\langle x^2+1 \rangle = \{ h'(x) \cdot (x+1) \}$$

$$\langle x^2+1 \rangle \subseteq \langle x+1 \rangle$$

$$\langle x+1 \rangle \subseteq \langle x^2+1 \rangle$$

$$h'(x) = h(x) \cdot x^2$$

$$(x^2+1)$$

$$(x+1) =$$

$$x^2(h(x)) \quad x^3-1$$

$$\begin{aligned} & \underline{(x+1)} \cdot \underline{(x^2+1)} \\ &= \underline{(x+1) \cdot x^2} + \underline{(x+1)} \\ &= x^2+1 + x+1 = x^2+x \\ & (x+1)(x^2+x+1) \\ &= \overset{\downarrow}{x^2}(x+1) + \overset{\downarrow}{x}(x+1) + \overset{\downarrow}{x+1} \\ & x^2+1 + x^2+x + x+1 = 0 \end{aligned}$$



What is missing is a way to characterize different ideals:

Each ideal is characterized by a unique divisor of x^3-1

Primitive ∇ this is primitive ∇

$$x^3-1 = (x+1)(x^2+x+1)$$

⊗ This is the hard part!

$$\langle x+1 \rangle \vee \{110, 101, 011, 000\}$$

$$\langle x^2+x+1 \rangle \{111, 000\}$$

$$\langle x^3 - 1 \rangle \rightarrow \{000\}$$

$$\langle 1 \rangle \rightarrow \{0, 1\}^3$$

To each code we associate a divisor $g(x)$ of $x^n - 1$ in \mathbb{F}_q . It is called a generator polynomial.

if C has a generator polynomial $g(x)$ degree $(g(x)) = \ell$

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_\ell & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \dots & g_{\ell-1} & g_\ell & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & g_0 & \dots & g_{\ell-1} & g_\ell \end{pmatrix} \leftarrow$$

$(m_0 \dots m_\ell)$

$$m \cdot G = C = (g_0 m_0, g_1 m_0 + g_0 m_1, g_2 m_0 + g_1 m_1 + g_0 m_2, \dots)$$

$$m(x) = m_0 + m_1 x + \dots + m_\ell x^\ell \in \mathbb{A}$$

$$\boxed{m(x) \cdot g(x)} = C(x) \quad (g_1 m_0 + m_1 g_0) x$$

$$\mathbb{A} = g_0 m_0$$

$$H \quad \downarrow \quad \downarrow$$

$$x^n - 1 = g(x) \cdot h(x)$$

$$1 \quad m_0 \quad \dots \quad 1 \quad h_{n-1} \quad \dots \quad h_0 \quad x^{n-k} \quad (h_{n-1} \dots h_{n-k})$$

~~_____~~

$$h(x) = h_0 + h_1 x + \dots + h_{n-1} x^{n-1} \quad (h_0 \dots h_{n-1})$$

$$\bar{h}(x) = h_{n-1} x^{n-1} + \dots + h_1 x + h_0 \quad \leftarrow (h_{n-1} \ h_{n-2} \ \dots \ h_0) \rightsquigarrow$$

∇

$$H = \begin{pmatrix} h_{n-1} & h_{n-2} & \dots & h_0 & 0 & 0 & 0 \\ 0 & h_{n-1} & \dots & h_0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_2 & h_1 & h_0 \end{pmatrix}$$