Cyclic Codes

idea: $\mathbb{F}_p^n \underset{\text{vec spaces}}{\cong} \mathbb{F}_p[x]/(x^n-1)$

rules: ① $p=0$ ② $x^n=1$

eg. $n=3$ $p=2$ $\boxed{\begin{matrix}2=0\\ x^3=0\end{matrix}}$

$$3x^3+7 = x^3+1 = 1+1 = 0 \qquad x^4 = x$$

$$\begin{pmatrix}a_0\\ \vdots\\ a_{n-1}\end{pmatrix} \longleftrightarrow a_{n-1}x^{n-1}+\dots+a_1x+a_0$$

Code of the form $g(x)\,\mathbb{F}_p[x]/(x^n-1)$ = all multiples of $g(x)$.

eg. $g(x) = 1+x^2+x^3+x^4$ in $\mathbb{F}_2[x]/(x^7-1)$ $\quad p=2,\ n=7 \quad 2=0,\ x^7=1$

7-dim'l vector space over $\mathbb{F}_2$.

codewords:

$$\begin{array}{r|ccccccc} & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ g(x)\cdot 0 = & 0&0&0&0&0&0&0\\ g(x)\cdot 1 = & 1&0&1&1&1&0&0\\ g(x)\cdot x = & 0&1&0&1&1&1&0\\ g(x)\cdot x^2 = & 0&0&1&0&1&1&1\end{array}$$

$$g(x)\cdot x = x+x^3+x^4+x^5$$

$g(x)\cdot x^3 = \underline{1001}011$

$g(x)\cdot x^4 = 1100101$

$g(x)\cdot x^5 = 1110010$

$g(x)\cdot x^6 = 0111001$

$g(x)\cdot x^7 = 1011100$

$g(x)\cdot(x^3+x) = 1100101$

Prop This list is complete!

$$g(x)(x^3+x^2+1) = (1+x^2+x^3+x^4)(x^3+x^2+1)$$

$$= \dots = x^7-1 = 0$$

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

This implies the codewords are all of the form

$$g(x)(ax^2+bx+c) \qquad a,b,c \in \mathbb{F}_2.$$

$$|\mathcal{C}| \leq 2^3 = 8$$

But we have 8 codewords listed above, so this list is complete, $|\mathcal{C}| = 8$.

$$\boxed{\text{A linear } [7,3]\text{-code}}$$

$$G = \begin{array}{c} \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \right) \end{array} \begin{array}{c} x^3 \\ x \\ x^2 \end{array}$$

Example.

send $g(x)(x^2+1) = $

$$\begin{array}{rl} & 1011100 \quad 1 \\ + & 0010111 \quad x^2 \\ \hline & \boxed{1001011} \end{array} \xrightarrow[\text{error}]{\times} 1001010 = u$$

message

receiver :

$$uH^T = (1001010)\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{array}{c} \times \\ \\ \\ \times \\ \\ \times \end{array} = \begin{array}{r} 1011 \\ 1000 \\ 0010 \\ \hline 0001 \end{array} = 0001$$

syndrome.

1000111 ← last entry!

so same syndrome as for (0000001)

coset leader!

⇒ guess error was in last position

1001010 + 0000001 = 1001011

codeword that was sent.