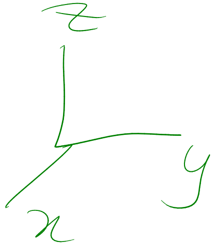
Note: grading error

$$C' = \{(0,0,0),\ (1,1,0),\ (1,0,1),\ (\overset{x}{0},\overset{y}{1},\overset{z}{1})\} \subset \mathbb{F}_2^{\,3}$$



Basis: $e_1\ (1,1,0)$ $\qquad e_1 + e_2 = (0,1,1)$

dim 2 $\quad e_2\ (1,0,1)$

rowspace $= C'$

matrix $\quad M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

$x + y + z = 0$ "even # of 1s"

General

Def^n. The/a coset leader is the element of least Hamming weight. (choose one if not unique)

A syndrome decoding table lists the cosets by coset leader & syndrome

The syndrome of a coset e is $(u+e)H^T$.

Example

$[4,2]$-code over $\mathbb{F}_2$

Space $\mathbb{F}_2^4$ $= 16$ elts

$$G = \left(\begin{matrix}1&0\\0&1\end{matrix}\;\overset{P}{\boxed{\begin{matrix}1&1\\1&0\end{matrix}}}\right) \qquad H^T = \begin{pmatrix}\boxed{\begin{matrix}1&1\\1&0\end{matrix}}\\ \begin{matrix}1&0\\0&1\end{matrix}\end{pmatrix}$$

	leader				syndrome
$e =$	0000	1011	0110	1101	00
$1000+e =$	1000	0011	1110	0101	11
$0100+e =$	0100	1111	0010	1001	10
$0010+e =$	~~0010~~	~~1001~~ repeat	~~0100~~	~~1111~~	
$0001+e =$	0001	1010	0111	1100	01

(error patterns)

eg. syndrome of $1000+e$ is

$$(1000)\begin{pmatrix}1&1\\1&0\\1&0\\0&1\end{pmatrix} = (11)$$

Decoding :

1) Compute the syndrome of received message.

2) Lookup the leader using the table

3) Subtract leader from the message, to get a codeword.

Example.

$v = 1110$

$$vH^T = (1110)\begin{pmatrix}1&1\\1&0\\1&0\\0&1\end{pmatrix}\begin{matrix}\times\\\times\\\times\\ \ \end{matrix} = 11$$

$\Rightarrow$ in coset w/ leader 1000

(supposed error)

$1110 - 1000$

$= 0110$

Goals:

a) high information rate

b) strong error correction/detection

c) fast encoding/decoding ← add structer (eg. linear codes)

Hamming Codes (binary linear codes)

Parameter : m

Parity check matrix is defined to be all non-0 binary m-tuples as colums (ordered so I @ end)

⇒ compute G

eg. $m = 3$

$$H^T = \left.\begin{pmatrix} \overset{P}{\boxed{\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{matrix}}} \\ \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \end{pmatrix}\right\}n \qquad G = [I \;\; P] = \underbrace{\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}}_{n}$$

$n = \text{length} = 2^m - 1$

$k = \dim = 2^m - m - 1$

min. dist $d(C) = 3$

Syndrome decoding: if you get row j of H^T, then error in j^{th} position.

Thm. $H = [-P^T \; I_{n-k}]$ is parity check matrix for $G = [I_k \; P]$.

Pf. ①
$$GH^T = k\left\{ \overbrace{\begin{bmatrix} I_k & P \end{bmatrix}}^{n} \right. \left. \overbrace{\begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}}^{n-k} \right\} n = \begin{bmatrix} -I_k \cdot P + P \cdot I_{n-k} \end{bmatrix}$$
$$= [0].$$

So $G \subset \underbrace{\text{left kernel } H^T}_{\dim \geq k}$.

② Rank of H is $n-k$ since it has an id. matrix in it.

$\Rightarrow G = \text{left ker } H^T$
(rank + nullity).

□

Cyclic codes. (type of linear code).

"cyclic" : $(c_1, \dots, c_n) \in \mathcal{C} \implies (c_n, c_1, \dots, c_{n-1}) \in \mathcal{C}$.

idea: $\mathbb{F}_p^n \underset{\text{vec spaces}}{\cong} \mathbb{F}_p[x] / (x^n - 1)$ ← "rules": $x^n = 1$, $p = 0$ eg. $x^{n+1} + 3 = x + 3$

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

Idea: Take a code of the form $g(x)\,\mathbb{F}_p[x]/(x^n-1)$ = all multiples of $g(x)$ in ring

$$= \{ g(x)f(x) : f(x) \in \mathbb{F}_p[x]/(x^n-1) \}.$$

Ex. $g(x) = 1 + x^2 + x^3 + x^4$ in $\mathbb{F}_2[x]/(x^7-1)$

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

2^7 elements.

code words:

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

~~$g(x)\cdot x^7 = 1\,0\,1\,1\,1\,0\,0$~~ repeating.

cyclic shift

other codewords are combinations

eg. $g(x)(x+1)$

$= g(x)\cdot x + g(x)\cdot 1$

$= 1110010$