Cosets of a Code

Def^n. If $\mathcal{C}$ is a linear code, and $\vec{u} \in \mathbb{F}^n$ (length n)

then $u + \mathcal{C} = \{ u + c : c \in \mathcal{C} \}$

is a <u>coset</u> of $\mathcal{C}$

$$\mathcal{C} \xrightarrow{\cdot H^T} \vec{0}$$

$$u_1 + \mathcal{C} \xrightarrow{\cdot H^T} u_1 H^T$$

u_i	$u_i H^T$
"coset representative"	"syndrome"

Example $\mathcal{C}$ linear code w/

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad \text{over } \mathbb{F}_2$$

Then $\mathcal{C} = \{(0000), (1011), (0110), (1101)\}$

$|\mathbb{F}_2^4| = 2^4 = 16 \qquad |\mathcal{C}| = 4$

leaders

					Syndrome
$\mathcal{C}$:	0000	1011	0110	1101	00
$1000 + \mathcal{C}$:	1000	0011	1110	0101	11
$0100 + \mathcal{C}$:	<u>0100</u>	1111	<u>0010</u>	1001	10
$0001 + \mathcal{C}$:	0001	1010	0111	1100	01

$$H^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Decoding: Receive $\vec{v}$, compute syndrome $\vec{v} H^T$, guess

Ex. Receive $v = 1110$
Compute $vH^T = 11$
Coset "leader" $= 1000$
Guess: error in 1st position

The cosets of $\mathcal{C}$ form equivalence classes for the equivalence relation

$$u \sim v \quad \text{if} \quad u - v \in \mathcal{C}. \qquad \text{(Exercise.)}$$

<u>Defn</u>. A <u>coset leader</u> is a vector of minimum Hamming weight in a coset.
The <u>syndrome</u> of a vector v is vH^T.

<u>Aside</u>: Finding the coset leader for a syndrome is a short vector problem.
Not always easy.

Hamming code (binary)

Parameter: m

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

$k = \text{dim} = 2^m - m - 1$

min. dist $d(C) = 3$

Note: $n - k = m$

Parity check matrix is all non-0 binary m-tuples as columns w/ ID matrix at the end.

e.g. $\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

$\Rightarrow$ compute G.

Syndrome decoding for 1 error: if you get column j, then j^{th} position is where error occurred.

McEliece Cryptosystem

$\mathbb{F}_2$

Alice

message $x \in \mathbb{F}_2^k$

Encrypt:

random $e \in \mathbb{F}^n$

$wt(e) = t$ (correctable error)

$y = x G_1 + e$

G_1, Public key

ciphertext y

Bob

Choose (secret)

1. G $k \times n$ gen. matrix binary $[n,k]$-code w/ $d = d(C)$.
2. S = $k \times k$ invertible over $\mathbb{F}_2$
3. P = $n \times n$ permutation

$G_1 = SGP$ ($k \times n$ matrix)

Decrypt

$$\begin{aligned} y_1 &= yP^{-1} \\ &= (xG_1 + e)P^{-1} \\ &= \underbrace{xSG}_{\text{codeword}} + e' \end{aligned}$$

also $wt(e') = t$

decode y_1

get $x_1 = xSG$.

find x_0 s.t. $x_0 G = x_1$ } ie. info bits

Compute $x = x_0 S^{-1}$ ☺

ie. $xS = x_0$ so $xSG = x_1$