Syndrome Decoding

$S = Hy$ is <u>syndrome</u> of y

H is a check matrix for C

$S = 0 \Leftrightarrow y \in C$

$x \to \hat{x} = x + e \Rightarrow$

$$S = H\hat{x} = H(x+e) = Hx + He = He.$$

error e is <u>detected</u> iff

$$S = He \neq 0$$

(T) Two vectors x, y from the same coset of C have the same syndrome

<u>Proof</u> $x, y \in a + C$, $a \notin C$

$x = a + v \qquad v \in C, \ Hv = 0$

$y = a + w \qquad w \in C, \ Hw = 0$

$S(x) = Hx = H(a+v) = Ha + Hv = Ha$

$S(y) = Hy = \cdots\cdots = Ha$

$Hy = Hx$

There is <u>one-to-one correspondence</u> between cosets and syndromes.

<u>Example</u> $q=2 \quad n=4$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \Rightarrow H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

$$S(0000) = H \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$S(1000) = H \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$S(0100) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$S(0010) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

STANDARD ARRAY

C =	0000	1011	0101	1110	00
	1000	0011	1101	0110	11
	0100	1111	0001	1010	01
	0010	1001	0111	1100	10

↑ coset leaders (first column) ↑ syndromes (last column)

by syndrome one can idendify a coset leader

$$S(1111) = S(1011) + S(1000) =$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} + S(1000) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

DECODING:

$$S \longrightarrow \text{coset leader} = e \Rightarrow x = \hat{x} \oplus e$$

$q=2$

$$S = H\hat{x} = He$$

SYNDROME

00	0000
11	1000
01	0100
10	0010

coset leaders.

DECODING PROCEDURE

1. COMPUTE $S = H\hat{x}$
2. If $S \neq 0$ error is detected
3. Compute error leader e corresponding to S
4. Compute
$$x = \hat{x} \ominus e.$$

A fundamental Theorem

Let G is a generating matrix for (n, q^k, d) code $\mathbb{C}$ and H is a check matrix for $\mathbb{C}$

Then <u>any</u> $d-1$ columns of C are linearly independent.

<u>Proof</u>

For any $x \in \mathbb{Z}_q^n$ if $\|x\| \le d-1$

$x \notin \mathbb{C}$ (since $0 \in \mathbb{Z}_q^n$ and $d(0, x) \le d-1$)

Thus $Hx \neq 0$. and Hx is a linear sum of at most $d-1$ ~~vec~~ columns of H

Example $n=6,\ q=7$

$$H=\begin{bmatrix}1&1&1&1&1&1\\1&2&3&4&5&6\end{bmatrix} \Rightarrow d=3$$

$$=[h_1\, h_2\, h_3\, h_4\, h_5\, h_6]$$

and $a h_i + b h_j \neq 0$
for any $a, b \in \{0, 1, \dots, 6)$
$i \neq j$

Any two columns are linearly independent $\Longrightarrow d=3.$

$$H \cdot \begin{array}{c}\\ \\ \\ i\\ \\ \\ \\ j\\ \\ \\ \\ \end{array}\begin{bmatrix}0\\ \vdots\\ 0\\ a\\ 0\\ \vdots\\ 0\\ b\\ 0\\ \vdots\\ 0\end{bmatrix} = h_i \cdot a + h_j b.$$