Classical Coding Theory (N+C 10.4.1)

Consider a code encoding

k logical bits

into

n physical bits

This is defined by its $n \times k$ 'generator matrix', G

This maps k-bit strings into their encoded n bit versions (known as code words)

Example 1 : $k=1$, $n=3$ repetition code

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$G[0] = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad , \quad G[1] = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Example 2 : $k = 2$, $n = 6$ repetition code

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$G\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad G\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$G\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad G\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

We can also define the parity check matrix, H

This is an $(n-k) \times n$ matrix such that

$$Hx = 0$$

Iff x is a valid codeword

Each row is an independent parity check: a condition that codewords must satisfy.

Example 1: $n=3$, $k=1$

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

✓ $H\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $H\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+1+0 \\ 0+1+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ (mod 2)

✗ $H\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $H\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $H\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Example 2: $n = 6,\ k = 2$

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

$$H\begin{bmatrix} a \\ a \\ a \\ b \\ b \\ b \end{bmatrix} = \begin{bmatrix} a+a \\ a+a \\ b+b \\ b+b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad H\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

✓ ✗

The result of the parity check matrix is called the 'syndrome'.

Deducing the most likely encoded logical from the syndrome is 'decoding'

Hamming distance between codewords is 'distance' of the code.

Adding parity checks creates alternative forms of the parity checks.

For example: the $n=7, k=4$ Hamming code

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

Three independent checks

$$h_1 = [0\,0\,0\,1\,1\,1\,1] \qquad h_1 + h_2 = [0\,1\,1\,1\,1\,0\,0]$$

$$h_2 = [0\,1\,1\,0\,0\,1\,1] \qquad h_1 + h_3 = [1\,0\,1\,1\,0\,1\,0]$$

$$h_3 = [1\,0\,1\,0\,1\,0\,1] \qquad h_1 + h_2 + h_3 = [1\,1\,0\,1\,0\,0\,1]$$

With this we can construct an alternative parity check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = \left(A \mid I_{n-k} \right)$$

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad I_{n-k} = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This is the 'standard form'

In this form

$$G = \begin{pmatrix} I_4 \\ \hline A \end{pmatrix}$$

$$= \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right)$$

So $G\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$, etc

columns of G and sums thereof are codewords

Clearly, for all codes

$$HG = 0$$

because the parity checks of H act on the code words of G.

This implies

$$(HG)^T = 0 \quad \therefore \quad G^T H^T = 0$$

So we could define a new code with

$$H' = G^T, \quad G' = H^T$$

This is the 'dual' of the original code

Example 1: $k = 1$, $n = 3$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$G' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad H' = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

Dual is a $k = 2$, $n = 3$ code.

Code words:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

00 10 01 11

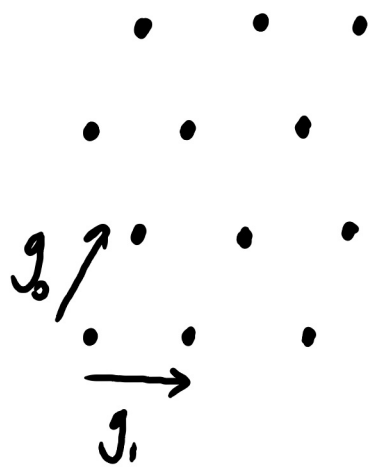
Here we looked at examples defined on bits (i.e. over the field $\mathbb{Z}_2$)

But we could do so over any finite field.

Only generalization:

$$G = \begin{pmatrix} I_k \\ \hline -A \end{pmatrix}$$

Codes are a bit like a lattice



$G = (g_0\ g_1)$

$Hx = 0$ implies you are on a point

Decoding is finding the nearest point

$n=4, k=2$