12-3 Classical Error-Correcting Codes

Hamming distance

bit string $x = x_1 x_2 ... x_n$

Hamming weight $w(x)$ = # of ones in x

ex) $w(010101) = 3$

$x = x_1 x_2 ... x_n$, $y = y_1 y_2 ... y_n$

Hamming distance $d(x, y)$ = # of bits with different values = $w(x \oplus y) = \sum_i x_i \oplus y_i$

ex) $d(010101, 110011) = 3$

Big picture

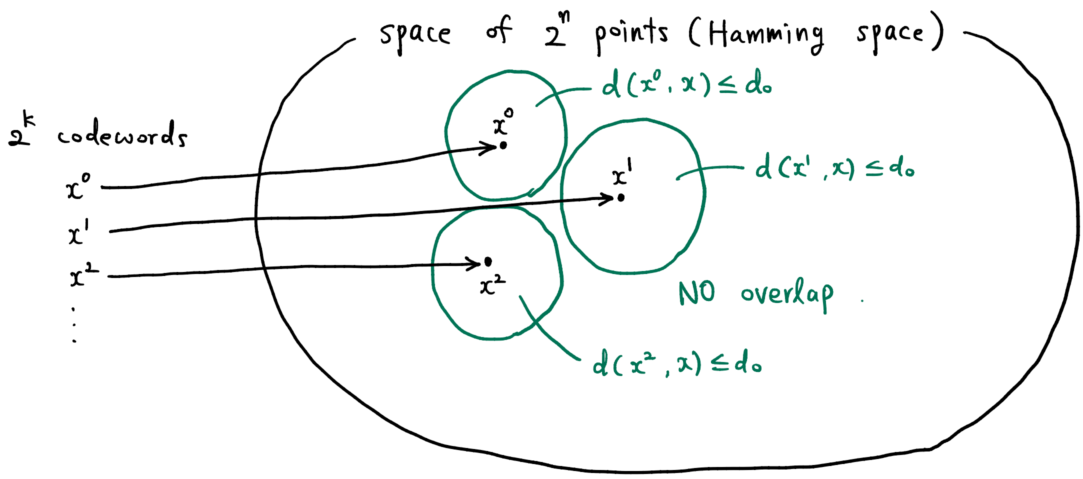
codewords: encoded bit messages

ex) $x^0 = 000$, $x^1 = 111$

Codeword 000 represents bit message 0.

Codeword 111 represents bit message 1.

$[n, k]$ codes encode k-bit messages into n-bit codewords.



This error-correcting code can correct d_0 errors.

$[n, k, d]$ code C $\quad d = d(C) \equiv \min_{\substack{x,y \in C \\ x \neq y}} d(x, y)$ $\quad$ distance of code C

(minimum distance bewteen codewords)

If error-correcting code C can correct up to d_0 errors, $2d_0 < d$.

ex) $x^0 = 000$, $x^1 = 111$

$[3, 1, 3]$ error-correcting code, correcting up to one error.

Classical linear codes

$[n, k]$ linear code

generator matrix G: $n \times k$ matrix with $G_{ij} \in \{0, 1\}$

k-bit message m: $k \times 1$ matrix (column vector)

codeword $x^m = G\,m$ (matrix multiplication)

parity check matrix H: $(n-k) \times n$ matrix with $H_{ij} \in \{0, 1\}$

$HG = 0$

codewords: all column vector x satisfying $Hx = 0$

💬 If you choose H, G is automatically determined, and vice versa.

ex) $x^0 = 000$, $x^1 = 111$: $[3, 1]$ code

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \qquad x^0 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad x^1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

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

$[7, 4, 3]$ Hamming code

$$\begin{array}{cc} & \begin{array}{ccccccc} 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{array} \\ H = & \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \\ & \begin{array}{ccccccc} P_1 & P_2 & P_3 & m_1 & m_2 & m_3 & m_4 \end{array} \end{array}$$

P_i : parity bit

m_i : message bit

$$\begin{array}{rl} m_1 \times & (1\ 1\ 0\ 1\ 0\ 0\ 0) \\ m_2 \times & (1\ 0\ 1\ 0\ 1\ 0\ 0) \\ m_3 \times & (0\ 1\ 1\ 0\ 0\ 1\ 0) \\ +)\ m_4 \times & (1\ 1\ 1\ 0\ 0\ 0\ 1) \\ \hline & \text{codeword} \end{array}$$

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

error correction

codeword $x \xrightarrow{\text{error}} x' = x + e$

$Hx' = \cancel{Hx} + He = He$ error syndrome

ex) $[7, 4, 3]$ Hamming code

$$e = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-th row} \quad \Rightarrow \quad He = (i\text{-th column of } H)$$

All columns in H are different!