Error Correcting Codes - Part I

Simon Zheng

Agenda

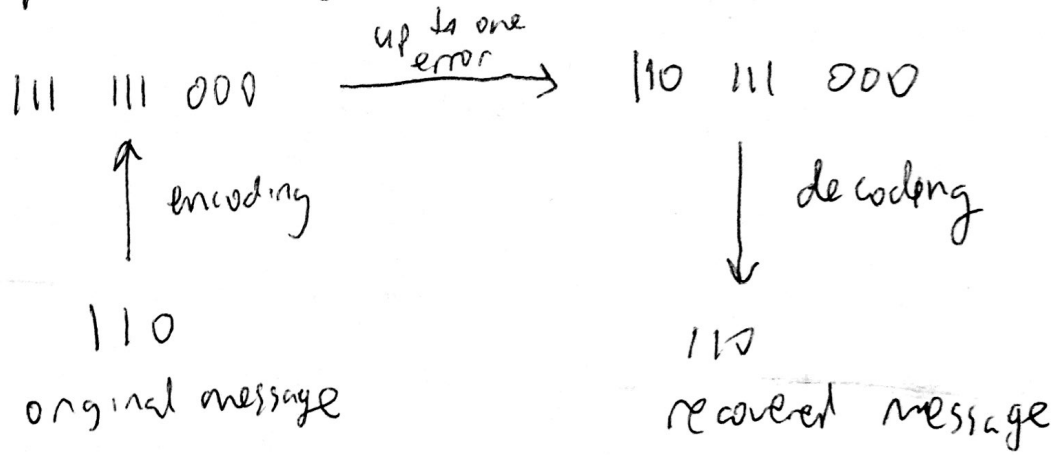
1. Background and setup
2. Linear Codes
3. Hamming code, $[n, n-\log_2(n+1), 3]_2$
4. Hadamard Code, $[n, \log_2 n, \frac{n}{2}]_2$

1. Background and setup

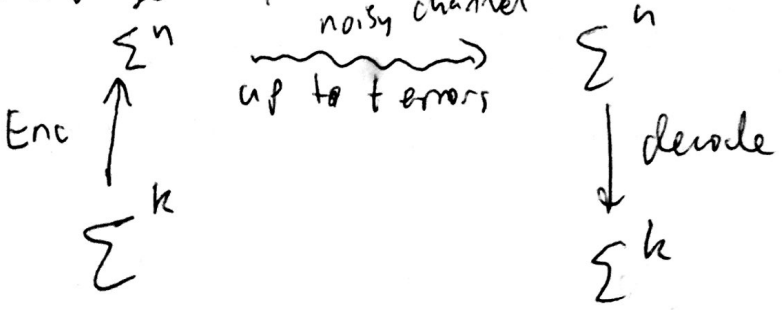
motivation: $\uparrow$ redundancy $\Rightarrow$ correct errors

applications: DVDs, sending messages to space probes

ex repetition code



def general set up



Let $n > k$ be positive integers, Σ be alphabet of size q. Let $Enc : \Sigma^k \to \Sigma^n$ be injective.

Σ^k message space

$C = im(Enc)$ code.

$\frac{k}{n}$ rate high rate → efficient code

def Let $x, y \in \Sigma^n$. The Hamming distance is

$$\Delta(x,y) = |\{1 \le i \le n \mid x_i \neq y_i\}|$$

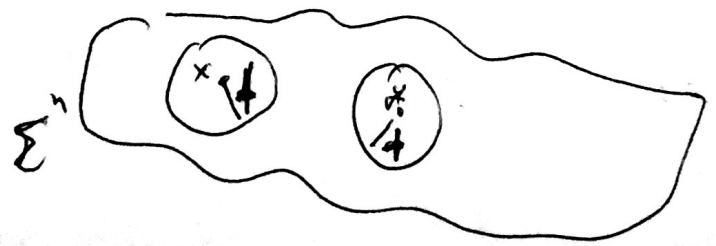
The minimum distance d of a code C is

$$d = \min_{\substack{x \neq y \\ x,y \in C}} \Delta(x,y).$$

Fact Suppose there are at most t errors ~~(but not more)~~ ~~when~~ $t = \frac{d}{2}$. Then we can uniquely decode if and only if $t < \frac{d}{2}$.

Proof Consider Hamming balls of radius t centered at each code word. If they don't intersect, then we can uniquely recover each ~~message~~.

$x, y \in C$



(2) Linear Codes, $\Sigma = \mathbb{F}_q$ (finite field q elements)

motivation: would like nice way to find min distance

def A linear code is a code in which every linear combination of codewords is a codeword.
Denoted $[n,k,d]_q$ or $[n,k]_q$.

def Let G be full rank $n \times k$ matrix (ensures injectivity).
Then set

$$\begin{aligned} Enc : \mathbb{F}_q^k &\to \mathbb{F}_q^n \\ x &\mapsto Gx \end{aligned}$$

This produces a linear code with generator matrix G.

ex $q=2, n=3, k=2$, $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{pmatrix}$$

$$C = im\, G = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

def The Hamming weight of $x \in C$ in a linear code is $wt(x) = \Delta(x, 0)$.

Fact In a linear code, the minimum distance d is equal to the minimum Hamming weight of a nonzero codeword.

Proof Suppose x_1, x_2 minimize $\Delta(x_1, x_2)$ and x_3 minimizes $wt(x_3) = \Delta(x_3, 0)$. Then

$$\Delta(x_1, x_2) \leq \Delta(x_3, 0) \quad \text{by def of } x_1, x_2$$

$$\Delta(x_3, 0) \leq \Delta(x_1 - x_2, 0) = \Delta(x_1, x_2)$$

0 and $x_1 - x_2$ are in code because the code is linear

def Given linear code $C = [n, k]_q$, define the orthogonal space

$$C^\perp = \{ x \in \mathbb{F}_q^n \mid x^T y = 0 \ \forall y \in C \}$$

This $C^\perp$ is known as the dual code of C. It has parameters $[n, n-k]_q$. Define the parity check matrix H of C as the $(n-k) \times n$ matrix satisfying

$$C^\perp = \text{Im}(\text{Enc}^\perp)$$

where

$$\text{Enc}^\perp : \mathbb{F}_q^{n-k} \to \mathbb{F}_q^n$$

$$w \mapsto H^T w.$$

ex using previous example,

$$C^\perp = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$$H = (1\ 1\ 1).$$

Fact $x \in C \iff Hx = 0$ (re-express code as null space of parity check matrix)

proof Note that $C^\perp$ is row span of H.

$$Hx = 0 \iff \begin{matrix} r_1^T x = 0 \\ \vdots \\ r_{n-k}^T x = 0 \end{matrix} \quad \text{where } r_i \text{ are rows of } H$$

$\iff \forall y \in C^\perp$, can write $y = \sum a_i r_i$

Then

$$y^T x = \sum a_i r_i^T x = 0$$

$$\iff x \in (C^\perp)^\perp = C$$

Corollary The minimum distance d is the min # of columns of H that are linearly dependent

proof

$$d = \min \{ wt(x) \mid x \in C,\ x \neq 0 \}$$

$$= \min \{ wt(x) \mid x \in C,\ Hx = 0 \}.$$

③ Hamming code : intuition: high rate, low error detection

$r \geq 1$. $r \times (2^r - 1)$ parity check matrix

$$H = \left(\begin{array}{c} \text{all} \\ \text{binary strings of length } r \\ \text{except } 0 \end{array} \right)$$

ex $r = 2$

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad C = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

Thm

~~Fact~~ Hamming code is $[2^r - 1, 2^r - 1 - r, 3]_2$ code.

proof since $0 \notin C$, 2 columns not linearly independent.

3 are: $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$

Remark let $n = 2^r - 1$. Then $[n, n - \log_2 n, 3]_2$.

error detection correct $\left\lfloor \frac{d}{2} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor = 1$ error

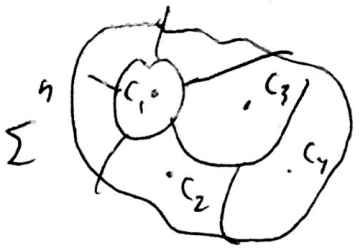
let $y = x + e_i$, e_i element of standard basis, $x \in C$. Then

$Hy = Hx + He_i = He_i$ convert this from binary to int i

ex $x = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $\overset{\text{error}}{\rightsquigarrow} y = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$

$$Hy = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow \text{index 3 changed}$$

"def perfect code C ; Hamming balls radius t (max #errors) partition Σ^n.



~~Proof~~

Thm Hamming code is perfect

Proof pick any $x \in \mathbb{F}_2^n$. If $Hx = 0$ done, $x \in C$.

If $Hx \neq 0$, then $Hx = H_i$ ↘ column i.

$$\Rightarrow H(x - e_i) = 0$$

$x - e_i \in C$

and x in Hamming ball

(4) Hadamard Code - intuition: opposite of Hamming Code: low rate, high error detection

Def Let $r \geq 1$. The generator matrix is a $2^r \times r$ matrix whose rows are all possible binary strings of length r.

ex $r=2$, $G = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Fact This is a $[2^r, r, 2^{r-1}]_2$ code.

proof Suffices to show that min weight of nonzero codeword is 2^{r-1}. Let $x \in \mathbb{F}_2^r$ be nonzero. $\exists j$ s.t. $x_j = 1$. Entries of Gx are of the form $\sum a_i x_i$ where $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^r$. Exactly 2^{r-1} vectors $a \in \mathbb{F}_2^r$ satisfy $a_j = 0$, and exactly 2^{r-1} vectors $a \in \mathbb{F}_2^r$ satisfy $a_j = 1$. Thus exactly 2^{r-1} nonzero entries exist for Gx for all nonzero x. By previous fact, min distance = min weight $= 2^{r-1}$.

Remark Let $n = 2^r$. Then $[n, \log_2 n, n/2]_2$. Good distance $\frac{n}{2}$, bad rate $\frac{\log_2 n}{n}$.