Error Correcting Codes

why? noisy channels

model: sending bits over a channel with probability p that any bit flips.

Basic Example: message 1 bit.

message	encoding →	codeword
0		000
1		111

this code { detect 2 errors; correct 1 error (majority rules)

detect = know it isn't a codeword (not how many / where errors)

Eg. suppose send 000

received	# errors	detected?	decoded
000	0		000
001	1	✓	000
010			
100			
110	2	✓	111 (incorrect)
011			
101			
111	3	☒	111 (incorrect)

Probability of correctly decoding

p = prob for each bit that an error occurs

$$(1-p)^3 + p(1-p)^2 + (1-p)p(1-p) + (1-p)^2 p$$

- $(1-p)^3$: prob. of no errors
- $p(1-p)^2$: error in 1st bit
- $(1-p)p(1-p)$: error in 2nd
- $(1-p)^2 p$: error in 3rd

If $p = 0.1$, this is 0.972.

Parity Check Code

message: 7 bits

encoded message: orig. message + 1 parity bit

= Σ of other bits mod 2

eg. 0111001

$\rightarrow$ 01110011

code = {8 bit strings: Σ bits $= 0 \bmod 2$} (even # of 1's)

= set of codewords

Can detect 1 error (2 bits → not detected)

correct 0 errors.

Fundamental Trade-Off:

space (how long are codewords compared to message)

vs.

robustness (correcting & detecting more errors)

Def^n. Let A be an alphabet (usually $A = \{0,1\}$).

A^n = n-tuples of letters from A ie. strings

A code of length n is a non-empty subset of A^n.

The elements of the code are called codewords.

If $|A| = 2$ then "binary code"
If $|A| = 3$ then "ternary code"
If $|A| = q$ then "q-ary code"

Basic example

000, 111

$A = \{0, 1\}$

code $= \{(0,0,0), (1,1,1)\}$

length 3 binary code w/ 2 codewords

Checksum code

$A = \{0, 1\}$

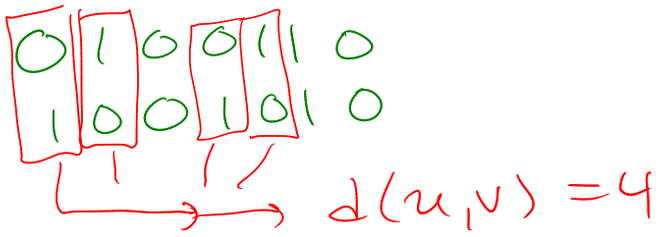
code $= \{$ 8 bit strings w/ $\Sigma = 0 \bmod 2\}$
$\subseteq A^8$

length 8 binary code
w/ 2^7 codewords

Def^n. Let $u, v \in A^n$

The Hamming distance $d(u,v)$ = # of positions at which u & v differ.

eg. $u = 0\,1\,0\,0\,1\,1\,0$
$v = 1\,0\,0\,1\,0\,1\,0$



Typically, decoding is done by choosing the nearest codeword in Hamming distance. "Nearest neighbour decoding"

Properties: (of H. dist.)

1) $d(u,v) \geq 0$ and ($d(u,v) = 0$ iff $u = v$)
2) $d(u,v) = d(v,u)$
3) $d(u,v) \leq d(u,w) + d(w,v)$

} exercise

(This means it's a metric.)

Defn. The minimum distance of a code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{ d(u,v) : u, v \in \mathcal{C}, u \neq v \}$$

eg. basic code 000/111

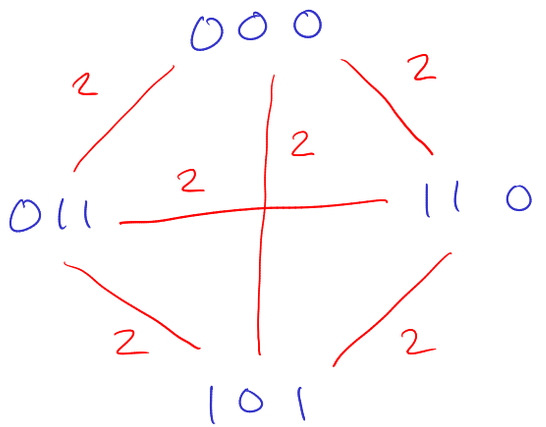
$d(\mathcal{C}) = 3$

$s = 2$

$t = 1$

eg.

code $\Rightarrow$ {000, 110, 011, 101}



$d(\mathcal{C}) = 2$

$s = 1$

$t = 0$

Defn. A code $\mathcal{C}$ can

(1) detect s errors if $d(\mathcal{C}) \geq s+1$

(2) correct t errors if $d(\mathcal{C}) \geq 2t+1$

$s \leq d(\mathcal{C}) - 1$

$t \leq \frac{d(\mathcal{C})-1}{2}$