Lecture 22

Tuesday, April 07, 2015 11:52 PM

Error Detection:

Single bit error detection using parity bit.

Information bits: 0010111 0 (parity bit.)

7 bits of information

Parity check: $\sum_{i=1}^{\infty} b_i \bmod 2 \stackrel{?}{=} 0$ (even)

- Cannot detect 2 errors
- Can detect odd numbers of errors

Correction:

Repetition is simplest: Repetition code (3, 1): Repeat each bit 3 times. Decode the majority

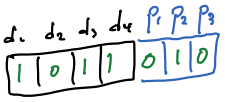
	Information	Codeword	
Repetition (3, 1)	0	000	Correct single errors.
	1	111	
Repetition (5, 1)	0	00000	Correct up to 2 errors.
	1	11111	

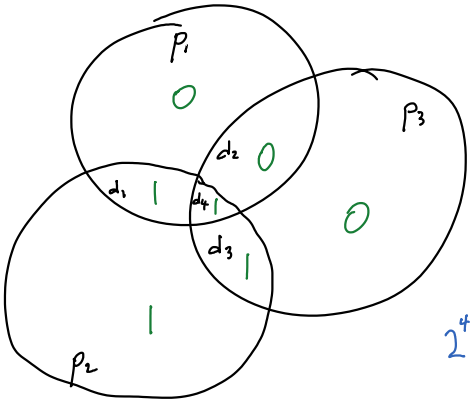
Hamming codes:

Correct 1 error.

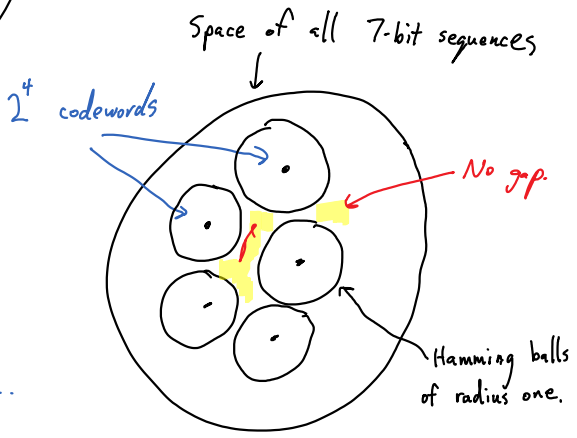
Family of code.

Hamming (7, 4) code:

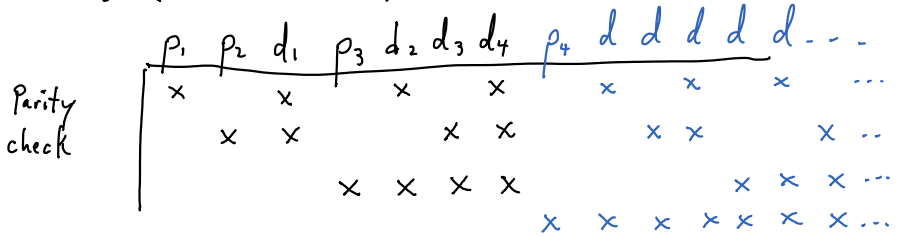




"Perfect code"



Hamming $(2^K - 1,\ 2^K - 1 - K)$



Analyze Prob. of error:

Under the "binary symetric channel" model.

Suppose each bit has error with prob. p_b.

Repetition (3,1): $P(\text{error}) = P(\text{two errors}) + P(\text{three errors})$

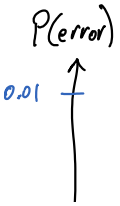
$= 3 \cdot p_b^2 \cdot (1 - p_b) + p_b^3 \approx 3 p_b^2$

Hamming (7,4): $P(\text{error}) = 1 - P(0 \text{ errors}) - P(1 \text{ error})$

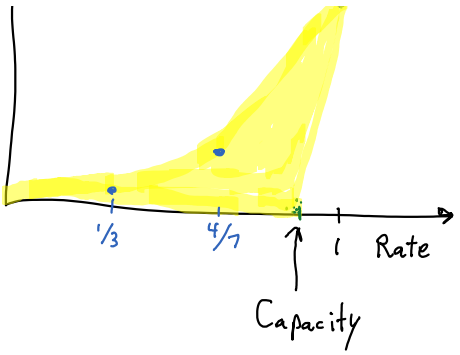
$= 1 - (1 - p_b)^7 - 7 p_b (1 - p_b)^6 \approx 21 p_b^2$

$p_b = 0.01$

	$P(\text{error})$	Rate
Repetition (3,1)	0.000298	1/3
Hamming (7,4)	0.00203	4/7



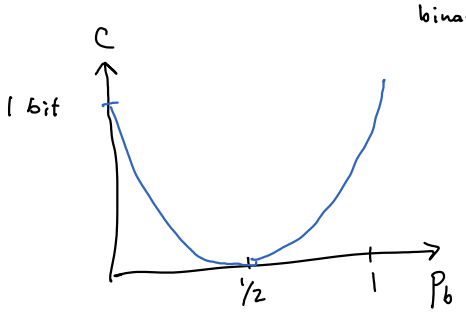
Repetition (3,1)	0.000298	1/3
Hamming (7,4)	0.00203	4/7
Uncoded (1,1)	0.01	1



C = 0.919 bits.

BSC:

$$C = 1 - \underbrace{p_b \log_2 \frac{1}{p_b} - (1-p_b)\log_2 \frac{1}{1-p_b}}_{\text{binary entropy function}}$$



Secrecy:

One-time-pad: (Perfect Secrecy)

Key: 0 1 1 0 1 1 1 0 0 1

Message: 1 1 1 1 1 0 0 0 0 0

xor

Decoder does XOR

Transmit: 1 0 0 1 0 1 1 0 0 1

Perfect Secrecy: Message independent of Transmittion.

$$p(\text{transmit} \mid \text{message}) = p(\text{transmit})$$

Puzzle: n bit information sequency.

Allow 1-bit error.

How many transmitted bits needed? $n - ?$

$\log_2(n+1)$

Use Hamming decoder to compress.