Worked-out Example Sheet

Date No

1. Repetition Code:

Original message : 1101

We will encode this message using "two out of three" repetition code.

Repetition code:

111 111 000 111

Alice → Bob

111 111 000 111 → 110 101 001 110

Decoded message:

1101

A binary symmetric channel is known to flip bits with probability 1/3. Alice decides to use "2 out of 3" repetition code.

(a) What is the new probability of error given this code is used ?

Answer :

Here, probability of error, $P = 1/3$

The repetition code fails, if all three of the bits flip, or 2 of th 3 bits flip

Therefore, the probability of failure is :

$$\alpha = \binom{3}{3}\left(\frac{1}{3}\right)^3\left(\frac{2}{3}\right)^0 + \binom{3}{2}\left(\frac{1}{3}\right)^2\left(\frac{2}{3}\right)^1$$

This is the modified error probability of the channel given a "2 out of 3 repetition code" is used.

(b) If Alice sends a 4-bit message using the above code, what is the probability that the message will be transmitted error free?

Answer:

The probability of error for any bit after using the repetition code is $\alpha = 7/27$

The probability of sending all 4 bits successfully is:

$$\left(\frac{20}{27}\right)^4$$

Exercise:

A binary symmetric channel is known to flip bits with probability 1/4. Alice decides to use "3 out of 5 repetition code".

(a) what is the new probability of error given this code is used?

(b) If Alice sends a 6-bit message using the above code, what is the probability that the message will be transmitted error free?

Date: No.

2. Hamming Code:

Original message = 1101

parity bit required,

$$2^r \geq m + r + 1 \qquad (1)$$

where,

r = parity bit

m = message

For $m = 4$ bit message, parity bit $r = 3$ satisfies eqn (1)

positions of the parity bit will be determined by —

$$2^0, 2^1, 2^2 \ldots 2^{r-1}$$

7	6	5	4	3	2	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	1	0	0	1	1	0

index	P_3	P_2	P_1
0	0	0	0
1	0	0	(1)
2	0	(1)	0
3	0	(1)	(1)
4	(1)	0	0
5	(1)	0	(1)
6	(1)	(1)	0
7	(1)	(1)	(1)

Message, $m = 1101$

Codeword, $C = 1100110$

Let, Bob receives the following codeword due to channel noise.

$C' = 1000110$ (bit 7 6 5 4 3 2 1)

location	bit
4	0
5	0
6	0
7	1

2	1
3	1
6	0
7	1

1	0
3	1
5	0
7	1

parity | 1 | 1 | 0 | → 6

There is something wrong. The computed parity bits should be zero.

The 6th bit is flipped.

Corrected message : 1100110

Exercise:
Bob receives a 7-bit code (1000010) encoded in Hamming code. The message may or may not contain error in this message. Recover the original message using Hamming error correction method.

3. Cascade

(a) Alice and Bob have their versions of raw-keys after running the quantum step and performing sifting for a QKD protocol. However, their keys are not the same. They have previously agreed to correct error using cascade algorithm. Alice and Bob's raw keys are given below:

Alice	Bob
11011001	11001001

Show the steps of the cascade algorithm by drawing the simulation tree.

(b) Give an example where cascade fails to reconcile information.

4. Sifted message length = 2048
QBER = 1/64 (Approximately 1%)

Compute:

(a) Expected number of errors
(b) Approximate block size
(c) Number of steps required in binary for each block?
(d) Total bit exposed during cascade
(e) Privacy survived?

5. Let,

Block size, B = 8

Exposed bit = $2 \times \log_2 8$

= 6

privacy survived = 2/8

= 1/4

= 25%

Block size, B = 16

Exposed bit = $2 \times \log_2 16$

= 2 × 4

= 8

Privacy survived = 8/16

= 1/2

= 50%.

Exercise:

From the above examples, what inference can you draw on how the privacy is impacted by the block size. Show in example.