Tutorial 9 Exercise Solutions

COMP526: Efficient Algorithms

02–03 December, 2024

Exercise 1. In lecture, we showed that the $(7,4)$-Hamming code can be used to correct a single error in a 7-bit codeword that encodes a 4 bit message. Suppose we use $(7,4)$-Hamming codes to detect, but not correct, errors. What is the maximum number of errors that can be *detected* using a $(7,4)$-Hamming code?

Solution. The maximum number of errors detected by a $(7,4)$-Hamming code is 2. To see this, recall that in lecture we argued that the $(7,4)$-Hamming code has code distance 3. Therefore, every two valid codewords are at Hamming distance at least 3 each other: every two valid codewords differ on at least 3 bits. Thus, starting from any codeword x and flipping one or two bits, we cannot obtain another codeword. Therefore, any error of one or two bits can be detected, as the resulting message will not be a valid codeword.

On the other hand, $(7,4)$-Hamming codes cannot detect 3 bit errors. To see this, observe that $x = \texttt{0000000}$ and $y = \texttt{0000111}$ are valid codewords that differ on 3 bits. Thus, it is impossible to distinguish an error-free transmission of y and a transmission of x with 3 bit errors. □

Exercise 2. You your friend agree to encode the beginning of the alphabet using the following scheme that uses 4 bits per character:

A	0000	I	1000
B	0001	J	1001
C	0010	K	1010
D	0011	L	1011
E	0100	M	1100
F	0101	N	1101
G	0110	O	1110
H	0111	P	1111

You receive the following message that your friend encoded using a (7,4)-Hamming code:

```
0010011 1101000 1000000 1010111]
```

What was the original message sent by your friend? Which bits were corrupted in the transmission of the message?

Solution. For the first string, we compute the check bits

$$\begin{aligned}
p_4 &= B_7 \oplus B_6 \oplus m_B \oplus B_4 \\
&= 0 \oplus 0 \oplus 1 \oplus 0 \\
&= 1 \\
p_2 &= B_7 \oplus B_6 \oplus B_3 \oplus B_2 \\
&= 0 \oplus 0 \oplus 0 \oplus 1 \\
&= 1 \\
p_1 &= B_7 \oplus B_5 \oplus B_3 \oplus B_1 \\
&= 0 \oplus 1 \oplus 0 \oplus 1 \\
&= 0
\end{aligned}$$

Therefore, there is an error in bit $p_4 p_2 p_1 = 110_2 = 6$. The error-corrected codeword is then obtained by flipping the bit at index 1 giving $B' =$ `0110011`. The original letter is then $B'_7 B'_6 B'_5 B'_3 = 0110$ which corresponds to "G."

Decoding the other letters similarly, we the word is "GOAL," and there are errors at indices 6, 5, 7, 2, respectively. □