Coding and cryptography

Weeks 1 and 2 (2021-2022)

Problems.

1. (Exercises 1.3.7 and 1.3.8) Find the maximum number of codewords of length $n = 4$ in a code in which any single error can be detected. What about for general n?

2. (Example 1.3.2) Consider the code $C = \{000000, 010101, 101010, 111111\}$. This is a repetition code. Show that C can detect any error of weight at most 2. Show that C can correct any error of weight 1.

3. Consider the code C whose codewords are obtained by repeating a word from $\{0,1\}^m$ r times, so that every codeword has length rm. Show that C can detect any error of weight $r-1$ and that there is at least one error of weight r that it cannot detect. Show also that C can correct any error of weight $\lfloor (r-1)/2 \rfloor$. What is the information rate of this code?

4. Let $C = \{001, 101\}$ and $p = 0.9$. Calculate $\theta_p(C, 001)$ and $\theta_p(C, 101)$.

5. Let $C = \{000000, 110000, 111111\}$. For each word w in $X = \{010100, 111100, 110100, 111110\}$ find the nearest neighbour in C. If we have a channel with reliability p, then for v in C and w in X find $\phi_p(v, w)$, the probability that w is received when v is sent over the channel.

6. Let $C = \{00101, 11011, 10100, 10010\}$. Find the Hamming distance $d(C)$.

7. Let C be the code consisting of all words of length n with even number of 1's. What is the size of C? Find the Hamming distance $d(C)$.

8. Let $C = \{000000, 010101, 101010, 111111\}$. Find the Hamming distance $d(C)$. What is the Hamming distance of the general repetition code in Problem 3?

9. Find the dimension of code $C = \langle S \rangle$ for the following S. Also find a generating matrix and a parity check matrix for these codes.

   (a) $S = \{000, 111\}$.

   (b) $S = \{1101, 1110, 1011\}$.

   (c) $S = \{1100, 1010, 1001, 0101\}$.

10. Let H be the matrix consisting of $2^r - 1$ distinct non-zero rows of length r. Show that the columns of H are linearly independent. Find the dimension of the code whose parity check matrix is H.

11. Find the distance of the codes in Problems 9 and 10.

12. Consider the code C for which the parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

    (the case $r = 3$ in Problem 10). What is the most likely codeword sent if we receive 1101101?

13. Let C be a linear code with $d = d(C)$ and u be a word in K^n such that $wt(u) \leq \lfloor (d-1)/2 \rfloor$. Show that u is the unique coset leader of $u + C$.

14. (Exercise 2.11.20) Let C be the code with parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Decode the following words: $110100, 111111, 101010$ and 000110.

15. Let C be a code of length 4 and distance $d = 3$. Show that the Hamming bound gives $|C| \leq 3$. Show that we in fact have $|C| \leq 2$.