1. (10 marks) **Distance**
If x_1 and x_2 are binary n-tuples, then $x_1 + x_2$ denotes the bitwise modulo 2 sum of x_1 and x_2. For example, $000111 + 011011 = 011100$.

(a) Let C be a binary $[n, M]$-code with distance d. Let $x \in \{0,1\}^n$, and let $C + x = \{c + x \ : \ c \in C\}$. Prove that the distance of $C + x$ is also d.

Proof. Suppose C is a binary $[n, M]$-code with distance d. That is, $C = \{c_1c_2\cdots c_n : c_i \in \{0,1\}, 1 \leq i \leq n\}$ where $|C| = M$. Observe that when adding x to each codeword, where $x \in \{0,1\}^n$, each codeword will differ in the exact same index i, $\forall i \in \{1, \ldots, n\}$ (that is, the indices where any two codewords were different before adding x, will still be different after adding x).

Suppose $d(C_1 = c_1c_2\cdots c_n, C_1' = c_1'c_2'\cdots c_n') = d$, and suppose that C_1 and C_1' differ in index $i = 1$, (i.e. $c_1 \neq c_1'$).

<u>Case 1</u>

$c_1 = 1$, $c_1' = 0$, and $x_1 = 1$. We get that $c_1 + x_1 = 0$, and $c_1' + x_1 = 1$. Thus, they still differ in the same index before and after being added by x (or x_1).

<u>Case 2</u>

$c_1 = 1$, $c_1' = 0$, and $x_1 = 0$. We get that $c_1 + x_1 = 1$, and $c_1' + x_1 = 0$. Thus, they still differ in the same index before and after being added by x (or x_1).

Since $d(c_1, c_1') = d(c_1', c_1)$, we can easily swap c_1 with c_1' in each case above and the result will be the same. Also, we can do this for all M codewords to each index (i.e. $\binom{M}{2}$ comparisons for each pair of codewords, and $\binom{n}{2}$ extra comparisons with Case 1 and Case 2). Thus, $d(C) = d(C + x) = d$ as the difference between any two codewords will be the exact same after adding x as the indices where the difference is obtained will be the same. $\square$

(b) Construct a binary $[8, 4]$-code with distance 5, or prove that no such code exists.

$C = \{c_1 = 00000000,\ c_2 = 11111000,\ c_3 = 10101111,\ c_4 = 01010111\}$.

We have $\binom{M}{2} = \binom{4}{2} = 6$ comparisons.

1. $d(c_1, c_2) = 5$
2. $d(c_1, c_3) = 6$
3. $d(c_1, c_4) = 5$
4. $d(c_2, c_3) = 5$
5. $d(c_2, c_4) = 6$
6. $d(c_3, c_4) = 5$

Thus, we have constructed a binary $[8, 4]$-code with $d(C) = 5$.

(c) Construct a binary $[7, 3]$-code with distance 5, or prove that no such code exists.

We will prove that no such code exists. Suppose $C = \{c_1,\ c_2,\ c_3\}$ where c_1, c_2, c_3 are all codes of length 7. Suppose that $d(C) \geq 5$ is attained by at least one pair of codewords, c_1 and c_3. We try all possible cases.

<u>Case 1</u> $d(c_1, c_3) = 5$

We know that c_1 and c_3 differ in five indices, and are the same in two indices. We immediately see that we can pick c_2 to be different in two indices (the same indices where c_1 and c_3 were the same). Now c_2 has five indices left to pick. If we were to pick c_2 to be different in three more indices when compared to c_1 (to get $d(c_1, c_2) = 5 \geq 5$), then we only have two more indices to select to be different when compared to c_3 (meaning we would get $d(c_2, c_3) = 4 < 5 \implies d(C) = 4 \neq 5$). Thus, no such $[7, 3]$-code where $d(C) = 5$ can exist when $d(c_1, c_3) = 5$.

<u>Case 2</u> $d(c_1, c_3) = 6$

We know that c_1 and c_3 differ in six indices, and are the same in one index. We immediately see that we can pick c_2 to be different in one index (the same index where c_1 and c_3 were the same). Now c_2 has six indices left to pick. If we were to pick c_2 to be different in four more indices when compared to c_1 (to get $d(c_1, c_2) = 5 \geq 5$), then we only have two more indices to select to be different when compared to c_3 (meaning we would get $d(c_2, c_3) = 3 < 5 \implies d(C) = 3 \neq 5$). Thus, no such $[7, 3]$-code where $d(C) = 5$ can exist when $d(c_1, c_3) = 6$.

<u>Case 3</u> $d(c_1, c_3) = 7$

We know that c_1 and c_3 differ in seven indices. If we were to pick c_2 to be different in five indices when compared to c_1 (to get $d(c_1, c_2) = 5 \geq 5$), then we only have two more indices to select to be different when compared to c_3 (meaning we would get $d(c_2, c_3) = 2 < 5 \implies d(C) = 2 \neq 5$). Thus, no such $[7, 3]$-code where $d(C) = 5$ can exist when $d(c_1, c_3) = 7$.

Thus, no such $[7, 3]$-code exists with $d(C) = 5$.