Mechanical Questions: *(1 point each)*

Q 1. Given a binary code with length 10, if probability of a bit arriving correctly is 0.7, what is the probability that it will be received with two errors?
Q 2. Give the rate of 2-D parity check code
Q 3. The **transpose** of the following matrix is not a generator matrix for any linear code: why?

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

Q4. Transpose of the following matrix generates a code. Determine the code

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

Some thinking required:

Q 5. *(2 points)* Show that the q-ary repetition code C is a linear code, where q is prime.

Q 6. *(2 points)* Given a p-length message, where p is prime, you insist on using the 2-D parity check code as illustrated in example 1.3 to encode your message. You choose to make your matrix with m row and n columns. Since *mn* cannot equal *p*, you can pad the message with *mn - p* zeroes so it fits nicely into your matrix. You choose m and n optimally to minimize the number of parity bits you will have to add. What is the minimum possible number of parity bits you could add?

Q 7. *(2 points)* In the 2-D parity check, how would we correct an error in one of the parity bits?

Q 8. (5 points) Show that A linear q-ary code of length n is cyclic if and only if *C* satisfies the following two conditions:

1. If *a(x)* and *b(x)* are code polynomials in *C*, then *a(x) - b(x)* ∈ *C*
2. If *a(x)* is a code polynomial in *C* and *r(x)* is any polynomial of degree less than n, then *r(x)a(x)* ∈ *C*

Q 9. (4 points) Prove that in a binary symmetric channel* with p < ½, maximum likelihood decoding* is equivalent to nearest neighbor decoding.

*A symmetric channel is one in which every symbol has same probability of error and if there's an error, the probability of it being changed to any other symbol is equally likely. All errors are independent of each other.

A *binary symmetric channel* has two probabilities:

$$\begin{aligned}\Pr[1 \text{ received} \mid 0 \text{ was sent}] &= \Pr[0 \text{ received} \mid 1 \text{ was sent}] = p \\ \Pr[1 \text{ received} \mid 1 \text{ was sent}] &= \Pr[0 \text{ received} \mid 0 \text{ was sent}] = 1 - p\end{aligned}$$

The probability p is called the crossover probability.

*Maximum likelihood decoding is -

Definition 1.12 *Let C be a code of length n over an alphabet A. The* maximum likelihood decoding *rule states that every $x \in A^n$ is decoded to $c_x \in C$ when*

$$\Pr[x \text{ received} \mid c_x \text{ was sent}] = \max_{c \in C} \Pr[x \text{ received} \mid c \text{ was sent}]$$

Q10. (6 points) Sometimes we can start with a known binary linear code and append an overall parity check digit to increase the minimum distance of a code. Suppose C is a linear (n, M, d) code. Then we can construct a code C′, called the extended code of C , by appending a parity check bit to each codeword x ∈ C to obtain a codeword x′ ∈ C′ This ensures that every codeword in the extended code has even Hamming weight.

Prove that C′ is a linear code, and that the minimum distance of C′ is d + 1 if d = d(C) is odd, and otherwise it is d.