ECE 259A: Solutions to the Midterm Exam

Problem 1.

a. We first use elementary row operations to put the generator matrix of C in systematic form:

\[
[I | A] = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

The parity-check matrix can then be found as \( H = [-A^t | I] \), which in this case gives:

\[
H = \begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

b. Since \( H \) contains rows of weight 2, it is easy to see that the minimum distance of \( C \) is 2.

c. Straightforward computation shows that the syndrome of \( y \) is \( Hy^t = (0 1 1 1 1 0 0 1) \).

d. On a binary symmetric channel, the most likely transmitted codeword is the one closest to \( y \). As the syndrome of \( y \) is nonzero, it is not, itself, a codeword. On the other hand, observe that the syndrome of \( y \) is precisely the first column of \( H \). Hence complementing the first bit in \( y \) produces the codeword \( x = (0 0 1 1 0 0 1 1 0 0 1 0) \) at distance 1 from \( y \). This codeword is the most likely.

Problem 2.

First, let us puncture \( C \) by deleting the last position in every codeword. Let \( C' \) denote the resulting linear code. It has length \( n - 1 \), dimension \( k \) (why couldn’t it be \( k - 1 \)?) and distance \( d' = d - 1 \) or \( d' = d \). Next, we produce \( C'' \) by adding an overall parity-check position to \( C' \). Then all the codewords of \( C'' \) have even weight by construction, and it remains to show that the minimum distance of \( C'' \) is \( d \). If \( d' = d - 1 \) then it is odd, so adding an overall parity-check increases the distance by 1. On the other hand, if \( d' = d \) then it is even, so adding an overall parity-check does not change the distance.

Problem 3.

a. Write

\[
H = \begin{bmatrix}
X_{1,1} & X_{1,2} & \cdots & X_{1,n} \\
X_{2,1} & X_{2,2} & \cdots & X_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
X_{r,1} & X_{r,2} & \cdots & X_{r,n}
\end{bmatrix}
\]

where \( X_{1,1}, X_{1,2}, \ldots, X_{r,n} \) are \( r n \) independent \( \text{Ber}(\frac{1}{2}) \) random variables that correspond to the \( r n \) coin tosses. Suppose \( wt(v) = w \) and let \( \{i_1, i_2, \ldots, i_w\} \) denote the nonzero positions in the
vector \( v \). Clearly \( v \in C \) if and only if this vector satisfies all the \( r \) parity checks defined by the matrix \( H \), namely:

\[
\begin{align*}
X_{1,j_1} + X_{1,j_2} + \cdots + X_{1,j_r} &= 0 \\
X_{2,j_1} + X_{2,j_2} + \cdots + X_{2,j_r} &= 0 \\
& \vdots \\
X_{r,j_1} + X_{r,j_2} + \cdots + X_{r,j_r} &= 0
\end{align*}
\]

(1)

where all the additions are modulo 2. Since \( X_{1,1}, X_{1,2}, \ldots, X_{r,n} \) are independent \( \text{Ber}(\frac{1}{2}) \) random variables, each of the \( r \) parity-checks in (1) is equally likely to evaluate to 0 or 1. Thus the probability that \( v \) satisfies any given parity-check equation in (1) is \( 1/2 \), and the probability that \( v \) satisfies all \( r \) of them is \( 1/2^r \). It follows that \( \Pr \{ v \in C \} = 2^{-r} \) for any nonzero vector \( v \).

b. We have \( d(C) \geq d \) if and only if none of the nonzero vectors of weight \( \leq d - 1 \) belongs to \( C \). Let us define:

\[
S(d-1) \overset{\text{def}}{=} \left\{ v \in \mathbb{F}_2^n \ : \ 0 < \text{wt}(v) \leq d - 1 \right\}
\]

Then

\[
\Pr\{ d(C) \geq d \} = \Pr\{ \text{none of the vectors in } S(d-1) \text{ belongs to } C \} = 1 - \Pr\{ \text{at least one of the vectors in } S(d-1) \text{ belongs to } C \} \geq 1 - \sum_{v \in S(d-1)} \Pr\{ v \in C \} = 1 - \frac{|S(d-1)|}{2^r} = 1 - 2^{-r} \sum_{i=1}^{d-1} \binom{n}{i} \tag{2}
\]

c. Obviously, \( \dim(C) = n - \text{rank}(H) \geq n - r = nR \) for all possible realizations of the matrix \( H \). Thus the event that \( \dim(C) \geq nR \) occurs with probability 1, and it remains to deal with the event that the minimum distance of \( C \) is at least \( d = \lfloor \delta n \rfloor + 1 \). Combining the fact that for all \( n \),

\[
\sum_{i=1}^{d-1} \binom{n}{i} \leq 2^{nH_2(\frac{d-1}{n})} \leq 2^{nH_2(\delta)}
\]

with the bound in (2), we conclude that

\[
\Pr\{ d(C) \geq d \} \geq 1 - \frac{2^{nH_2(\delta)}}{2^r} = 1 - \frac{2^{nH_2(\delta)}}{2n(1-R)} = 1 - \frac{1}{2n(1-R-H_2(\delta))} \tag{3}
\]

For any \( \delta \) such that \( H_2(\delta) < 1 - R \), the exponent of 2 in (3) is positive and therefore \( \Pr\{ d(C) \geq d \} \) approaches 1 (exponentially fast) as \( n \to \infty \).

Problem 4.

a. Assume to the contrary that the covering radius of \( C \) is \( \rho(C) \geq d \). Then there is a vector \( v \in \mathbb{F}_2^n \) at distance \( \geq d \) from \( C \). Adjoining this vector to \( C \), we obtain an \( (n, M+1, d) \) code \( C' = C \cup \{ v \} \). But this contradicts the given assumption that an \( (n, M+1, d) \) binary code does not exist.

b. Let \( H = [h_1, h_2, \ldots, h_n] \) be an \( r \times n \) parity-check matrix for \( C \), and let \( s \) be an arbitrary nonzero vector in \( \mathbb{F}_2^n \), where \( r = n - k \). Consider the \( r \times (n+1) \) matrix \( H' = [h_1, h_2, \ldots, h_n, s] \) and let \( C' \) be the corresponding binary linear code. It is easy to see that the length of \( C' \) is \( n + 1 \) and its dimension is \( (n+1) - \text{rank}(H') = (n+1) - r = k + 1 \). Since an \( (n+1,k+1,d) \) code does not
exist, the minimum distance of \( C' \) is at most \( d - 1 \). Consequently, there exists a set \( S \) of at most \( d - 1 \) linearly dependent columns of \( H' \). That is, \( S \subset \{1, 2, \ldots, n, n+1\} \) with

\[
\sum_{i \in S} h_i = 0 \quad \text{and} \quad |S| \leq d - 1
\]  

(4)

where we have adopted the convention \( h_{n+1} \overset{\text{def}}{=} s \). We claim that the last column \( h_{n+1} = s \) is necessarily included in \( S \). Indeed, otherwise (4) would imply that some \( \leq d - 1 \) columns of the original matrix \( H \) are linearly dependent, which contradicts the fact that the minimum distance of \( C \) is \( d \). Consequently, we can define the set \( S' = S \setminus \{n+1\} \) and re-write (4) as

\[
s = \sum_{i \in S'} h_i \quad \text{with} \quad |S'| \leq d - 2
\]  

(5)

This implies that \( s \) is a linear combination of at most \( d - 2 \) columns of \( H \). Since this is true for any nonzero vector \( s \) in \( \mathbb{F}_2^r \), the covering radius of \( C \) is at most \( d - 2 \).