ECE 259A: Midterm Exam

Instructions: There are four problems, weighted as shown below. The exam is open book and open notes: you may use any auxiliary material that you like as long as it is on paper.

Good luck!

Problem 1. (20 points)

Let $C$ be the binary linear code generated by the following matrix

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

a. Write down a parity-check matrix for this code.

b. What is the minimum distance of $C$? What is the minimum distance of $C^\perp$, the dual code of $C$?

c. There are eight possible syndromes with respect to the parity-check matrix found in part (a). For each syndrome, write down the corresponding coset leader(s). If the coset leader is not unique, list all the vectors of minimum weight in the corresponding coset.

d. If the vector $(1 \ 0 \ 0 \ 0 \ 1 \ 1)$ is observed at the output of a binary symmetric channel, what is the most likely transmitted codeword of $C$? Is the answer unique?

Problem 2. (30 points)

Let $H_m$ denote the binary Hamming code of length $2^m - 1$, and assume that the columns of the parity-check matrix for $H_m$ are binary representations of the integers $1, 2, \ldots, 2^m - 1$, in this order. Further, let $C_m$ be the $(n, k, d)$ dual code of $H_m$. This problem is concerned with the properties of $C_m$.

a. What are the length $n$ and dimension $k$ of $C_m$? For $m = 4$, write down a generator matrix for $C_m$.

b. Show that $C_2 = \{(000), (011), (101), (110)\}$, whereas for $m \geq 3$, the code $C_m$ can be defined recursively as follows:

$$
C_m = \bigcup \{ (x|0|x) : x \in C_{m-1} \} \bigcup \{ (x|1|x) : x \in C_{m-1} \}
$$

where $\overline{x}$ denotes the complement of $x$ and $(\cdot|\cdot)$ denotes vector concatenation.

c. What is the minimum distance $d$ of $C_m$?  

Hint: Use part (b) and induction on $m$.  

**Problem 3.** (25 points)

Let $C$ be an $(n, k, d)$ binary linear code with *all nonzero codewords having the same weight*. Further assume that $k \geq 3$ and that the minimum distance $d^\perp$ of the dual code of $C$ is at least 2.

**a.** Express the minimum distance $d$ of $C$ in terms of $n$ and $k$.

*Hint:* Recall our proof of the Plotkin bound.

**b.** Here is one interpretation of the Gilbert-Varshamov bound: given $n$ and $d$, the Gilbert-Varshamov bound predicts the existence of binary linear codes of a certain size $M(n, d)$. Show that the code $C$ beats the Gilbert-Varshamov bound — that is, $|C|$ exceeds the size $M(n, d)$ predicted by the Gilbert-Varshamov bound for its parameters $n$ and $d$.

**Problem 4.** (25 points)

In this problem, we consider an $(n, k, d)$ binary linear code $C$ defined in terms of its generator matrix $G$.

Let $g_1, g_2, \ldots, g_n$ denote the columns of $G$, and let $v_i = (0 \cdots 010 \cdots 0)^t$ denote a column vector of length $k$ and weight one, with the single nonzero at position $i$. We say that a subset $R = \{j_1, j_2, \ldots, j_m\}$ of $\{1, 2, \ldots, n\}$ is a recovery set for the $i$-th information bit if $g_{j_1} + g_{j_2} + \cdots + g_{j_m} = v_i$.

**a.** Let $x = (u_1, u_2, \ldots, u_k)G$ be a codeword of $C$, and suppose $R = \{j_1, j_2, \ldots, j_m\}$ is a recovery set for the $i$-th information bit. Prove that $u_i = x_{j_1} + x_{j_2} + \cdots + x_{j_m}$.

**b.** Suppose that $G$ is such that there exist seven disjoint recovery sets $R_1, R_2, \ldots, R_7$ for the first information bit $u_1$. However, you do not have access to the codeword $x = uG$. Rather, you have access to $y = x + e$ where $\text{wt}(e) \leq 3$. How would you recover $u_1$?

**c.** Now suppose that $G$ is such that for every information bit $u_1, u_2, \ldots, u_k$, there exist some $r$ disjoint recovery sets. Give a lower bound on the minimum distance $d$ of $C$ in terms of $r$. 