E2 205 Midterm Exam Solutions

1. [10 marks] A binary linear code $C$ has parity-check matrix

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

A codeword $c = (c_1c_2c_3c_4c_5) \in C$ is picked uniformly at random (i.e., all codewords are, a priori, equally likely) and transmitted across a binary symmetric channel with cross-over probability $p = 2/5$. Suppose that $y = (1 1 1 1 1)$ is the received word.

(a) What are the dimension and minimum distance of $C$?

**Solution:** Clearly, the rank of $H$ is 2, since it has a $2 \times 2$ identity matrix as a submatrix. Hence, $\dim(C) = n - \text{rank}(H) = 5 - 2 = 3$.

All columns of $H$ are nonzero, so $C$ has no codewords of weight 1. The first and last columns of $H$ are identical, so 10001 is a codeword. Hence, $d_{\text{min}}(C) = 2$.

(b) Decode $y = (1 1 1 1 1)$ using the maximum a posteriori (MAP) decoding rule, i.e., determine a $c \in C$ that maximizes $\Pr[c | y = 11111]$. You may implement MAP decoding in any of its equivalent forms, but you must provide enough detail to verify the correctness of your decoder.

**Solution:** Since all codewords are, a priori, equally likely, MAP decoding is equivalent to maximum-likelihood (ML) decoding. Moreover, since the channel is a binary symmetric channel with bit-flip probability $p < 1/2$, ML decoding is equivalent to minimum distance decoding. We can implement minimum distance decoding using coset leaders and syndromes. The syndrome corresponding to the received word $y$ is $Hy^T = [1 \ 1]^T$. There is a unique vector $e$ of weight 1 that gives rise to this syndrome, namely, $e = [0 \ 0 \ 1 \ 0 \ 0]$, so this is the vector of least weight within the coset associated with the syndrome $[1 \ 1]^T$. Hence, minimum distance decoding produces the codeword $y - e = (1 \ 0 \ 0 \ 1 \ 1)$.

2. [10 marks] A certain application requires the design of a binary linear code of blocklength $n = 10$ that can correct all error vectors in the set $\mathcal{E}_1 \cup \mathcal{E}_2$, where

- $\mathcal{E}_1$ consists of all binary vectors of length 10 and Hamming weight at most 1;
- $\mathcal{E}_2$ consists of all binary vectors of length 10 and Hamming weight equal to 2 or 3, in which all 1s occur in the first five coordinates (e.g., 0100100000 and 1101000000, but not 1001001000).

(a) Let $I_5$ denote the $5 \times 5$ identity matrix. Design a $5 \times 5$ matrix $A$ such that the [10, 5] binary linear code $C$ with parity-check matrix $H = [I_5 \ A]$ has the required error-correcting capability under syndrome decoding.

**Solution:** For all single-error patterns to be correctable, $H$ must have all columns distinct and nonzero. Since $I_5$ contains all the possible columns of weight 1, $A$ cannot have any columns of weight 0 or 1. The error vectors in $\mathcal{E}_2$ result in syndromes of weight 2 or 3. To keep these distinct from the syndromes
arising from error vectors in $\mathcal{E}_1$, $A$ must not have columns of weight 2 or 3 either. Thus, we can populate $A$ with columns of weight 4 and 5 only to obtain a code with the required error-correction capability under syndrome decoding. For instance, we can take

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix},$$

resulting in

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

(b) Does there exist a $[10, 6]$ binary linear code with the required error-correcting capability under syndrome decoding? If yes, give an explicit construction; otherwise, argue why such a code cannot exist. [5]

**Solution:** The number of error vectors that must be corrected is $|\mathcal{E}_1| + |\mathcal{E}_2|$. Note that $\mathcal{E}_1$ consists of 1 vector of weight 0 and 10 vectors of weight 1, so $|\mathcal{E}_1| = 11$. $\mathcal{E}_2$ contains $\binom{5}{2} = 10$ vectors of weight 2, and $\binom{5}{3} = 10$ vectors of weight 3; hence, $|\mathcal{E}_2| = 20$. Thus, $|\mathcal{E}_1| + |\mathcal{E}_2| = 11 + 20 = 31$. A $[10, 6]$ binary linear code has only $2^{10-6} = 16$ cosets. Hence, there does not exist a $[10, 6]$ binary linear code with the required error-correcting capability under syndrome decoding.


(a) By the Gilbert-Varshamov bound, there exists a double-error-correcting binary linear code of length 11 and dimension at least _____. [2]

**Answer:** For the binary alphabet, the Gilbert-Varshamov (GV) bound states that if \[ \sum_{\ell=0}^{d-2} \binom{n-1}{\ell} < 2^{n-k}, \] then there exists an $[n, k]$ binary linear code with minimum distance at least $d$. In our case, we have $n = 11$ and for the code to be double-error-correcting, we take $d = 5$. The left-hand side of the inequality above then becomes

$$\binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3} = 176.$$  

The largest value of $k$ for which the inequality $176 < 2^{11-k}$ holds is $k = 3$. Thus, the GV bound guarantees the existence of a double-error-correcting binary linear code of length 11 and dimension at least 3.

(b) Let $C$ be a maximum distance separable (MDS) code of length $n$ and dimension $k$. What is the minimum distance of the dual code $C^\perp$? [2]

**Answer:** We have seen in Homework Assignment 3 that if $C$ is MDS, then so is its dual code $C^\perp$. The code $C^\perp$ has blocklength $n$ and dimension $n-k$. Since it is MDS, its minimum distance is $n - (n-k) + 1 = k + 1$. 
(c) Give the definition of the characteristic of a finite field. \[ \text{Answer: The characteristic } \chi(F) \text{ of finite field } F \text{ is the least positive integer } m \text{ such that the sum of } m \text{ 1’s is equal to 0.} \]

(d) Find the multiplicative inverse of \( x \) in the field \( \mathbb{F}_2[x]/f(x) \), where \( f(x) \) is the irreducible (over \( \mathbb{F}_2 \)) polynomial \( x^3 + x + 1 \)? \[ \text{Answer: Note that } f(x) = x(x^2+1)+1, \text{ from which we obtain } x(x^2+1) = 1+f(x). \text{ Reducing modulo } f(x), \text{ we obtain } 1 = x(x^2 + 1) \text{ in the field } \mathbb{F}_2[x]/f(x), \text{ which shows that } x^2 + 1 \text{ is the multiplicative inverse of } x \text{ in the field.} \]

(e) How many primitive elements does a field of size \( q = 27 \) have? \[ \text{Answer: Fix a primitive element } \alpha \in \mathbb{F}_{27}. \text{ The nonzero elements of } \mathbb{F}_{27} \text{ are all expressible as } \alpha^k, \text{ where } k = 1, 2, \ldots, 26. \text{ From a problem in Homework Assignment 4, we have that if } \text{ord}(\alpha) = q - 1, \text{ then } \text{ord}(\alpha^k) = \frac{q-1}{\gcd(q-1,k)}. \text{ Hence, } \alpha^k \text{ is also primitive iff } k \text{ is co-prime with } q - 1 = 26. \text{ The integers } k \text{ between 1 and 26 that are co-prime with 26 are the odd integers other than 13. There are 12 such: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Hence, there are 12 primitive elements in } \mathbb{F}_{27}. \]

4. [10 marks] Consider the binary linear code \( C \) of length 15 with parity check matrix

\[
H = \begin{bmatrix}
1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12}
\end{bmatrix},
\]

where \( \alpha \) is the element \((0100)\) in \( \mathbb{F}_{16} = \mathbb{F}[x]/(x^4 + x^3 + 1) \), the field constructed in class. Thus, each column of \( H \) is of the form \( \begin{bmatrix} \alpha^j \\ \alpha^{3j} \end{bmatrix} \). It is known that \( \alpha^5 \) is a root of the polynomial \( x^2 + x + 1 \).

(a) Consider a binary error vector \( e = (e_0, e_1, e_2, \ldots, e_{14}) \) of Hamming weight equal to 3, with \( e_j = e_{j+5} = e_{j+10} = 1 \), for some \( j \in \{0, 1, 2, 3, 4\} \). Compute the corresponding syndrome \( s = He^T \). \[ \text{Solution: Since } \alpha^5 \text{ is a root of the polynomial } x^2 + x + 1, \text{ we have } \alpha^{10} + \alpha^5 + 1 = 0. \text{ The syndrome obtained from the given error vector } e \text{ is } \]

\[
s = He^T = \begin{bmatrix}
\alpha^j + \alpha^{5+j} + \alpha^{10+j} \\
\alpha^{3j} + \alpha^{3(5+j)} + \alpha^{3(10+j)}
\end{bmatrix} = \begin{bmatrix}
\alpha^j(1 + \alpha^5 + \alpha^{10}) \\
\alpha^{3j}(1 + \alpha^{15} + \alpha^{30})
\end{bmatrix} = \begin{bmatrix}
0 \\
\alpha^{3j}
\end{bmatrix},
\]

where we have used \( 1 + \alpha^5 + \alpha^{10} = 0 \) and \( 1 + \alpha^{15} + \alpha^{30} = 1 + 1 + 1 = 1 \).

(b) What is the least integer \( w \) such that a binary error vector of Hamming weight \( w \) gives rise to the syndrome \( s \) in part (a)? You must justify your answer. \[ \text{Solution: Note that } w \geq 1 \text{ since the vector of weight 0 results in the syndrome } [0 \ 0]^T. \text{ Moreover, since the entries in the first row of the } H \text{ matrix are all nonzero and distinct, a binary error vector of Hamming weight 1 or 2 cannot result in a syndrome with first entry 0; hence } w \geq 3. \text{ The error vector } e \text{ given in part (a) has weight equal to 3; hence, } w = 3. \]