Introduction to Coding Theory - Spring 2025
Assignment 3
Submission Deadline: 7 March

1. Consider a binary linear block with a parity check matrix given by

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

   Suppose a codeword is transmitted over BSC(p) and the received vector is $\mathbf{y}$. Use standard array decoding to estimate the transmitted codeword in the following cases:

   (a) $p = 0.2$, $\mathbf{y} = [0, 1, 0, 0, 1]$

   (b) $p = 0.9$, $\mathbf{y} = [1, 0, 1, 0, 1]$ (When $p < 0.5$, we find the closest codeword to the received vector. Is that a good strategy in this case?)

2. Consider an $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_2$, with $d = 2t + 1$, for some $t \in \mathbb{N}$. Suppose that in the standard array corresponding to $\mathcal{C}$, there are no coset leaders of weight strictly larger than t. What, then, is the probability of error under standard array decoding, when $\mathcal{C}$ is used over a BSC with cross-over probability $p < 0.5$?

3. Show that the only possibly binary MDS linear codes of length n are $\{0, 1\}^n$, the repetition code, and the single parity-check code.

   [**Hint:** Assume that the parity-check matrix H is of the form $[I_{n-k}|A]$, for some A. Use the fact that the minimum distance, d, is the largest integer such that every set of $d - 1$ columns of H is linearly independent, to obtain the structure of A.]

4. It is desired to construct a $[6, 4]$ linear, binary block code having as large a minimum distance d as possible. Which of the two bounds, the Hamming bound or the Singleton bound, imposes the tighter restriction on d, i.e., which of the two bounds yields a smaller upper bound on d?

5. Use the bounds covered in class to determine the best upper and lower bounds on the maximum size of a binary block code of length $n = 15$ and minimum distance $d = 7$.

6. Prove that the minimum distance of a perfect code must be odd.

7. Let $\mathcal{A}$ be any alphabet (i.e., a set of possible elements involved in the transmission) containing q elements. Let $\mathcal{B}_d(\mathbf{v})$ denote the set of all vectors in a Hamming ball of radius d around the vector $\mathbf{v}$, i.e.,

$$\mathcal{B}_d(\mathbf{v}) = \{\mathbf{u} \in \mathcal{A}^n : d_H(\mathbf{v}, \mathbf{u}) \leq d\}.$$

Show that, there exists a code $\mathcal{C}^* \subseteq \mathcal{A}^n$, such that the following is true:

$$|\mathcal{C}^*| \geq \frac{q^n}{|\mathcal{B}_{t'}|},$$

where $t' = d_{\min}(\mathcal{C}^*) - 1$. [Hint: Consider $\mathcal{C}^*$ to be the maximal (containing most codewords) code with minimum distance $d_{\min}(\mathcal{C})$. Draw balls of radius $d_{\min}(\mathcal{C}) - 1$ around all the codewords. Show that there will be a contradiction with the maximality of $\mathcal{C}^*$, if some vector lies outside the union of all these balls. Hence prove the result.]