University of California San Diego Fall 2021

ECE 259A: Solutions to the Midterm Exam

Problem 1.

a. We first use elementary row operations to put the generator matrix of $\mathbb{C}$ in systematic form:

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

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

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

b. Since H contains rows of weight 2, it is easy to see that the minimum distance of $\mathbb{C}^\perp$ is 2.

c. Straightforward computation shows that the syndrome of $\underline{y}$ is $H\underline{y}^t = (0,1,1,1,1,0)^t$.

d. On a binary symmetric channel, the most likely transmitted codeword is the one closest to $\underline{y}$ in the Hamming metric. Since the syndrome of $\underline{y}$ is non-zero, it is not, itself, a codeword. On the other hand, we observe that the syndrome of $\underline{y}$ is precisely the first column of H. Hence complementing the first bit in $\underline{y}$ produces the codeword $\underline{x} = (0,0,1,1,0,0,1,1,0,0)$ at distance 1 from $\underline{y}$. This codeword is the most likely.

Problem 2.

Let $\underline{x}_1, \underline{x}_2$ be two arbitrary, not necessarily distinct, codewords of $\mathbb{C}$. We have

$$\mathrm{wt}(\underline{x}_1 + \underline{x}_2) \;=\; \mathrm{wt}(\underline{x}_1) + \mathrm{wt}(\underline{x}_2) - 2\mathrm{wt}(\underline{x}_1 \wedge \underline{x}_2) \qquad (*)$$

where $\underline{x}_1 \wedge \underline{x}_2$ is the vector that has 1's at those positions where both $\underline{x}_1$ and $\underline{x}_2$ have 1's. Note that $\underline{x}_1 \cdot \underline{x}_2 = \mathrm{wt}(\underline{x}_1 \wedge \underline{x}_2) \bmod 2$, so that $\underline{x}_1$ and $\underline{x}_2$ are orthogonal to each other if and only if $\mathrm{wt}(\underline{x}_1 \wedge \underline{x}_2)$ is even. Since $\underline{x}_1 + \underline{x}_2 \in \mathbb{C}$ by linearity and $\mathbb{C}$ is doubly-even, it follows that both sides of $(*)$ are divisible by 4. Thus 4 divides $2\mathrm{wt}(\underline{x}_1 \wedge \underline{x}_2)$, which implies that $\mathrm{wt}(\underline{x}_1 \wedge \underline{x}_2)$ is even.

Hence every codeword of $\mathbb{C}$ is orthogonal to all the codewords of $\mathbb{C}$, which means that $\mathbb{C} \subseteq \mathbb{C}^\perp$. Since $\mathbb{C}^\perp$ is also doubly-even, the same argument shows that $\mathbb{C}^\perp \subseteq (\mathbb{C}^\perp)^\perp = \mathbb{C}$. Having established that $\mathbb{C} \subseteq \mathbb{C}^\perp$ and $\mathbb{C}^\perp \subseteq \mathbb{C}$, we can conclude that $\mathbb{C} = \mathbb{C}^\perp$.

Problem 3.

This is a generalization of the Gilbert bound from Problem Set #2. Define $\mathcal{S}(\underline{x}) = \underline{x} + \mathcal{E} = \{\underline{x} + \underline{e} : \underline{e} \in \mathcal{E}\}$. Then, for any $\mathbb{C} \subset \mathbb{F}_2^n$, we have

$$\mathcal{N} \stackrel{\text{def}}{=} \frac{\sum_{\underline{x}\in\mathbb{F}_2^n} |\mathcal{S}(\underline{x}) \cap \mathbb{C}|}{2^n} = \frac{M\,|\mathbb{C}|}{2^n}$$

Indeed, count in two ways the number $2^n\mathcal{N}$ of codewords of $\mathbb{C}$ contained in the sets $\mathcal{S}(\underline{x})$, where $\underline{x}$ runs through all the points in $\mathbb{F}_2^n$. The obvious way is the definition of $\mathcal{N}$. On the other hand, every codeword of $\underline{c} \in \mathbb{C}$ lies in exactly $|\mathcal{E}| = M$ such sets $\mathcal{S}(\underline{x})$, corresponding to all $\underline{x} \in (\underline{c} + \mathcal{E})$. Thus every codeword is counted exactly M times in $\sum_{\underline{x}\in\mathbb{F}_2^n} |\mathcal{S}(\underline{x}) \cap \mathbb{C}| = M|\mathbb{C}|$.

Now, given a code $\mathbb{C}$ that detects all error patterns in $\mathcal{E}$, we may assume that $\mathcal{N} \geqslant 1$. Otherwise there is at least one point $\underline{x} \in \mathbb{F}_2^n$, such that $(\underline{x} + \mathcal{E}) \cap \mathbb{C} = \varnothing$. We could then adjoin $\underline{x}$ to $\mathbb{C}$ to obtain a larger code that corrects all error patterns in $\mathcal{E}$. This process can be iterated until we obtain a code such that $\mathcal{N} = M|\mathbb{C}|/2^n \geqslant 1$, or equivalently $|\mathbb{C}| \geqslant 2^n/M$.

Problem 4.

a. Since neither of the two Golay codes is MDS, $\mathbb{C}$ is necessarily a Hamming code $\mathcal{H}_m$ and hence $d = 3$. Since the code is MDS, we have $k = n - d + 1 = n - 2$. Since the code is perfect and $t = \lfloor (d-1)/2 \rfloor = 1$, we have

$$1 + (q-1)\binom{n}{1} = q^{n-k} = q^2$$

which implies $n = (q^2-1)/(q-1) = q+1$. Thus, $n = q+1$, $k = q-1$, and $d = 3$.

b. To write down a parity-check matrix of the Hamming code $\mathcal{H}_2$ over $\mathrm{GF}(q)$, we need $n = q+1$ 2-tuples over $\mathrm{GF}(q)$ such that no two of them are linearly dependent over $\mathrm{GF}(q)$. One way to do this is as follows

$$H_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{bmatrix}$$