EC Exam
Algebraic Coding Theory
Math 525
Stephen Giang RedID: 823184070

Problem 1: Let C be the linear code with parity-check matrix H given by

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

Find the generator matrix in RREF for C. Show all working leading to your answer.

First, we can transpose H, such that:

$$H^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad RREF(H^T) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Now we have H^T in the form of $[I_4|X^T]$. This would mean we get $H = \left[\frac{I_4}{X}\right]$, such that we get $G = [X|I_5]$, such that:

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

We can verify this by seeing that $\boldsymbol{GH = 0}$

Problem 2: Let C be a linear code of length n and dimension k. Assume that C is a systematic code, that is, its generator matrix G is given by $G = [I_k|X]$, where I_k denotes the $k \times k$ identity matrix and X is a certain binary matrix. Prove that if $n - k \geq 2$, then the minimum distance of C is at most $n - k$.

Because $G = [I_k|X]$, then we get that $H = \left[\frac{X}{I_{n-k}}\right]$.

Let $k > 1$, such that X contains at least one row, r, with $wt(r) < n - k$. Suppose we had a row, R, with weight $0 \leq a \leq n - k - 1$. Then we could find the minimum distance by adding R with a rows from I_{n-k} and getting the zero element. For $a = n - k - 1$, we would need to add R with $n - k - 1$ rows of I_{n-k} to get the zero element. This means that the minimum distance of C is at most $1 + n - k - 1 = n - k$.