Math 307 Homework
September 23, 2015

1. Let $A \in \mathcal{M}_{n,m}(\mathbb{F})$ and $B \in M_{p,n}(\mathbb{F})$. Show that if $BA = 0$, then $C(A) \subseteq \ker(B)$.

For the rest of this assignment, let

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \in \mathrm{M}_{7,4}(\mathbb{F}_2)$$

be the encoding matrix and

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \in \mathrm{M}_{3,7}(\mathbb{F}_2)$$

be the parity check matrix for the Hamming code.

As we discussed in class, if $\mathbf{y} = \mathbf{Ax} \in \mathbb{F}_2^7$ is transmitted with at most one error and $\mathbf{z} \in \mathbb{F}_2^7$ is received, we can look at $\mathbf{Bz} \in \mathbb{F}_2^3$ to tell whether an error occured, and if so, in which bit the error occured.

2. Suppose that two or more errors occur. What will $\mathbf{Bz}$ look like in that case? What does this imply about the usefulness of the Hamming code for a very noisy channel?

3. It would be nice if we could do the error checking and decoding for the Hamming code linearly in one step. That is, we'd like to have a matrix $\mathbf{C} \in \mathrm{M}_{4,7}(\mathbb{F}_2)$ such that

$$\mathbf{Cz} = \mathbf{x},$$

both when $\mathbf{z} = \mathbf{y} = \mathbf{Ax}$, and whenever $\mathbf{z} = \mathbf{y} + \mathbf{e}_i$ for $i = 1, \ldots, 7$. Prove that there is no such matrix $\mathbf{C}$.

Hint: Think first about the case $\mathbf{x} = \mathbf{0}$. What can you conclude about the columns $\mathbf{Ce}_i$? Then think about when $\mathbf{x} \neq \mathbf{0}$.