Math 350
Spring, 2003

HOMEWORK #3

Do 50 points of the following problems (due 1/30/03).

25 pts. **1** Find a necessary condition on the length n so that the binary $(n, M, 3)$ code is perfect. What are the conditions for a perfect q-ary $(n, M, 3)$ code?

The fraction $\frac{2^n}{(1+\binom{n}{1})}$ must be an integer. The only way that can happen is if $n+1$ is a power of 2, or if $n = 2^x - 1$ for some x. For q-ary, the fraction $\frac{q^n}{(1+(q-1)\binom{n}{1})}$, so $n = \frac{q^x-1}{q-1}$. We will see later in the course that we can always construct perfect q-ary codes of these lengths.

25 pts. **2** Let $a, b \in Z_p$ for p a prime: show that $(a+b)^p \equiv a^p + b^p \bmod p$. Explain how that can be extended to $(a+b+\cdots+z)^p \equiv a^p+b^p+\cdots+z^p \bmod p$. Use this to show that $x^p \equiv x \bmod p$ for every $x \in Z_p$.

By the binomial theorem, $(a+b)^p \equiv a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \bmod p$. Since p is prime, each of the binomial coefficients $\binom{p}{i}$ is divisible by p (there is nothing in the denominator to divide the p), so they are all 0 mod p as required. The extension to $(a+b+\cdots+z)^p$ can be done by induction (or just an explanation of how to go from one step to the next). If we write $x = 1+1+\cdots+1$, then $x^p = (1+1+\cdots+1)^p = 1^p + 1^p + \cdots + 1^p = 1+1+\cdots+1 = x$.

25 pts., ⋆ **3** Consider the following matrix: $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Show that the set of vectors $u = (u_1, u_2, \ldots, u_7)$ that satisfy $Hu^T = (000)$ form a binary linear code. How many elements are there in this code? Use properties of the matrix H to determine the minimum distance of the code (don't just use brute force).

In terms of linear algebra, we are saying that the code is the Null Space of the matrix H. Since the rank of the matrix is 3, the dimension of the Null Space is 4, so there are $2^4 = 16$ codewords in this code. Any pair of columns are linearly independent (they are distinct, and no pair are scalar multiples of eachother), so it takes at least 3 columns added together to get 0. That tells us the minimum weight, and the minimum weight can be shown to be the minimum distance of the code. If we add the first, second, and third columns, we get 0, so 1110000 is in the code.