Pries: M467 - Abstract Algebra II, Spring 2011

Homework 5: Error-Correcting Codes Due: Friday April 15.

1. Consider the code C over $\mathbb{F}_2$ with the following generator matrix, also called C:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

   (a) Find the parameters n and k of C.

   (b) What is the minimum distance d of C? Is $d = n - k + 1$?

   (c) You receive the transmission $(1, 0, 0, 1, 1, 1, 0)$. Is this a codeword? If not, what was the intended codeword?

   (d) How many codewords are there in C?

   (e) How many errors can C correct? How many can it detect?

2. Prove that the minimum distance of a linear code C is the same as the minimum weight of any codeword in C except $\vec{o}$.

3. Let's investigate the Reed-Solomon code RS$(2, 5)$.

   (a) What is a basis for the codewords? How many codewords are there? What is the generator matrix $M_{2,5}$?

   (b) If the data is $\vec{c} = (1, 3)$, what is the codeword?

   (c) If the codeword is $\vec{b} = (1, 0, 4, 3)$, what is the data?

   (d) If the codeword is $\vec{b} = (1, 0, 2, 4)$, show that an error occurred in transmission. What is the best guess for the data vector $\vec{c}$?

   (e) What is the distance invariant for RS$(2, 5)$? How many errors can this code detect? How many errors can this code correct?

4. What is the smallest choice of q that will produce a Reed-Solomon code with at least 200 codewords that will correct 2 errors?

5. Explain how to find a codeword in $RS(k, q)$ whose weight equals the minimal distance $d = n - k + 1$.

6. Define $A_q(n, d)$ to be the maximum value of M such that there is a linear code of length n with M codewords and minimum distance d. Use the Singleton bound to give an upper bound on $A_q(n, d)$ for linear codes in terms of n, q, and d.

7. Define $V_q(n, r)$ to be the number of points of $\mathbb{F}_q^n$ in the ball $B_r(\vec{x}) = \{\vec{y} \in \mathbb{F}_q^n : D(\vec{x}, \vec{y}) \leq r\}$ of points whose Hamming distance from $\vec{x}$ is at most r. Prove that

$$V_q(n, r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

   where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ denotes the binomial coefficient.

   Use this to prove the *Gilbert-Varshamov Bound*:

$$A_q(n, d) \geq \frac{q^n}{V_q(n, d-1)}.$$