Math 567, Homework 5 (Revised)

Due Thursday, April 7

Assignment:

Problems marked with an asterisk are harder than the others. All these problem are optional.

1. Do Chapter 5.1, Exercise 14.

2. Do Chapter 5.1, Exercise 25.

3. Consider a Hamming code $C = H_5(r)$ over F_5 with parameter $r = 2$. This is an $[n, n-r, 3]$ code with $n = \frac{q^r-1}{q-1}$ so it is a $[6, 4, 3]$ code. (We only consider codes up to equivalence.)

(a) Find a 2×6 parity check matrix H for this code.

(b) Find a 4×6 generator matrix G for this code.

(c) Show that the weight enumerator for the dual code $L = C^{\perp}$ is $W_L(s) = 1 + 24s^5$. (One option is to find all codewords).

(d) Use the McWilliams identity to find the weight enumerator $W_C(s)$ for the Hamming code C.

*(e) [Extra credit - 5pt] Now let q and $r \geq 1$ be general. Show that the weight enumerator of the code L that is dual to the q-ary Hamming code $H_q(r)$ is

$$W_L(s) = 1 + (q^r - 1)s^{q^{r-1}}.$$

4. (a) Let L be a binary $[n, k]$ linear code that contains the vector of all 1's. Show that the weight enumerator $W_L(s)$ of this code satisfies the identity

$$W_L(s) = s^n W_L(1/s).$$

(b) Do Section 5.2, Exercise 14.

5. [Krawtchouk polynomials] (Section 5.2, Exercise 18).

(a) Show that for all $n \geq 1$ and $0 \leq k \leq n$ that these polynomials are equal:

$$K_k(x; n, 2) = (-1)^k K_k(n - x; n, 2).$$

Note here that $q = 2$.

(b) Show that for arbitrary q and for all $n \geq 1$ and $0 \leq i \leq n$, $0 \leq k \leq n$ that

$$(q-1)^i \binom{n}{i} K_k(i; n, q) = (q-1)^k \binom{n}{k} K_i(k; n, q).$$

(c) Use (a) and (b) to show for $q = 2$ and for all $n \geq 1$ and $0 \leq i \leq n$, $0 \leq k \leq n$ that

$$K_k(2i; n, 2) = K_{n-k}(2i; n, 2).$$

(d) [Bonus Question –5pt] Show that the Krawtchouk polynomial $K_k(x; n, q)$ is identically zero if $k \geq n + 1$.

6. [Binary Golay code G_{24}] Do Section 6.1, Exercise 8. (Prove Lemma 6.1.4).

7. [Ternary Golay code G_{11}] (a) Do section 6.1, Exercise 16.

*(b) [extra credit-5pts], determine the complete weight distribution of the ternary Golay code G_{11}, using the fact that it is a ternary $[11, 6, 5]$ perfect code.

8. [Bonus problem.] Define a *lexicographically least binary code* as follows. Let integers M= code size and d=distance be given. The block size n is not specified at first, but is assumed to be as large as is necessary. Start with codeword $c = \mathbf{0}$, and $c_1 = (0, 0, 1, 1, ..., 1)$ of weight d ending in d ones. The codewords are picked one at a time. After the first k codewords are picked, the next codeword c_{k+1} is picked to be the lexicographically smallest word that has distance at least d from all the preceding codewords. (That is, the 1's in the word are as far to the right as possible.) If a new coordinate 1 is needed to do this, it is added on the left to all codewords (and it is zero for all earlier codewords.) Halt after M steps and choose the block size of the codewords to be the minimal necessary. That is, for each coordinate position there is some codeword that is nonzero in that position. Note that this construction generally gives a nonlinear code.

(a) Carry out this construction for $d = 2$ and $M = 16$. It begins with 0000000, 0000011, 0000101, 0000110 (note that final block size n may be smaller than seven.)

*(b) Show that for $d = 2$ when $M = 2^k$ that (miraculously) the resulting code is a linear code.

*(c) Show when $d = 3$ that the Hamming codes $H_2(r)$ occur among these codes (up to equivalence).