Math 350
Spring, 2000

HOMEWORK #7

Do 100 points of the following problems (due 3/16/00).

15 pts. **1** Define C to be self-dual if $C = C^{\perp}$. Find a generator matrix of a linear binary self-dual code of length 10.

The matrix formed by placing two 5×5 identity matrices side by side will generate a self-dual code of length 10. The code will be contained in its dual because any row of the generator matrix will have a dot product of 0 with any other row. Since the dimension of both the code and its dual is 5, we have that $C = C^{\perp}$ as required.

15 pts. **2** Find the largest n so that there is a linear binary code with $d = 3$ and at most 3 redundancy bits.

The 3 redundancy bits correspond to the number of rows in the parity check matrix. For the code to have minimum distance of 3, the columns of the parity check matrix must be distinct (and not 0). Since there are 7 distinct 3-tuples, the maximum n is 7.

20 pts. **3** Let $R_{r,q}$ denote the rate of the Hamming code $H(r, q)$. Find an equation for $R_{r,q}$, and calculate $\lim_{r\to\infty} R_{r,q}$.

The Hamming code has length $n = \frac{q^r-1}{q-1}$ and dimension $k = \frac{q^r-1}{q-1} - r$, so the rate of the Hamming code is $R_{r,q} = \frac{k}{n} = \frac{\frac{q^r-1}{q-1}-r}{\frac{q^r-1}{q-1}} = 1 - \frac{r}{\frac{q^r-1}{q-1}}$. By L'Hopital's rule, the limit of the last fraction as $r \to \infty$ is the same as the limit of $\frac{q-1}{\ln(q)q^r}$. Thus, $\lim_{r\to\infty} R_{r,q} = 1 - 0 = 1$. This implies that for long Hamming codes, most of the bits are used for information rather than redundancy.

⋆ 35 pts. **4** Show that the minimum distance of the ternary Golay code of length 11 is 5. You may either use the generator matrix on page 102, or you can construct a parity check matrix for this in the same spirit as Theorem 8.4.

For the parity check approach, put the 5×5 identity matrix in the front of the parity check matrix. For the rest of the parity check matrix, the following will work: $\begin{pmatrix} 0 & 1 & 1 & 2 & 2 & 1 \\ 1 & 0 & 2 & 2 & 1 & 1 \\ 1 & 2 & 0 & 1 & 2 & 1 \\ 2 & 2 & 1 & 0 & 1 & 1 \\ 2 & 1 & 2 & 1 & 0 & 1 \end{pmatrix}$. We need to verify that this will satisfy the property that no 4 columns of the full parity check matrix are linearly dependent. Ignoring the last column for the moment, if we add or subtract any pair of columns 6 through 10, we will get a vector of weight at least 3 (sometimes it will be 4): It will take at least 3 of the first 5 columns to get a sum of 0. If we any 3 of the columns (or subtract), we cannot get a weight lower than 2, so we are still OK. Finally, if we add any 4 of columns 6 through 10, we cannot get 0. Incorporating the last column is easy: when added to any of the previous examples, it will not decrease the weight below the threshold. This proves the result. (There are similar arguments straight from the generator matrix or from the cyclic point of view, but you need to argue all of the cases).

20 pts. **5** Find all cyclic codes of length p over $GF(p)$, where p is a prime.

To find all cyclic codes of a given length, we are required to factor $x^p - 1$ in the given field. By previous work with binomial expansion, $x^p - 1 \equiv (x-1)^p \bmod p$ (each of the "middle terms" in the binomial expansion of $(x-1)^p$ have a factor of p and are therefore 0). Therefore, the codes all have the form $\langle (x-1)^k \rangle$ for $0 \leq k \leq p$. (There are $p+1$ distinct cyclic codes of length p over $GF(p)$).

15 pts. **6** Find all ternary cyclic codes of length 6.

As in the previous problem, this boils down to factoring $x^6 - 1$ over Z_3. We see that $x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x-1)^3(x+1)^3$, so the codes all have the form $\langle (x-1)^i (x+1)^j \rangle$ for $0 \leq i, j \leq 3$. (There are 16 distinct cyclic codes of length 6 over Z_3).

15 pts. **7** Find THE generating polynomial for the binary code of length 8 that is generated by $x^6 + x^4 + x^2$. What is its check polynomial?

We want to find the smallest degree polynomial contained in the code generated by $x^6 + x^4 + x^2$. If we shift this codeword by x^2 and add it to the original, we get $1 + x^6 + x^4 + x^6 + x^4 + x^2 = 1 + x^2$. If we shift this by x^2 and add it to $1 + x^2 + x^4$, we get $x^2 + x^4 + 1 + x^2 + x^4 = 1$, so 1 is in the code. That must be the smallest nonzero monic polynomial, so it is THE generator polynomial. The check polynomial is $x^8 - 1$.