Math 422 Winter 2007 - Midterm Exam

March 1, 2007

No books, no notes, no calculators are allowed.

Good Luck!

Problem 1. [12] Let C be the linear $[7, k, d]$-code over $\mathbb{Z}_2$ with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

a) Find k and the number of elements in C. Justify your answer.

b) Find a parity check matrix H for C. If possible, find one in standard form.

c) Is C a Hamming code? Explain.

d) Encode the message vector 1001.

e) Suppose you receive the vector 1110111. Decode it using syndrome decoding with your matrix H from b). Show your work (in particular, compute the syndrome). (*Hint:* You do not have to write down a syndrome table...)

Solution.

a) $k = 4$ because G has 4 rows which form a basis for C. C has $2^k = 2^4 = 16$ elements, because this is the number of distinct linear combinations of four linearly independent vectors over $\mathbb{Z}_2$.

b) G may be transformed into standard form without any column swaps. The result is

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Unsing the formula $H = [-A^t\, I]$ one then obtains

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

c) Yes, C is a Hamming code: by inspection, H contains **every** nonzero vector of length 3 as exactly one column. By the construction of Hamming codes, this makes C a Hamming code.

d) $[1\,0\,0\,1]G$ is the sum of the first and last row of G: $[1\,0\,0\,1\,0\,1\,0]$.

e) The syndrome is $H\mathbf{y}^t = [1\,0\,1]^t$, which is the fourth column of H. Thus, $\mathbf{e} = [0\,0\,0\,1\,0\,0\,0]$, and $\mathbf{y}$ is decoded to 1111111.

Problem 2. [10] Let C be the linear code of length 5 over $\mathbb{Z}_{11}$ given by the equations

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= 0 \\ x_2 + 2x_3 + 2x_4 + x_5 &= 0 \\ x_1 - 8x_2 + 9x_3 &= 0 \end{aligned}$$

a) Find a generator matrix for C.

b) Find a parity check matrix H for C.

c) Find a basis for the dual code of C.

d) Find the maximum number N such that any collection of N columns of H (cf. b)) is linearly independent. Justify your answer.

e) Find $d(C)$. Is C a perfect code? Justify your answer.

Solution.

a) C is the solution set of linear equations, so we have to row reduce

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & -8 & 9 & 0 & 0 \end{bmatrix}$$

The reduced echelon form of A is

$$U = \begin{bmatrix} 1 & 0 & 0 & 6 & 2 \\ 0 & 1 & 0 & 10 & 8 \\ 0 & 0 & 1 & 7 & 2 \end{bmatrix}$$

and so C is spanned by $[5\,1\,4\,1\,0]$ and $[9\,3\,9\,0\,1]$ and a generator matrix is

$$\begin{bmatrix} 5 & 1 & 4 & 1 & 0 \\ 9 & 3 & 9 & 0 & 1 \end{bmatrix}$$

b) C is basically the nullspace of A and U (up to transposition), and $\operatorname{rank} A = 3 = 5 - \dim C$. Thus $H = A$ or $H = U$ will do. Of course, there are other possibilities.

c) The rows of $A = H$ will do: $[1\,1\,1\,1\,1], [0\,1\,2\,2\,1], [1\,-8\,9\,0\,0]$.

d) N does not depend on whether we compute it for H or its row echelon form. Clearly, $N \leq 3$ because $N \leq \operatorname{rank} U$. (and every column is a linear combination of the first three columns of U). It is also clear that no two columns of I_3 together with one of the last two columns of U form a linearly dependent set. It remains to see that any column of I_3 together with the last two columns of U is linearly independent. But that is clear because they always form an invertible matrix.

e) By d) $N = 3$ and by a theorem we know $d(C) = N + 1 = 4$. We have seen (homework/sample midterm/class) that a code with even minimum distance is never perfect.

Problem 3. [8] For each of the following statements indicate whether it is true or false. No justification is needed.

a) If G is the generator matrix of a linear code (of dimension k with $1 \leq k < n$), then G is also a parity check matrix for some (possibly different) linear code of dimension $n - k$.

b) There is no linear 3-ary $(7, 16, 3)$-code.

c) An $(n, M, 2t)$-code can be used to correct t errors, using nearest neighbour decoding.

d) An (n, M, d)-code can be used to detect $d - 1$ errors.

e) Two equivalent codes have the same minimum distance.

f) A (nonempty) binary code is linear if and only if the sum of any two (not necessarily distinct) codewords is again a codeword.

g) For every pair of positive integers $n > d$, there is always a perfect (n, M, d)-code (for some M).

h) If C is a linear $[n, k]$-code with generator matrix G, then $\mathbf{x} \in F_q^n$ is a codeword if and only if $G\mathbf{x}^t = \mathbf{0}$.

a) TRUE: G is a PCM for $C^{\perp}$.

b) TRUE: 16 is not a power of 3,

c) FALSE: We can correct only $t-1 = [(d-1)/2]$ errors using nearest neighbour decoding.

d) TRUE

e) TRUE

f) TRUE: This is special for binary codes; there are no non-trivial scalar multiples to ckeck ($\lambda\mathbf{x}$ is either $\mathbf{x}$ or $\mathbf{0}$), and since $\mathbf{0} = \mathbf{x} + \mathbf{x}$ every axiom of a subspace is satisfied.

g) FALSE: This is (if at all) possible only if the Hamming bound is sharp (but even then, it is not always possible).

h) FALSE: This is the condition for the dual code $C^\perp$.

Problem 4. [8] Let C be a linear $[3, k, 3]$-code over $\mathbb{Z}_3$ with $k \geq 1$. Show that k (i.e. $\dim C$) is equal to 1. How many linear codes with these parameters are there? Justify your answer.

Solution. There are many possible ways to do this. Here is one: We know that $A_q(n, n) = q$. So $A_3(3, 3) = 3$. A $[3, k, 3]$-code has 3^k elements. Thus we must have $3^k \leq 3$, or $k \leq 1$. Hence $k = 1$.
Alternatively: we know that any such code is a subcode of the binary repetition code of length 3 or some equivalent thereof, Hence $3^k \leq 3$, and again $k \leq 1$.
Other solutions are equally fine.
As for the number: since $k = 1$, C is specified by a single basis vector. As any nonzero element of C has weight 3, C is specified by a vector of weight 3. There are $8 = 2^3$ such vectors (for each place a choice of 1 or 2), and two vectors will result in the same code. Hence the total number of different codes is 4.

Problem 5. [6] Recall that $A_q(n, d)$ is the largest value for M such that there exists a q-ary (n, M, d)-code.
Let C be a q-ary (n, M, d)-code with $n, d > 0$ and $M \geq 2$. Suppose that M is maximal, i.e. that $M = A_q(n, d)$.
Prove: For every vector $\mathbf{y} \in F_q^n$ there is a codeword $\mathbf{x}$ such that $d(\mathbf{x}, \mathbf{y}) < d$. In other words, every vector is a distance of at most $d - 1$ away from a codeword.
(*Hint:* M is maximal.)
Solution. Let $\mathbf{y}$ be a vector. If $d(\mathbf{x}, \mathbf{y}) \geq d$ for all $\mathbf{x} \in C$, we may add y to C and still have a code with minimum distance d. But now the number of elements would be $M + 1 > A_q(n, d)$, a contradiction. Thus $d(\mathbf{x}, \mathbf{y}) < d$ for some $\mathbf{x} \in C$.