Math 422 Winter 2007 - Final Exam

April 24, 2007

No books, no notes, no calculators are allowed.

Good Luck!

Remark: The equation to find the error locator polynomial for a BCH code is of the form

$$\begin{bmatrix} S_1 & S_2 & \dots & S_t \\ S_2 & S_3 & \dots & S_{t+1} \\ \vdots & \vdots & \dots & \vdots \\ S_t & S_{t+1} & \dots & S_{2t-1} \end{bmatrix} \begin{bmatrix} b_t \\ b_{t-1} \\ \vdots \\ b_1 \end{bmatrix} = - \begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix}$$

Problem 1. [14] Let $n > 0$ and let C be the binary *even-weight code* of length n: that is, C consists of all length n vectors that have even weight.

$$C = \{\mathbf{x} \in \mathbb{Z}_2^n \mid w(\mathbf{x}) \text{ is even}\}$$

a) Find a parity check check matrix H for C. (*Hint:* $w(\mathbf{x}) \equiv x_1 + x_2 + \cdots + x_n \mod 2$)

b) Find a generator matrix for C.

c) Compute the minimum distance of both, C and its dual code $C^\perp$. Justify your answers.

d) How many elements does C contain? How many elements does $C^\perp$ contain? Justify your answer.

e) Suppose n is odd. Is $C^\perp$ perfect? Why or why not?

f) Again let $n > 2$ be odd. Is $C \subseteq C^\perp$? Is $C^\perp \subseteq C$?

g) Prove or disprove: C is a cyclic code.

Solution.

a) For any binary vector $\mathbf{x} = x_1 x_2 \dots x_n$, its weight $w(\mathbf{x})$ modulo 2 is equal to $\sum_i x_i$ in $\mathbb{Z}_2$. $w(\mathbf{x})$ even just means $w(\mathbf{x}) \equiv 0 \mod 2$, and so C is given by a single equation, namely $\sum_{i=1}^n x_i = 0$ in $\mathbb{Z}_2$. Thus

$$H = [\underbrace{1\,1\,1\,\dots\,1}_{n \text{ times}}]$$

is a PCM.

b) (If $n = 1$, $C = \{0\}$ and no generator matrix exists. So we assume $n \geq 2$.) $H = [\, A \, I_1 \,]$ is in standard form, so G may be given as $G = [\, I_{n-1} \; -A^t \,]$:

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

where G has $n-1$ rows and n columns. Alternatively, you could solve the system $H\mathbf{x} = \mathbf{0}$, which would give you as a basis the (column) vectors $e_1 + e_n$, $e_2 + e_n$, $\dots$, $e_{n-1} + e_n$. After transposing these columns and using them as rows for G, the resulting matrix would be the same (up to potential reordering of the rows).

c) Again, here $d(C)$ is defined only if $n \geq 2$. The minimum distance d of C is the minimum number such that there exist d linearly dependent columns in H: now any column of H is linearly independent (as it is nonzero). On the other hand, any two columns are linearly dependent (they are equal!), so $d = 2$. Alternatively, $d(C) = w(C)$. Any nonzero element of C has even weight by definition of C, so $w(C) \geq 2$. On the other hand, C contains *all* vectors of even weight, so in particular, $110\dots0 \in C$. But this is a weight 2-vector, so $w(C) \leq 2$. It follows $w(C) = d(C) = 2$.

H is a generator matrix for $C^\perp$. Obviously, this means $C^\perp$ is the binary repetition code of length n. Its minimum distance is therefore n.

Alternatively: any $n-1$ columns of G (which is a PCM for $C^\perp$) are linearly independent (this is clear for the first $n-1$ as those are the columns of I_{n-1}; any $n-2$ columns of I_{n-1} are of course also linearly independent, but their span does never contain the last column, because all elements in their span will have one coordinate (corresponding to the missing column of I_{n-1}) equal to zero. Thus, any $n-2$ columns of I_{n-1} together with the last column are independent as well). But n columns are not independent (can't be as the columns have only $n-1$ entries); also the last column is the sum of the first $n-1$ columns. Thus $d(C^\perp) = n$.

d) If n is odd, then $C^\perp$ is equal to an odd-length binary repetion code. This is a perfect code.

e) If $n > 2$ then $\dim C = n - 1 > 1$. Thus C cannot be a subspace of $C^\perp$. So no, $C \not\subseteq C^\perp$.

Let $\mathbf{x} = [\, 1\, 1 \, \dots \, 1 \,]$ be the basis element of $C^\perp$ given by the row of H. Then $C^\perp \subseteq C$ if and only if $\mathbf{x} \in C$. Now $\mathbf{x} \in C$ implies that $\mathbf{x}$ has even weight. But $w(\mathbf{x}) = n$ is odd, so no, $C^\perp \not\subseteq C$.

Alternatively, $\mathbf{x} \in C$ implies that $\mathbf{x}$ is perpendicular to $C^\perp$, so in particular, $\mathbf{x} \cdot \mathbf{x} = 0$. But this is $\sum_{i=1}^n x_i^2 = \sum_{i=1}^n 1 = n \neq 0 \in \mathbb{Z}_2$ as n is odd.

f) Let T be the cyclic shift: $T(x_1 x_2 \dots x_n) = x_n x_1 \dots x_{n-1}$. $\mathbf{x} \in C$ if and only if $w(\mathbf{x})$ is even. Now $w(T\mathbf{x}) = w(\mathbf{x})$ because both numbers are equal to the number of nonzero

entries of $\mathbf{x}$ which does not depend on the order. Hence $T\mathbf{x} \in C$ for all codewords $\mathbf{x}$ and we see that C is cyclic.

Alternatively, C is cyclic if and only if $C^\perp$ is cyclic. We know well that $C^\perp$ is cyclic, because it's the binary repetition code of length n. Thus, C is cyclic as well.

Problem 2. [16] Let $F_9 = \mathbb{Z}_3[x]/\langle x^2+1\rangle$. We denote $\bar{x} \in F_9$ by a. Then $\alpha = 1 + a$ is primitive.
Let C be the BCH code of design-distance 3 over $\mathbb{Z}_3$ corresponding to α, α^2.

a) What is the length of C? Justify your answer.

b) Find the generator polynomial g for C.

c) Find the check polynomial h for C.

d) What are the dimensions of C and $C^\perp$? Justify your answer.

e) How many errors can C at least correct?

f) Suppose you receive the vector 00101100. Translate this into a polynomial and compute the syndromes S_1 and S_2.

g) Decode the received vector in f) to a codeword if possible, using the decoding scheme for BCH codes. How many errors did occur?

h) Is the BCH code corresponding to $\alpha, \alpha^2, \alpha^3$ (design-distance 4) the same code as C? Why or why not?

(You may freely refer to Table 1.)

Element	Minimal polynomial	Power of α
1	$x - 1 = x + 2$	α^8
2	$x - 2 = x + 1$	α^4
a	$x^2 + 1$	α^6
$2a$	$x^2 + 1$	α^2
$1 + a$	$x^2 + x + 2$	α^1
$1 + 2a$	$x^2 + x + 2$	α^3
$2 + a$	$x^2 + 2x + 2$	α^7
$2 + 2a$	$x^2 + 2x + 2$	α^5

Table 1. Elements of F_9, their minimal polynomials over $\mathbb{Z}_3$, and their expression as powers of the primitive element.

Solution.

a) The length of C is the order of α. Since α is primitive, its order is $q^s - 1$. Here $q^s = 9$, so the order is 8. (The length is also given away by part e), since the received vector has the same length as a codeword.)

b) We need m_α and m_{α^2}. We know that $m_\alpha = x^2 + x + 2$ from the table. But also, here $q = 3$, so we need to check the subsequent q-th powers $\alpha, \alpha^3, \alpha^9 = \alpha$, so $m_\alpha = (x-\alpha)(x-\alpha^3) = x^2+x+2$. Also $m_{\alpha^2} = (x-\alpha^2)(x-\alpha^6) = x^2+1$ because $(\alpha^2)^9 = \alpha^2$. So $g = (x^2+1)(x^2+x+2) = 2 + x + x^3 + x^4$.

c) $h = (x^8-1)/g$. We know that $x^8 - 1$ is the product of all distinct minimal polynomials for the nonzero elements in F_9 ($x^8 - 1 = \prod_{\beta \in F_9 - \{0\}}(x - \beta)$). So h is the product of all those, not appearing in g, i.e.

$$h = (x+1)(x+2)(x^2+2x+2)$$

d) The dimension of C is the degree of h (or, $n - \deg g$). Thus $\dim C = 4$.

The dimension of $C^\perp$ is the degree of g (or, $n - \deg h$). Thus $\dim C^\perp = 4$.

e) The design distance of C is 3. So we know that $d(C) \geq 3$. Thus C can correct at least $(d-1)/2 = 1$ error.

f) The received vector is 00101100. As a polynomial this is $f = x^2 + x^4 + x^5$. The two syndromes are $S_1 = f(\alpha) = \alpha^2 + \alpha^4 + \alpha^5 = 2a + 2 + 2 + 2a = 1 + a = \alpha$; and $S_2 = f(\alpha^2) = \alpha^4 + \alpha^8 + \alpha^{10} = 2 + 1 + 2a = 2a = \alpha^2$.

g) The syndrome equation becomes with $M = [S_1]$

$$S_1 b_1 = -S_2$$

thus $\alpha b_1 = -\alpha^2$ and so $b_1 = -\alpha = 2\alpha$.

The error locator polynomial is then $\sigma = b_1 x + 1 = 2\alpha x + 1$. Its single root is $\beta = -2\alpha^{-1} = \alpha^{-1}$. Thus $\alpha_1 = \beta^{-1} = \alpha$ and the error occurred at position 1 (in the coefficient of x).

$e = e_1 x$. To find e_1, we may use $M = VDV^T$ to get the equation $S_1 = e_1\alpha$ and hence $e_1 = 1$. No further consistency checks are necessary.

Thus, we conlcude $e = x$ and f is decoded to $f - e = f + 2e$, the decoded codeword is 02101100 and only one error occurred.

If you multiplied out the generator polynomial g in b) above, then you will recognize the decoded codeword as corresponding to xg.

h) Yes, the code corresponding to $\alpha, \alpha^2, \alpha^3$ is the same, because its generator polynomial is the same: $m_{\alpha^3} = m_\alpha$, so the generator polynomial is still $m_\alpha m_{\alpha^2}$.

Problem 3. [6] For each nonzero element in F_9 (defined as in Problem 2), find its order. Justify your answer.

Solution. We will of course use Table 1. Notice that $q-1=8$, so the only possible orders are 1, 2, 4 and 8. The only element of order 1 is of course 1.
2 has order 2 because $2^2=4=1$ (and $2\neq 1$). It is the only such element because $\pm 2=1,2$ are the only solutions of $x^2-1=0$.
There are 2 elements of order 4, namely a and $2a$: any element of order 2 is also a solution of $x^4=1$, so there can be only two elements of order 4 bringing the total of solutions to 4. Now $a^2=2\neq 1$, and $a^4=2^2=1$, so a is a solution. But then $2a=a^3$ is a solution as well because $(2a)^4=2^4a^4=1$.
Finally, the elements of order 8 must now be the remaining ones $1+a, 2+a, 1+2a, 2+2a$.
Anothe way of solving this would be to observe that the order of $\alpha=1+a$ is 8, and then that the order of α^l is equal to $8/\gcd(8,l)$. So if $l=1,3,5,7$ this gives 8; if $l=2,6$ this gives 4, and if $l=4$ this gives 2 and finally if $l=0$ or 8 (i.e. if $\alpha^l=1$) this gives 1.

Problem 4. [4] Prove the singleton bound:
If C is a linear $[n,k,d]$-code over F_q, then $k\leq n-d+1$ or, equivalently, $d\leq n-k+1$.
(*Hint:* You need to show only one of the two inequalities. For the second one, you could use the criterion involving a parity check matrix for C.)

Solution. There are several methods.
$k\leq n-d+1$ is equivalent to $d\leq n-k+1$. So we will show only the second inequality.
If a linear code C has a PCM H, then $d(C)$ is the minimum number l such that there are l columns that are linearly dependent.
So let H be a PCM for C (if $C=F_q^n$, i.e. if C does not have a PCM, then the inequality says $d\leq 1$ which is correct.). H has $n-k$ rows, and $n-k>0$, thus every column has $n-k$ entries, thus at most $n-k$ columns can be linearly independent. C has a minimum distance so $k\neq 0$ and thus $n-k<n$. It follows that *any* $n-k+1$ columns are dependent, so in particular there exist $n-k+1$ linearly dependent columns. Thus $d\leq n-k+1$.
Alternate method: the first $n-d+1$ symbols uniquely determine a codeword. Indeed, if two codewords have the same first $n-d+1$ symbols, then they differ in at most $d-1$ places. Since $d(C)=d$, this means they are equal.
Thus the number of codewords is at most the number of different vectors of length $n-d+1$ which is q^{n-d+1}. Since C has dimension k this means C has $q^k\leq q^{n-d+1}$ codewords, and so $k\leq n-d+1$ proving the first inequality.

Problem 5. [10] For each of the following statements, indicate whether it is true or false. No justification is needed.

a) For a linear code C with a parity check matrix H, its minimum distance is the smallest positive number d such that there are d linearly dependent columns of H.

b) The minimum distance of a Hamming code is always 5.

c) There is a perfect ternary code of length 11 and dimension 6.

d) A binary Hamming code is equivalent to a cyclic code.

e) The degree of the generator polynomial of a cyclic code is equal to the dimension of the code.

Solution.

a) TRUE: this is even almost true for the "weird" case that $C = \{0\} \subset F_q^n$ $(n > 0)$ because then both, $d(C)$ and this number d are not defined. (We defined codes with PCM always as codes of positive dimension.)

b) FALSE: It is always 3.

c) TRUE: The ternary Golay code will do.

d) TRUE.

e) FALSE: The dimension is equal to the degree of the check polynomial, or to the length minus the degree of the generator polynomial.

Problem 6. [4] Let $q = p^l$ for some prime p and some integer $l > 0$, and let F_q be a finite field with q elements. Show that for each $a \in F_q$, the polynomial $f = x^p - a$ has a unique root in F_q.
(*Hint:* Powers of a?)

Solution. Let $a \in F = F_q$. If $a = 0$, then 0 is the only root of $f = x^p - a$, because $\alpha^p = 0$ implies that $\alpha = 0$.
So suppose $a \neq 0$. Then the order o of a is defined and divides $q - 1$. In particular, $\gcd(p, o) = 1$ because p divides q and so does not divide $q-1$, let alone o (p is prime). Thus, we find integers n, m such that $1 = mo + np$.
Then $a = a^1 = a^{mo+np} = a^{mo}a^{np} = 1 \cdot (a^n)^p$ (this is even true if any or all of n, m are negative, or zero). It follows $\alpha := a^n$ is a solution.
How to find this solution using the hint: the hint suggests that the root is of the form a^n, so we want $(a^n)^p = a$, or $a^{np} = a$. Now we cannot solve $np = 1$ for n but we do know that $a = a^{1+ko}$ for all k, so we want that $np = 1 + ko$ has a solution for n, k. But this is true because $\gcd(o, p) = 1$.
As for uniqueness: if α, β are solutions of f, then $\alpha^p - \beta^p = 0$, so $(\alpha - \beta)^p = 0$, so $\alpha = \beta$; we are in characteristic p so $(u+v)^p = u^p + v^p$; $(\alpha^p - \beta^p) = (\alpha - \beta)^p$ is true if $p = 2$ because $-1 = 1$, if $p \neq 2$, then p is odd, and so $(-\beta)^p = -\beta^p$ and so $(\alpha - \beta)^p = \alpha^p + (-\beta)^p = \alpha^p - \beta^p = 0$.
Alternative solution prove uniqueness first as above. Write $F = a_1, a_2, \ldots, a_q$ and write down a new list $a_1^p, a_2^p, \ldots, a_q^p$. Because of uniqueness, $a_i^p = a_j^p$ if and only if $i = j$. Thus, the new list comprises q distinct elements. In other words, it comprises all elements of F_q. It follows a is also listed, so there is i such that $a_i^p = a$.