Math 422 Winter 2007 - Sample problems - Solutions

Problem 1.

a) We have to solve the linear system

$$x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} = 0$$

As this is only one equation we know that a basis is given by

$$\begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} -10 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Writing them as rows instead of columns, and combining them into a generator matrix G we get

$$G = \begin{bmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -7 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -8 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

b) The equation in a) defines the PCM: it is

$$H = [\,1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,]$$

(It is clearly a linearly independent row, defining an element in the dual code. The dual code has dimension $10 - 9 = 1$ and so H is a PCM.)

Or: First solve $G\mathbf{y}^t = \mathbf{0}$: by the form of G it is clear, that if $G\mathbf{y}^t = \mathbf{0}$, then $2y_1 = y_3$, $3y_1 = y_3$ and so on, hence $\mathbf{y}$ is a multiple of $[\,1, 2\,3\,4\,5\,6\,7\,8\,9\,10\,]$.

c) The dimension of C is the number of rows of G, i.e. 9. The dimension of $C^\perp$ is $n - \dim C = 1$.

d) We know that the minimum distance of a linear code with PCM H is the minimum positive d such that there are d linearly dependent columns in H. For C this means: H has just one row, without a zero entry, thus no single column is linearly dependent, but any two columns are, hence $d(C) = 2$. On the other hand, the last 9 columns of G are clearly linearly dependent. Also any collection of 9 columns of G which include the first row are linearly independent. (Every row of a 9×9-submatrix of G contains a pivot position for that submatrix.) Hence $d(C^\perp) = 10$ (because clearly, all ten columns must be dependent, as there are only nine rows, and indeed, the first column is a linear combination of the last 9).

e) Then syndrome is $H\mathbf{y}^t = 10 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 + 8 \cdot 8 + 9 \cdot 9 + 10 \cdot 10$ (remember $X = 10$). We are in $\mathbb{Z}_{11}$, so this is equal to

$$10 + 4 + 9 + 5 + 3 + 1 + 4 + 9 + 4 + 1 = 6.$$

We may use the vectors with a nonzero single entry in the first position together with $\mathbf{0}$ as coset leaders. Then $H[\, a\, 0\, 0\, 0 \ldots 0\,]^t = a = 6$ implies that $\mathbf{e} = (6, 0, \ldots, 0)$ is the coset leader for $\mathbf{y}$. And the original codeword then is $\mathbf{y} - \mathbf{e} = 423456789X$. At least one error occurred.

f) There is no unique nearest neighbour. Since the minimum distance of C is 2, there are vectors which have distance 1 to more than one codeword. Indeed, our decoding above depends on the choice of coset leaders, because every coset contains a lot weight 1 vectors. Had we chosen the vectors with entry in the second column we would have concluded that the error vector is $\mathbf{e}' = (0, 3, 0, \ldots, 0)$ because $H\mathbf{e}'^t = 2 \cdot 3 = 6$, and hence we would have decoded to a different vector.

Problem 2.

a) We have $\alpha^8 = \alpha$, but $\alpha, \alpha^2, \alpha^4$ are distinct by the table. Thus

$$m_\alpha = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x^2 + 1.$$

b) We have to multiply the distinct minimal polynomials of $\alpha, \alpha^2, \alpha^3, \alpha^4$. By a), $\alpha, \alpha^2, \alpha^4$ have the same minimal polynomial. $\alpha^3 = a^2$ has the same minimal polynomial as a, and hence it is $1 + x + x^3$. Together this implies that

$$g = (1 + x + x^3)(1 + x^2 + x^3)$$

is the generator polynomial.

c) The length of C is 7, the degree of g is 6, so the dimension of C is $7 - 6 = 1$.

d) We know that $h = (x^7 - 1)/g = x - 1 = x + 1$ is the check polynomial.

e) $\mathbf{y}$ corresponds to the polynomial $f = 1 + x + x^3 + x^5 + x^6$.

$$hf = 1 + x + x^3 + x^5 + x^6 + x + x^2 + x^4 + x^6 + x^7 = 1 + x^2 + x^3 + x^4 + x^5 + x^7.$$

This is clearly nonzero in $R_{2,7}$ because $x^7 - 1$ does not divide hf (they both have degree 7, so the would have to be associated, which is absurd). So $\mathbf{y}$ is not a codeword.

f) We have to compute the syndromes $S_1 = f(\alpha), S_2 = f(\alpha^2) = f(\alpha)^2, S_3 = f(\alpha^3), S_4 = f(\alpha^4) = f(\alpha)^4$ (because $q = p = 2$). $S_1 = 1 + \alpha + \alpha^3 + \alpha^5 + \alpha^6 = 1 + (1 + a) + a^2 + a + (a + a^2) = a$. Thus $S_2 = a^2 = \alpha^3$, and $S_4 = a^4 = \alpha^6$. Now

$$S_3 = 1 + \alpha^3 + \alpha^9 + \alpha^{15} + \alpha^{18} = 1 + a^2 + (1 + a^2) + (1 + a) + (1 + a + a^2) = a^2 = \alpha^3.$$

Now

$$M_2 = \begin{bmatrix} \alpha^5 & \alpha^3 \\ \alpha^3 & \alpha^3 \end{bmatrix}$$

and $\det M_2 = \alpha^8 - \alpha^6 = \alpha + a + a^2 = 1 + a^2 = \alpha^2 \neq 0$.

So at least 2 errors occurred. Using $(\alpha^2)^{-1} = \alpha^5$ we obtain

$$M^{-1} = \alpha^5 \begin{bmatrix} \alpha^3 & \alpha^3 \\ \alpha^3 & \alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha & \alpha \\ \alpha & \alpha^3 \end{bmatrix}$$

We have to solve the equation

$$M \begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = - \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^6 \end{bmatrix}$$

Applying M^{-1} on both sides

$$\begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = \begin{bmatrix} \alpha^4 + \alpha^7 \\ \alpha^4 + \alpha^9 \end{bmatrix} = \begin{bmatrix} \alpha^6 \\ \alpha^5 \end{bmatrix}$$

It follows that the error locator polynomial is $\sigma = 1 + \alpha^5 x + \alpha^6 x^2 = (1 - e_1 x)(1 - e_2 x)$ (where $\sigma(e_i^{-1}) = 0$) if it has two roots. Notice that for this degree 2 polynomial it is a little simpler to find the inverses of the roots directly, rather than first finding the roots. In general, however, one first solves for the roots and then takes inverses.

Thus e_1, e_2 satisfy (always using that $-1 = 1$) $e_1 + e_2 = a$ and $e_1 e_2 = a + a^2$. The first equation has the possible solutions

e_1	e_2
0	a
1	$1 + a$
$1 + a^2$	$1 + a + a^2$
$a + a^2$	a^2

Of these, obviously only the third one is a candidate also for the second equation. And indeed, $(1+a^2)(1+a+a^2) = \alpha^2\alpha^4 = \alpha^6$

We find $e_1 = 1+a^2 = \alpha^2$ and $e_2 = 1+a+a^2 = \alpha^4$. The error positions are therefore 2 and 4, and the error polynomial is $e = x^2 + x^4$.

The codeword is then $f - e = f + e = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$, which translates into 1111111. (Since our code here is the binary repetition code of length 7, we know that this is a codeword.)

Notice that here no final checks are necessary, because we could solve the equation for $t = (d-1)/2$ so our solution satsifies all $2t$ syndrome-equations.

Problem 3.

a) A Hamming code has minimum distance 3. By definition, its parity check matrix contains the $2^r - 1$ nonzero vectors in $\mathbb{Z}_2^r$ for some r. Thus its length is $2^r - 1$, and the dimension of the dual code is r. It thus has dimension $2^r - 1 - r$ and so contains $M = 2^{2^r-1-r}$ elements.

The Hamming bound says

$$M(1 + \binom{2^r - 1}{1}) \leq 2^{2^r-1}$$

because $d = 3$ so $t = 1$. Hence $M2^r \leq 2^{2^r-1}$. But $M2^r = 2^{2^r-1-r}2^r = 2^{2^r-1}$ and so this bound is sharp.

b) We have to list one representative of each line through the origin in F_q^2. Let $(a,b) \in F_q^2$. Then, if $a \neq 0$, we may scale, and $(1, b/a)$ and (a,b) are in the same line. Moreover $(1,a)$ and $(1,b)$ are in the same line if and only if $a = b$. Finally. $(1,a)$ and $(0,1)$ are never in the same line. Let $F_q = \{0, 1, q_2, q_3, \ldots, q_{q-1}\}$

Thus we get a list: $(0,1), (1,0), (1,1), (1,q_2), \ldots, (1,q_{q-1})$, this list comprises $q+1$ elements (which is the length of a redundancy 2 Hamming code: $(q^2-1)/(q-1) = q+1$). So

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 1 & q_2 & q_3 & \ldots & q_{q-1} \end{bmatrix}$$

Problem 4.

a) TRUE: It is equivalent to a primite BCH code of design distance 3.

b) TRUE: $x^n - 1 = (x-1)g$ is irreducible if and only if g is a unit. This is true if and only if $\deg g = 0$ and $n = 1$.

c) TRUE: $256 = 2^8$ is a prime power.

d) FALSE: $255 = 5 \cdot 51$ and 51 is not a power of 5 so 255 is not a prime power.

e) TRUE: The number of rows is the number of cosets which is q^{n-k} where n is the length and k is the dimension of the code.

f) FALSE: The number of elements in linear code is the power of some prime. For example there is no linear code with 6 elements.

Problem 5. WARNING: The problem obviously should have read: "every nonzero element *different from* 1 ..." because 1 is primitive if and only if $F_q = \mathbb{Z}_2$.
Let $a \in F_q$ be a nonzero element, different from 1. We know that the order of a must divide $q-1$. Since $q-1$ is prime by assumption, it follows that $\text{ord}(a)$ is a either 1 or equal to $q-1$. It cannot be 1 because $a \neq 1$ and so it must be $q-1$. But this implies that $a, a^2, \ldots, a^{q-1}$ are all distinct and so the list contains all nonzero elements of F_q, i.e. a is primitive.

Problem 6.

a) Clearly $f(1) = 1$ and $f(0) = 1$, so f has no root in $\mathbb{Z}_2$, it therefore has no divisor of degree 1. Suppose it has an irreducible divisor of degree 2. Then also the quotient is irreducible of degree 2 for otherwise there is a degree 1-divisor, and hence a root. The only irreducible polynomial of degree 2 is $1+x+x^2$. So $f = (1+x+x^2)(1+x+x^2) = 1+x^2+x^4$ which is absurd, and so f is not the product of two irreducibles of degree 2. But then it is irreducible, because if a degree 3 polynomial divides f, the other divisor must have degree 1, which can't happen.

b) The degree of the minimal polynomial of a primitive element is always the dimension of the field extension, that is 4 in this case.

Method 1: $\alpha, \alpha^2, \alpha^4, \alpha^8$ are all distinct because the order of α is 16. However, $\alpha^1 6 = \alpha$. We have seen that this means the minimal polynomial is equal to $(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$ and so has degree 4.

Method 2: By a homework problem we know that there is a copy of $F = \mathbb{Z}_2[x]/\langle m_\alpha \rangle$ contained in F_{16} containing α (because m_α has a root in F_{16}, and m_α is irreducible, so F is a field). But hence F contains all powers of α. Thus $F = F_{16}$. F having 16 elements is equivalent to $\deg m_\alpha = \dim_{\mathbb{Z}_2} F = 4$.

c) The only assumption in b) was that α is primitive. If α^7 is also primitive, then $\deg m_{\alpha^7} = 4$ as well. But the order of α and 7 are coprime. So by our formula for the order of α^7, it follows that α^7 has order 15 as well, hence is primitive.