ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Final Exam June 30, 2011

Introduction to Coding Theory

June 30, 2011

- Any document or material is forbidden, except a hand-written recto verso A4 formula sheet.
- Use a separate sheet of paper for every problem you are working on, write your name on and number additionnal sheets.
- Within the same problem, you can use the answer of a question to solve the following ones.
- There are a total of 90 points to obtain.
- You have exactly three hours. Good luck!

Name:

Problem 1 / 10 points	Problem 2 / 10 points	Problem 3 / 15 points	Problem 4 / 20 points	Problem 5 / 25 points	Problem 6 / 10 points

Total

CONVENTIONS & REMINDERS

- $\mathbb{F}_q$ stands for the finite field with q elements.
- If $\mathcal{C}$ is a code, *puncturing* $\mathcal{C}$ at position i means that you delete the ith coordinate of all codewords ; *shortening* $\mathcal{C}$ at position i means that you puncture at position i the subcode of $\mathcal{C}$ formed by all codewords with a zero at the ith coordinate.
- If $\mathcal{C}$ is a code over $\mathbb{F}_{q^t}$ for some $t \geq 1$, $\mathcal{C}_{|\mathbb{F}_q} = \mathcal{C} \cap \mathbb{F}_q^n$ stands for the *subfield subcode*.
- The MacWilliams identity is between a q-ary code $\mathcal{C}$ and its dual $\mathcal{C}^\perp$ is

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(y - x, y + (q-1)x).$$

Problem 1 [10 points]. Let G be the generating matrix of a $[n,k,d]_q$-code. Show that every $k \times (n-d+1)$ submatrix of G has rank k and that furthermore, d is the largest number with that property.

Solution :
We can assume without loss of generality that we are considering the $s \times k$ submatrix B formed by the last columns and write $G = [A|B]$. By permutation we can always bring the positions under consideration to the end. If the rank of B is less than k, there exists a non-zero linear combination $u \in \mathbb{F}_q^k \setminus \{0\}$ such that $uB = 0$. Then $c = uG$ is a codeword of weight $\leq n - s$. The word c cannot be zero since G is of rank k and $u \neq 0$. So $d \leq \mathrm{wgt}(c) \leq n - s$, i.e. $s \leq n - d$. The result follows.

Problem 2 [10 points]. Let $\mathcal{C}$ be a $[n,k]_4$-code and $(A_i)_{0\leq i\leq n}$ its weight distribution.

1. Show that $\mathcal{C}^\perp$ contains $\frac{1}{4^k}\sum_{i=0}^{n} A_i 3^{n-i}(-1)^i$ codewords of weight n.
2. Show that if $\mathcal{C}$ has only even weight codewords, then $\mathcal{C}^\perp$ has a vector of weight n.

Solution :

1. We apply Mac Williams identity :

$$W_{\mathcal{C}^\perp} = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(y-x, y+(q-1)x) = \frac{1}{4^k}\sum_{i=1}^{n} A_i (y+3x)^{n-i}(y-x)^i.$$

   The coefficient of x^n is $\frac{1}{4^k}\sum_{i=0}^{n} A_i 3^{n-i}(-1)^i$

2. If the code has only even weight words, there are $\frac{1}{4^k}\sum_{i'=0}^{n/2} A_i 3^{n-2i'}$ codewords of weight n. This number is clearly strictly positive.

Problem 3 [15 points]. Let $t \geq 1$ be an integer.

1. Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_{q^t}$. Show that the subfield subcode $\mathcal{C}_{|\mathbb{F}_q}$ is also a cyclic code over $\mathbb{F}_q$.

2. Let α be a root of $x^2 - x + 2 \in \mathbb{F}_5[x]$ and $\mathbb{F}_{25}$ be defined as $\mathbb{F}_5[\alpha]$. The element α is primitive in $\mathbb{F}_{25}$. Show that the code $\mathcal{C}$ given by the following check matrix is cyclic

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^8 & \alpha^{16} & 1 & \alpha^8 & \alpha^{16} \\ 1 & \alpha^{20} & \alpha^{16} & -1 & \alpha^8 & \alpha^4 \end{pmatrix}.$$

3. Find a check matrix as well as its generating polynomial for the subfield subcode $\mathcal{C}_{|\mathbb{F}_5}$ of the code defined in the previous question.

Solution :

1. We need to check that $\mathcal{C}' = \mathcal{C}_{|\mathbb{F}_q}$ is stable under cyclic shift. Let $c = (c_0, \ldots, c_{n-1})$ be a code word of $\mathcal{C}'$. By definition, $c \in \mathbb{C}$, so by cyclicity of $\mathcal{C}$, $c' = (c_{n-1}, c_0, \ldots, c_{n-2})$ belongs to $\mathbb{C}$. But $c' \in \mathbb{F}_q^n$, so c' is in $\mathcal{C}'$ and thus $\mathcal{C}'$ is cyclic.

2. We observe that each row of H contains the successive powers of 1, α^8 and α^20 successively, which are 6-th roots of unity. If we interpret a codeword $c = (c_0, \ldots, c_{n-1})$ as a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, that imposes on c that $c(1) = c(\alpha^8) = c(\alpha^{20}) = 0$. In other word, $c(x)$ is a multiple of $g(x) = (x-1)(x-\alpha^8)(x-\alpha^{20})$.

3. A check relation over $\mathbb{F}_{25}$ can be brought to 2 linear relation over $\mathbb{F}_5$ by projection of the coefficient on the basis $(1, \alpha)$. Now, $\alpha^4 = 2 + 2\alpha$, $\alpha^8 = 1 + 2\alpha$, $\alpha^{16} = \alpha^{12}\alpha^4 = -\alpha^4 = 3 + 3\alpha =$ and $\alpha^{20} = -\alpha^8 = 4 + 3\alpha$. We obtain the following equations :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 1 & 1 & 3 \\ 0 & 2 & 3 & 0 & 2 & 3 \\ 1 & 4 & 3 & 4 & 1 & 2 \\ 0 & 3 & 3 & 0 & 2 & 2 \end{pmatrix}.$$

   We can eliminate the second line, to adjust the rank and the size of the matrix to get

$$\widetilde{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 3 \\ 0 & 2 & 3 & 0 & 2 & 3 \\ 1 & 4 & 3 & 4 & 1 & 2 \\ 0 & 3 & 3 & 0 & 2 & 2 \end{pmatrix}.$$

   as a a check matrix. To find the generator polynomial, we can note that if β is a root of the $g(x)$, all the conjugates by the Frobenius now must be roots of $\widetilde{g}(x)$, the generating polynomial of $\mathcal{C}'$. But $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. The minimal polynomial of α^8 and its conjugates is $x^2 + x + 1$, the minimal polynomial of α^{20} and its conjugates is $x^2 - x + 1$. So $\widetilde{g}(x) = (x-1)(x^2+x+1)(x^2-x+1)$.

Problem 4 [20 points]. The two parts of this problem are independent.

Part A

Let $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, $q(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$, and α be a root of p. Let $\mathcal{E}$ be the elliptic curve defined by the equation $f(x, y) = x^3 + x + 1 + y + y^2 = 0$.

1. Show that p and q are irreducible. Identify $\mathbb{K} = \mathbb{F}_2[\alpha]$. Express the roots of p and q in $\mathbb{K}$.
2. Show that for any root β of q, we have $p(\beta) = \beta + \beta^2$.
3. Count the number of points of $\mathcal{E}$ on $\mathbb{F}_2$ and on $\mathbb{K}$.
4. Describe the space $\Gamma_{<m}$ of polynomial functions on $\mathcal{E}$ over $\mathbb{K}$ and give its dimension.
5. Construct a $[12, 9, 3]_8$-code. Compare its parameters with the Singleton bound.

Part B (not part of the exam)

We denote by $M_8(n, k)$ the largest minimal distance of a $[n, k]_8$-code. In the sequel, $\mathcal{C}$ stands for a $[n, k, d]$-code and $\mathcal{C}'$ for a $[n', k', d']$-code with $d, d' \geq 2$.

1. Suppose that $\mathcal{C}'$ obtained from $\mathcal{C}$ by shortening. Compare the parameters of $\mathcal{C}$ and $\mathcal{C}'$. Deduce that $M_8(n + 1, k + 1) \leq M_8(n, k)$.
2. Assume that $\mathcal{C}'$ obtained from $\mathcal{C}$ by puncturing. Compare the parameters of $\mathcal{C}$ and $\mathcal{C}'$. Deduce that $M_8(n + 1, k) \leq M_8(n, k) + 1$.
3. Let H be the check matrix of a $[10, 8]_8$-code. Show that there must be two linearly dependent columns in H. Deduce that $M_8(10, 8) \leq 2$.
4. Prove that a $[12, 9, 3]_8$-code has an optimal minimum distance.

Solution :

Part A

1. As p and q have degree 3, they are decomposable if and only if they are divisible by a linear factor, i.e. if they have a zero on the ground field $\mathbb{F}_2$. This is not the case as $p(0) = p(1) = q(0) = q(1) = 1$. Thus α defines a field extension of degree 3. So $\mathbb{K}$ is the field $\mathbb{F}_8 = \{0, 1, \alpha, \ldots, \alpha^6\}$. The roots of p are the conjugates of α : α, α^2 and α^4. Since q is irreducible of degree 3, the roots of q are the remaining elements : α^3, α^5 and α^6. (On can check that they are conjugate).
2. If $q(\beta) = \beta^3 + \beta^2 + 1 = 0$, one clearly has that $p(\beta) = \beta^3 + \beta^2 + 1 - \beta^2 + \beta = \beta^2 + \beta$.
3. We need to solve the equation $y^2 + y + p(x) = 0$ in $\mathbb{F}_8$ for various values of $x \in \mathbb{F}_8$. If $x = 0$ or $x = 1$, we get $y^2 + y + 1 = 0$, so y should be a third root of unity which does not exist in $\mathbb{F}_8$ (we would need to be in an extension of $\mathbb{F}_4$, i.e. in $\mathbb{F}_{2^k}$ with k even). If x is a root of p, y is 0 or 1. If $x = \beta$ is a root of q, we have an obvious solution $y = \beta$ from the question before and thus a second solution (which by the way is $y = \beta + 1$). In total that give us $3 \cdot 2 + 3 \cdot 2 = 12$ points on $\mathcal{E}$ over $\mathbb{F}_8$ and no points over $\mathbb{F}_2$.

4. We have
$$\Gamma_{<m} = F_8[y]_{<m} \oplus xF_8[y]_{<m-1} \oplus x^2F_8[y]_{<m-2}$$
and dimension is $3m-3$.

5. We take the AG code $C(\mathcal{E}, m=4)$. We have directly a $[12, 3m-3, 15-3m]_8$-code, i.e. a $[12,9,3]_8$-code. The singleton bound would give $12 = k+d \leq n+1 = 13$. We have a defect of 1.

Part B

1. We have $n' = n-1$, $k' = k-1$ (except if there are only zeros at the ith position), $d = d'$. Now if $\mathcal{C}$ is a code that achieves $M_8(n+1, k+1)$, $\mathcal{C}'$ is a $[n,k]_8$ code with minimum distance d so $d \leq M_8(n,k)$, i.e. $M_8(n+1,k+1) \leq M_8(n,k)$.

2. We have $n' = n-1$, $k' = k$ (because $d > 1$ and so the ith axe is not a line contained in $\mathcal{C}$) and $d' = d$ or $d-1$ depending wether there exists a minimal codeword with support containing the position that is punctured. Now if $\mathcal{C}$ is a code that achieves $d = M_8(n+1,k)$, we can construct a code $\mathcal{C}'$ such that $d' = d$ or $d-1$ and by definition $d' \leq M_8(n,k)$. So $\min(d, d-1) \leq M_8(n,k)$. Thus $M_8(n+1,k) \leq M_8(n,k)+1$.

3. Either there is a zero column in H. Or, if not, we observe that there are 9 lines in the plane $\mathbb{F}_8^2$ (directed by the vectors $(1,\alpha)$, $\alpha \in \mathbb{F}_8$ or $(0,1)$). So any 2×10 matrix over $\mathbb{F}_8$ has two columns that span the same line, thus two linearly dependant columns. This shows that a $[10,8]_8$ code has surely a codeword of weight 2 (deduced from the linear relation on H). So $M_8(10,8) \leq 2$.

4. We have, by combining the previous questions, $M_8(12,9) \leq M_8(11,8) \leq M_8(10,8)+1 \leq 3$. This proves optimality.

Problem 5 [25 points]. Let $\mathcal{R}$ be a $[N, K, D]$-Reed-Solomon code over $\mathbb{F}_{2^m}$ where $N = 2^m - 1$. Let α be a primitive element of $\mathbb{F}_{2^m}$.

1. What is the minimal distance D of $\mathcal{R}$?
2. Let $\mathcal{C}$ be the code
$$\mathcal{C}_0 = \{(a_0, a_0; a_1, \alpha a_1; a_2, \alpha^2 a_2; \ldots; a_{N-1}, \alpha^{N-1} a_{N-1}) \in \mathbb{F}_{2^m}^{2N}; a \in \mathcal{R}\}.$$
What are the parameters of $\mathcal{C}_0$?
3. We identify $\mathbb{F}_{2^m}$ with $\mathbb{F}_2^m$ and consider the binary code $\mathcal{C}$ obtained from $\mathcal{C}_0$ where each component of a codeword in $\mathcal{C}_0$ is replaced by the corresponding binary m-tuple. What is the length, the dimension and the rate of $\mathcal{C}$?
4. Let $a \in \mathcal{R}$. Show that the blocks corresponding to $(a_i, \alpha^i a_i)$ and $(a_j, \alpha^j a_j)$ are always different unless $i = j$ or $a_i = a_j = 0$.
5. Show that in any non-zero codeword $c \in \mathcal{C}$, there are at least D blocks of length $2m$ with a non-zero pattern that do not pairwise intersect.
6. Let ℓ satisfy the condition $\sum_{i=1}^{\ell} \binom{2m}{i} \leq D$. By a worst case analysis, show that the minimum distance of $\mathcal{C}$ is at least $\sum_{i=1}^{\ell} i\binom{2m}{i}$.

Solution :

1. Reed-Solomon codes are MDS, so $D = N - K + 1$
2. The length of $\mathcal{C}_0$ is obviously $2N$. The dimension is still K as the map $\phi : \mathbb{F}_{2^m}^N \to \mathbb{F}_{2^m}^{2N}$ that maps $a \in \mathcal{R}$ to $(a_0, a_0; a_1, \alpha a_1; a_2, \alpha^2 a_2; \ldots; a_{N-1}, \alpha^{N-1} a_{N-1})$ is injective. (The kernel is trivial). Now the weight of $\phi(a)$ is twice the weight of a, so the minimal distance is $2D$.
3. The length of $\mathcal{C}$ is $n = 2Nm$. The dimension is $k = mK$. The rate is $k/n = K/2N$.
4. If $(a_i, \alpha^i a_i) = (a_j, \alpha^j a_j)$, we get $a_i = a_j$ and $\alpha^i = \alpha^j$ if $a_i \neq 0$. So $i = j \mod N$, i.e. $i = j$.
5. Let $a \in \mathcal{R}$. Since the minimum distance is D, at least D symbols of a are non zero. The corresponding elements $a_i, \alpha a_i$ are non zero, so their representation in $\mathbb{F}_2^m$ are also non-zero. This yields at least D non-zero blocks of length $2m$.
6. We have seen that there are at least D blocks with a non zero pattern and also that all those patterns are different. So in the worst case, i.e. when all the patterns have the lowest possible weight, we have $\binom{2m}{1}$ blocks of weight 1, $\binom{2m}{2}$ blocks of weight 2, and so on. So in total we have $\sum_{i=1}^{\ell} \binom{2m}{\ell}$ blocks of total weight $\sum_{i=1}^{\ell} i\binom{2m}{\ell}$.

Problem 6 [10 points]. Prove that the only binary MDS $[n,k]_2$-codes (with $0 < k < n$) are those with parameters $[n,1,n]_2$ and $[n,n-1,2]_2$. Give the name of those two exceptional codes.

Solution :
Let G be a generating matrix of a binary MDS $[n,k,d]_2$-code with $d = n-k+1$. Up to a reordering of the columns, one can assume that $G = [A|B]$ with A a $k \times k$ invertible matrix. But then, $G' = A^{-1}G$ is still a generating matrix of the code. Now, because of the minimal weight constraint, the rows of G' can only finish with $n-k$ non-zero symbols:

$$G' = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & \ddots & \ddots & \vdots & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & 0 & 1 & \cdots & 1 \\ 0 & \dots & 0 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

If $n-2 \geq k \geq 2$, we can form the code word $(1,1,0,\dots,0)$ which has weight $2 < d = n-k+1 \geq 3$. The only binary MDS codes are the $[n,1,n]_2$ repetition codes, the $[n,n-1,2]_2$ parity codes or $\mathbb{F}_2^n$.