ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Mock Exam May 12, 2011

Introduction to Coding Theory

May 12, 2011

- Any document or material is forbidden, except a hand-written recto verso A4 formula sheet.
- If you are using additional sheets, write your name and the number of the problem solved on that sheet clearly on top of the page.
- Use a separate sheet of paper for every problem you are working on. Number additionnal sheets.
- This mock exam will have no impact on your final grade.
- You have exactly 120 minutes and 120 points. Good luck!

Name:

Problem 1 / 27 points	Problem 2 / 32 points	Problem 3 / 10 points	Problem 4 / 18 points	Problem 5 / 33 points

Total
/ 120 points

Problem 1 [27 points]. Let $\mathcal{C}$ be a $[n,k]_q$-linear code over the field $\mathbb{F}_q$. We denote

$$\widetilde{C} = \{(x_0, x_1, \dots, x_n) \in \mathbb{F}_q^{n+1};\ (x_1, \dots, x_n) \in \mathcal{C} \text{ and } x_0^2 + \cdots + x_n^2 = 0)\}$$

1. Assume q is a power of 2, show that $\widetilde{\mathcal{C}}$ is linear.
2. Assume $\mathcal{C}$ is self-dual, show that $\widetilde{\mathcal{C}}$ is linear.
3. Assume $n = k = 1$ and $\mathcal{C} = \mathbb{F}_q$ (q odd), is $\widetilde{\mathcal{C}}$ linear ?
4. [Bonus] Under what condition is $\widetilde{\mathcal{C}}$ linear ?

Solution :

1. Let x and x' be codewords of $\widetilde{\mathcal{C}}$, we need to show that $x + x' \in \widetilde{\mathcal{C}}$. But

   $$(x_0 + x_0')^2 + (x_1 + x_1')^2 + \cdots + (x_n + x_n')^2 = x_0^2 + x_0'^2 + x_1^2 + x_1'^2 + \cdots + x_n^2 + x_n'^2 = 0$$

   Besides $0 \in \widetilde{C}$. So linearity is satisfied.

2. If $\mathcal{C}$ is self-dual, for any $x \in \widetilde{\mathcal{C}}$, $x_1^2 + \cdots + x_n^2 = 0$ and x_0 has to be zero. So $\widetilde{\mathcal{C}}$ is clearly linear.

3. If $\mathcal{C} = \mathbb{F}_q$, and $x \in \mathcal{C}$, x can be extended if $x = 0$ or if -1 is a square. Suppose $-1 = \alpha^2$ (that is the case iff $q \equiv 1 \mod 4$) , then x can be extended to $y = (\alpha x, x)$ and $y' = (-\alpha x, x)$. But by linearity $(y + y')/2 = (0, x)$ should also belong to $\widetilde{C}$ which is not the case. To sum up, either -1 is a square and then, $\widetilde{C}$ is not linear or else $\widetilde{C}$ is just reduced to the zero codeword.

4. We show that the only conditions under which $\widetilde{\mathcal{C}}$ is linear form three cases : the characteristic is two, or the characteristic is odd and the code is self-dual, or -1 is not a square and the restriction of the quadratic form $-x_1^2 + \cdots - x_n^2$ to $\mathcal{C}$ has rank one and represents only non-square.

   We can assume that the characteristic is not two. Then, if $x \in \widetilde{\mathcal{C}}$, then both $x = (x_0, x_1, \dots, x_n)$ and $x' = (-x_0, x_1, \dots, x_n)$ belong to $\widetilde{\mathcal{C}}$. By linearity, $x + x' \in \widetilde{\mathcal{C}}$, thus $4(x_1^2 + \cdots + x_n^2) = 0$. Thus for any codeword $x \in \mathcal{C}$, $x_1^2 + \cdots + x_n^2$ is 0 or the opposite of a non-square.

   Now, if -1 is a square, we can use the previous question to show that $x_1^2 + \cdots + x_n^2$ is zero on $\mathcal{C}$. Otherwise, $\widetilde{\mathcal{C}}$ cannot be linear. Thus, $\mathcal{C}$ is a self-dual code. If -1 is a non-square and the form is not zero on $\mathcal{C}$, then, we need to use the fact that any quadratic form of rank 2 represents -1 (this is a consequence of the theorem of Chevalley-Warning for instance), so if $k \geq 2$, we could find codewords $x = (x_0, x_1, \dots, x_n)$ and $x' = (-x_0, x_1, \dots, x_n)$ that belong to $\widetilde{\mathcal{C}}$ which would contradict linearity. We are left with the last case we had announced.

Problem 2 [32 points]. Let $\mathcal{C}$ be an $[n,k,7]_2$ perfect binary code.

1. Using the sphere packing bound (or Hamming bound), prove that
$$(n+1)\left((n+1)^2 - 3(n+1) + 8\right) = 3 \cdot 2^{n-k+1}.$$
2. Prove that $n+1$ is either 2^b or $3 \cdot 2^b$ with $b \leq n-k+1$.
3. Prove that $b < 4$.
4. Prove that $n = 23$ or $n = 7$.
5. Give the name of a perfect code with $n = 7$ and $n = 23$.

Solution :

1. The sphere packing bound gives :
$$\left(1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6}\right) 2^k = 2^n$$
which is equivalent to what is expected. (To do the computation, you should pose $n+1 = m$).
2. Since $n+1$ divides $3 \cdot 2^{n+1-k}$, it has to be of the form 2^b or $3 \cdot 2^b$ with $b \leq n-k+1$.
3. We note that $8 = 2^3$. Thus if $n+1 = 3^\alpha \cdot 2^b$ and $b \geq 4$, we have $3^\alpha \cdot 2^{b+3}(3^{2\alpha} \cdot 2^{2b-3} - 3^{\alpha+1} \cdot 2^{b-3} + 1) = 3 \cdot 2^{n-k+1}$. For $b \geq 4$, the second factor is equal to 1 modulo 2, so it contains a prime factor > 3 which is impossible. So we need to have $b \leq 3$.
4. We test all the possibilities (using the fact that $n \geq 7$) :

α	b	$(n+1)[(n+1)^2 - 3(n+1) + 8]$	n	k
0	3	$2^7 \cdot 3$	7	1
1	2	$3 \cdot 2^4 \cdot 29$		
1	3	$3 \cdot 2^{12}$	23	12

We deduce that we must have $n = 23$ or $n = 7$.

5. For $n = 7$, we can have the repetition code; for $n = 23$, the Golay code.

Problem 3 [10 points]. Show that a binary cyclic code of blocklength n is invariant under the transformation $c(x) \mapsto c(x^2) \bmod x^n - 1$.

Solution :
Note that $c(x^2) = c(x)^2$ on a field of characteristic 2. If the codeword $c(x)$ is given as $c(x) = m(x) \cdot g(x)$, then $c(x^2) = c(x)^2 = m(x)^2 \cdot g(x)^2$, which is also a multiple of $g(x)$ and thus a codeword.

Problem 4 [18 points]. Let $g(x)$ be the generator polynomial of a binary cyclic code of length n.

a Show that if $(x+1)$ is a factor of $g(x)$, the code contains no odd-weight codewords.

b If n is odd and $(x+1)$ is not a factor of $g(x)$, show that the code contains the all-ones codeword (Hint: recall that if $h(x)$ is a check polynomial for a cyclic code $\mathcal{C}$ of dimension k, then $x^k h(x^{-1})$ is a generator polynomial for $\mathcal{C}^\perp$).

Solution :

a If $(x+1)$ is a factor of $g(x)$, it is a factor of every codeword $c(x) = \sum_i c_i x^i$, so that $c(1) = 0$ and thus $\sum_i c_i = 0$. This implies that the codeword c is of even weight.

b Let $h(x)$ be the check polynomial for the code. As $g(x)h(x) = x^n - 1$ and $x+1$ divides $x^n - 1$, if $x+1$ is not a factor of $g(x)$ then it must be a factor of $h(x)$. It is thus a factor of the generator polynomial $x^k h(x^{-1})$ of the dual code. Therefore, all words of the dual code have even weight, which means that the all-ones vector must belong to the original code.

Problem 5 [33 points]. We work in the field $\mathbb{F}_{32} = \mathbb{F}_2[\alpha]$ given by the following log table.

1	$[0,1,0,0,0]$	2	$[0,0,1,0,0]$	3	$[0,0,0,1,0]$	4	$[0,0,0,0,1]$
5	$[1,0,1,0,0]$	6	$[0,1,0,1,0]$	7	$[0,0,1,0,1]$	8	$[1,0,1,1,0]$
9	$[0,1,0,1,1]$	10	$[1,0,0,0,1]$	11	$[1,1,1,0,0]$	12	$[0,1,1,1,0]$
13	$[0,0,1,1,1]$	14	$[1,0,1,1,1]$	15	$[1,1,1,1,1]$	16	$[1,1,0,1,1]$
17	$[1,1,0,0,1]$	18	$[1,1,0,0,0]$	19	$[0,1,1,0,0]$	20	$[0,0,1,1,0]$
21	$[0,0,0,1,1]$	22	$[1,0,1,0,1]$	23	$[1,1,1,1,0]$	24	$[0,1,1,1,1]$
25	$[1,0,0,1,1]$	26	$[1,1,1,0,1]$	27	$[1,1,0,1,0]$	28	$[0,1,1,0,1]$
29	$[1,0,0,1,0]$	30	$[0,1,0,0,1]$	31	$[1,0,0,0,0]$	$-\infty$	$[0,0,0,0,0]$

For example, you can read from the table that $\alpha^{25} = 1 + \alpha^3 + \alpha^4$.

1. Find the minimal polynomial of α, α^2, α^3 and α^4.
2. Check that the generator polynomial of the BCH code of length 31 and designed distance 5 is
$$g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1.$$
How many errors can this code correct ?
3. The following message has been received : $r(x) = x^{13} + x^8 + x^7$. Does it belong to the code ? If not, find the most likely codeword $m(x)$ that was sent.
4. What are the parameters of the code ?

Solution :

1. The elements α, α^2, and α^4 are conjugate and thus have the same minimal polynomial. The field extension in 5, so we need to express α^5 in terms of the lower powers of α. We have directly from the table that $g_1(x) = x^5 + x^2 + 1$ is the minimal polynomial. The minimal polynomial of α^3 requires more work. We could of course develop the conjugates :
$$g_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{17}) = x^5 + x^4 + x^3 + x^2 + 1.$$
An other way to obtain g_3 is to look directly for coefficients $(\epsilon_0, \dots, \epsilon_4) \in \mathbb{F}_2^5$ such that $\alpha^{15} + \epsilon_4\alpha^{12} + \cdots + \epsilon_1\alpha^3 + \epsilon_0 = 0$. This is equivalent to the system :
$$\begin{cases} \epsilon_0 & = & 1 \\ \epsilon_2 + \epsilon_3 + \epsilon_4 & = & 1 \\ \epsilon_4 & = & 1 \\ \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 & = & 1 \\ \epsilon_3 & = & 1 \end{cases}$$
which is easy to solve.
2. We develop the product $g_1 \cdot g_3$ to obtain g. This code has minimal distance at least 5, so it can correct 2 errors.

3. The received message cannot belong to the code as it is of weight 3. At least two errors must have occured. We have $r(x) = m(x) + x^r + x^s$ for a certain r and s. We have

$$r(\alpha) = \alpha^r + \alpha^s = \alpha^5 =: S_1$$

$$r(\alpha^2) = \alpha^{2r} + \alpha^{2s} = \alpha^{10} =: S_2$$
$$r(\alpha^3) = \alpha^{3r} + \alpha^{3s} = \alpha^{27} =: S_3$$
$$r(\alpha^4) = \alpha^{4r} + \alpha^{4s} = \alpha^{20} =: S_4$$

Fix the notation $X = \alpha^r$ and $Y = \alpha^s$, we have $X+Y = S_1 = 1+\alpha^2$ and $XY = \frac{S_1^3 - S_3}{S1} = S_2 + S_3/S_1 = \alpha^2$. We solve the equation

$$(z - X)(z - Y) = z^2 + S_1 z + S_2 - S_3/S_1 = z^2 + (1 + \alpha^2)z + \alpha^2$$

which have the two trival solutions 1 and α^2. So, up to permutation, $r = 1$ and $s = 2$. So the sent message was :

$$m(x) = x^{13} + x^8 + x^7 + x^2 + 1.$$

4. This code is $[31, 21, 5]_2$. The minimal distance comes from the fact that we have indeed found a codeword of weight 5 in the previous question.