ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Midterm Exam April 15, 2010

Introduction to Coding Theory

April 15, 2010

- 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.
- There are a total of 105 points to obtain. You need at least 70 points to pass.
- You have exactly three hours. Good luck!

Name:

Problem 1	Problem 2	Problem 3	Problem 4	Problem 5	Problem 6	Problem 7
/10 points	/20 points	/20 points	/10 points	/10 points	/10 points	/25 points

Total

Problem 1 [10 points]. Let C be a binary code of length 16 such that:

1. Every codeword has Hamming weight 6;
2. The distance between any two distinct codewords is always 8.

Given two real numbers a and b, one can construct vectors in $\mathbb{R}^n$ from codewords of C by replacing the 0's by a and the 1's by b. Compute the inner product of any two vectors. By choosing an appropriate value of a and b, derive an upper bound on the size of C.

Solution :
If $c \neq c'$ and v, v' stand for the corresponding vectors, $\langle v, v' \rangle = 2b^2+8ab+6a^2 = 2(a+b)(a+3b)$. By choosing $a = 1$ and $b = -1$, we obtain a family of orthonormal vectors of $\mathbb{R}^{16}$. Thus $|C| \leq 16$.

A construction of such a code can be the following. Represent $\mathbb{F}_2^{16}$ by 4×4 matrices. For each $i, j \in \{1, \ldots, 4\}$, consider the codeword $A_{i,j} \in \mathbb{F}_2^{4\times 4}$ where 1's are written in the ith line and jth column except at position (i, j).

Problem 2 [20 points]. Recall that the set of $n_1 \times n_2$ matrices can be seen as a vector space of dimension $n_1 n_2$. Let C_i be a $[n_i, k_i, d_i]_2$ linear code for $i = 1$ and 2. We consider the set C of those $n_1 \times n_2$ matrices for which every column, respectively every row, is a codeword in C_1, respectively C_2. Show that C is a $[n_1 n_2, k_1 k_2, d_1 d_2]$ linear code.

Solution :

La longueur du nouveau code est clairement $n_1 n_2$.

Soient G_1 et G_2 les matrices génératrices de C_1 et C_2 respectivement. Pour chaque vecteur ligne u de G_1 et v de G_2, on construit la matrice $A_{u,v}$ telle que $A_{u,v}[i,j] = u[i]v[j]$ où $A_{u,v}[i,j]$ est le coefficient en position i, j. Vérifions que cet ensemble de matrice est libre. Supposons que pour certains scalaires $\lambda_{u,v}$,

$$\sum_{u,v} \lambda_{u,v} A_{u,v} = 0$$

Soit $v^\star$ le vecteur dual d'un certain v_0 dans la base donnée par G_2. En multipliant la relation ci-dessus par $v^\star$, on obtient

$$\sum_{u} \lambda_{u,v_0} u = 0,$$

qui implique que tous les λ_{u,v_0} sont nuls. Comme v_0 est quelconque, la famille de matrice ainsi construite est bien libre. Donc la dimension du code est supérieure à $k_1 k_2$.

Pour voir que la dimension est exactement $k_1 k_2$, on peut sélectionner les indices $I = \{i_1, i_2, \ldots, i_{k_1}\}$ de k_1 colonnes indépendantes de G_1 et $J = \{j_1, j_2, \ldots, j_{k_2}\}$ de k_2 colonnes indépendantes de G_2. Une matrice du code C est alors entièrement déterminée par sa sous-matrice extraite aux positions $I \times J$.

Étant donné une matrice A non-nulle de C, il existe au moins une ligne non-nulle possédant par conséquent au moins d_1 coefficients non-nuls. Mais alors il existe au moins d_1 colonnes non-nulles, qui ont toutes un poids supérieur à d_2. Donc A a un poids supérieur à $d_1 d_2$. La construction ci-dessus avec deux mots u et v de C_1 et C_2 de poids minimaux montre que la distance minimale est bel et bien $d_1 d_2$.

Problem 3 [20 points]. The goal of this problem is to show that there is no $[15, 8, \geq 5]$ binary code.

1. Show that the Hamming bound is not good enough to exclude such a code.
2. Show that a $[15, 8, \geq 5]$ binary code must contain a word of weight 5 exactly by showing that there is no $[14, 8, 5]$-code.
3. Suppose C is a $[15, 8, 5]$-code. We consider a generator matrix of C whose first row is of weight 5 and the subcode C' generated by the other rows punctured at the 5 positions where the first row is not zero. What are the parameters of C' ? Show that the minimum distance of C' is larger than 3.
4. Show that C' cannot exist and conclude.

Solution :

1. The Hamming ball of radius 2 has volume $V = 1 + \binom{15}{1} + \binom{15}{2} = 121$ while $2^{15-8} = 128$. So the Hamming bound is not enough to exclude a $[15, 8, \geq 5]$ code.
2. The Hamming bound applies to exclude the existence of a $[14, 8, 5]$-code : the volume of the ball is then $V = 1 + \binom{14}{1} + \binom{14}{2} = 106$ while $2^{14-8} = 64$. Now a $[15, 8, > 5]$-code could be punctured at any position to give rise to a $[14, 8, 5]$ code which is impossible.
3. The length of C' is 10 and the dimension is 7.

   Denote by w the first row of the generator matrix of C. Suppose c' is a codeword from C' stemming from a word $c \in C$. Denote by α the number of positions where w and c both have 1, by β where w is 1 and c is 0 and by γ where w is 0 and c is 1. We have $\alpha + \beta = 5$, $\alpha + \gamma \geq 5$ and, since $c + w$ is a codeword, $\beta + \gamma \geq 5$. Combining these, we get $\gamma \geq \frac{5}{2}$. So the minimum distance of C' is ≥ 3.
4. Again the Hamming bound excludes the existence of a $[10, 7, 3]$ code since the volume of the ball of radius 1 is $v = 1 + 10 = 11$ while $2^{10-7} = 8$. So there is no $[15, 8, \geq 5]$ binary code.

Problem 4 [10 points]. Let r be an integer and C be a $[2^r-1, 2^r-1-r, 3]_2$-code. Show that, up to permutation of the coordinates, C is equal to a Hamming code.

Solution :
Let H be a check matrix of C. Then H is a $r \times (2^r - 1)$ matrix of rank r. If H has two equal columns at position i and j, then the word of weight 2 with ones in position i and j is a codeword of weight 2, which is impossible. If H has a column of zero in position i and c is a codeword, then the word c' obtained from c by flipping the bit in position i is also a codeword. But $c + c'$ has weight 1, which is impossible. Now there are only $2^r - 1$ non zero vectors of length r and all of them must appear. So up to ordering of the columns, H is the check matrix of the Hamming code.

Problem 5 [10 points]. If C is a binary code such that $C \subseteq C^{\perp}$, show that every codeword has even weight. Furthermore, if each row of the generator matrix of C has weight divisible by 4, show that so does every codeword.

Solution :
Let c be in C, then by assumption $\langle c, c\rangle = 0 = \sum_{i=1}^{n} c_i^2 = \sum_{i=1}^{n} c_i \mod 2$.

Suppose that c and c' have both weight divisible by 4. Denote by α the number of positions where c and c' are both equal to 1, β where c is 1 and c' is 0, γ where c is 0 and c' is 1. We have thus $\alpha+\beta \equiv 0 \mod 4$, $\alpha+\gamma \equiv 0 \mod 4$ and $\alpha \equiv \langle c, c'\rangle \equiv 0 \mod 2$. So $2\alpha \equiv 0 \mod 4$ and $2\alpha+\beta+\gamma \equiv 0 \mod 4$, i.e. $\beta+\gamma \equiv 0 \mod 4$. But $\beta+\gamma$ is the weight of $c+c'$. Now by induction, any codeword is a finite sum of rows of the generator matrix and has thus a weight divisible by 4.

Problem 6 [10 points]. We set $n = 2^r - 1$. Let β be a primitive n-th root of unity in $\mathbb{F}_{2^r}$. We consider the code defined by

$$C = \{c(x) \in \mathbb{F}_2[x]; \deg c < n \text{ and } c(\beta) = 0\}.$$

What is the dimension of C ? Identify C.

Solution :
A way to write a check matrix for C is to fix a basis of $\mathbb{F}_{2^r}$ as a $\mathbb{F}_2$-vector space and to project the condition $c(\beta) = 0$ on each coordinate. Since β is a primitive n-th root of unity, β^i describe exactly once $\mathbb{F}_{2^r} \setminus \{0\}$ when $i = 1, \ldots, n-1$, so the columns of the check matrix are exactly all the $2^r - 1$ possible non-zero vectors of $\mathbb{F}_2^r$. Thus C is the Hamming code of dimension$n - r$.

Problem 7 [25 points]. Let $\mathbb{F}_9$ be defined as $\mathbb{F}_3[\omega]$ where $\omega^2 = -1$ and define $\beta = 1 + \omega$. A BCH code of designed distance 4 and associated with the first powers of β (β^0, β^1, ...) is being used. We receive $y(z) = 1 + z + z^7$.

1. Construct the power table of β.
2. Find the generating polynomial $g(x)$ of the code. What are the parameters of the code? How many errors can this code accept ?
3. Decode the received message.

Solution :

1. Here is the table

i	β^i	i	β^i
1	$1+\omega$	5	$-1-\omega$
2	$-\omega$	6	ω
3	$1-\omega$	7	$-1+\omega$
4	-1	8	1

2. The conjugate root of β is β^3. The conjugate root of β^2 is β^6. So we get $g(z) = (z-1)(z-\beta)(z-\beta^2)(z-\beta^3)(z-\beta^6) = z^5 - z^3 + z^2 + z + 1$. The code is $[8, 3, 5]_3$-code.
3. We can correct up to 2 errors. Suppose $y(z) = c(z) + e(z)$ with $e(z) = az^r + bz^s$, where $a, b \in \mathbb{F}_3$ and $r, s \leq 7$. Set $X = \beta^r$ and $Y = \beta^s$. We have

$$S_0 = y(\beta^0) = e(\beta^0) = 0 = a + b$$

$$S_1 = y(\beta^1) = 1 - \omega = aX + bY$$

$$S_2 = y(\beta^2) = 1 = aX^2 + bY^2$$

So $a = -b$, $S_2/S_1 = X + Y = \frac{1}{1-\omega} = -1 - \omega$.

We can assume without loss of generality that $a = 1$ (if $a = -1$, this will exchange X and Y). So $X - Y = 1 - \omega$. So $X = -\omega = \beta^2$ and $Y = -1 = \beta^4$. So $e(z) = z^2 - z^4$. The sent message was thus $z^7 + z^4 - z^2 + z + 1 = g(x)(z^2 + 1)$