ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Final Exam June 30, 2010

Introduction to Coding Theory

June 30, 2010

- 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.
- There are a total of 105 points to obtain. You need at least 60 points to pass.
- You have exactly three hours. Good luck!

Name:

Problem 1 /8 points	Problem 2 /30 points	Problem 3 /15 points	Problem 4 /12 points	Problem 5 /20 points	Problem 6 /20 points

Total

CONVENTIONS & REMINDERS

- $\mathbb{F}_q$ stands for the finite field with q elements, $\mathbb{Z}/n\mathbb{Z}$ stands for the ring of integers modulo n.
- A q-ary code of minimum distance d is called *perfect* if the space $\mathbb{F}_q^n$ is exactly the disjoint union of the Hamming balls of radius $\lfloor (d-1)/2 \rfloor$ around the codewords.

Problem 1 [8 points]. Let C_1 be a $[n,k,d]_q$-code and C_2 be a $[n,k-1,d+1]_q$-code such that $C_2 \subseteq C_1$. We fix a vector $v \in C_1 \smallsetminus C_2$.

1. Show that any codeword c of C_1 has a unique decomposition $c = w + xv$ where $w \in C_2$ and $x \in \mathbb{F}_q$.
2. Show that the set C of concatenated words (c, x) of length $n+1$, where $c = w+xv \in C_1$, is a $[n+1,k,d+1]_q$-code.

Solution :

1. The code C_2 is a codimension 1 subspace of C_1. As v doesn't belong to C_2, $C_1 = C_2 \oplus \mathbb{F}_q v$, whence the result.
2. Either x is zero and c belongs to C_2, then $(c,x) = (w,0)$ has weight $\geq \min C_2 = d+1$, or x is non zero and c has weight $\geq \min C_1 = d$, so (w,x) has weight $\geq d+1$.

Problem 2 [30 points]. The goal of this problem is to study the asymptotic behavior of the largest possible dimension k of codes on $\mathbb{F}_q$ when the minimum distance d is fixed and the length n goes to infinity. For fixed d and q, we define

$$\varkappa_q(d) = \liminf_{n\to\infty} \left(\inf_{C\ [n,k,d]_q\text{-code}} \frac{n-k}{\log_q n} \right).$$

1. (a) Prove that for any $[n,k,d]_q$-code, we have

$$n-k \geq \log_q \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i.$$

   (b) Show that $\log_q \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i \sim_{n\to\infty} \lfloor \frac{d-1}{2} \rfloor \log_q n$ and that

$$\left\lfloor \frac{d-1}{2} \right\rfloor \leq \varkappa_q(d).$$

2. (a) Let I_1 be $\{1,\dots,d-1\}$ and $I_0 = I_1 \setminus (qI_1)$. What is the cardinality of I_0 ?

   (b) Let α be a primitive element of $\mathbb{F}_{q^m}$ and $g(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of the set $(\alpha^i)_{i\in I_1}$. Consider $I \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $g(x) = \prod_{i\in I} x - \alpha^i$. Show that

$$I = I_0 \cup qI_0 \cup \dots \cup q^{m-1} I_0 \mod n.$$

   Deduce an upper bound on I.

   (c) Show that for any integer $m \geq 2$, there exists a code of parameters $[n,k,\geq d]_q$ with $n = q^m - 1$ and

$$k \geq n - m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor \right).$$

   (d) Show that

$$\varkappa_q(d) \leq \left\lfloor \frac{(d-1)(q-1)}{q} \right\rfloor$$

3. Compute explicitly the value of $\varkappa_2(d)$ for any d.

4. (a) Consider the q-ary Hamming code $\mathcal{H}_m$ defined over $\mathbb{F}_q$ by the following check matrix H_m ($m \geq 2$). The matrix H_m has m rows. For each line of $\mathbb{F}_q^m$, select an arbitrary basis vector and use it as a column of H_m. Show that $\mathcal{H}_m$ is a $\left[n = \frac{q^m-1}{q-1}, n-m, 3\right]_q$-code.

   (b) Use the family of Hamming codes to prove that for any q, $\varkappa_q(3) = 1$.

Solution :

1. (a) This is the Hamming bound

(b) For fixed d, $A(n) = \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i$ is a polynomial of degree $\delta = \lfloor \frac{d-1}{2} \rfloor$ in n, say $a_\delta n^\delta + \cdots + a_0$, so $\log_q \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i = \log_q n^\delta + \log_q \left(a_\delta + a_{\delta-1}\frac{1}{n} + \cdots + a_0 \frac{1}{n}\right)$, which gives the equivalence. Now we deduce that for any code,

$$\frac{\log_q A(n)}{\log_q n} \leq \frac{n-k}{\log_q n}$$

But $\lim_{n\to\infty} \frac{\log_q A(n)}{\log_q n} = \delta$, so

$$\left\lfloor \frac{d-1}{2} \right\rfloor \leq \varkappa_q(d).$$

2. (a) $|I_0| \leq d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor$.

(b) The roots of g are exactly the α^i for $i \in I_1$ and their conjugates under the action of the Frobenius, i.e. when i belongs to I, $q \cdot i \mod n$ belongs also to I. Since $I_1 \subseteq I_0 \cup qI_0$ and $J = I_0 \cup qI_0 \cup \cdots \cup q^{m-1}I_0 \mod n$ is stable under the multiplication by q, $I \subseteq J$.
On the other hand $I_0 \subseteq I_1 \subseteq I$ and J is the smallest stable set spanned by I_0 under the multiplication by q, so $J \subseteq I$.
It is thus clear that $|I| \leq m|I_0| = m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor\right)$.

(c) We consider the BCH code of designed distance d of length $n = q^m - 1$. Its generating polynomial is exactly $g(x)$, thus its dimension k satisfies $n - k = \deg g = |I| \leq m\left(d - 1 - \left\lfloor \frac{d-1}{q} \right\rfloor\right)$.

(d) From the previous question we know that when $n = q^m - 1$,

$$\inf \frac{n-k}{\log_q n} \leq \frac{m \left\lfloor \frac{(d-1)(q-1)}{q} \right\rfloor}{\log_q n}$$

But $m = \log_q(n+1) \sim_{n\to\infty} \log_q n$. So, taking the $\liminf$,

$$\varkappa_q(d) \leq \left\lfloor \frac{(d-1)(q-1)}{q} \right\rfloor$$

3. Both inequalities agrees and yield $\varkappa_2(d) = \lfloor \frac{d-1}{2} \rfloor$.

4. (a) Any of the $|\mathbb{F}_q^m| - 1$ non zero vectors of $\mathbb{F}_q^m$ is the basis of a line, but $|\mathbb{F}_q^\times| = q - 1$ vectors give rise to the same line, so there are exactly $n = \frac{q^m-1}{q-1}$ columns in H_m. The matrix H_m contains in particular a submatrix of the diagonal shape (the basis vectors of the axis), so its rank is m and $k = n - m$. Finally, there must be column vectors

$$\begin{pmatrix} a \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \quad \begin{pmatrix} 0 \\ b \\ 0 \\ \vdots \end{pmatrix}, \quad \begin{pmatrix} c \\ d \\ 0 \\ \vdots \end{pmatrix}$$

with $abcd \neq 0$. So $(\frac{c}{a}, \frac{d}{b}, -1, 0 \cdots)$ is a codeword of weight 3. On the other hand, any codeword of weight ≤ 2 would imply that two columns are linearly independent, which is excluded by construction.

(b) According to the previous question, $\inf \frac{n-k}{\log_q n} \leq \frac{m}{\log_q \frac{q^m-1}{q-1}}$. But $\log_q \frac{q^m-1}{q-1} \sim \log_q m$, so $\varkappa_q(3) \leq 1$. On the other hand, using the first question, $\varkappa_q(3) \geq 1$.

Problem 3 [15 points]. Let $\mathbb{F}_{25}$ be given by $\mathbb{F}_5[\alpha]$ where $\alpha^2 - \alpha + 2 = 0$. You can use without a proof that α spans the multiplicative group $\mathbb{F}_{25}^\times$. Consider the plane curve $\mathcal{X}$ defined over $\mathbb{F}_{25}$ by the equation

$$y^2 = x^6 + 1.$$

1. Show that $x^6 + 1$ is not a square and deduce that $\mathcal{X}$ is irreducible.
2. Show that the application $\mathcal{N} : z \mapsto z^6$ is a well-defined surjective group homomorphism from $\mathbb{F}_{25}^\times$ to $\mathbb{F}_5^\times$.
3. Count the number of points of $\mathcal{X}$.
4. Give a basis of polynomial functions on $\mathcal{X}$ of degree < 6, < 7 and < 8.
5. Design linear codes with parameters $[44, 21, \geq 14]_{25}$, $[44, 27, \geq 8]_{25}$ and $[44, 33, \geq 2]_{25}$. Justify your answer.

Solution :

1. As α is primitive, $\alpha^{12} = -1$ and so $x^6+1 = \prod_{i=0}^{5}(x-\alpha^{2+4i})$ has 6 distinct roots. Thus it is not a square in $\mathbb{F}(x)$. (It is also possible to expand the polynomial $(x^3+ax^2+bx+1)^2$, identify the coefficients with $x^6 + 1$ and observe that this is impossible). The only factorisation of $y^2 - (x^6 + 1)$ in $\mathbb{F}(x)[y]$ would be $(y - a)(y + a)$ for some $a \in \mathbb{F}(x)$ but we have seen that this impossible.
2. $\mathcal{N}$ is clearly a group homomorphism, since the multiplication is commutative. Now $\left(x^6\right)^5 = x^{30} = x^{24+6} = x^6$ so for any x, x^6 belongs to $\mathbb{F}_5^\times$. Its is surjective, since $\alpha^6 = 2$ which spans $(\mathbb{F}_5^\times, \times)$. We deduce that $\mathcal{N}$ is a $6 - 1$ map.
3. Rewrite the defining equation as $y^2 - 1 = x^6$. We need that $\sigma = y^2 - 1$ belongs $\mathbb{F}_5$, in which case we have the following possibilities.

σ	y	$\sharp\{x; \mathcal{N}(x) = \sigma\}$
0	± 1	1
1	$\pm\alpha^3$	6
2	$\pm\alpha^9$	6
3	± 2	6
4	0	6

   So we have $2 \cdot 1 + 2 \cdot 6 + +2 \cdot 6 + 2 \cdot 6 + 1 \cdot 6 = 44$ points.

4. We need to give a basis of $\mathbb{F}_{25}[x, y]/\langle y^2 - x^6 - 1\rangle$. Using a Euclidean division or the theorem of the course, it's enough to consider only the following monomials.

$$\Gamma_{<6} = \langle 1, y, y^2, y^3, y^4, y^5, x, xy, xy^2, xy^3, xy^4, x^2, x^2y, x^2y^2, x^2y^3, x^3, x^3y, x^3y^2, x^4, x^4y, x^5\rangle$$
$$\Gamma_{<7} = \langle \Gamma_{<6}, y^6, xy^5, x^2y^4, x^3y^3, x^4y^2, x^5y\rangle$$
$$\Gamma_{<8} = \langle \Gamma_{<7}, y^7, xy^6, x^2y^5, x^3y^4, x^4y^3, x^5y^2\rangle$$

5. We use the AG codes obtained by evaluating the functions of $\Gamma_{<m}$ on the 44 points of the curve (m = 6, 7, 8). Bezout theorem ensures that the minimal distance is at least $44 - 6(m - 1)$ which agrees with the question. The dimension of the codes can be directly computed from the last question.

Problem 4 [12 points].

1. How many binary cyclic codes of length 7 are there?
2. Let C_1 and C_2 be the binary cyclic codes of length 7 with generator polynomials $g_1(x) = x-1$ and $g_2(x) = x^6+x^5+x^4+x^3+x^2+x+1$, respectively. What are their parameters?
3. Consider C, the binary cyclic code of length 7 generated by the polynomial $g(x) = x^4+x^3+x^2+1$. What are its parameters?
4. A burst error of length t is an error of weight t on t consecutive positions. Show that C can correct all burst errors of length 2.

Solution :

1. $x^7 - 1$ can be factored into irreducible factors as
$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1).$$
For each irreducible factor, we have two choices (to take it or not to take it as a factor of the generator polynomial), hence there are 8 binary cyclic codes of length 7.
2. C_1 with generator polynomial $g_1(x) = x-1$ has dimension 6 and minimum distance 2. In fact, it is the code containing all words of even weight.
C_2 with generator $g_2(x) = x^6+x^5+x^4+x^3+x^2+x+1$ has dimension 1. In fact, it contains only the all-zero and all-one words and has distance 7.
3. C is a $[7, 3, d]$-code. We know that $d \leq 4$ since C contains the word 00011101 corresponding to $g(x)$. To see that $d = 4$, note that $g(x) = (x-1)(x^3+x+1)$. Let ω be a root of x^3+x+1. It is easy to check that ω is a primitive 7-th root of unity. Then we have that $g(1) = g(\omega) = g(\omega^2) = 0$ so that $d = 4$ by the BCH bound.
Alternatively, note that C contains the codeword 00011101 and all its cyclic shifts. There are 8 such distinct cyclic shifts, and C has dimension 3, so that C consists exactly of the cyclic shifts of 00011101, all of which have weight 4.
4. Let e_i denote the vector of length 7 consisting of 1's in the ith and $i+1$st coordinates and 0's everywhere else. C can correct all bursts of length 2 if and only if all the error vectors e_i have distinct syndromes. Let H be a check matrix of C and suppose C cannot correct all bursts of length 2; that is, there exist $i \neq j$ such that $He_i = He_j$, i.e., $H(e_i + e_j) = 0$. This means that the word $e_i + e_j$ belongs to the code. Since C has minimum distance 4, $e_i + e_j$ must have weight at least 4, so that i, $i+1$, j and $j+1$ are all distinct. The corresponding codeword thus has two sets of consecutive 1's; but no such codeword can exist, since all codewords are cyclic shifts of 00011101.

Problem 5 [20 points]. Let C be an (n, M, d) binary code. The Hamming distance between a vector $y \in \mathbb{F}_2^n$ and C, denoted by $d(y, C)$, is the smallest Hamming distance between y and a codeword in C, *i.e.*,

$$d(y, C) = \min_{c \in C} d(y, c).$$

The *covering radius* r of C is the largest distance from C to any vector y in $\mathbb{F}_2^n$, *i.e.*,

$$r = \max_{y \in \mathbb{F}_2^n} d(y, C).$$

1. Find the covering radii of the binary repetition code and the binary Hamming code of length $2^\ell - 1$.
2. Show that
$$M \cdot V_2(n, r) \geq 2^n,$$
where $V_2(n, r)$ denotes the volume of a Hamming ball of radius r in $\mathbb{F}_2^n$.
3. Show that a binary perfect code has an odd minimum distance.
4. Show that $r \geq (d-1)/2$ with equality if and only if C is perfect.
5. A code is called *maximal* if and only if the addition of any new codeword to it reduces its minimum distance. Show that if C is maximal then $r < d$.
6. A *coset* of C defined by the vector $y \in \mathbb{F}_2^n$ is the set $y + C = \{y + c | c \in C\}$. A *coset leader* is a minimal weight codeword in a coset. Show that if C is a linear $[n, k, d]_2$ code, then r is the largest among the Hamming weights of the coset leaders of C in $\mathbb{F}_2^n$.

Solution :

1. The repetition code consists of the all-zero and the all-one codewords. In this case it is easy to see that the covering radius is $\lfloor n/2 \rfloor$.

   Consider an $[n = 2^\ell - 1, k = 2^\ell - \ell - 1, 3]_2$-Hamming code. Since it has minimum distance 3, the spheres of radius 1 centered around the codewords are disjoint. Each sphere of radius 1 contains $n + 1 = 2^\ell$ vectors of $\mathbb{F}_2^n$. There are $2^k = 2^{2^\ell - \ell - 1}$ such spheres, so that the spheres cover $2^\ell 2^{2^\ell - \ell - 1} = 2^{2^\ell - 1} = 2^n$ vectors. The spheres of radius 1 centered around the codewords thus cover the whole space $\mathbb{F}_2^n$. Therefore any word in the space falls in one of these spheres, so that the covering radius of the Hamming code is 1.
2. By definition of the covering radius, the balls of radius r around the codewords cover the space $\mathbb{F}_2^n$ (with possibly some overlaps). The bound follows.
3. If C is perfect, then the balls of radius $\lfloor (d-1)/2 \rfloor$ centered around the codwords cover the space $\mathbb{F}_2^n$. Suppose d was even. Take two codewords c_1, c_2 such that $d(c_1, c_2) = d$ and let B_1, B_2 be the balls of radius $\lfloor (d-1)/2 \rfloor$ centered around c_1 and c_2 respectively. Let y be such that y is exactly at distance $d/2$ from both c_1 and c_2. Then y belongs

neither to B_1 nor to B_2. It cannot belong either to any other ball B_3 centered around some c_3, since then y would be at distance $d/2$ from c_1 and $\leq \lfloor (d-1)/2 \rfloor < d/2$ from c_3, thus violating the minimum distance property stating that $d(c_1, c_3) \geq d$. y is thus not contained in any of the balls centered around the codewords, a contradiction.

4. Consider the (disjoint) balls of radius $\lfloor \frac{d-1}{2} \rfloor$ around the codewords. If they don't cover the space, there exists a vector y that does not belong to any of the balls, i.e., $d(y, C) > \lfloor \frac{d-1}{2} \rfloor$, hence $r > \lfloor \frac{d-1}{2} \rfloor$. It is easy to check that whether d is odd or even, this implies that $r > \frac{d-1}{2}$.

   Now consider the case where the disjoint balls of radius $\lfloor \frac{d-1}{2} \rfloor$ centered around the codewords cover the space, i.e., C is a perfect code and $\frac{d-1}{2} = \lfloor \frac{d-1}{2} \rfloor$ is an integer. In this case, $r \leq \frac{d-1}{2}$. To prove equality, it is enough to exhibit any y such that $d(y, C) = \frac{d-1}{2}$. For this, take any y at distance exactly $\frac{d-1}{2}$ from some codeword c. y cannot be closer to any other codeword c' by the minimum distance property. Hence $d(y, C) = \frac{d-1}{2}$ and thus $r = \frac{d-1}{2}$. Conversely, suppose $r = \frac{d-1}{2}$. Then by definition, the balls of radius $\frac{d-1}{2}$ centered around the codewords cover the space so that C is perfect.

5. C is maximal if and only if for any vector y in $\mathbb{F}_2^n \backslash C$, there exists a codeword c of C such that $d(c, y) < d$. This means that for all y in $\mathbb{F}_2^n \backslash C$, $d(y, C) < d$. Since for all $c \in C$, $d(c, C) = 0$, we have that for all y in $\mathbb{F}_2^n$, $d(y, C) < d$ and thus $r < d$.

6. For a given y, the weights of the elements of the coset $y + C$ are the distances of y to all the codewords of the code C. The coset leader of this coset is exactly $d(y, C)$. Therefore $r = \max_{y \in \mathbb{F}_2^n} d(y, C)$ is exactly the maximum weight of a coset leader.

Problem 6 [20 points]. Let $n = 2k$ and consider the field $\mathbb{F}_{2^k}$. We identify $\mathbb{F}_{2^k}$ as a $\mathbb{F}_2$-vector space with $\mathbb{F}_2^k$. We construct the following family of codes: for each $\alpha \in \mathbb{F}_{2^k}$, let

$$C_\alpha = \{(x, \alpha x) | x \in \mathbb{F}_{2^k}\}.$$

Here $(x, \alpha x)$ denotes the n-bit vector obtained when viewing x and αx as elements of $\mathbb{F}_2^k$.

1. Show that the C_α's are linear codes of rate 1/2. How many such codes are there?
2. Show that for $\alpha \neq \beta$, $C_\alpha \cap C_\beta = \{0\}$.
3. Let $d(C_\alpha)$ denote the minimum distance of C_α and $V(n, d)$ denote the volume of the ball of radius d in $\mathbb{F}_2^n$. For $\varepsilon > 0$, show that if d satisfies

$$\frac{1}{\varepsilon} V(n, d) \leq 2^k,$$

then at most $\varepsilon 2^k$ codes among the C_α's verify $d(C_\alpha) \leq d$.

(Hint: bound the number of "bad" C_α's by considering their intersections with $B_n(0, d)$, the ball of radius d centered at 0.)

4. Prove that for all $\varepsilon > 0$, there exist an n_0 such that for any even $n \geq n_0$, all but an ε-fraction of the codes C_α defined as above are $[n, \frac{n}{2}, \geq (H^{-1}(1/2) - \varepsilon)n]_2$-codes.

Solution :

1. Clearly, for any α, $0 \in C_\alpha$ and corresponds to the choice $x = 0$. Moreover, for two codewords $(x, \alpha x)$ and $(y, \alpha y)$, we have that $(x, \alpha x) + (y, \alpha y) = (x + y, \alpha(x + y)) \in C_\alpha$ by linearity of addition in $\mathbb{F}_{2^k}$. Hence the C_α are linear codes of size 2^k, i.e., of dimension k, which corresponds to a rate of $k/n = 1/2$.
There are 2^k such codes.
2. Suppose that for some α and β, there exists a nonzero codeword in the intersection $C_\alpha \cap C_\beta$. Then this codeword must be of the form $(x, \alpha x) = (x, \beta x)$. In addition, $x \neq 0$ (since otherwise $(x, \alpha x)$ is the zero codeword). Hence from $\alpha x = \beta x$, we get that $\alpha = \beta$.
3. If C_α is such that $d(C_\alpha) \leq d$, then $C_\alpha \cap B_n(0, d)$ contains at least one nonzero element. But we know that the C_α's are disjoint, so that no more than $|B_n(0, d)| = V(n, d)$ of them can intersect with $B_n(0, d)$. Therefore,

$$\sharp\{C_\alpha : d(C_\alpha) \leq d\} \leq V(n, d).$$

If d is such that $\frac{1}{\varepsilon} V(n, d) \leq 2^k$, then

$$\sharp\{C_\alpha : d(C_\alpha) \leq d\} \leq \varepsilon 2^k.$$

4. Given any $\varepsilon > 0$, we want to choose d as large as possible such that $V(n,d)/2^k \leq \varepsilon$. We use the fact that $V(n,d) = 2^{nH(d/n)+o(n)}$ to get the following requirement on d:

$$2^{n(H(d/n)-1/2)+o(n)} \leq \varepsilon.$$

Asymptotically, it is enough to have $H(d/n) - 1/2 < 0$ for $2^{n(H(d/n)-1/2)+o(n)}$ to be as small as we want for n large enough. Thus d should be such that

$$d/n < H^{-1}(1/2).$$

In particular, if d is such that

$$d \geq (H^{-1}(1/2) - \varepsilon)n,$$

we know from part 3 that at most an ε-fraction of the C_α's are such that $d(C_\alpha) \leq d$. The other C_α's are $[n, \frac{n}{2}, \geq (H^{-1}(1/2) - \varepsilon)n]_2$-codes. These are codes of rate $r = 1/2$ and relative minimum distance δ such that

$$H^{-1}(r) - \varepsilon \leq \delta < H^{-1}(r).$$

Since the entropy function is increasing on $[0, 1/2]$, we have that

$$H(\delta) \geq r - \varepsilon'$$

and thus

$$r \geq 1 - H(\delta) + \varepsilon'$$

for ε' as small as we want.