Théorie de l'Information et Codage: Fiche d'exercices 4

à rendre pour le 4 juin 2013.

Instructions: merci à chacun de rendre une copie manuscrite. Si vous avez réfléchi à plusieurs sur un problème, mettez les noms de vos collaborateurs.
Les problèmes 1,2,3,4 constituent ce dernier devoir. Les problèmes 5,6,7,8 sont facultatifs et ne seront corrigés que s'il vous manque des points pour valider le cours.

Problème 1: Paradoxe de St Petersbourg (6 points)
On considère le jeu suivant: pour un prix d'entrée de c euros, un joueur recoit 2^k euros avec probabilité 2^{-k}. Certains disent qu'ils ont 'intérêt' à jouer quelque soit la valeur de c. Pourquoi? Bernoulli dans Specimen theoriae novae de mensura sortis (1738) propose de résoudre le paradoxe en intoduisant une fonction d'utilité logarithmique pour l'argent: une somme s a une utilité $\ln s$. L'utilité moyenne devient alors $E[\ln X] = \ln 4$ et donc Bernoulli accepte de jouer uniquement si $c < 4$. Le choix de la fonction d'utilité logarithmique étant arbitraire, nous allons étudier une autre solution de ce paradoxe.

1. On suppose maintenant que le joueur peut acheter une part du jeu. Par exemple, s'il investit $c/2$ euros dans le jeu, il recoit $X/2$ avec $P(X = 2^k) = 2^{-k}$. On suppose les $X_1, X_2, \ldots$ i.i.d. et que le joueur est obligé de réinvestir la totalité de sa fortune à chaque étape. Soit $F_n(c)$ sa fortune au temps n. On suppose que $F_0(c) = 1 \leq c$. Montrer qu'il existe c^* tel que pour $c < c^*$ sa fortune tend vers l'infini et si $c > c^*$ elle tend vers 0. Calculer la valeur du prix 'équitable' c^* et pour une distribution différente de X.

2. Etudier le cas où le joueur peut choisir de ne miser qu'une fraction de sa fortune. Pour quelle valeur de c, le joueur va-t-il choisir de parier toute sa fortune?

3. Question bonus: Si on a $P(X = 2^{2^k-1}) = 2^{-k}$, faut-il investir la totalité de sa fortune pour toute valeur de c?

Dans les deux problèmes qui suivent, les codes de Reed-Solomon sont supposés tels que leur polynôme générateur g n'ait pas 1 comme racine, $g(1) \neq 0$.

Problème 2: construction de codes binaires à partir de codes de Reed-Solomon (5 points)
Soit $\xi_1, \ldots, \xi_m$ une base de l'espace vectoriel $F(2^m)$ sur $F(2)$. Alors si $\beta = \sum_{i=1}^m b_i \xi_i$ est un élément de $F(2^m)$ avec $b_i \in F(2)$, on représente β par $b_1, \ldots, b_m$.

1. Montrer que cette correspondance transforme un code linéaire sur $F(2^m)$ en un code linéaire sur $F(2)$. Donner la dimension et une borne sur la distance minimale du code obtenu.

2. En utilisant la base $1, \alpha$ pour $F(4)$ sur $F(2)$ avec $\alpha^2 + \alpha + 1 = 0$, expliciter les mots code du code binaire de longueur 6 obtenu à partir du code de Reed-Solomon sur $F(4)$ vu en cours (de polynôme générateur $g(X) = X + \alpha^2$).

3. Donner la dimension et une borne sur la distance minimale des deux codes suivants: si $c = (c_1, \ldots, c_{N-1})$ est un mot code d'un code de Reed-Solomon sur $F(2^m)$ de distance D,

   (i) on remplace chaque c_i par un m-uplet binaire auquel on rajoute un bit de parité (de tel sorte que le nombre de 1 dans le $m+1$ uplet est paire).

   (ii) on rajoute d'abord un bit de parité au mot code c (i.e. code de Reed-Solomon étendu), puis on fait la meme construction que précédement.

Problème 3: Codes MDS (7 points) Pour un code linéaire de dimension k et de longueur n, la distance minimale du code doit satisfaire $d \leq n - k + 1$. Un code MDS (maximum distance separable) est un code tel que $d = n - k + 1$.

1. Montrer que les codes de Reed-Solomon étendus (i.e. à chaque mot code est ajouté un bit de parité $c_N = -\sum_{i=0}^{N-1} c_i$) sont MDS.

2. Montrer qu'un code est MDS si et seulement si tout ensemble de $n - k$ colonnes de la matrice de parité H sont linéairement indépendent.

3. Montrer que si un code est MDS, son dual aussi.

4. En utilisant les deux résultats précédents, montrer qu'un code est MDS si et seulement si pour tout ensemble de d coordonnées, il existe un mot-code de poids minimal chargeant uniquement ces d coordonnées.

5. Montrer que pour tout $k \in \{1, \ldots, 2^m + 1\}$, il existe un code cyclique MDS de longueur $2^m + 1$ et dimension k sur $F(2^m)$. On pourra montrer au préalable que tous les facteurs sur $F(2^m)$ de $X^{2^m+1} + 1$ autres que $X + 1$ sont quadratiques.

Problème 4 (2 points)
On considère un système de cryptographie: P est le message à transmettre, C est le message crypté. Il est obtenu à partir de P et d'une clé aléatoire K, donc il existe une fonction déterministe telle que $C = f(P, K)$. Le récepteur a accès à la clé K et au message crypté C et doit pouvoir retrouver le message original. Il existe donc une fonction déterministe telle que $g(C, K) = P$. Pour un tiers qui ne possède pas la clé, le message crypté ne doit fournir aucune information sur le message à transmettre, donc P et C sont indépendants. La question est alors: quelle doit être la longueur minimale de la clé aléatoire pour rendre le message crypté indéchiffrable par un tiers? On pourra montrer que $H(K) \geq H(P)$.

Problème 5 (2 points)

1. On considère un système d'encodage ayant la contrainte suivante: chaque mot code doit commencer par un symbole $\{A, B, C\}$ et ensuite utiliser les symboles binaires $\{0, 1\}$. On a donc un code ternaire pour le premier symbole puis binaire. En adaptant le codage de Huffman donner les mots code pour une distributionde probabilité:

$$p = \left(\frac{16}{69}, \frac{15}{69}, \frac{12}{69}, \frac{10}{69}, \frac{8}{69}, \frac{8}{69}\right).$$

   Est-ce un code uniquement décodable optimal (i.e. ayant le nombre moyen minimum de symboles)?

2. Soit $\mathcal{X} = \{0, 1\}$ et $\mathcal{Y} = \{1, 2, 3, \}$. Calculer les capacités des canaux ayant comme alphabet d'entrée $\mathcal{X}$ et de sortie $\mathcal{Y}$ et probabilité de transition repective:

$$Q_1 = \begin{pmatrix} p_1 & p_2 & p_3 \\ p_1 & p_2 & p_3 \end{pmatrix} \quad \text{et} \quad Q_2 = \begin{pmatrix} p_1 & p_2 & p_3 \\ p_3 & p_2 & p_1 \end{pmatrix}$$

Problème 6 (2 points)

Une variable aléatoire prend ses valeurs dans un alphabet de K lettres et chaque lettre a la même probabilité. Ces lettres sont encodées dans des mots binaires de façon à minimiser la longueur moyenne des mots code. On définit l'entier j et $1 \leq x < 2$ par $K = x2^j$.

1. Montrer que tous les mots code ont pour longueur j ou $j + 1$.

2. Quelle est la longueur moyenne d'un mot code?

Problème 7 (3 points)

1. Deux sources discrètes sans mémoire émettent des symboles dans $\mathcal{U} = \{1, 2, 3\}$. La source 1 a pour statistique: $p_1 = (1 - \alpha, \alpha, 0)$ et la source 2 pour statistique $p_2 = (0, \alpha, 1 - \alpha)$ avec $\alpha \in (0, 1)$. Le but est d'encoder en binaire la suite de symboles dans $\mathcal{U}$ sans savoir quelle source $i = 1, 2$ va émettre. Pour simplifier, nous allons négliger les contraintes assurant que les longueurs des mots code sont des entiers. Un code est donc simplement une distribution de probabilité q sur $\mathcal{U}$, les longueurs des mots code correspondant étant $\ell(u) = -\log q(u)$. Nous avons vu en cours que si nous savons quelle source émet, il est possible de construire un code avec des mots code de longeur $\ell(u) = -\log p_i(u)$, ce code ayant une longueur moyenne égale à l'entropie de la source $H_i(U) = -\sum_{u \in \mathcal{U}} p_i(u) \log p_i(u)$. On définit la redondance d'un code comme la différence entre sa longueur moyenne et l'entropie de la source. Ainsi pour un code donné q, $R_i(q)$ est la redondance si la source qui émet est $i \in \{1, 2\}$. La redondance pire cas est alors $R(q) = \max\{R_1(q), R_2(q)\}$. Expliciter le code q minimisant la redondance pire cas $R(q)$.

2. On considère le canal de $\{1, 2\}$ dans $\mathcal{U}$ suivant: si i est transmis, la loi du symbole émis en sortie est p_i. Calculer la capacité du canal.

3. Comparer la redondance pire cas et la capacité du canal. Est-ce une coïncidence?

Problème 8 (4 points)

1. On considère deux canaux discrets sans mémoire, $(\mathcal{X}_1, p(y_1|x_1), \mathcal{Y}_1)$ et $(\mathcal{X}_2, p(y_2|x_2), \mathcal{Y}_2)$, de capacités respectives C_1 et C_2. On forme alors le nouveau canal $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1|x_1)p(y_2|x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ où on utilise simultanément les deux canaux en parallèle. Quelle est la capacité de ce nouveau canal?

2. Etant donné un canal discret sans mémoire $(\mathcal{X}, p(y|x), \mathcal{Y})$ de capacité C, on considère le canal où deux sorties indépendantes sont observées pour chaque entrée: $(\mathcal{X}, p(y_1, y_2|x) = p(y_1|x)p(y_2|x), \mathcal{Y} \times \mathcal{Y})$ de capacité C_2. Montrer que $C_2 \leq 2C$.