Introduction aux Systèmes de Communication EPFL Semestre d'hiver 2007/2008

22 janvier 2008

Examen, (module 4 in English!)

Vous avez 4 heures. Nous n'attendons pas forcément de vous que vous finissiez tous les problèmes. Ne perdez pas trop de temps sur chacun d'entre eux, mais essayez plutôt de collecter le maximum de points.

Vous ne devrez pas utiliser de notes de cours, calculatrices, natels, formulaires ou copies de vos voisins. N'écrivez que ce qui est nécessaire dans vos réponses!

Bonne chance!!

Nom: _____

Question I	/ 25
Question II	/ 25
Question III	/ 25
Question IV	/ 25
Total	/100

Question I (25 points)

Considérez le signal $x(n)$ donné par

$$x(n) = \delta(n) + 2\,\delta(n-1) + \frac{1}{2}\,\delta(n-2) + \delta(n-3) + \frac{3}{2}\,\delta(n-4)\,.$$

où $\delta(n)$ est l'impulsion unité définie comme

$$\delta(n) = \begin{cases} 1, & \text{si } n = 0, \\ 0, & \text{sinon.} \end{cases}$$

Le signal $x(n)$ est passé dans un système S qui ne modifie pas les échantillons d'indice pair mais qui met la valeur des échantillons d'indice impair zéro. La sortie du système, notée $y(n)$, peut donc tre exprimée par

$$y(2n) = x(2n) \quad \text{et} \quad y(2n+1) = 0, \quad \text{pour } n \in \mathbb{Z}.$$

1. (2 pts) Dessinez les signaux $x(n)$ et $y(n)$.

2. (4 pts) Le système S est-il linéaire? Le système S est-il invariant dans le temps? Justifiez votre réponse.

Nous désirons maintenant interpoler la valeur des échantillons impairs partir des autres échantillons. Pour ce faire, nous passons le signal $y(n)$ dans un filtre de réponse impulsionelle $h(n)$. Le résultat de cette opération, noté $\hat{x}(n)$, peut donc tre exprimé en utilisant l'opérateur de convolution comme

$$\hat{x}(n) = h(n) * y(n) = \sum_{k \in \mathbb{Z}} h(k) y(n-k) \, .$$

Nous considérons tout d'abord une interpolation constante par moreaux, i.e. le filtre $h(n)$ est donné par

$$h(n) = \delta(n) + \delta(n-1).$$

3. (5 pts) Exprimez mathématiquement le signal filtré $\hat{x}(n)$ en fonction du signal $y(n)$. Dessinez aussi $h(n)$ et le signal de sortie $\hat{x}(n)$.

4. (5 pts) Répétez la sous-question 3 en utilisant une interpolation linéaire, i.e. le filtre $h(n)$ est donné maintenant par

$$h(n) = \frac{1}{2}\,\delta(n-1) + \delta(n) + \frac{1}{2}\,\delta(n+1).$$

5. (5 pts) Répétez la sous-question 3 en utilisant le filtre $h(n)$ donné par

$$h(n) = \delta(n) + \delta(n-1) + \delta(n-2).$$

6. (4 pts) Lesquels des filtres des sous-questions 3, 4, et 5, satisfont la propriété d'interpolation pour les échantillons pairs, i.e. tel que $x(2n) = \hat{x}(2n)$. Justifiez votre réponse.

Question II (25 points)

Note: tous les codes de cette question sont binaires (les mots-codes formés seulement des bits 0 et 1).

1. (3 pts) Soit une source d'information S_a de $M = 2^n$ symboles s_i différents, $1 \leq i \leq 2^n$, avec $n \in \mathbb{N}$ un entier positif non nul, émis de manière équiprobable (chaque symbole a la même probabilité 2^{-n} d'être émis) et indépendamment les uns des autres. Calculez l'entropie $H(S_a)$ de cette source.

2. (3 pts) Quelle est la longueur moyenne des mots-codes que obtiendriez avec un code de Shannon-Fano de la source S_a de la sous-question 1 ?

3. (2 pts) Le code de Shannon-Fano de la source S_a obtenu à la sous-question précédente (2) est-il optimal (c'est-à-dire avec la longueur moyenne des mots-codes la plus faible possible) ? Si oui, expliquez pourquoi, sinon donnez un méthode de codage sans pertes plus efficace, c'est-à-dire vous permettant d'obtenir des mots-codes dont la longueur moyenne est plus faible.

4. (4 pts) On considère une source d'information S_b de $M = 5$ symboles s_i, $1 \leq i \leq 5$, émis indépendamment les uns des autres, avec les probabilités $P(S_b = s_i) = p_i$, $1 \leq i \leq 5$, données par $p_1 = 1/3$, $p_2 = p_3 = 1/5$ et $p_4 = p_5 = 2/15$. Quel est le code instantané $C = \{c_1, c_2, c_3, c_4, c_5\}$ optimal de cette source (donnez tous les mots-codes), et que vaut la longueur moyenne des mots-codes ?

5. (5 pts) On considère à nouveau la source d'information S_b de la sous-question 4, mais pour des raisons techniques, on suppose que le premier symbole s_1 *doit* être codé par le mot-code $c_1 = 0$ formé du seul bit 0, même si ce n'est pas le meilleur choix de mot-code possible. Par contre, on est libre de choisir comme on veut les 4 autres mots-codes c_2, c_3, c_4, c_5. Etant donné cette contrainte sur $c_1 = 0$, quel est le meilleur code instantané $C = \{0, c_2, c_3, c_4, c_5\}$ que vous pourriez trouver (donnez tous les mots-codes), et que vaut la longueur moyenne des mots-codes ?

6. (8 pts = 4 $\times$2) Le(s)quel(s) des codes suivants ne peut pas être un code de Huffman d'une source S, quelles que soient les probabilités d'émission (supposées non nulles) des 4 symboles qu'elle peut émettre ? Lorsqu'un code ne peut pas être un code de Huffman de la source, expliquez *précisémment* pourquoi.

a. $C_a = \{0, 10, 110, 1111\}$.

b. $C_b = \{0, 10, 110, 111\}$.

c. $C_c = \{00, 10, 110, 111\}$.

e. $C_d = \{0, 11, 101, 111\}$.

Question III (25 points)

1. (4 pts) Une source émet des messages qui consistent en une suite de symboles binaires 0 et 1. Le symbole 0 est émis avec probabilité p et le symbole 1 avec probabilité $(1-p)$, avec $0 < p < 1$, et la source émet ces symboles *indépendamment* les uns des autres. Ces symboles sont cryptés par substitution monoalphabétique. Il y deux clés $K \in \{0, 1\}$ possibles et équiprobables: $K = 0$, auquel cas le symbole crypté est le même que le symbole en clair; ou $K = 1$, auquel cas le symbole 0 est crypté en 1, et vice-versa.

Y a t-il une ou plusieurs valeur(s) de p pour la(les)quelle(s) ce cryptage résiste bien à une attaque à texte crypté seul (cyphertext only attach) ? Si oui, donnez cette (ces) valeur(s) et expliquez précisemment pourquoi le cryptostème est sûr. Sinon, expliquez précisemment pourquoi le système n'est pas sûr contre une attaque à texte crypté seul.

2. (3 pts) S'il existe, déterminez un entier x tel que $0 \leq x \leq 14$ et que

$$x \equiv 24^{10} \pmod{15}.$$

Si cet entier n'existe pas, expliquez pourquoi.

3. (3 pts) S'il existe, déterminez un entier x tel que $0 \leq x \leq 14$ et que

$$x \equiv 24^{-1} \pmod{15}.$$

Si cet entier n'existe pas, expliquez pourquoi.

4. (5 pts) On considère un système de cryptographie à clé publique de type RSA, dont les conditions initiales sont $p = 11$ et $q = 23$. La clé de l'émetteur est $K = 9$. Calculer la clé du récepteur k correspondante ($k > 0$).

5. (4 pts) Soit $m = p \cdot q \cdot r$ où p, q, r sont trois grands nombres premiers distincts. Soit a un nombre tel que $\text{pgcd}(a, m) = 1$. Est-il possible de déterminer rapidement et facilement l'entier x, tel que $0 \leq x \leq m - 1$ et que

$$a^x \equiv 1 \pmod{m}?$$

Si oui, expliquez précisemment comment vous calculez ce nombre x. Sinon, expliquez pourquoi ce nombre est difficile à calculer.

6. (6 pts) Soient p et q deux nombres premiers (pouvant être distincts ou non). Déterminez toutes les valeurs possibles, suivant les valeurs de p et/ou q, que peut prendre l'entier x tel que $0 \leq x \leq p^2 - 1$ et que

$$x \equiv q^{p(p-1)} \pmod{p^2}.$$

Justifiez votre réponse.

Question IV (25 points)

1. (12 points) Assume that we use a code that maps the four number $\{1, 2, 3, 4\}$ to the codewords $C = \{000000, 101010, 010101, 111111\}$.

(a) (1 point) What is the rate of this code?

(b) (1 point) Is this a linear code or not and why?

(c) (3 points) How many erasures can it correct? How many errors can it correct? How many errors can it detect?

For points (d-e) assume that we want to use this code to transmit over a noisy channel.

(d) (3 points)In which of the following cases the receiver can correctly decode, and what does it decode?

i. The receiver receives the sequence $(?, 0, ?, 0, 1, 0)$ (2 erasures)

ii. The receiver receives the sequence $(?, ?, ?, 0, 0, 0)$ (3 erasures)

(e) (2 points) Can you find an example with three erasures that the code cannot correct?

(f) (2 points) If the receiver receives the sequence $(1, 1, 1, 1, 0, 0)$ what is the minimum and what is the maximum number of errors that the channel has introduced?

2. (6 points) Consider a Hamming code with parameter $m = n - k = 2$. Write a parity-check matrix for this code.

3. (7 points) Assume that we want to reliably transmit a bit (i.e., two values, 0 or 1) through a channel that:

(a) If we send two consecutive zeros through the channel, we may receive two consecutive ones. Similarly, if we send two consecutive ones, we may receive two consecutive zeros. (For example, if we send through the channel the codeword, say 0011, we may receive 0011, 0000, or 1111)

(b) After the previous changes have occured, the channel may also erase three symbols.

Find a code with 2 codewords and the codeword length n being as small as possible that allows us to reliably transmit through this channel.