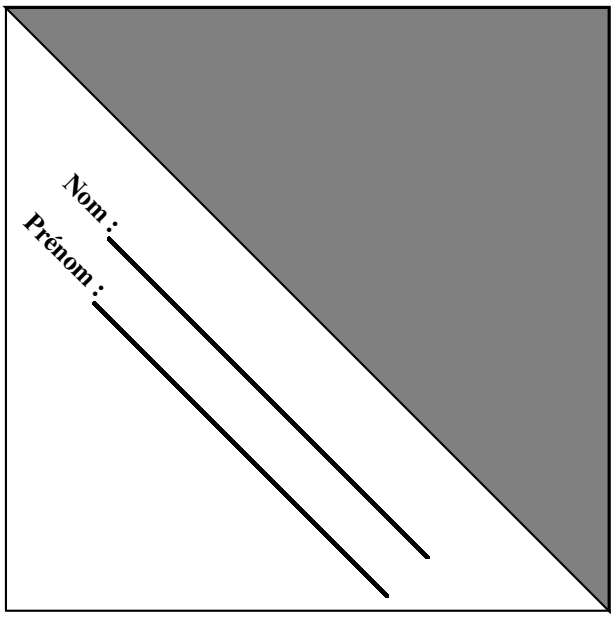
Université Côte d'Azur 2024–2025
Licence 3 Informatique, Licence 3 Math-Info

Codes, cryptographie & calcul symbolique

Contrôle continu du 25 octobre



Durée : 1h30
*Une feuille manuscrite **recto** autorisée*

Note :

Exercice 1 : (4 points) Lempel-Ziv Compressez le texte suivant avec l'algorithme LZ77, les fenêtres de recherche et de lecture étant respectivement de taille 31 et 7 *(on suppose que la recherche de motif considère la première occurrence, la plus à gauche donc)* :

`Rosa rosa rosam Rosae rosae rosa Rosae rosae rosas Rosarum rosis rosis.`

(0, 0, 'R')	(0, 0, 'o')	(0, 0, 's')	(0, 0, 'a')	(0, 0, '␣')	(0, 0, 'r')	…
…	…	…	…	…	…	…
…	…	…	…	…	…	…

Exercice 2 : (4 points) Codes de Huffman

Voici la distribution de probabilités p d'une source Ω que l'on se propose de coder en binaire :

Symbole	Proba. d'apparition	Code
a	0,30	…
b	0,12	…
c	0,05	…
d	0,15	…
e	0,10	…
f	0,25	…
g	0,03	…

1. Donnez la formule générale de l'entropie puis calculez celle de la source probabilisée (Ω, p).

2. Dessinez l'arbre de Huffman obtenu et attribuez à chaque symbole son mot de code dans la table précédente *(on demande en prime que la probabilité des fils gauches n'excède pas celle des fils droits)*.

3. Calculez la longueur moyenne pondérée du code obtenu. Commentez.

Exercice 3 : (3 points) Burrows-Wheeler On se propose de coder le mot `DECODAGE` par la transformée de Burrows-Wheeler afin de réduire son entropie.

1. Commencez par calculer la colonne $\mathbb{L}$:

$\mathbb{F}$
A
C
D_1
D_2
E_1
E_2
G
O

$\mathbb{L}$
…
…
…
…
…
…
…
…

$\mathbb{H}$
…
…
…
…
…
…
…
…

2. Calculez le *vecteur de transformation* $\mathbb{H}$ entre $\mathbb{F}$ et $\mathbb{L}$ de sorte que : $\forall j \quad \mathbb{L}[\,\mathbb{H}[j]\,] = \mathbb{F}[j]$
3. Précisez ce qu'est l'*index primaire* ip et donnez sa valeur.

Exercice 4 : (5 points) Code de Hamming On considère le code de Hamming entièrement spécifié par la matrice de contrôle H suivante :

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

1. Le récepteur reçoit le message $\mathcal{R} = 1100001$. Vérifiez si le message reçu $\mathcal{R}$ est bien celui qui a été transmis. Le cas échéant, proposez une correction de $\mathcal{R}$ qui corresponde au message $\mathcal{T}$ réellement transmis.

2. Trouvez la matrice génératrice G de ce même code de Hamming qui est entièrement conditionné par la matrice de contrôle H.

3. Déduisez-en la valeur du message initial $\mathcal{M}$ codé par ajout de redondance en $\mathcal{T}$.

4. Expliquez en quoi un tel $(7, 4)$-code de Hamming est un code linéaire *parfait*.

Exercice 5 : (4 points) Autres questions

1. On code le message $m = 10011010$ par le code CRC de polynôme générateur : $g(x) = x^3 + x^2 + 1$. Trouvez les bits de redondance à ajouter à la fin du message avant transmission *(vous poserez la division de polynomes)*.

2. Qu'est-ce que le standard AES ?

3. En tant qu'informaticiens et apprentis cryptographes, sauriez-vous retrouver l'origine du nom de l'ordinateur HAL dans le film de Stanley Kubrick *2001, l'0dyssée de l'espace* ?

4. On utilise le *chiffrement affine* suivant sur les seules lettres minuscules (les lettres `a`, `b`, `c` ... sont préalablement codées $0, 1, 2 \ldots$, les autres caractères sont inchangés) :

$$\begin{array}{ccc} \mathbb{Z}_{26} & \rightarrow & \mathbb{Z}_{26} \\ x & \mapsto & (11x + 7) \mod 26 \end{array}$$

   Déchiffrez le message reçu suivant en expliquant un minimum votre méthode : `sfu iq !`