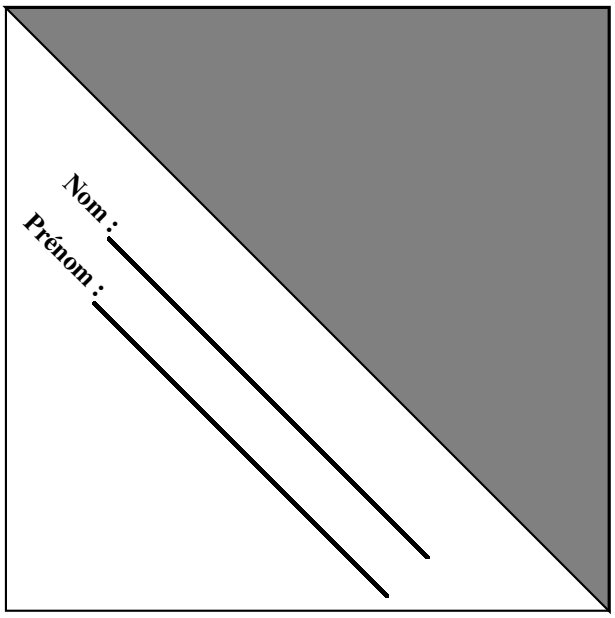
Université Côte d'Azur 2025–2026
L3 Informatique, L3 Math-Info

Codes, cryptographie & calcul symbolique

Contrôle continu du 7 novembre



Durée : 1h30
Une feuille manuscrite RECTO autorisée

Note :

Exercice 1 : (2,5 points) Transformée de Burrows-Wheeler
Voici la colonne de lettres triée $\mathbf{F}$ et le vecteur de transformation $\mathbf{H}$ permettant de retrouver un mot tel qu'il était avant sa transformation :

F
E
E
I
N
O
P
R
T

H
3
0
1
7
5
2
4
6

L
...
...
...
...
...
...
...
...

1. Commencez par retrouver la colonne $\mathbf{L}$ à partir de la colonne $\mathbf{F}$ et du vecteur $\mathbf{H}$ sachant que :
$$\forall j \quad \mathbf{L}[\,\mathbf{H}[j]\,] = \mathbf{F}[j]$$
2. Rappelez l'algorithme pour reconstruire le mot initial à partir de $\mathbf{L}$, de $\mathbf{H}$ et de l'index primaire ip.

3. Décodez le mot initial sachant que l'index primaire $ip = 3$ ici.

Exercice 2 : (4,5 points) Codes de Huffman
Voici la distribution de probabilités d'une source Ω que l'on se propose de coder en binaire :

Symbole	Probabilité d'apparition	Mot de code
a	0,25	...
b	0,20	...
c	0,05	...
d	0,20	...
e	0,25	...
f	0,05	...

1. Calculez l'entropie de cette source Ω en rappellant la formule au préalable.

2. Construisez et dessinez (en haut à droite de cette page) un arbre de Huffman afin d'attribuer à chaque symbole son mot de code *(on demande en plus ici que la probabilité des fils gauches soit inférieure ou égale à celle des fils droits)*.
3. Remplissez la dernière colonne de la table en attribuant à chaque symbole de la source Ω le mot de code lui correspondant.
4. Calculez la longueur moyenne pondérée des mots du code puis prouvez l'optimalité de votre code de Huffman.

5. A quelle famille de codes appartiennent les codes de Huffman ? Pourquoi ?

Exercice 3 : (3 points) Compression LZ77

Je chante, tu chantes, il chante, nous chantons.

On veut compresser cette phrase en utilisant des fenêtres de recherche et de lecture de taille respective 31 et 7. L'espace sera écrit ␣. Voici le début de la compression :

(0, 0, 'J') (0, 0, 'e') (0, 0, '␣') (0, 0, 'c') (0, 0, 'h') (0, 0, 'a') (0, 0, 'n') (0, 0, 't') (7, 1, ',') ...

Continuez la suite des triplets correspondant à la compression de cette phrase :

Exercice 4 : (5 points) Code de Hamming

On considère le code de Hamming entièrement spécifié par la matrice de contrôle H suivante :

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

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

2. Trouvez une matrice génératrice G de ce code de Hamming à partir de la matrice de contrôle H précédente.

3. Déduisez-en la valeur du message $\mathcal{M} = x_1x_2x_3x_4$ codé en le message $\mathcal{T}$ par ajout de redondance.

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

Exercice 5 : (2 points) Protocole de Diffie-Hellman

Alice et Bob se mettent d'accord pour utiliser ce protocole afin d'obtenir un secret en commun. Ils choisissent les paramètres $g = 5$ et $p = 23$. Eve espionne leurs communications, elle connaît donc les paramètres g et p. Elle voit passer un nouvel envoi d'Alice, elle en déduit que $g^a \mod p = 10$ sans connaître l'entier a choisi par Alice. De même elle déduit d'un envoi de Bob que $g^b \mod p = 8$ sans connaître le b choisi par Bob.
Les paramètres sont petits là, Eve peut en déduire leur secret. Calculez ce secret en expliquant votre méthode.

Exercice 6 : (3 points) Questions diverses

1. **Algorithme de Sardinas-Paterson** Déroulez cet algorithme sur le langage :

   $$L = \{1, 011, 01110, 1110, 10011\}$$

   afin de décider si c'est un code ou non.

2. **Le rail de chemin de fer** Le plus simple est d'illustrer le principe de ce petit chiffre par un exemple. Le cryptogramme `CIEL?EHFESIBNCRTO` est ici obtenu pour une hauteur de $n = 2$:

   $$\begin{array}{ccccccccccccccc} C & & & & I & & & & E & & & & L & & ? \\ & E & & H & & F & & E & & S & & I & & B & & N & \\ & & C & & & & R & & & & T & & & & O & & \end{array}$$

   Déchiffrez le cryptogramme `AAELCMH?OSACRR` obtenu pour une hauteur de 3 en précisant quelle est la nature et quelle est la clef de cet algorithme de chiffrement.

3. **Codage arithmétique** La compression du mot `MISSISSIPI` tient en un réel de l'intervalle $[0, 1]$. Donnez au moins les 3 premières décimales de ce réel.