



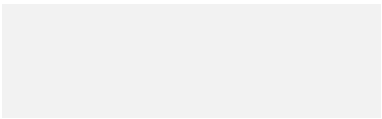
1

Ens. : O. Lévêque, M. Stojilovic  
Information, Calcul, Communication - A  
Lundi 3 juillet 2023  
Durée : 180 minutes

# U.N.Owen













SCIPER : 0

Salle : INF 1

Signature : 

Attendez le début de l'épreuve avant de tourner la page. Ce document est imprimé recto-verso, il contient 20 pages, les dernières pouvant être vides. Ne pas dégrafer.

- Posez votre carte d'étudiant sur la table.
- Document autorisé pour cet examen : partie programmation : tous vos documents de cours ; partie théorique : un formulaire constitué de deux pages A4 recto-verso, manuscrites (ou préparées avec stylet+tablette).
- L'utilisation de tout appareil électronique (calculatrice, ordinateur, smartphone/watch, tablette) est interdite pendant l'épreuve.
- L'examen est composé de trois parties :
  - une partie avec 11 questions à choix multiple sur la théorie ; chaque question admet une seule réponse correcte parmi 4 possibilités : la réponse correcte vaut 2 points ; toute autre option (pas de réponse, réponse fausse, ou plusieurs cases cochées) vaut 0 point. Cette partie vaut donc en tout **22 points**.
  - une partie avec 10 questions sur la programmation ; chaque réponse vaut 2,5 points, et cette partie vaut donc en tout **25 points**.
  - une partie avec 4 exercices sur la théorie, valant chacun 7 points, donc en tout **28 points**.
- Merci d'avance de soigner la présentation de vos réponses !
- Si une question est erronée, les enseignants se réservent le droit de l'annuler.

Respectez les consignes suivantes   Observe this guidelines   Beachten Sie bitte die unten stehenden Richtlinien		
choisir une réponse   select an answer Antwort auswählen   	ne PAS choisir une réponse   NOT select an answer NICHT Antwort auswählen 	Corriger une réponse   Correct an answer Antwort korrigieren  
ce qu'il ne faut <b>PAS</b> faire   what should <b>NOT</b> be done   was man <b>NICHT</b> tun sollte		
     		



## Première partie, questions à choix multiple sur la théorie

Pour chaque question, marquer la case correspondante à la réponse correcte sans faire de ratures. Il n'y a qu'une seule réponse correcte par question. Chaque réponse correcte vaut **2 points**, et toute autre réponse que la réponse correcte (i.e., réponse fausse, plusieurs réponses ou pas de réponse) vaut 0 point.

### Question 1

<b>algo1</b>
entrée : liste $L$ de nombres entiers positifs, de taille $n$ sortie : nombre entier positif $s$
$s \leftarrow 0$ <b>Pour</b> $i$ allant de 1 à $n$ <b>Pour</b> $j$ allant de 1 à $n$ <b>Si</b> $L(i) > L(j)$ $s \leftarrow s + 1$ <b>Sortir</b> : $s$

Pour une valeur de  $n$  fixe en entrée, quelle est la valeur maximale de la sortie  $s$  de **algo1**( $L, n$ ) ?

$\frac{n(n-1)}{2}$

$n$

$\frac{n(n+1)}{2}$

$n^2$

### Question 2

<b>algo2</b>
entrée : nombre entier relatif $n$ sortie : nombre entier relatif $s$
<b>Si</b> $n \leq 0$ <b>Sortir</b> : $n$ <b>Sortir</b> : <b>algo2</b> ( $n - 1$ ) + <b>algo2</b> ( $n - 2$ )

Que sait-on de la sortie  $s$  de **algo2**( $n$ ) ?

$s \leq 0$  pour tout  $n \leq 0$ ;  $s \geq 0$  pour tout  $n \geq 1$

$s = -F(n)$  pour tout  $n \geq 1$ , où  $F(n)$  est le  $n^e$  nombre de la suite de Fibonacci

$s < 0$  pour tout  $n \in \mathbb{Z}$

$s = -1$  pour tout  $n \geq 1$

### Question 3

Quelle est la complexité temporelle de **algo2**( $n$ ) ?

(Note: On considère pour cette question que le nombre  $n$  en entrée prend uniquement des valeurs positives.)

$\Theta(2^{n/2})$  ou plus

$\Theta(1)$

$\Theta(n^2)$

$\Theta(n)$

**Question 4**

<b>algo4</b>
entrée : liste $L$ de nombres entiers positifs, de taille $n$ sortie : ???
$m \leftarrow n$ <b>Tant que</b> $m > 1$ <b>Pour</b> $j$ allant de 1 à $m - 1$ <b>Si</b> $L(j) > L(m)$ <b>permuter</b> ( $L, j, m$ ) $m \leftarrow m - 1$ <b>Sortir</b> : $L$

où on rappelle que l'algorithme **permuter**( $L, j, m$ ) vu en cours permute les éléments d'indices  $j$  et  $m$  de la liste  $L$ . Quelle est sortie de **algo4**( $L, n$ ) ?

- La liste  $L$  triée dans l'ordre croissant
- La liste  $L$  avec le plus grand élément placé à la fin de la liste, mais sans autre ordre particulier
- La liste  $L$  triée dans l'ordre décroissant
- La liste  $L$  avec le plus grand élément placé au début de la liste, mais sans autre ordre particulier

**Question 5**

Quelle est la complexité temporelle de l'algorithme **algo4**( $L, n$ ), dans le pire des cas ?

- $\Theta(n \cdot \log_2(n))$         $\Theta(n^2)$         $\Theta(1)$         $\Theta(n)$

**Question 6**

Si  $n$  bits sont utilisés pour représenter le nombre entier positif  $x$ , de combien de bits a-t-on besoin pour représenter le nombre  $x^2$  ?

- $n + 4$         $2n$         $n + 2$         $n^2$

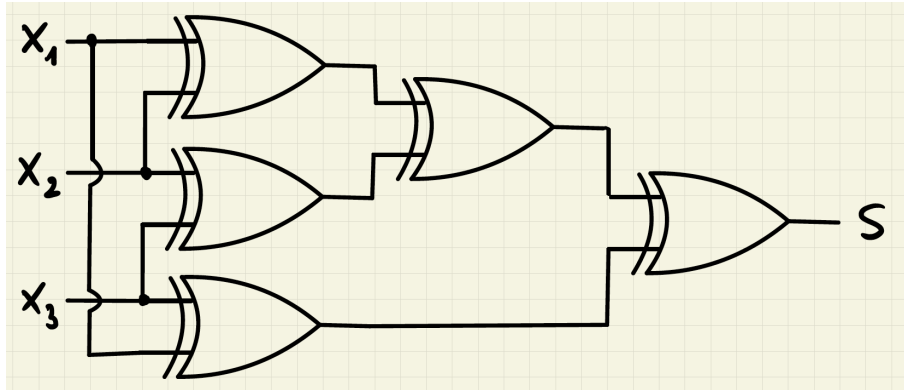
**Question 7**

$n$  équipes participent à un jeu collaboratif: chaque équipe  $j$  obtient un score  $s_j$  entre 0 et  $m - 1$ , et on calcule le score final des  $n$  équipes comme suit:  $S = s_1 \cdot s_2 \cdot \dots \cdot s_n$ . De combien de bits a-t-on besoin pour représenter le score final  $S$  ?

- $\lceil \log_2(m) \rceil^n$         $m \cdot n$         $\lceil \log_2(m) \rceil \cdot n$         $m^n$

**Question 8**

On considère le circuit suivant:



Laquelle des affirmations suivantes est-elle vraie ?

- $s = x_1 \oplus x_2 \oplus x_3$
- Quels que soient les bits  $x_1, x_2, x_3$  en entrée, la sortie de ce circuit vaut toujours  $s = 0$ .
- $s = 1$  si et seulement si  $x_1 = x_2 = x_3 = 1$
- $s = 1$  si et seulement si  $x_1 + x_2 + x_3$  est pair

**Question 9**

Laquelle des séquences de lettres ci-dessous a-t-elle pour entropie  $H = 2 \cdot \log_2(3) - \frac{4}{3}$  ?

- AAAABBBBCD       AAAABBBBC       AAAABBCCD       AAAABBCC

**Question 10**

Si deux nœuds  $A_1, A_2$  utilisent l'algorithme AIMD pour transmettre des paquets à des taux  $W_1, W_2$  (respectivement) à travers internet, alors:

- La différence  $|W_1 - W_2|$  reste identique quand un problème de congestion survient.
- La différence  $|W_1 - W_2|$  s'éloigne de 0 quand il n'y a pas de problème de congestion.
- La différence  $|W_1 - W_2|$  reste identique quand il n'y a pas de problème de congestion.
- La différence  $|W_1 - W_2|$  se rapproche de 0 quand il n'y a pas de problème de congestion.

**Question 11**

Une clé  $K$  de 20 bits est utilisée avec un système de cryptographie à clé secrète pour chiffrer des messages. Eve utilise une attaque par force brute sur ce système et trouve en 5 minutes la valeur de la clé  $K$ . Si maintenant une clé  $K'$  de 20 chiffres de 0 à 9 était utilisée, combien de minutes Eve mettrait-elle avec la même attaque par force brute pour trouver la clé  $K'$  ?

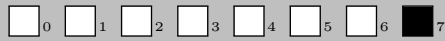
- environ  $5 \cdot 10^{20}$  minutes       environ 25 minutes
- environ  $5 \cdot 10^{14}$  minutes       environ  $5 \cdot 10^8$  minutes



### Troisième partie, questions de type ouvert sur la théorie

Répondre dans l'espace dédié. Votre réponse doit être soigneusement justifiée, toutes les étapes de votre raisonnement doivent figurer dans votre réponse. Laisser libres les cases à cocher : elles sont réservées au correcteur.

**Question 22 :** Cette question est notée sur 7 points.



**a) (4 points)** Ecrivez un algorithme qui prenne en entrée un nombre entier relatif  $x$  ainsi qu'une liste  $L$  de  $n$  nombres entiers relatifs et dont la sortie soit oui si et seulement s'il existe  $i, j \in \{1, \dots, n\}$  tels que  $i < j$  et  $L(i) + L(j) \geq x$ . De plus, la complexité temporelle de votre algorithme doit être un  $\Theta(n)$ .

**Réponse:** Un algorithme possible est le suivant:

algo
entrée : liste $L$ de nombres entiers positifs, de taille $n$ , nombre entier positif $x$ sortie : oui/non
<pre>y ← max(L(1), L(2)) z ← min(L(1), L(2)) <b>Pour</b> <math>i</math> allant de 3 à <math>n</math>     <b>Si</b> <math>L(i) \geq y</math>         <math>z \leftarrow y</math>         <math>y \leftarrow L(i)</math>     <b>Sinon, si</b> <math>L(i) \geq z</math>         <math>z \leftarrow L(i)</math> <b>Si</b> <math>y + z \geq x</math> (Note: <math>y</math> et <math>z</math> sont les deux plus grands nombres de la liste <math>L</math>)     <b>Sortir</b> : oui <b>Sinon</b>     <b>Sortir</b> : non</pre>

**b) (1 point)** On considère maintenant le problème plus général suivant:

“Étant donné un nombre entier relatif  $x$  et une liste  $L$  de  $n$  nombres entiers relatifs, existe-t-il un sous-ensemble  $S \subset \{1, \dots, n\}$  tel que  $\sum_{j \in S} L(j) \geq x$  ?”

Ce problème fait-il partie de la classe NP ? Justifiez votre réponse.

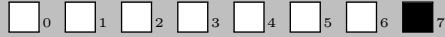
**Réponse:** Oui. Si on nous propose un sous-ensemble  $S$  comme solution, il suffit alors d'effectuer la somme  $\sum_{j \in S} L(j)$  et de comparer celle-ci à la valeur  $x$  (ce qui se fait en temps polynomial, même en  $\Theta(n)$ ).

**c) (2 points)** Sait-on si le problème de la question b) fait également partie de la classe P ? A nouveau, justifiez votre réponse.

**Réponse:** Oui, il fait partie de la classe P: il suffit de parcourir une seule fois la liste  $L$  (complexité  $\Theta(n)$ ) et de ne retenir que les nombres positifs de celle-ci. Si leur somme est plus grande ou égale à  $x$ , la réponse est oui; sinon, la réponse est non.



**Question 23 :** Cette question est notée sur 7 points.



On considère un filtre un peu particulier dont l'effet est le suivant:

si le signal en entrée vaut  $X(t) = a \sin(2\pi ft + \delta)$ , alors le signal en sortie vaut  $\tilde{X}(t) = \frac{a}{f} \sin\left(2\pi ft + \frac{\delta}{f}\right)$ .

A noter ici que  $f$  est la valeur de la fréquence mesurée en Hertz.

**a) (2 points)** Argumentez pourquoi un tel filtre est un filtre passe-bas ou non.

**Réponse:** Un tel filtre est un filtre passe-bas, car il atténue plus l'amplitude des hautes fréquences que celle des basses fréquences.

**b) (2 points)** Considérons maintenant le signal  $X(t) = \cos(6\pi t) + \frac{1}{10} \sin(30\pi t)$ . Que vaut le signal  $\tilde{X}(t)$  ?  
*Rappel:*  $\cos(x) = \sin(x + \frac{\pi}{2})$  pour tout  $x \in \mathbb{R}$ .

**Réponse:** Selon l'indication,  $X(t) = \sin(6\pi t + \frac{\pi}{2}) + \frac{1}{10} \sin(30\pi t)$ , et donc

$$\tilde{X}(t) = \frac{1}{3} \sin(6\pi t + \frac{\pi}{6}) + \frac{1}{150} \sin(30\pi t)$$

(car les deux fréquences  $f_1$  et  $f_2$  valent respectivement 3 Hz et 15 Hz).

**c) (2 points)** Pour rappel, l'amplitude d'une sinusoïde de fréquence  $f$  Hz passant à travers un filtre à moyenne mobile de période d'intégration  $T_c$  est diminuée d'un facteur

$$\left| \frac{\sin(\pi f T_c)}{\pi f T_c} \right|$$

Si on considère la composante  $\frac{1}{10} \sin(30\pi t)$  du signal  $X(t)$  ci-dessus comme du bruit, quel filtre permet de mieux atténuer cette composante: le filtre de la question a) (signal sortant  $\tilde{X}(t)$ ) ou un filtre à moyenne mobile de période d'intégration  $T_c = 0.2$  sec (signal sortant  $\hat{X}(t)$  vu en cours) ? Justifiez votre réponse.

**Réponse:** D'après la formule, l'amplitude de la composante  $\frac{1}{10} \sin(30\pi t)$  sortant du filtre à moyenne mobile vaut:

$$\left| \frac{\sin(\pi \cdot 15 \cdot 0.2)}{\pi \cdot 15 \cdot 0.2} \right| = \left| \frac{\sin(3\pi)}{3\pi} \right| = 0$$

donc c'est le filtre à moyenne mobile qui permet de mieux atténuer le bruit; il atténue même parfaitement celui-ci.

**d) (1 point)** Si on échantillonne le signal  $\hat{X}(t)$  sortant du filtre à moyenne mobile à une fréquence  $f_e = 20$  Hz, assistera-t-on à l'effet stroboscopique ? Justifiez votre réponse.

**Réponse:** Vu que la bande passante du signal filtré vaut 3 Hz, on n'assistera pas à l'effet stroboscopique.



**Question 24 :** Cette question est notée sur 7 points.



Pour encoder sous forme binaire une séquence de 8 lettres, on utilise le dictionnaire suivant:

A	B	C	D
111	110	10	0

a) (2 points) Sachant que le dictionnaire ci-dessus a été établi à l'aide de l'algorithme de Huffman, quelle peut être la séquence de 8 lettres ?

**Réponse:** Une séquence de 8 lettres possible est ABCCDDDD.

b) (1 point) Combien de bits par lettre en moyenne sont-ils utilisés avec ce dictionnaire ?

*Note:* Vous pouvez laisser le résultat sous forme de fraction irréductible.

**Réponse:**  $\frac{2}{8} \cdot 3 + \frac{2}{8} \cdot 2 + \frac{4}{8} \cdot 1 = \frac{6+4+4}{8} = \frac{14}{8} = \frac{7}{4} (= 1.75)$

On désire maintenant modifier le dictionnaire ci-dessus pour encoder une séquence composée des mêmes 8 lettres, ainsi que de 8 fois la lettre E (donc la nouvelle séquence est composée de 16 lettres en tout).

c) (3 points) Proposez un nouveau dictionnaire pour les lettres A, B, C, D et E, respectant les conditions suivantes:

1. Chaque nouveau mot de code doit contenir l'ancien mot de code (p.ex., un nouveau mot de code pour la lettre A pourrait être 0111, 1110, 1111 ou encore 01111 etc.).
2. Le dictionnaire doit être optimal pour l'encodage de la séquence de 16 lettres, et la séquence de bits ainsi produite doit être uniquement décodable.

**Réponse:** Une réponse possible est:

A	B	C	D	E
1111	1110	110	10	0

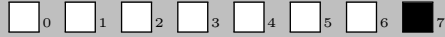
d) (1 point) Combien de bits par lettre en moyenne sont-ils utilisés avec ce nouveau dictionnaire ?

*Note:* A nouveau, vous pouvez laisser le résultat sous forme de fraction irréductible.

**Réponse:**  $\frac{2}{16} \cdot 4 + \frac{2}{16} \cdot 3 + \frac{4}{16} \cdot 2 + \frac{8}{16} \cdot 1 = \frac{8+6+8+8}{16} = \frac{30}{16} = \frac{15}{8} (= 1.875)$



**Question 25:** Cette question est notée sur 7 points.



Pour envoyer à Bob un message encodé initialement sur 3 bits  $x_1, x_2, x_3$ , Alice envoie le message suivant composé de 7 bits:

$$x_1, \quad x_2, \quad x_3, \quad x_1 \oplus x_2, \quad x_1 \oplus x_3, \quad x_2 \oplus x_3, \quad x_1 \oplus x_2 \oplus x_3$$

où  $x \oplus y$  est l'opération XOR vue en cours.

**a) (4 points)** Quelle est la distance minimale  $d$  de ce code correcteur d'erreurs ? Justifiez pleinement votre réponse !

**Réponse:** La distance minimale  $d = 4$ : considérons pour ça deux mots de code  $x$  et  $y$ :

- si  $x_1, x_2, x_3$  et  $y_1, y_2, y_3$  diffèrent en 1 position, alors  $x_4, x_5, x_6, x_7$  et  $y_4, y_5, y_6, y_7$  diffèrent en 3 positions.
- si  $x_1, x_2, x_3$  et  $y_1, y_2, y_3$  diffèrent en 2 positions, alors  $x_4, x_5, x_6, x_7$  et  $y_4, y_5, y_6, y_7$  diffèrent en 2 positions.
- si  $x_1, x_2, x_3$  et  $y_1, y_2, y_3$  diffèrent en 3 positions, alors  $x_4, x_5, x_6, x_7$  et  $y_4, y_5, y_6, y_7$  diffèrent en 1 position.

A noter que dans ce code particulier, *tous* les mots de code sont exactement à distance 4 l'un de l'autre (ex: 0000000 et 1110001).

**b) (2 points)** En conséquence, combien d'effacements et d'erreurs un tel code permet-il de corriger ?

**Réponse:** Vu que la distance minimale  $d = 4$ , ce code peut corriger 3 effacements et 1 erreur.

**c) (1 point)** En particulier, si Bob reçoit le message 0001111, peut-il en déduire les valeurs des bits  $x_1, x_2, x_3$  ? Justifiez votre réponse.

**Réponse:**

Non, dans ce cas, la distance du message reçu avec un mot de code (1001101, 0101011 ou 0010111) est au minimum 2, et il n'est donc pas possible de corriger l'erreur.