Corrigé du BTS Services informatiques aux organisations
Métropole 13 mai 2019

Épreuve obligatoire

Exercice 1 **9 points**

Partie A

Le site comporte 6 pages notées A, B, C. D. E et F. Les pages ainsi que les liens hypertextes d'une page vers une autre sont représentés par un graphe orienté de sommets A, B, C, D. E, F, en convenant qu'un lien hypertexte d'une page X vers une page Y est représenté par une flèche orientée du sommet X vers le sommet Y.
Le tableau ci-après récapitule tous les liens entre les sommets.

Sommet	Prédécesseurs
A	–
B	A
C	A
D	B
E	C, D
F	D, E

1. Il y a 6 sommets donc la matrice d'adjacence du graphe est une matrice carrée d'ordre 6.
On met un 1 à l'intersection de la ligne correspondant au sommet X et de la colonne correspondant au sommet Y s'il existe un arc allant du sommet X au sommet Y, autrement dit si le sommet X est un prédécesseur du sommet Y. Sinon on met un 0.
La matrice d'adjacence est donc

$$\begin{array}{c|cccccc} & A & B & C & D & E & F \\ A & 0 & 1 & 1 & 0 & 0 & 0 \\ B & 0 & 0 & 0 & 1 & 0 & 0 \\ C & 0 & 0 & 0 & 0 & 1 & 0 \\ D & 0 & 0 & 0 & 0 & 1 & 1 \\ E & 0 & 0 & 0 & 0 & 0 & 1 \\ F & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

2. Dans le tableau donnant les prédécesseurs, on cherche les sommets n'en ayant pas : il n'y a que le sommet A donc le sommet A est de niveau 0.

On supprime du tableau le sommet A :

Sommet	Prédécesseurs
~~A~~	–
B	~~A~~
C	~~A~~
D	B
E	C, D
F	D, E

puis on cherche les sommets n'ayant pas de prédécesseurs : il y a les sommets B et C qui sont donc de niveau 1.

On supprime du tableau les sommets B et C :

Sommet	Prédécesseurs
~~A~~	–
~~B~~	~~A~~
~~C~~	~~A~~
D	~~B~~
E	~~C~~ , D
F	D, E

puis on cherche les sommets n'ayant pas de prédécesseurs : il y a le sommet D qui est donc de niveau 2.

On supprime du tableau le sommet D :

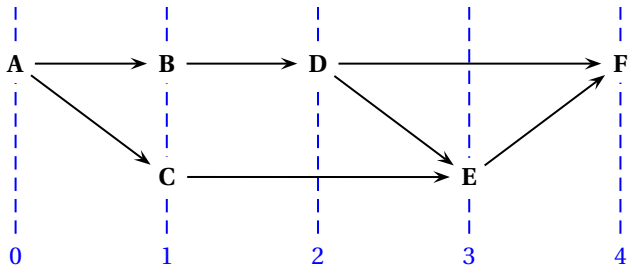
Sommet	Prédécesseurs
~~A~~	–
~~B~~	~~A~~
~~C~~	~~A~~
~~D~~	~~B~~
E	~~C~~ , ~~D~~
F	~~D~~ , E

puis on cherche les sommets n'ayant pas de prédécesseurs : il y a le sommet E qui est donc de niveau 3.

On supprime le sommet E du tableau ; il ne reste que le sommet F qui est donc de niveau 4.

Sommet	A	B	C	D	E	F
Niveau	0	1	1	2	3	4

On peut alors dessiner ce graphe ordonné par niveaux :



3. Pour obtenir la matrice de fermeture transitive de ce graphe, on met un 1 à l'intersection de la ligne correspondant au sommet X et de la colonne correspondant au sommet Y s'il existe un **chemin** allant du sommet X au sommet Y. Sinon on met un 0.
La matrice de fermeture transitive de ce graphe est donc

$$\begin{array}{c} \curvearrowright \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

4. Dans la matrice de fermeture transitive de ce graphe, il n'y a que des 0 sur la 1re diagonale et en dessous, il n' y a donc aucun chemin de retour possible vers un quelconque sommet ; ce graphe ne contient donc aucun circuit.

Partie B

Chaque page du site comprend 4 questions, qui peuvent rapporter des points ou en faire perdre.
Un utilisateur peut accéder à une page suivante lorsque l'une au moins des conditions suivantes est satisfaite :

— l'utilisateur a répondu correctement à 3 questions au minimum,
ou
— l'utilisateur a répondu correctement à strictement moins de 3 questions et a marqué 5 points au minimum sur la page,
ou
— l'utilisateur a marqué strictement moins de 5 points sur la page et il est titulaire du BTS SIO

On définit les variables booléennes suivantes :

- $a = 1$ si l'utilisateur a répondu correctement à 3 questions au minimum, $a = 0$ sinon ;
- $b = 1$ si l'utilisateur a marqué 5 points au minimum, $b = 0$ sinon ;
- $c = 1$ si l'utilisateur est titulaire du BTS SIO, $c = 0$ sinon.

1. La première condition correspond à a, la deuxième correspond à $\overline{a}$ et b donc à $\overline{a}.b$, et la troisième condition correspond à $\overline{b}$ et c donc à $\overline{b}.c$.
Donc $F = a + \overline{a}.b + \overline{b}.c$.

2. On utilise des tableaux de Karnaugh pour déterminer une écriture simplifiée de F sous la forme d'une somme de trois variables booléennes élémentaires :

a

a \ bc	00	01	11	10
0				
1	1	1	1	1

$\overline{a}.b$

a \ bc	00	01	11	10
0			1	1
1				

$\overline{b}.c$

a \ bc	00	01	11	10
0		1		
1		1		

$a + \overline{a}.b + \overline{b}.c$

a \ bc	00	01	11	10
0		1	1	1 — b
1	1	1	1	1 — a

c

Donc $F = a + b + c$.

Autre méthode - Par calcul, en utilisant les propriétés $1 + x = 1$ et $x + \overline{x} = 1$, on a :
$F = a + \overline{a}.b + \overline{b}.c = a.(1 + b) + \overline{a}.b + \overline{b}.c = a.1 + a.b + \overline{a}.b + \overline{b}.c = a + (a + \overline{a}).b + \overline{b}.c = a + 1.b + \overline{b}.c$
$= a + b + \overline{b}.c = a + b.(1 + c) + \overline{b}.c = a + b.1 + b.c + \overline{b}.c = a + b + (b + \overline{b}).c = a + b + 1.c$
$= a + b + c$

Un utilisateur ne peut pas accéder à une page suivante dans le cas $\overline{a + b + c}$, c'est-à-dire $\overline{a}.\overline{b}.\overline{c}$, donc s'il a répondu correctement à moins de 3 questions, s'il a marqué moins de 5 points et s'il n'est pas titulaire du BTS SIO.

Exercice 2 **6 points**

Cet exercice met en œuvre sur de petits nombres le premier système de cryptage asymétrique. Dans ce système, une personne destinataire qui veut recevoir des informations confidentielles publie une clé permettant à quiconque de lui envoyer des messages sous forme cryptée. Cependant seule la personne destinataire peut décrypter les messages à l'aide d'une autre clé connue d'elle seule.

Partie A - Détermination de la clé publique servant au cryptage

1. On choisit deux nombres : $p = 78$ et $q = 95$.
   $p = 2 \times 3 \times 13$ et $q = 5 \times 19$ donc le seul diviseur commun à p et q est 1 : les entiers p et q sont premiers entre eux.
2. La personne destinataire choisit 5 entiers $b_1 = 45$, $b_2 = 22$, $b_3 = 13$, $b_4 = 4$, $b_5 = 2$.
   La clé de cryptage est formée des 5 nombres entiers $(a_1, a_2, a_3, a_4, a_5)$ ainsi calculés :
   pour tout i de l'ensemble $\{1,2,3,4,5\}$, $0 \leqslant a_i \leqslant 77$ et $b_i \times q = a_i$, mod p.

Pour déterminer a_1 on calcule $b_2 \times q = 22 \times 95 = 2\,090 = 26 \times 78 + 62$.
Donc $2\,090 \equiv 62 \bmod 78$, et 62 est bien compris entre 0 et 77. Donc $a_2 = 62$.

Partie B - Cryptage d'un message

On admet dans la suite de l'exercice que $a_3 = 65$, $a_4 = 68$ et $a_5 = 34$.
La clé de cryptage est donc $(a_1, a_2, a_3, a_4, a_5) = (63,62,65,68,34)$.
Cette clé, publiée par la personne destinataire, permet à quiconque de lui envoyer un message crypté.
Cette partie va expliquer comment on crypte le message.
On associe d'abord à chaque lettre son rang dans l'alphabet, selon la correspondance suivante :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang	1	2	3	4	5	6	7	8	9	10	11	12	13
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	14	15	16	17	18	19	20	21	22	23	24	25	26

Pour crypter une lettre :

— on détermine son rang à l'aide du tableau de correspondance précédent ;

— on écrit ce nombre en base 2 sur 5 bits ; on ainsi obtient 5 chiffres (m_1,m_2,m_3,m_4,m_5), chaque chiffre étant égal à 0 ou à 1 ;

— on détermine alors la valeur cryptée, égale à la somme $\sigma = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5$.

On remarque qu'une lettre est ainsi cryptée par un nombre entier.
On veut crypter la lettre « W ».

— Le rang de W est 23_{10} ;

— on écrit ce nombre en base deux sur 5 bits : $9_{10} = 16 + 0 + 4 + 2 + 1 = 10111_2$,

— on calcule la somme $\sigma = 1 \times 63 + 0 \times 62 + 1 \times 65 + 1 \times 68 + 1 \times 34 = 230$.

La lettre « W » est donc cryptée par l'entier 230.

Exercice 3 **5 points**

Cet exercice étudie la suite (u_n) dont les termes sont définis par leur écriture en base deux : $u_0 = 1$, et, pour tout entier $n \geqslant 1$, $u_n = 1{,}1\ldots1$ où sont écrits n chiffres 1 à droite de la virgule.

1. $u_1 = 1{,}1_2 = 1 + \dfrac{1}{2} = 1{,}5$
   $u_2 = 1{,}11_2 = 1 + \dfrac{1}{2} + \dfrac{1}{2^2} = 1 + 0{,}5 + 0{,}25 = 1{,}75$
2. • $u_1 - u_0 = 1{,}5 - 1 = 0{,}5$ et $u_2 - u_1 = 1{,}75 - 1{,}5 = 0{,}25$;
   $u_1 - u_0 \neq u_2 - u_1$ donc la suite (u_n) n'est pas arithmétique.

- $\dfrac{u_1}{u_0} = \dfrac{1{,}5}{1} = 1{,}5$ et $\dfrac{u_2}{u_1} = \dfrac{1{,}75}{1{,}5} \approx 1{,}15$;
  $\dfrac{u_1}{u_0} \neq \dfrac{u_2}{u_1}$ donc la suite (u_n) n'est pas géométrique.

3. On pose $A = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \dfrac{1}{16}$.

a. $A = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \dfrac{1}{16} = 1 + \dfrac{1}{2} + \dfrac{1}{2^2} + \dfrac{1}{2^3} + \dfrac{1}{2^4} = 1{,}1111_2 = u_4$

b. $A = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \dfrac{1}{16} = 1 + 0{,}5 + 0{,}25 + 0{,}125 + 0{,}0625 = 1{,}9375$.

4. On admet dans cette question que, pour tout $n \geqslant 1$: $u_n = 1 + \dfrac{1}{2} + \left(\dfrac{1}{2}\right)^2 + \ldots + \left(\dfrac{1}{2}\right)^n$

$1 + q + \ldots + q^n = \dfrac{1 - q^{n+1}}{1 - q}$ donc

$$u_n = 1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \ldots + \left(\frac{1}{2}\right)^n = \frac{1 - \left(\dfrac{1}{2}\right)^{n+1}}{1 - \dfrac{1}{2}} = 2 \times \left(1 - \left(\frac{1}{2}\right)^{n+1}\right) = 2 - 2 \times \left(\frac{1}{2}\right)^{n+1} = 2 - \left(\frac{1}{2}\right)^n$$

5. On résout l'inéquation $u_n > 1{,}999$:

$$u_n > 1{,}999 \iff 2 - \left(\frac{1}{2}\right)^n > 1{,}999 \iff 0{,}001 > \left(\frac{1}{2}\right)^n \iff \ln(0{,}001) > \ln\left(0{,}5^n\right)$$
$$\iff \ln(0{,}001) > n \times \ln(0{,}5) \iff \frac{\ln(0{,}001)}{\ln(0{,}5)} < n$$

Or $\dfrac{\ln(0{,}001)}{\ln(0{,}5)} \approx 9{,}97$ donc la plus petite valeur de n telle que $u_n > 1{,}999$ est 10.

On peut vérifier à la calculatrice :

$u_9 = 2 - \left(\dfrac{1}{2}\right)^9 \approx 1{,}99805 < 1{,}999$ et $u_{10} = 2 - \left(\dfrac{1}{2}\right)^{10} \approx 1{,}99902 > 1{,}999$.