∽ BTS Métropole 13 mai 2019 ∾
Services informatiques aux organisations

Épreuve obligatoire

Exercice 1 **9 points**

Les parties A et B de cet exercice sont relatives aux pages d'un site web. Elles peuvent être traitées de manière indépendante.

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. Donner la matrice d'adjacence du graphe que l'on peut construire à partir de ce tableau, les sommets étant rangés par ordre alphabétique.
2. Donner le niveau de chaque sommet puis dessiner ce graphe ordonné par niveaux.
3. Déterminer la matrice de la fermeture transitive de ce graphe.
4. Montrer que ce graphe ne contient pas de 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. Écrire une expression booléenne F traduisant les conditions permettant à un utilisateur de passer à une page suivante.
2. À l'aide d'un tableau de Karnaugh ou d'un calcul booléen, déterminer une écriture simplifiée de F sous la forme d'une somme de trois variables booléennes élémentaires.

   Écrire sous forme d'une phrase, les conditions pour lesquelles un utilisateur ne peut pas accéder à une page suivante,

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 premiers entre eux : $p = 78$ et $q = 95$.

   Justifier que 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.

   Exemple : pour le calcul de a_1 on calcule $b_1 \times q = 45 \times 95 = 4\,275$.

   Or $4\,275 \equiv 63 \bmod p$, et 63 est bien compris entre 0 et 77. Donc $a_1 = 63$.

Question : en détaillant le calcul, montrer que $a_3 = 62$.

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 $\sigma = a_1 m_1 + a_2 m_2 + a_3 m_3 + a_4 m_4 + a_5 m_5$.

On remarque qu'une lettre est ainsi cryptée par un nombre entier.
Exemple : on veut crypter la lettre « I ».

— Le rang de I est 9_{10} ;

— on écrit ce nombre en base deux sur 5 bits : $9_{10} = 8 + 1 = 01001$,

— on calcule la somme $\sigma = 0 \times 63 + 1 \times 62 + 0 \times 65 + 0 \times 68 + 1 \times 34 = 96$.

La lettre « I »est donc cryptée par l'entier 96.
Question : crypter la lettre « W ».

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. Vérifier que, écrit en base dix, $u_1 = 1,5$.
   Donner l'écriture en base dix de u_2.
2. Justifier le fait que la suite (u_n) n'est ni arithmétique ni géométrique.
3. On pose $A = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \dfrac{1}{16}$.
   a. Vérifier que le nombre A est l'un des termes de la suite (u_n). Donner son rang.
   b. Déterminer l'écriture décimale du nombre A.
4. On admet dans cette question que, pour tout $n \geqslant 1$: $u_n = 1 + \dfrac{1}{2} + \left(\dfrac{1}{2}\right)^2 + \ldots + \left(\dfrac{1}{2}\right)^n$
   Démontrer que, pour tout $n \geqslant 1$, on a $u_n = 2 - \left(\dfrac{1}{2}\right)^n$.
   On pourra utiliser le formulaire ci-après.
5. Déterminer la plus petite valeur de n telle que $u_n > 1,999$.

Formulaire

Si q est un réel différent de 1 et n un entier naturel non nul, on a : $1 + q + \ldots + q^n = \dfrac{1 - q^{n+1}}{1 - q}$.