BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES
AUX ORGANISATIONS

SESSION 2017

SUJET

ÉPREUVE E2 – MATHÉMATIQUES POUR L'INFORMATIQUE

Sous-épreuve E21 – Mathématiques

Épreuve obligatoire

Durée : 2 heures **coefficient : 2**

Calculatrice autorisée, *conformément à la circulaire n° 99-186 du 16 novembre 1999 :*
« Toutes les calculatrices de poche, y compris les calculatrices programmables, alphanumériques ou à écran graphique, à condition que leur fonctionnement soit autonome et qu'il ne soit pas fait usage d'imprimante, sont autorisées.
Les échanges de machines entre candidats, la consultation des notices fournies par les constructeurs ainsi que les échanges d'informations par l'intermédiaire des fonctions de transmission des calculatrices sont interdits ».

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Il comprend 5 pages numérotées de la page 1/5 à 5/5.

Exercice 1 (8 points)

Cet exercice envisage deux problèmes relatifs à l'équipement d'une salle informatique rénovée, dans une entreprise. Les deux parties sont indépendantes.

Partie 1 : Choix d'un réseau

Le réseau informatique qui équipera la salle doit satisfaire au moins l'une des conditions suivantes :

- le réseau compte 5 postes ou plus et il existe un poste qui ne reçoit pas de données en entrée ;
- il existe un poste qui ne reçoit pas de données en entrée, et le réseau compte strictement moins de 5 postes, et il comporte strictement plus de 12 connexions ;
- le réseau comporte 12 connexions ou moins.

On définit les variables booléennes suivantes :

- $a = 1$ si le réseau compte 5 postes ou plus, $a = 0$ sinon ;
- $b = 1$ s'il existe un poste qui ne reçoit pas de données en entrée, $b = 0$ sinon ;
- $c = 1$ si le réseau comporte 12 connexions ou moins, $c = 0$ sinon.

1. Cette question est une question à choix multiple. Une seule réponse est correcte. Recopier sur la copie seulement la réponse correcte. On ne demande pas de justification.

Parmi les quatre phrases suivantes, donner celle qui traduit la variable $\overline{b}$:

- réponse A : « il existe un poste qui reçoit des données en entrée » ;
- réponse B : « tout poste reçoit des données en entrée » ;
- réponse C : « il existe un poste qui envoie des données en sortie » ;
- réponse D : « aucun poste ne reçoit des données en entrée ».

2. Donner l'expression booléenne E traduisant les critères voulus pour un réseau informatique.

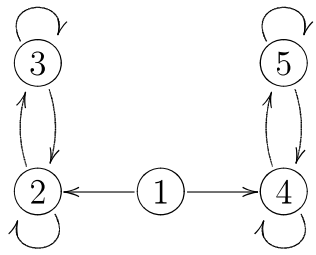
3. À l'aide d'un tableau de Karnaugh ou par des calculs, exprimer E comme somme de deux variables booléennes.

4. Traduire les critères de sélection simplifiés, à partir de l'expression obtenue à la question **3.**

5. Un réseau dans lequel 2 postes ne reçoivent pas de données en entrée et qui comporte 15 connexions répond-il aux critères voulus ? Justifier la réponse.

Partie 2 : Étude des connexions

La salle informatique doit comprendre cinq postes numérotés de 1 à 5 et branchés en réseau selon le graphe orienté ci-contre.
Dans ce graphe, une flèche d'un poste A vers un poste B traduit le fait que l'on peut envoyer des données de A vers B.



1. Donner la matrice d'adjacence M de ce graphe en prenant les numéros des postes dans l'ordre croissant.

2. Déterminer la matrice $\hat{M}$ de la fermeture transitive de ce graphe.

3. Pour permettre l'envoi de données entre les postes, même en cas de défaillance d'une connexion, on utilise la fermeture transitive du graphe.
Dessiner sur la copie le graphe correspondant à cette fermeture transitive.

Exercice 2 (7 points)

Le but de cet exercice est d'étudier, sur des exemples numériques simples, deux variantes d'une méthode de cryptage inventée par Gilbert Vernam en 1917, et appelée « masque jetable ».
Dans tout l'exercice, on note respectivement *M* le mot initial, *K* la clé de cryptage et *Y* le mot crypté.
Les trois nombres *M*, *K*, *Y* sont des entiers naturels.
Les deux parties de cet exercice sont indépendantes.

Partie 1 : Masque jetable binaire

La méthode décrite dans cette partie utilise le connecteur logique « *xor* », appelé « ou exclusif », qui est défini par la table de vérité suivante :

P	*Q*	*P xor Q*
0	0	0
0	1	1
1	0	1
1	1	0

Table 1

Par exemple les deux premières lignes signifient que $0 \ xor \ 0 = 0$ et que $0 \ xor \ 1 = 1$.

1. Recopier intégralement la table de vérité ci-après et compléter la dernière colonne.

P	*Q*	*P xor Q*	(*P xor Q*) *xor Q*
0	0	0	
0	1	1	
1	0	1	
1	1	0	

Table 2

2. Parmi les quatre propositions *P*, *Q*, (*P xor Q*) et ((*P xor Q*) *xor Q*), deux sont équivalentes. À l'aide de la table 2 complétée, déterminer lesquelles, en expliquant la réponse.

Dans la suite de l'exercice, on note a_b l'écriture du nombre entier *a* en base *b*.

3. Donner la représentation binaire de l'entier qui s'écrit 26_{10} en décimal.

4. Soit *M* et *K* deux entiers naturels écrits en binaire, tels que la longueur de l'écriture de *K* est supérieure ou égale à celle de *M*.

Pour crypter le mot *M* avec la clé *K*, on procède comme suit : pour chaque chiffre *m* du mot initial *M*, on considère le chiffre *k* de la clé *K* qui a la même position que *m* dans l'écriture.
On obtient alors le chiffre *y* du mot crypté *Y* qui a la même position que *m* dans l'écriture du mot initial *M*, par la relation : $y = m \ xor \ k$.

L'écriture binaire du mot crypté *Y* est la juxtaposition dans le même ordre des chiffres *y* calculés pour chaque chiffre *m* du mot *M*.

Exemple : avec $M = 01_2$ et $K = 10_2$

- Avec le chiffre de rang 1 en partant de la droite : $m = 1$ et $k = 0$; donc $y = 1$ *xor* $0 = 1$;
- avec le chiffre de rang 2 : $m = 0$ et $k = 1$; donc $y = 0$ *xor* $1 = 1$.

Donc le mot crypté est $Y = 11_2$.

Question : avec le mot initial $M = 011_2$ et la clé $K = 101_2$, déterminer le mot crypté *Y*.

Remarque : d'après la question 2, le décryptage s'effectue de la même manière que le cryptage.

Partie 2 : Masque jetable hexadécimal

Cette partie envisage le cryptage de nombres entiers écrits dans le système hexadécimal.
Les chiffres hexadécimaux sont notés 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

1. Questions préliminaires

a) Donner la représentation en hexadécimal de l'entier binaire 1011101_2.

b) Calculer en travaillant dans le système hexadécimal les sommes $7_{16} + 4_{16}$ et $A_{16} + C_{16}$.

2. Soit *M* et *K* deux entiers naturels écrits en hexadécimal, tels que la longueur de l'écriture de *K* est supérieure ou égale à celle de *M*, et tels que l'écriture de *K* ne comporte aucun chiffre 0.

Pour crypter le mot *M* avec la clé *K*, on procède comme suit : pour chaque chiffre *m* du mot initial *M*, on considère le chiffre *k* de la clé *K* qui a la même position que *m* dans l'écriture.
On obtient alors le chiffre *y* du mot crypté *Y* qui a la même position que *m* dans l'écriture du mot initial *M*, de la façon suivante : *y* est le chiffre hexadécimal des unités de la somme $m + k$.
Le mot crypté *Y* est déterminé en hexadécimal par la juxtaposition dans le même ordre des chiffres *y* calculés pour chaque chiffre *m* du mot *M*.

Exemple : avec $M = 49_{16}$ et $K = 19_{16}$

- Avec le chiffre de rang 1 en partant de la droite : $m = 9$ et $k = 9$; donc $m + k = 12_{16}$ et par suite $y = 2$;
- avec le chiffre de rang 2 : $m = 4$ et $k = 1$; donc $m + k = 5_{16}$ et par suite $y = 5$.

Donc le mot crypté est $Y = 52_{16}$.

Question : avec le mot initial $M = 7A_{16}$ et la clé $K = 4C_{16}$, déterminer le mot crypté *Y*.

3. Par cette méthode, on admet que le décryptage suit les mêmes étapes en remplaçant la clé *K* par une autre clé K'. Lorsque l'écriture de *K* comporte au maximum deux chiffres hexadécimaux, la clé K' est l'écriture en hexadécimal de la différence (écrite en décimal) $272_{10} - K_{10}$.

Cette question est une question à choix multiple. Une seule réponse est exacte. Recopier sur la copie seulement la réponse exacte. On ne demande pas de justification.

Avec la clé de cryptage $K = 19_{16}$, la clé de décryptage K' est égale à :

Réponse A : 253_{16} **Réponse B** : 247_{16}

Réponse C : FD_{16} **Réponse D** : $F7_{16}$

Exercice 3 (5 points)

Pour effectuer des calculs, un ordinateur représente les nombres en binaire. Cet exercice étudie l'effet d'une perte de précision initiale sur une suite de calculs.

Dans tout l'exercice, on note a_b l'écriture du nombre *a* en base *b*.

1. Représentation binaire de quelques nombres décimaux

a) Cette question est une question à choix multiple. Une seule réponse est exacte. Recopier sur la copie seulement la réponse exacte. On ne demande pas de justification.

La représentation binaire du nombre qui s'écrit en décimal $15,5_{10}$ est :

Réponse A : $10101,101_2$ **Réponse B** : $1111,1_2$

Réponse C : $1111,0101_2$ **Réponse D** : $10101,1_2$

b) Justifier que le nombre décimal $15,625_{10}$ a pour représentation binaire $1111,101_2$.

2. On considère la suite géométrique (u_n) de terme initial $u_0 = 32$ et de raison 15,625.

a) Calculer la valeur exacte de u_1.

b) Donner l'expression de u_n en fonction de *n*.

3. Pour calculer les termes de la suite (u_n), on utilise un logiciel qui arrondit le nombre $15,625$ et le transforme en $15,5$. L'arrondi se répercute sur tous les termes calculés, qui sont alors ceux de la suite géométrique (v_n) qui a le même terme initial que la suite (u_n), c'est-à-dire $v_0 = u_0 = 32$, et dont la raison est égale à $15,5$.

Ainsi, par exemple, $v_1 = 496$.

Pour tout entier naturel *n*, on définit la perte de précision relative e_n sur le *n*-ième terme par la relation :

$$e_n = \frac{v_n}{u_n}.$$

a) Démontrer que la suite (e_n) est la suite géométrique de terme initial $e_0 = 1$ et de raison $0,992$.

b) Déterminer le plus petit entier naturel *n* tel que $e_n < 0,9$.