Corrigé du BTS Services informatiques aux organisations
Métropole – 11 mai 2017

Épreuve obligatoire

Exercice 1 — 8 points

Cet exercice envisage deux. problèmes relatifs à l'équipement d'une salle informatique d'une entreprise.

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

— réponse A : « il existe un poste qui reçoit des données en entrée »;

— réponse B : $\boxed{\text{« tout poste reçoit des données en entrée »;}}$

— réponse C : « il existe un poste qui envoie des données en sortie »;

— réponse D : « aucun poste ne reçoit des données en entrée ».

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

- « Le réseau compte 5 postes ou plus et il existe un poste qui ne reçoit pas de données en entrée » correspond à « a et b », donc a pour expression booléenne ab.
- « 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 » correspond à « b et $\overline{a}$ et $\overline{c}$ », donc a pour expression booléenne $\overline{a}\,b\,\overline{c}$.
- « Le réseau comporte 12 connexions ou moins » a pour expression booléenne c.

Donc l'expression booléenne E traduisant les critères voulus pour un réseau informatique est

$$E = ab + \overline{a}\,b\,\overline{c} + c$$

3. À l'aide de tableaux de Karnaugh, on exprime E comme somme de deux variables booléennes.

ab

a \ bc	00	01	11	10
0				
1			1	1

$\overline{a}\,b\,\overline{c}$

a \ bc	00	01	11	10
0				1
1				

c

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

$$E = ab + \overline{a}\,b\,\overline{c} + c$$

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

b

c

Donc l'expression simplifiée de E est $E = b + c$.

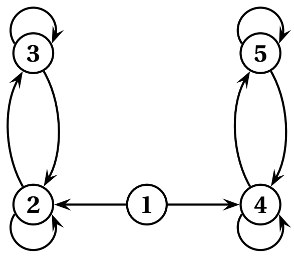
4. Un réseau correspond donc aux critères voulus s'il existe un poste qui ne reçoit pas de données en entrée ou s'il comporte 12 connexions ou moins.

5. Un réseau dans lequel 2 postes ne reçoivent pas de données en entrée et qui comporte 15 connexions correspond à l'expression booléenne $b\,\overline{c}$ donc il répond aux critères voulus.

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. Pour déterminer la matrice d'adjacence M 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 arc allant du sommet X au sommet Y. Sinon on met un 0.

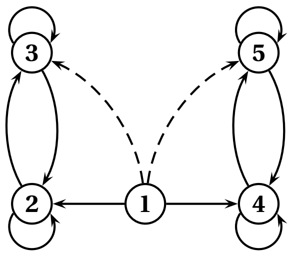
$$M = \begin{array}{c} \circlearrowright \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

2. 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.

$$\widehat{M} = \begin{array}{c} \circlearrowright \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

On peut aussi calculer $\widehat{M}$ par $\widehat{M} = M^{[1]} \oplus M^{[2]} \oplus M^{[3]} \oplus M^{[4]} \oplus M^{[5]}$.

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.
   On dessine 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.

Partie 1 : Masque jetable

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

1. On complète la table de vérité ci-après.

P	Q	P `xor` Q	(P `xor` Q) `xor` Q
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

2. Parmi les quatre propositions P, Q, (P `xor` Q) et ((P `xor` Q) `xor` Q), deux sont équivalentes.
   Les deux colonnes correspondant à P et ((P `xor` Q) `xor` Q) sont identiques donc les propositions P et ((P `xor` Q) `xor` Q) sont équivalentes.
   On a aussi : $((P \texttt{ xor } Q) \texttt{ xor } Q) = (P \texttt{ xor } (Q \texttt{ xor } Q)) = (P \texttt{ xor } FAUX) = P$

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

3. $26_{10} = 16+8+2 = 1\times 2^4 + 1\times 2^3 + 0\times 2^2 + 1\times 2^1 + 0\times 2^0 = 11010_2$
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 : $y = m \texttt{ xor } k$.
   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.

Avec le mot initial $M = 011_2$ et la clé $K = 101_2$, on détermine le mot crypté Y.

En partant de la droite :

- `1 xor 1` $= 0$;
- `1 xor 0` $= 1$;
- `0 xor 1` $= 1$.

Donc le mot crypté est $Y = 110_2$.

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.** On donne la représentation en hexadécimal de l'entier binaire 1011101_2.
     En prenant des tranches de 4 bits en commençant par la droite :
     - $1101_2 = (1+2^2+2^3)_{10} = 13_{10} = \text{D}_{16}$
     - $101_2 = (1+2^2)_{10} = 5_{10} = 5_{16}$

     Donc $1011101_2 = 5\text{D}_{16}$.
   - **b.** On calcule les sommes $7_{16}+4_{16}$ et $\text{A}_{16}+\text{C}_{16}$.
     - $7_{16}+4_{16} = 7_{10}+4_{10} = 11_{10} = \text{B}_{16}$
     - $\text{A}_{16}+\text{C}_{16} = 10_{10}+12_{10} = 22_{10} = 16_{10}+6_{10} = 16_{16}$
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.

   Avec le mot initial $M = 7\text{A}_{16}$ et la clé $K = 4\text{C}_6$, on détermine le mot crypté Y.
   En partant de la droite :
   - $\text{A}_{16}+\text{C}_{16} = 16_{16}$ donc on garde 6.
   - $7_{16}+4_{16} = \text{B}_{16}$ donc on garde B.

   Le mot crypté est B6.
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** : $\boxed{\text{F}7_{16}}$

   K$= 19_{16} = 16_{10}+9_{10} = 25_{10}$; donc K$' = 272_{10} - 25_{10} = 247_{10} = (15\times 16+7)_{10} = \text{F}7_{16}$

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

Réponse A : $10101,101_2$	**Réponse B** : $\boxed{1111,1_2}$
Réponse C : $1111,0101_2$	**Réponse D** : $10101,1_2$

$15,5_{10} = \left(1\times 2^3 + 1\times 2^2 + 1\times 2^1 + 1\times 2^0 + 1\times 2^{-1}\right)_{10} = 1111,1_2$

b. $15,625_{10} = \left(8+4+2+1+\dfrac{1}{2}+\dfrac{1}{8}\right)_{10}$
$= \left(1\times 2^3 + 1\times 2^2 + 1\times 2^1 + 1\times 2^0 + 1\times 2^{-1} + 0\times 2^{-2} + 1\times 2^{-3}\right)_{10}$
$= 1111,101_2$

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

a. $u_1 = u_0 \times 15,625 = 32 \times 15,625 = 500$

b. La suite (u_n) est géométrique de premier terme $u_0 = 32$ et de raison $q = 15,625$ donc, pour tout entier n, $u_n = u_0 \times q^n = 32 \times 15,625^n$.

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, $v_1 = 496$.

On peut donc dire que pour tout n, on a : $v_n = 32 \times 15,5^n$.

Pour tout entier naturel n, on définit la perte de précision relative e_n sur le n-ième terme par la relation : $e_n = \dfrac{v_n}{u_n}$.

a.
- $e_0 = \dfrac{v_0}{u_0} = \dfrac{32}{32} = 1$
- $u_n = 32 \times 15,625^n$ et $v_n = 32 \times 15,5^n$ donc $e_n = \dfrac{v_n}{u_n} = \dfrac{32 \times 15,5^n}{32 \times 15,625^n} = \left(\dfrac{15,5}{15,625}\right)^n = 0,992^n$

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

b. À la calculatrice, on trouve $e_{13} \approx 0,901 > 0,9$ et $e_{14} \approx 0,894 < 0,9$ donc le plus petit entier naturel n tel que $e_n < 0,9$ est $n = 14$.

On peut aussi résoudre l'inéquation $e_n < 0,9$:

$e_n < 0,9 \iff 0,992^n < 0,9 \iff \ln\left(0,992^n\right) < \ln(0,9) \iff n \times \ln(0,992) < \ln(0,9)$
$\iff n > \dfrac{\ln(0,9)}{\ln(0,992)}$

Or $\dfrac{\ln(0,9)}{\ln(0,992)} \approx 13,1$ donc le plus petit entier naturel n tel que $e_n < 0,9$ est bien 14.