Median IT40

Exercice 1 : Étude de deux Algorithmes (8 points)

On rappelle le théorème de la division euclidienne sur les entiers qui assure que pour tout couple d'entier $(a, b) \in \mathbb{N}^2$ il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que

$$a = bq + r \text{ et } r < b. \tag{1}$$

L'entier q est appelé le quotient de la division de a par b et r est appelé le reste.

1. On considère l'algorithme suivant qui prend en entrée un couple d'entiers $(a, b) \in \mathbb{N}^2$ et retourne un couple $(q, r) \in \mathbb{N}^2$.

Algorithme 1

```
div_euclide(a, b)
q ← 0
r ← a
while r ≥ b do
    q ← q + 1
    r ← r − b
end while
Return (q, r)
```

(a) Prenons le couple $(a, b) = (8, 3)$. Déroulez l'algorithme à la main et en déduire ce que renvoie l'appel de div_euclide$(8, 3)$.

Itération	q	r	$r \geq b$?
0 (initialisation)	0	8	V
1	1	5	V
2	2	2	F

et donc $(q, r) = (2, 2)$ à la fin de l'algorithme.
Même question pour $(a, b) = (10, 5)$.

Itération	q	r	$r \geq b$?
0 (initialisation)	0	10	V
1	1	5	V
2	2	0	F

et donc $(q, r) = (2, 0)$ à la fin de l'algorithme.

(b) On note q_n, r_n les valeurs des variables q et r après le n-ième passage en boucle et q_0, r_0 les valeurs avant le premier passage. On considère la propriété suivante,

$$a = bq_n + r_n \qquad (\mathcal{P}_n). \tag{2}$$

Montrer que $(\mathcal{P}_n)$ est un invariant de boucle.

Base Pour $n = 0$ on a l'initialisation $q_0 = 0$ et $r_0 = a$ et donc $a = bq_0 + r_0$. $(\mathcal{P}_0)$ est vérifiée ;

Recurrence Supposons que la propriété $(\mathcal{P}_n)$ est vérifiée. À l'itération $(n + 1)$ on aura $q_{n+1} = q_n + 1$ et $r_{n+1} = r_n - b$. Donc

$$bq_{n+1} + r_{n+1} = b(q_n + 1) + (r_n - b) = bq_n + b + r_n - b = bq_n + r_n = a$$

d'après l'hypothèse de récurrence. Ce qui montre que $(\mathcal{P}_n)$ est un invariant de boucle.

(c) Montrer que l'algorithme converge.

La suite r_n est une suite de nombre positif **strictement** décroissante. Cela nous assure que pour tout couple (a, b), il existe un nombre n_0 (qui dépend de a et b) tel que $r_{n_0} < b$. L'algorithme est donc convergent (il s'arrête).

(d) Conclure que l'algorithme calcule bien le quotient et le reste de la division euclidienne de a par b.

D'après les questions précédentes, pour tout couple (a, b) il existe n_0 tel que $r_{n_0} < b$ et on a la propriété $a = bq_{n_0} + r_{n_0}$. L'algorithme calcule donc bien la division euclidienne de a par b

2. On considère maintenant un second algorithme

Algorithme 2

div_euclide2(a, b)
$n \leftarrow 0$
while $2^n b \leq a$ **do**
  $n \leftarrow n + 1$
end while
$\alpha \leftarrow 2^{n-1}$
$\beta \leftarrow 2^n$
for $k = 1$ to $n - 1$ **do**
  $\gamma \leftarrow \frac{\alpha+\beta}{2}$
  if $\gamma b \leq a$ **then** $\alpha \leftarrow \gamma$
  else $\beta \leftarrow \gamma$
  end if
end for
Return$(\alpha, a - b\alpha)$

On notera comme précédemment q et r le quotient et le reste de la division euclidienne de a par b. Le but des questions qui suivent est de montrer que $q = \alpha$ (où α est la valeur de la variable α en sortie de boucle **For**) et donc $r = a - b\alpha$.

(a) Justifier que la première boucle **While** permet de déterminer l'unique entier n tel que,

$$2^{n-1} \leq q < 2^n \tag{3}$$

La valeur de n est incrémentée de 1 jusqu'à ce que $2^n b > a$. Fixons cette valeur de n.
En effectuant la division **entière** par b des deux cotés de l'inégalité, on trouve l'inégalité $2^n > q$.
Pour $n - 1$, on a l'inégalité $2^{n-1}b \leq a$, en effectuant la division entière par b on trouve l'inégalité $2^{n-1} \leq q$.
D'où la conclusion demandée.

(b) On note α_k et β_k les valeurs de α et β après le $k$ème passage dans la boucle **For** (et α_0, β_0 les valeurs avant le premier passage).

i. Montrer que pour tout $k \leq n - 1$ on a

$$\beta_k - \alpha_k = \frac{\beta_{k-1} - \alpha_{k-1}}{2} \qquad (\mathcal{P}_k). \tag{4}$$

On a $\alpha_0 = 2^{n-1}$ et $\beta_0 = 2^n$ ainsi que la récurrence

$$\alpha_{k+1} = \begin{cases} \frac{\alpha_k+\beta_k}{2} & \text{si } \frac{\alpha_k+\beta_k}{2} \times b \leq a \\ \alpha_k & \text{sinon} \end{cases}$$

et

$$\beta_{k+1} = \begin{cases} \frac{\alpha_k+\beta_k}{2} & \text{si } \frac{\alpha_k+\beta_k}{2} \times b > a \\ \beta_k & \text{sinon.} \end{cases}$$

On vérifie ensuite la propriété $\mathcal{P}_k$ par récurrence.
Base Pour $k = 0$, si $\frac{\alpha_0+\beta_0}{2} \times b \leq a$ alors

$$\beta_1 - \alpha_1 = \beta_0 - \frac{\alpha_0 + \beta_0}{2} = \frac{\beta_0 - \alpha_0}{2} \qquad \left(= \frac{2^n - 2^{n-1}}{2} = 2^{n-2}\right).$$

et si $\frac{\alpha_0+\beta_0}{2} \times b > a$ alors

$$\beta_1 - \alpha_1 = \frac{\alpha_0 + \beta_0}{2} - \alpha_0 = \frac{\beta_0 - \alpha_0}{2} \qquad \left(= \frac{2^n - 2^{n-1}}{2} = 2^{n-2}\right).$$

Recurrence Pour $k > 0$, si $\frac{\alpha_k+\beta_k}{2} \times b \leq a$ alors

$$\beta_{k+1} - \alpha_{k+1} = \beta_k - \frac{\alpha_k + \beta_k}{2} = \frac{\beta_k - \alpha_k}{2}$$

et si $\frac{\alpha_k+\beta_k}{2} \times b > a$ alors

$$\beta_{k+1} - \alpha_{k+1} = \frac{\alpha_k + \beta_k}{2} - \alpha_k = \frac{\beta_k - \alpha_k}{2}.$$

ii. En déduire qu'en sortie de boucle **For** on a $\beta_{n-1} - \alpha_{n-1} = 1$.
On a vu à la question précédente que $\beta_0 - \alpha_0 = 2^{n-1}$. Comme à chaque itération la différence $\beta_k - \alpha_k$ est divisée par 2, au bout de $n-1$ itérations cette différence vaudra 1.

iii. Montrer par récurrence que pour tout $k \leq n-1$ on a $\alpha_k \leq q < \beta_k$.
On a vu à la question (a) que l'encadrement est vérifié pour $k = 0$. Supposons qu'à l'itération k, on a $\alpha_k \leq q < \beta_k$.
Si $\frac{\alpha_k+\beta_k}{2} \times b \leq a$ alors la division entière de

$$\alpha_{k+1} \times b = \frac{\alpha_k + \beta_k}{2} \times b \qquad (\leq a)$$

par b sera inférieure à q et comme $\beta_{k+1} = \beta_k$ on aura q inférieur à β_{k+1} d'après l'hypothèse de récurrence.
Le raisonnement est semblable lorsque $\frac{\alpha_k+\beta_k}{2} \times b > a$.

iv. Conclure que $\alpha_{n-1} = q$.
Comme $\beta_{n-1} - \alpha_{n-1} = 1$ et $\alpha_{n-1} \leq q < \beta_{n-1}$ on a l'égalité $q = \alpha_{n-1}$.

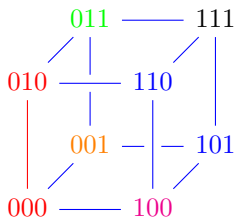
Exercice 2 : Monômes premiers d'une fonction booléenne (6 points)

Soit $\mathcal{B} = \{0, 1\}$. On note x' le complément de x. On considère la fonction f de trois variables booléennes définie par :

$$\forall (x, y, z) \in \mathcal{B}^3 \quad f(x, y, z) = x'z' + x'yz + xy'z' + xyz + x'y'z.$$

1. Fournir une représentation dans l'espace qui fasse apparaître les points "couverts" par f, c'est-à-dire ceux où elle prend la valeur 1.

$$f(x, y, z) = x'z' + x'yz + xy'z' + xyz + x'y'z.$$



2. Déterminer l'ensemble des monômes inférieurs à f. Lesquels sont premiers ?

	degrés 3 (points)	degrés 2 (arêtes)	degrés 1 (faces)
1	$x'y'z'$	$y'z'$	x'
2	$x'yz'$	$x'z'$	
3	$x'yz$	$x'y'$	
4	$xy'z'$	$x'y$	
5	xyz	$x'z$	
6	$x'y'z$	yz	

TABLE 1 – Monômes premiers de f. En rouge les monômes premiers.

Parmi les monômes de degré deux, tous ceux qui ne sont pas indiqués comme premiers sont inférieurs à x'.
Parmi les monômes de degré 3, les monômes sur les lignes 1,2,3 et 6 sont inférieurs à x', le monôme de la ligne 4 est inférieur à $y'z'$, celui de la ligne 5 est inférieur à yz.
Donc aucun monôme de degré 3 n'est premier.

3. Montrer directement, sans utiliser le théorème de cours, que f est égale à la somme de ses monômes premiers. L'écriture est-elle optimale en termes de simplification ? Pourquoi ?
   On se sert de la représentation dans l'espace comme d'un diagramme de Karnaugh. On obtient la simplification de f suivante
   $$f(x,y,z) = x' + y'z' + yz.$$
   Cette simplification est optimale puisqu'il n'est pas possible de supprimer un des termes de la somme sans modifier la fonction.

Exercice 3 : Enquête logique (6 points)

Lors d'une enquête, on a recueilli les témoignages de trois suspects :

Brown : "Jones est coupable et Smith est innocent".

Jones : "Si Brown est coupable, alors Smith l'est aussi."

Smith : "Je suis innocent mais au moins l'un des deux autres est coupable".

Ces trois témoignages seront notées B, J et S. En utilisant la convention :

p "Brown est coupable"

q "Jones est coupable"

r "Smith est coupable"

Répondre aux questions suivantes :

1. Exprimer le témoignage de chacun des suspects dans le langage de la logique propositionnelle.
   B $q \wedge \neg r$
   J $p \to r$
   S $\neg r \wedge (p \vee q)$
2. Si tous disent vrai, lequel(s) est (sont) coupable(s) ? Vous écrirez les contraintes logiques et donnerez la (les) solution(s) de ces contraintes.
   Si tous les énoncés sont équivalents au "Vrai" alors
   $$q\bar{r} = 1, \qquad \bar{p} + r = 1, \qquad \bar{r}(p+q) = 1.$$
   de la première équation on déduit que $q = 1$ et $r = 0$. En remplaçant dans la deuxième et dans la troisième équation on obtient
   $$q = 1, \qquad r = 0, \qquad \bar{p} = 1 \Leftrightarrow p = 0, \qquad (p+1) = 1 \Leftrightarrow 1 = 1.$$
   Il n'y a donc qu'un coupable "**Jones**".
3. Dans cette partie, on ne suppose plus que les trois suspects disent nécessairement la vérité.
   (a) Faire une table de vérité avec p, q et r et en déduire les valeurs de vérité de B, J et S dans les 8 cas.

p	q	r	B	J	S
F	F	F	F	V	F
F	F	V	F	V	F
F	V	F	V	V	V
F	V	V	F	V	F
V	F	F	F	F	V
V	F	V	F	V	F
V	V	F	V	F	V
V	V	V	F	V	F

   (b) Un des témoignages se déduit des 2 autres, lequel ?
   Par examen de la table de vérité, on remarque que $S \equiv J \to B$.
   (c) Si tous sont innocents, lequel(s) a (ont) menti ?
   Si tous sont innocents alors $p \equiv q \equiv r \equiv F$ et donc "**Brown**" et "**Smith**" mentent.
   (d) **Hors barème** Si tous les innocents disent vrai, lequel est coupable ?
   Il y avait plusieurs façon de traiter cette question. En voilà une
   — Supposons que "**Brown**" est innocent : cela correspond aux quatre premières lignes de la table de vérité. Dans ce cas il ne dit la vérité (ligne 3 de la table) que lorsque "**Jones**" est coupable et lorsque "**Smith**" est innocent. On vérifie que pour cette solution "**Smith**" dit aussi la vérité.
   — Si on suppose que "**Brown**" est le coupable (4 dernières lignes de la table) alors il n'est pas possible que "**Jones**" et "**Smith**" soient innocents car dans ce cas "**Jones**" ment (ligne 5).
   Donc la seule solution avec *un seul* coupable (attention à la façon dont la question est tournée !) est lorsque "**Brown**" et "**Smith**" sont innocents.