ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
Section d'Informatique et de Systèmes de Communication

Corrigé de la série 1 26 Sep. 2011

1. Spécification formelle I

a) L'input est un *ensemble*, donc $4, 7 \notin I$ (ce ne sont pas des ensembles). Les éléments de l'ensemble doivent être des nombres naturels, donc $\{-1, 100, 2\} \notin I$ (puisque $-1 \notin \mathbb{N}$) et $\mathrm{Pot}(\mathbb{N}) \notin I$ (puisque ses éléments ne sont pas dans $\mathbb{N}$, par exemple $\{1, 2\} \notin \mathbb{N}$). $\mathbb{N} \notin I$, puisque $\mathbb{N}$ n'est pas fini.

On a donc $\{1, 2\}, \quad \{1\}, \quad \{1, \ldots, 100\} \quad \in I$.

b) L'input est un sous-ensemble fini de $\mathbb{N}$, l'ensemble de tous les inputs possibles est donc l'ensemble de tous les sous-ensembles finis de $\mathbb{N}$: $I = \mathrm{Pot}^*(\mathbb{N})$.

c) $(2, vrai), (7, faux) \notin R$ puisque $2, 7 \notin I$. On voit également que $\{\mathbb{N}, faux\} \notin R$, puisque $\mathbb{N} \notin I$ (car $\mathbb{N}$ n'est pas fini). Pour $(\{1, 2, 4, 6\}, vrai)$, on a bien $\{1, 2, 4, 6\} \in I$ et $vrai \in O$, mais tous les éléments de $(\{1, 2, 4, 6\}$ ne sont pas pairs, l'output attendu pour ce input est donc $faux$. On a donc $(\{1, 2, 4, 6\}, vrai) \notin R$.

On obtient : $(\{2\}, vrai)$, $(\{1, \ldots, 100\}, faux) \in R$.

d) On a donc :

$$
\begin{aligned}
R \quad = \quad & \left\{(S, \text{vrai}) \in I \times O \;\middle|\; \forall x \in S \ : \ \exists k \in \mathbb{N} : x = 2k\right\} \\
& \bigcup \left\{(S, \text{faux}) \in I \times O \;\middle|\; \exists x \in S \ : \ \exists k \in \mathbb{N} : x = 2k + 1\right\}
\end{aligned}
$$

e) Le input est le même que dans le problème précédant, on a donc $I_2 = \mathrm{Pot}^*(\mathbb{N})$

f) Si on donne l'input S (où S est un sous-ensemble de $\mathbb{N}$), on veut comme output le nombre d'éléments de S qui sont pairs. Le output est donc un nombre. On a donc $\{2, 4\}, \{2k \mid k \in \mathbb{N}\}, \mathbb{N} \notin O_2$ puisque ce ne sont pas des nombres. Par contre $1, 0, 258 \in O_2$.

g) $O_2 = \mathbb{N}_0$ (puisque 0 est autorisé comme output).

h) $(\{1, 2, 3\}, 1) \in R$, puisque $\{1, 2, 3\} \in I$, $1 \in O$ et $\{1, 2, 3\}$ a bien 1 élément pair. De même, $(\{1, 8, 6, 2\}, 3) \in R$ puisque $\{1, 8, 6, 2\}$ a bien 3 éléments pairs. Par contre $(\{1, 2, 3, 4, 5\}, \{2, 4\}) \notin R$, car $\{2, 4\} \notin O$.-

i) $\exists T \subseteq S \ : (\ |T| = n \ \wedge \ \forall x \in T \ : \ \exists k \in \mathbb{N} \ : \ x = 2k)$

j) On aura $(S, m) \in R$ si et seulement si il existe $T \subseteq S$ avec :
- T est l'ensemble des nombres pairs de S, c'est-à-dire que
  - tous les éléments de T sont pairs
  - tous les éléments de $S \backslash T$ sont impairs
- $|T| = m$

$$
\begin{aligned}
R \;=\; \Bigg\{(S,m)\in I\times O \;\Bigg|\; & \exists T\subseteq S\ : \\
& [\ \ |T| = m\ \wedge \\
& \forall x\in T \quad\ :\ \exists k\in\mathbb{N}\ :\ x=2k\ \wedge \\
& \forall x\in S\backslash T\ :\ \exists k\in\mathbb{N}\ :\ x=2k+1]\Bigg\}
\end{aligned}
$$

2. *Spécification formelle II*

On rappelle qu'une *spécification formelle* d'un problème consiste en 3 ensembles I, O et R. I est l'ensemble de tous les inputs possibles, O est l'ensemble de tous les outputs possibles, et R est la *dépendance relationelle*. C'est une relation entre I et O (c'est-à-dire un sous-ensemble de $I\times O$). La dépendance relationelle vérifie par définition

$(i,o)\in R \iff o$ est un output valable quand l'input i est donné au problème.

a) Étant donné un nombre naturel $n\in\mathbb{N}$, on veut savoir si n est impair. Le input au problème est le nombre naturel n, donc l'ensemble de tous les inputs possibles est l'ensemble $\mathbb{N}$.

Si on avait une machine pour résoudre ce probléme, quand on lui donne un $n\in\mathbb{N}$, elle nous répondrait soit "vrai" (si n est impair), soit "faux" (si n est pair). L'ensemble des outputs possibles est donc $\{\text{vrai},\text{faux}\}$.

Si on donne à notre machine l'input 7, l'output attendu est "vrai". Donc par définition de R, on a $(7,\text{vrai})\in R$. De manière générale, si on lui donne un nombre impair, elle nous retournerait "vrai". Donc $(x,\text{vrai})\in R$ pour tous les nombres impairs x et de même, on a $(y,\text{faux})\in R$ pour tous les nombres pairs y.

En résumé :

$$
\begin{aligned}
I &= \mathbb{N}\\
O &= \{\text{vrai},\text{faux}\}\\
R &= \Big\{(n,\text{vrai})\in I\times O \;\Big|\; \exists k\in\mathbb{N}: n=2k+1\Big\}\\
&\quad \bigcup \Big\{(n,\text{faux})\in I\times O \;\Big|\; \exists k\in\mathbb{N}: n=2k\Big\}
\end{aligned}
$$

Un problème dans lequel il faut déterminer si une propriété est vraie ou fausse s'appelle un *problème de décision*. L'ensemble des outputs est dans ce cas toujours l'ensemble $\{\text{vrai},\text{faux}\}$. Bien sûr on peut très bien utiliser des variantes comme $\{\text{Oui},\text{Non}\}$, $\{1,0\}$ ou dans ce cas $\{\text{impair},\text{pair}\}$.

b) L'input au problème est le nombre n. Tous les nombres naturels sauf 1 sont autorisés, on a donc $I=\mathbb{N}\backslash\{1\}$.

L'output est le plus grand diviseur de n qui soit inférieur à n. Par exemple si on donne au problème l'input 12, ses diviseurs sont $1,2,3,4,6$ et 12. Le plus grand de ces diviseurs qui soit inférieur à 12 est 6, l'output attendu est donc 6. De même si on donne comme input 15, l'output sera 5, si on donne comme input 17, l'ouput sera 1, etc...

L'output attendu est donc un nombre naturel (et pour tout nombre naturel x il existe un input pour lequel x est l'output), l'ensemble des outputs possibles est donc l'ensemble de tous les nombre naturels, on a donc $O = \mathbb{N}$.

Pour la relation, soient $n \in I$ et $a \in O$. On aura $(n, a) \in R$ si et seulement si :
- a est un diviseur de n et $a < n$
- si $b < n$ est un diviseur de n, alors $b \leq a$ (donc a est le *plus grand* élément parmi les diviseurs de n qui sont inférieurs à n).

De manière générale quand on veut trouver le plus grand élément qui a une certaine propriété on le specifie souvent de cette manière : Il faut trouver un élément (a) qui verifie la propriété (a divise n et $a < n$), et tel que si un autre élément (b) veŕifie la propriété alors b est inférieur ou égal à a.

Nous n'avons donc plus qu'à écrire ces conditions de manière formelle :

$$\begin{aligned} I &= \mathbb{N} \backslash \{1\} \\ O &= \mathbb{N} \\ R &= \left\{ (n, a) \in I \times O \;\middle|\; (a \mid n \;\; \wedge \;\; a < n) \;\; \bigwedge \;\; \forall b \in \mathbb{N} : \Big((b \mid n \;\; \wedge \;\; b < n) \implies b \leq a \Big) \right\} \end{aligned}$$

c) Étant donné deux mots $S, T \in \mathcal{A}^+$, Le but du problème est de déterminer si S est un sous-mot de T. Il s'agit encore d'un problème de décision, on sait donc que l'ensemble des outputs sera $O = \{\text{vrai}, \text{faux}\}$. L'input consiste en deux mots sur $\mathcal{A}$, c'est-à-dire deux élément de $\mathcal{A}^+$, c'est-à-dire un élément de $\mathcal{A}^+ \times \mathcal{A}^+$. L'ensemble de tous les inputs possibles est donc $I = \mathcal{A}^+ \times \mathcal{A}^+$

Pour la relation, on rappelle que R est un sous-ensemble de $I \times O$, dans ce cas on aura donc $R \subseteq (\mathcal{A}^+ \times \mathcal{A}^+) \times \{\text{vrai}, \text{faux}\}$. On a $[(S, T), \text{vrai}] \in R$ si et seulement si S est un sous-mot de T. Par exemple, on a $[((e, n, d), (f, e, n, d, e, r)), \text{vrai}] \in R$. Il nous faut donc exprimer cette condition.

On pose $n = |S|$ et $m = |T|$. On a donc $S = \{s_0, \ldots, s_{n-1}\}$ et $T = \{t_0, \ldots, t_{m-1}\}$ avec tous les s_i et t_i dans $\mathcal{A}$. Pour que S soit un sous-mot de T il faut que $t_i = s_0$, $t_{i+1} = s_1$, $\ldots$, $t_{i+n} = s_n$ pour un certain indice $i \in \{1, \ldots, m\}$. Formellement on a :

$$\exists i \in \{0, \ldots, m-1\} \; : \; (n \leq m - i \wedge \forall j \in \{0, \ldots, n-1\} : \; s_j = t_{i+j})$$

En résumé :

$$
\begin{aligned}
I &= \mathcal{A}^+ \times \mathcal{A}^+ \\
O &= \{\text{vrai}, \text{faux}\} \\
R &= \Bigg\{ [((s_0, \ldots, s_{n-1}), (t_0, \ldots, t_{m-1})), \text{vrai}] \in I \times O \ \Bigg| \\
&\qquad \exists i \in \{0, \ldots, m-1\} \ : \ (n \leq m - i \wedge \forall j \in \{0, \ldots, n-1\} : \ s_j = t_{i+j}) \Bigg\} \\
&\bigcup \Bigg\{ [((s_0, \ldots, s_{n-1}), (t_0, \ldots, t_{m-1})), \text{faux}] \in I \times O \ \Bigg| \\
&\qquad \nexists i \in \{0, \ldots, m-1\} \ : \ (n \leq m - i \wedge \forall j \in \{0, \ldots, n-1\} : \ s_j = t_{i+j}) \Bigg\}
\end{aligned}
$$

3. Induction

a)

n	$A(n)$	$n!$
1	1	1
2	5	2
3	23	6
4	119	24
5	719	120

b) Il semblerait que

$$A(n) = (n+1)! - 1 \tag{1}$$

c) On veut montrer par induction que la formule (1) est juste pout tout $n \geq 1$.

Base : Quand $n = 1$, on a $(1+1)! - 1 = 2 - 1 = 1 = A(1)$.

Pas : Supponsons maintentant que (1) est vraie pour n. Nous voulons montrer qu'elle est ausi vraie pour $n + 1$.

$$
\begin{aligned}
A(n+1) &= \textstyle\sum_{k=1}^{n+1} k \cdot k! \\
&= \textstyle\sum_{k=1}^{n} k \cdot k! + (n+1) \cdot (n+1)! \\
&= A(n) + (n+1) \cdot (n+1)! \\
&= (n+1)! - 1 + (n+1) \cdot (n+1)! \quad \text{(par hypothèse d'induction)} \\
&= ((n+1) + 1) \cdot (n+1)! - 1 \\
&= (n+2)! - 1
\end{aligned}
$$

et donc par induction (1) est vraie pour tout $n \geq 1$.