TD 12. Révisions : exercices supplémentaires

Exercice 1. Terminaison de programme (Examen 2022)

Considérons le programme Java ci-dessous :

```java
public static void main(String[] args) {
    int n1 = Integer.parseInt(args[0]);
    int n2 = Integer.parseInt(args[1]);
    while (n2 - n1 <= 0 && n1 + n2 >= 1)
        n2 = n2 - 2*n1 + 1;
}
```

Ce programme prend en entrée deux entiers relatifs n_1 et n_2 passés en argument de la ligne de commande, puis boucle en soustrayant $2 \cdot n_1$ et ajoutant 1 à n_2 à chaque tour de boucle. Le but de cet exercice est de voir comment montrer que ce programme termine pour toutes les valeurs initiales dans $\mathbb{Z}$ de n_1 et n_2, à l'aide d'une *fonction de rang*.

Signature et théorie. On se place sur la signature $L \stackrel{\text{def}}{=} (\{+^2, r^{(2)}\}, \{<^{(2)}, =^{(2)}\})$ dotée d'un symbole de fonction binaire pour l'addition, d'un symbole de fonction binaire r, et de deux symboles de relations binaires $<$ et $=$ pour l'ordre et l'égalité. La théorie logique que nous utilisons est l'arithmétique de Presburger $\mathrm{Th}(\mathbb{Z}, +, <)$ étendue par le symbole non-interprété r. Autrement dit, notre théorie est $T \stackrel{\text{def}}{=} \mathrm{Th}(\mathcal{K})$ où $\mathcal{K}$ est l'ensemble des interprétations de la forme $I = (\mathbb{Z}, +, r^I, <)$, où $D_I \stackrel{\text{def}}{=} \mathbb{Z}$, $+^I$, $<^I$ et $=^I$ sont l'addition, l'ordre et l'égalité usuels sur les entiers relatifs, et $r^I : \mathbb{Z}^2 \to \mathbb{Z}$ est une fonction binaire – il y a autant d'interprétations dans $\mathcal{K}$ que de telles fonctions r^I.

Quelques définitions sur $(\mathbb{Z}, +, <)$. Commençons par nous placer dans la théorie $\mathrm{Th}(\mathbb{Z}, +, <)$. On peut y définir les formules suivantes pour manipuler des constantes de $\mathbb{Z}$:

$$\begin{aligned}
\mathit{zero}(x) &\stackrel{\text{def}}{=} x + x = x\\
x \leq y &\stackrel{\text{def}}{=} x < y \lor x = y\\
\mathit{un}(x) &\stackrel{\text{def}}{=} \exists z.\mathit{zero}(z) \land z < x \land \forall y.z < y \Rightarrow x \leq y\\
\mathit{deux}(x) &\stackrel{\text{def}}{=} \exists y.\mathit{un}(y) \land x = y + y\\
\mathit{trois}(x) &\stackrel{\text{def}}{=} \exists y.\mathit{un}(y) \land x = y + y + y\\
&\vdots
\end{aligned}$$

Les formules précédentes peuvent être utilisées dans vos réponses aux questions ci-dessous. Aussi, si vous ne trouvez pas comment définir la formule d'une question, cela ne vous empêche pas de l'utiliser dans les questions suivantes.

1. On souhaite représenter la condition de notre boucle `while` dans la théorie $\mathrm{Th}(\mathbb{Z}, +, <)$. Définir une formule $\mathit{condition}(x_1, x_2)$ avec deux variables libres x_1 et x_2 telle que $(\mathbb{Z}, +, <), \rho \models \mathit{condition}(x_1, x_2)$ ssi $\rho(x_2) - \rho(x_1) \leq 0$ et $\rho(x_1) + \rho(x_2) \geq 1$.
   Attention : on ne dispose pas d'un symbole de soustraction dans $\mathrm{Th}(\mathbb{Z}, +, <)$.
2. On souhaite représenter l'effet d'une itération de notre boucle `while` dans la théorie $\mathrm{Th}(\mathbb{Z}, +, <)$. Définir une formule $\mathit{effet}(x_1, x_2, y_1, y_2)$ avec quatre variables libres x_1, x_2, y_1 et y_2 telle que $(\mathbb{Z}, +, <), \rho \models \mathit{effet}(x_1, x_2, y_1, y_2)$ ssi $\rho(y_1) = \rho(x_1)$ et $\rho(y_2) = \rho(x_2) - 2 \cdot \rho(x_1) + 1$.
   Attention : on ne dispose pas d'un symbole de multiplication dans $\mathrm{Th}(\mathbb{Z}, +, <)$.

Synthèse de fonction de rang. Passons maintenant dans la théorie $\mathrm{Th}(\mathcal{K})$. Nous allons écrire une formule close $\varphi_1 \overset{\text{def}}{=} \varphi_{1,a} \land \varphi_{1,b}$ telle qu'il existe $I \in \mathcal{K}$ avec $I \vDash \varphi_1$ si et seulement s'il existe une *fonction de rang* pour notre programme Java, qui est une interprétation $r^I : \mathbb{Z}^2 \to \mathbb{Z}$ du symbole r qui satisfait les deux conditions suivantes :

(a) si la condition de la boucle est respectée par deux entiers relatifs n_1 et n_2, alors

$$r^I(n_1, n_2) \geq 0$$

(b) si la condition de la boucle est respectée par deux entiers relatifs n_1 et n_2 et si n_1' et n_2' sont leurs nouvelles valeurs après un passage dans la boucle, alors

$$r^I(n_1, n_2) > r^I(n_1', n_2')\ .$$

On va utiliser dans la suite les formules *condition*(x_1, x_2) et *effet*(x_1, x_2, y_1, y_2).

3. Donner une formule close $\varphi_{1,a}$ telle que $(\mathbb{Z}, +, r^I, <) \vDash \varphi_{1,a}$ ssi r^I satisfait la condition (a) ci-dessus.
4. Donner une formule close $\varphi_{1,b}$ telle que $(\mathbb{Z}, +, r^I, <) \vDash \varphi_{1,b}$ ssi r^I satisfait la condition (b) ci-dessus.
5. Montrer que la fonction $r^I : \mathbb{Z}^2 \to \mathbb{Z}$ définie par $r^I(n_1, n_2) \overset{\text{def}}{=} n_1 + n_2$ est une fonction de rang pour notre programme.

Exercice 2. Séquences sur l'alphabet $\{A, B\}$ (Examen 2022)

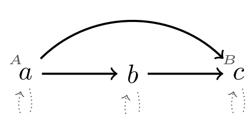
On se place dans cet exercice sur la signature $L \overset{\text{def}}{=} (\emptyset, \{<^{(2)}, =^{(2)}, A^{(1)}, B^{(1)}\})$ et dans la théorie axiomatique $\mathrm{Th}(S)$ définie par les axiomes suivants :

(irréflexivité de $<$)	$\forall x.$	$\neg(x < x)$
(transitivité de $<$)	$\forall x \forall y \forall z.$	$(x < y \land y < z) \Rightarrow x < z$
(totalité de $<$)	$\forall x \forall y.$	$x < y \lor x = y \lor y < x$
(partition A, B)	$\forall x.$	$A(x) \Leftrightarrow \neg B(x)$
(réflexivité de $=$)	$\forall x.$	$x = x$
(symétrie de $=$)	$\forall x \forall y.$	$x = y \Rightarrow y = x$
(transitivité de $=$)	$\forall x \forall y \forall z.$	$(x = y \land y = z) \Rightarrow x = z$
($<$-congruence)	$\forall x_1 \forall x_2 \forall y_1 \forall y_2.$	$(x_1 = y_1 \land x_2 = y_2) \Rightarrow (x_1 < x_2 \Rightarrow y_1 < y_2)$
(A-congruence)	$\forall x_1 \forall y_1.$	$(x_1 = y_1) \Rightarrow (A(x_1) \Rightarrow A(y_1))$
(B-congruence)	$\forall x_1 \forall y_1.$	$(x_1 = y_1) \Rightarrow (B(x_1) \Rightarrow B(y_1))$

Les six dernières formules de cette axiomatisation sont celles de l'axiomatisation $A_{\text{cgr}}(L)$.

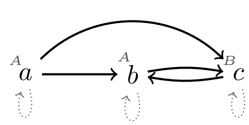
1. Pour chacune des interprétations suivantes, où les sommets représentent les éléments du domaine d'interprétation, les arcs pointillés représentent $=^I$, les arcs pleins représentent $<^I$, et les étiquettes A et B indiquent si l'élément du domaine est dans A^I ou B^I, dire si elle est un modèle de $\mathrm{Th}(S)$, et dans le cas contraire, montrer qu'au moins un axiome n'est pas satisfait.

(a)



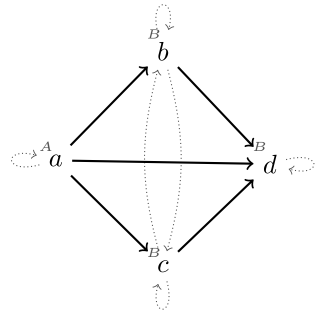
$D_I \overset{\text{def}}{=} \{a, b, c\}$
$<^I \overset{\text{def}}{=} \{(a, b), (a, c), (b, c)\}$
$=^I \overset{\text{def}}{=} \{(a, a), (b, b), (c, c)\}$
$A^I \overset{\text{def}}{=} \{a\}$
$B^I \overset{\text{def}}{=} \{c\}$

(b)



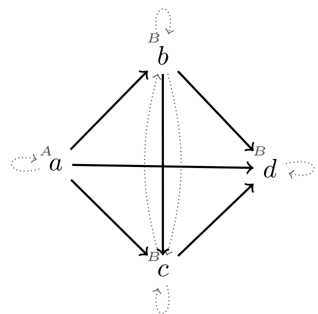
$D_I \overset{\text{def}}{=} \{a, b, c\}$
$<^I \overset{\text{def}}{=} \{(a, b), (a, c), (b, c), (c, b)\}$
$=^I \overset{\text{def}}{=} \{(a, a), (b, b), (c, c)\}$
$A^I \overset{\text{def}}{=} \{a, b\}$
$B^I \overset{\text{def}}{=} \{c\}$

(c)



$D_I \stackrel{\text{def}}{=} \{a,b,c,d\}$
$<^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(a,d),(b,d),(c,d)\}$
$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(b,c),(c,b),(c,c),(d,d)\}$
$A^I \stackrel{\text{def}}{=} \{a\}$
$B^I \stackrel{\text{def}}{=} \{b,c,d\}$

(d)



$D_I \stackrel{\text{def}}{=} \{a,b,c,d\}$
$<^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(a,d),(b,c),(b,d),(c,d)\}$
$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(b,c),(c,b),(c,c),(d,d)\}$
$A^I \stackrel{\text{def}}{=} \{a\}$
$B^I \stackrel{\text{def}}{=} \{b,c,d\}$

2. On s'intéresse à des interprétations qui modélisent des requêtes A et des réponses B au cours du temps. On définit pour cela un nouvel ensemble S' d'axiomes qui contient tous les axiomes de S plus deux nouvelles formules :

($<$ non borné à droite)	$\forall x \exists y.$	$x < y$
(toute requête A reçoit un jour une réponse B)	$\forall x.$	$A(x) \Rightarrow (\exists y. x < y \wedge B(y))$

   Montrer que la formule $\varphi_2 \stackrel{\text{def}}{=} \forall x \exists y. x < y \wedge B(y)$ appartient à la théorie $\mathrm{Th}(S')$.

Exercice 3. Calcul des séquents (Examen 2022)

On se place sur la signature $L \stackrel{\text{def}}{=} (\{a^{(0)}\}, \{R^{(2)}, P^{(1)}\})$ et on définit l'ensemble d'axiomes A contenant les trois formules closes ci-dessous.

$$P(a)$$
$$\forall x. R(a,x)$$
$$\forall x \forall y. \big(R(x,y) \wedge P(x)\big) \Rightarrow P(y)$$

On souhaite montrer à l'aide d'une preuve en calcul des séquents du premier ordre que la formule

$$\psi \stackrel{\text{def}}{=} \forall x. P(x)$$

appartient à la théorie $\mathrm{Th}(A)$.

1. Donner la formule φ_3 qui dépend de A et de ψ, et qui est valide si et seulement si ψ appartient à $\mathrm{Th}(A)$. Justifier.
2. Donner $\mathrm{nnf}(\varphi_3)$ la forme normale négative de φ_3.
3. Donner une dérivation en calcul des séquents du premier ordre de $\mathrm{nnf}(\varphi_3)$, ce qui montrera bien la validité de φ_3 par le théorème de correction.