Devoir Maison 2

Devoir maison à rendre sur la page moodle du cours pour le 20 janvier 2022. Le barème sur 15 points donné dans la marge est indicatif.

Exercice 1. Conjectures en théorie des nombres

Plusieurs conjectures fameuses en mathématiques peuvent assez aisément s'exprimer en logique du premier ordre, et pourraient être données en entrée à un solveur SMT. Nous allons en voir un exemple dans cet exercice.

Signature et théorie. On se place pour sur la signature $L \stackrel{\text{def}}{=} (\{+^2, \times^2\}, \{=^{(2)}\})$ dotée de deux symboles de fonctions binaires pour l'addition et la multiplication ainsi que d'un symbole de relation binaire pour l'égalité. La théorie logique que nous utilisons est l'arithmétique sur les entiers naturels $\mathrm{Th}(\mathbb{N}, +, \times)$. Comme vu dans l'exemple 13.6 des notes de cours, on peut définir de nouvelles formules dans cette théorie qui vont permettre de représenter les constantes telles que 0, 1, 2, ..., l'ordre sur les entiers naturels, et le fait qu'un nombre soit premier :

$$\begin{aligned}
\mathit{zero}(x) &\stackrel{\text{def}}{=} x + x = x \\
\mathit{un}(x) &\stackrel{\text{def}}{=} \neg \mathit{zero}(x) \wedge x \times x = x \\
\mathit{deux}(x) &\stackrel{\text{def}}{=} \exists y.\mathit{un}(y) \wedge x = y + y \\
&\vdots \\
x < y &\stackrel{\text{def}}{=} \exists z.\neg \mathit{zero}(z) \wedge y = x + z \\
\mathit{premier}(x) &\stackrel{\text{def}}{=} \neg \mathit{zero}(x) \wedge \neg(\exists y \exists z.x = y \times z \wedge \neg \mathit{un}(y) \wedge \neg \mathit{un}(z))
\end{aligned}$$

Les formules ci-dessus 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.

Préliminaires. Pour x, y deux entiers naturels dans $\mathbb{N}$, on va noter

$$\mathrm{Premiers}(x, y) \stackrel{\text{def}}{=} \{p \text{ premier} \mid x < p \leq y\}$$

pour l'ensemble des nombres premiers strictement compris entre x et $y + 1$. On peut représenter cet ensemble en logique du premier ordre dans la théorie $\mathrm{Th}(\mathbb{N}, +, \times)$, comme le montre la question ci-dessous.

[0,5] 1. Définir une formule $\mathit{entre}(p, x, y)$ avec trois variables libres p, x, y telle que $(\mathbb{N}, +, \times), \rho \vDash \mathit{entre}(p, x, y)$ ssi $\rho(p)$ appartient à l'ensemble $\mathrm{Premier}(\rho(x), \rho(y))$, c'est-à-dire ssi $\rho(p)$ est un nombre premier strictement compris entre $\rho(x)$ et $\rho(y) + 1$.

Seconde conjecture de Hardy-Littlewood. On définit aussi

$$\pi(x, y) \stackrel{\text{def}}{=} |\mathrm{Premiers}(x, y)|$$

comme le nombre de nombres premiers strictement compris entre x et $y + 1$. La *seconde conjecture de Hardy-Littlewood* dit que pour tous nombres entiers x et y tous deux strictement supérieurs à un, $\pi(x, x+y) \leq \pi(0, y)$, autrement dit qu'il n'y a pas plus de nombres premiers entre x et $x + y + 1$ qu'entre 0 et $y + 1$. On va chercher à exprimer le fait que cette conjecture est *fausse* comme un problème de satisfiabilité modulo théorie.

Un obstacle pour cela est que la logique du premier ordre ne permet pas de « compter » les éléments de l'ensemble $\mathrm{Premier}(x, y)$ et de représenter directement $\pi(x, y)$. On peut s'en sortir en étendant notre signature L avec

un nouveau symbole de fonction « non-interprété » $f^{(1)}$ unaire. On travaille pour cela dans la théorie $T \stackrel{\text{def}}{=} \text{Th}(\mathcal{K})$ où $\mathcal{K}$ est l'ensemble des interprétations de la forme $I = (\mathbb{N}, +, \times, f^I)$ où $D_I \stackrel{\text{def}}{=} \mathbb{N}$, $+^I$, $\times^I$ et $=^I$ sont l'addition, la multiplication et l'égalité usuelles sur les entiers naturels, et f^I est de type $\mathbb{N} \to \mathbb{N}$; il y a donc autant d'interprétations dans $\mathcal{K}$ que de fonctions de type $\mathbb{N} \to \mathbb{N}$.

L'idée dans les questions ci-dessous va être de mettre des conditions sur l'interprétation f^I de ce symbole de fonction :
- quand on se restreint au sous-domaine Premiers$(0, y)$, on veut que f^I soit injective à image dans l'ensemble Premiers$(x, x + y)$, ce qui imposera que $\pi(0, y) \leq \pi(x, x + y)$,
- de plus, on veut qu'il existe un nombre premier dans Premiers$(x, x + y)$ qui ne soit l'image d'aucun élément de Premiers$(0, y)$, et on aura donc $\pi(0, y) < \pi(x, x + y)$.

[1] 2. Définir une formule *image*(x, y) telle que $(\mathbb{N}, +, \times, f^I), \rho \vDash$ *image*(x, y) ssi, pour tout $p \in$ Premiers$(0, \rho(y))$, $f^I(p) \in$ Premiers$(\rho(x), \rho(x) + \rho(y))$.

[1] 3. Définir une formule *injective*(x, y) telle que $(\mathbb{N}, +, \times, f^I), \rho \vDash$ *injective*(x, y) ssi, pour tous nombres $p_1, p_2 \in$ Premiers$(0, \rho(y))$, si $f^I(p_1) = f^I(p_2)$ alors $p_1 = p_2$.

[1] 4. Définir une formule *nonimage*(x, y) telle que $(\mathbb{N}, +, \times, f^I), \rho \vDash$ *nonimage*(x, y) ssi il existe un nombre dans Premiers$(\rho(x), \rho(x) + \rho(y))$ qui n'est pas l'image par f^I d'un nombre de Premiers$(0, \rho(y))$.

[1] 5. En déduire une formule close φ_1 telle qu'il existe une interprétation $I = (\mathbb{N}, +, \times, f^I)$ dans $\mathcal{K}$ avec $I \vDash \varphi$ ssi la seconde conjecture de Hardy-Littlewood est fausse.

Exercice 2. Graphes non orientés bipartis

On se place dans cet exercice sur la signature $L_G \stackrel{\text{def}}{=} (\emptyset, \{E^{(2)}, =^{(2)}\})$ et on commence par considérer l'ensemble A_G d'axiomes suivant :

(irréflexivité de E)	$\forall x.$	$\neg E(x, x)$
(symétrie de E)	$\forall x \forall y.$	$E(x, y) \Rightarrow E(y, x)$
(réflexivité de $=$)	$\forall x.$	$x = x$
(symétrie de $=$)	$\forall x \forall y.$	$x = y \Rightarrow y = x$
(transitivité de $=$)	$\forall x \forall y \forall z.$	$(x = y \wedge y = z) \Rightarrow x = z$
(E-congruence)	$\forall x_1 \forall x_2 \forall y_1 \forall y_2.$	$(x_1 = y_1 \wedge x_2 = y_2) \Rightarrow (E(x_1, x_2) \Rightarrow E(y_1, y_2))$

Les deux premiers axiomes imposent que l'interprétation du symbole E sera bien l'ensemble des arêtes d'un graphe non-orienté (par symétrie) simple (par irréflexivité). Les quatre derniers axiomes sont ceux de l'axiomatisation $A_{\text{cgr}}(L_G)$ définie dans l'exemple 15.3 des notes de cours. On ajoute ensuite à A_G une infinité d'axiomes pour interdire les cycles de longueur impaire : pour tout $n \in \mathbb{N}$ avec $n > 0$, l'axiome suivant est ajouté :

(C_{2n+1} exclu)
$$\neg \exists x_0 \exists y_0 \exists x_1 \exists y_1 \cdots \exists x_{2n} \exists y_{2n}. \qquad \bigwedge_{0 \leq i \leq 2n} (x_i = y_i \wedge E(y_i, x_{(i+1) \bmod 2n}))$$

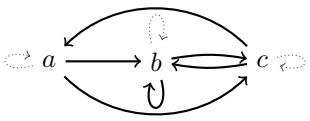
par exemple, pour le cas $n = 1$, cela donne l'axiome

(C_3 exclu) $\neg \exists x_0 \exists y_0 \exists x_1 \exists y_1 \exists x_2 \exists y_2.$ $x_0 = y_0 \wedge E(y_0, x_1) \wedge x_1 = y_1 \wedge E(y_1, x_2) \wedge x_2 = y_2 \wedge E(y_2, x_0)$

On note A_B cette nouvelle axiomatisation ; Th(A_B) est la théorie des graphes non-orientés sans cycles de longueur impaire.

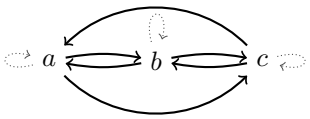
[4] 1. Pour chacune des interprétations suivantes, où les sommets représentent les éléments du domaine d'interprétation, les arcs pointillés représentent $=^I$ et les arcs pleins représentent E^I, dire si elle est un modèle de Th(A_B), et dans le cas contraire, montrer qu'au moins un axiome n'est pas satisfait.

(a)



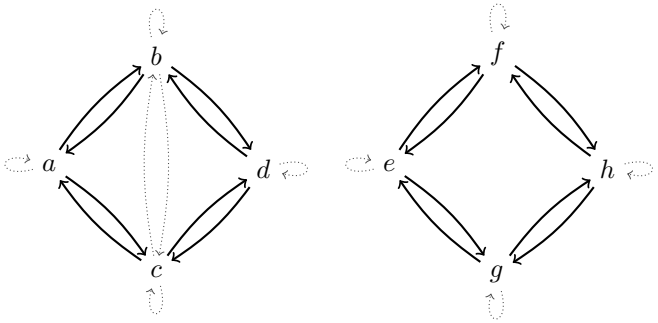
$D_I \stackrel{\text{def}}{=} \{a, b, c\}$
$E^I \stackrel{\text{def}}{=} \{(a, b), (a, c), (b, b), (b, c), (c, a), (c, b)\}$
$=^I \stackrel{\text{def}}{=} \{(a, a), (b, b), (c, c)\}$

(b)



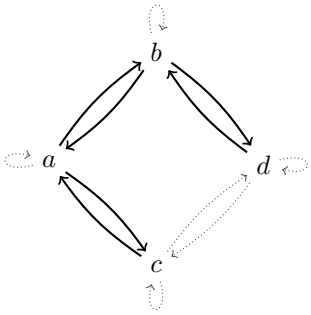
$D_I \stackrel{\text{def}}{=} \{a, b, c\}$
$E^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(b,a),(b,c),(c,a),(c,b)\}$
$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(c,c)\}$

(c)



$D_I \stackrel{\text{def}}{=} \{a, b, c, d, e, f, g, h\}$
$E^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(b,a),(b,d),(c,a),(c,d),$
$(d,b),(d,c),(e,f),(e,g),(f,e),(f,h)\}$
$(g,e),(g,h),(h,f),(h,g)\}$
$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(b,c),(c,b),(c,c),(d,d),$
$(e,e),(f,f),(g,g),(h,h)\}$

(d)



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

[1] 2. Montrer que la formule suivante appartient à $\mathrm{Th}(A_B)$:

$$\forall x \forall y \forall z. \Big(\big(E(x,y) \wedge E(y,z)\big) \Rightarrow \neg E(x,z) \Big).$$

Exercice 3. Calcul des séquents

On se place sur la signature $L \stackrel{\text{def}}{=} (\{f^{(1)}, a^{(0)}\}, \{P^{(1)}\})$. On travaille dans la théorie axiomatique $\mathrm{Th}(A)$ définie par deux axiomes :

$$A \stackrel{\text{def}}{=} \{\forall x. \big(P(x) \Rightarrow P(f(x))\big)\ ,\ P(a)\}\ .$$

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

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

appartient à $\mathrm{Th}(A)$. On suit pour cela une approche assez similaire à celle de l'exemple 17.4 des notes de cours.

[1,5] 1. Donner une formule φ_3 qui est valide si et seulement si la formule ψ appartient à $\mathrm{Th}(A)$; expliquer votre raisonnement.

[1] 2. Donner $\mathrm{nnf}(\varphi_3)$ la forme normale négative de φ_3.

[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.