Université Paris Cité

VÉRIFICATION DES APTITUDES ET DES CONNAISSANCES

▼

DATE : 8 janvier 2024

UE : Logique (L3 informatique)

Après avoir rempli l'en-tête, rabattre et coller le coin noirci

Nom : ....

Prénom : ....

N° d'étudiant·e : ....

Examen

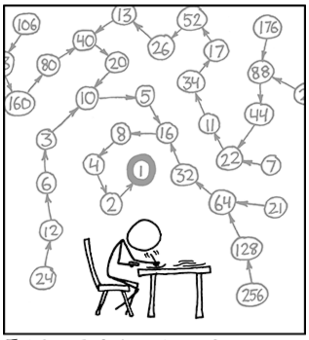
Durée : 2h15. Tous documents papier autorisés ; appareils électroniques (y compris téléphones portables) interdits.

Répondre dans les espaces prévus, ou au besoin en page 8. Le barème sur 20 points donné en marge est indicatif.

Exercice 1. Conjecture de Collatz

Considérons la méthode Java ci-dessous :

```java
public static int collatz (int n) {
    assert (n > 0);
    if (n % 2 == 0)
        return collatz (n / 2);
    else
        return collatz (3 * n + 1);
}
```



THE COLLATZ CONJECTURE STATES THAT IF YOU PICK A NUMBER, AND IF IT'S EVEN DIVIDE IT BY TWO AND IF IT'S ODD MULTIPLY IT BY THREE AND ADD ONE, AND YOU REPEAT THIS PROCEDURE LONG ENOUGH, EVENTUALLY YOUR FRIENDS WILL STOP CALLING TO SEE IF YOU WANT TO HANG OUT.

Source : xkcd, sous licence CC-BY-NC

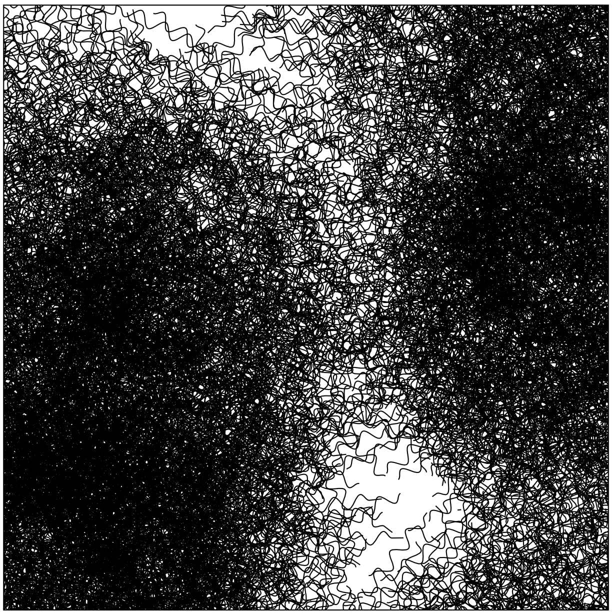
Cette méthode récursive prend en entrée un entier naturel $n > 0$ passé en argument, puis s'appelle récursivement sur $n/2$ si n est pair et sur $3n+1$ si n est impair. Par la suite, on notera « $n \to n'$ » comme dans l'illustration ci-contre quand n' est la valeur passée en argument de l'appel récursif, c'est-à-dire quand $n' = n/2$ si n est pair et $n' = 3n+1$ si n est impair.

La *conjecture de Collatz* énonce que, quelle que soit la valeur $n \in \mathbb{N}$ strictement positive passée en argument initial, cette méthode finit par boucler sur le cycle $1 \to 4 \to 2 \to 1$. Cette conjecture a maintenant un siècle et on ne sait toujours pas la démontrer ni l'infirmer. Le but de l'exercice est de déterminer s'il existe un autre cycle possible (ce qui impliquerait que la conjecture est fausse), en modélisant la question comme un problème de satisfiabilité modulo théorie d'une formule du premier ordre.

Signature et théorie. On se place pour cela sur la signature $L \stackrel{\text{def}}{=} (\{+^2\}, \{C^{(1)}, =^{(2)}\})$ dotée d'un symbole de fonction binaire pour l'addition, d'un symbole de relation binaire pour l'égalité, et d'un symbole de relation unaire C. La théorie logique que nous utilisons est l'arithmétique de Presburger $\mathrm{Th}(\mathbb{N}, +)$ étendue par le symbole non-interprété C. Autrement dit, notre théorie est $T \stackrel{\text{def}}{=} \mathrm{Th}(\mathcal{K})$ où $\mathcal{K}$ est l'ensemble des interprétations normales de la forme $I = (\mathbb{N}, +, C^I)$, où $D_I \stackrel{\text{def}}{=} \mathbb{N}$, $+^I$ et $=^I$ sont l'addition et l'égalité usuelles sur les entiers naturels, et $C^I \subseteq \mathbb{N}$ dénote un sous-ensemble des entiers naturels – il y a autant d'interprétations dans $\mathcal{K}$ que de sous-ensembles $C^I \subseteq \mathbb{N}$.

Quelques définitions sur $(\mathbb{N}, +)$. Commençons par nous placer dans la théorie $\mathrm{Th}(\mathbb{N}, +)$. On peut y définir les formules suivantes pour manipuler des constantes de $\mathbb{N}$ et utiliser l'ordre (l'exemple 13.6 des notes

▲
Ne rien inscrire ici



NE RIEN ÉCRIRE ICI

de cours donne des définitions similaires, mais sur $(\mathbb{N}, +, \times)$, alors qu'ici nous n'avons pas le symbole de multiplication $\times^{(2)}$) :

$$
\begin{aligned}
\textit{zero}(x) &\stackrel{\text{def}}{=} x + x = x \\
x < y &\stackrel{\text{def}}{=} \exists z. \neg \textit{zero}(z) \wedge y = x + z \\
\textit{un}(x) &\stackrel{\text{def}}{=} \exists z. \textit{zero}(z) \wedge z < x \wedge \forall y. z < y \Rightarrow (x = y \vee x < y) \\
\textit{deux}(x) &\stackrel{\text{def}}{=} \exists y. \textit{un}(y) \wedge x = y + y \\
\textit{trois}(x) &\stackrel{\text{def}}{=} \exists y. \textit{un}(y) \wedge x = y + y + y \\
&\vdots
\end{aligned}
$$

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. Attention : notre signature ne contient pas de symbole pour les constantes comme 1, ni de symbole pour la multiplication.

[0,5] 1. Définir une formule *double*(x, y) avec deux variables libres x et y, telle que $(\mathbb{N}, +), \rho \vDash \textit{double}(x, y)$ ssi $\rho(x) = 2 \cdot \rho(y)$.

[0,75] 2. Définir une formule *impair*(x) avec une variable libre x, telle que $(\mathbb{N}, +), \rho \vDash \textit{impair}(x)$ ssi $\rho(x)$ est impair.

[0,75] 3. Définir une formule *3foisplus1*(x, y) avec deux variables libres x et y, telle que $(\mathbb{N}, +), \rho \vDash \textit{3foisplus1}(x, y)$ ssi $\rho(x)$ est impair et $\rho(y) = 3 \cdot \rho(x) + 1$.

[0,5] 4. En déduire une formule *successeur*(x, y) avec deux variables libres x et y, telle que $(\mathbb{N}, +), \rho \vDash$ *successeur*(x, y) ssi $\rho(x) \to \rho(y)$.

Recherche de multi-cycle fini. Passons maintenant dans la théorie $\mathrm{Th}(\mathcal{K})$. Nous allons écrire une formule close φ_1 telle qu'il existe $I \in \mathcal{K}$ avec $I \vDash \varphi_1$ si et seulement s'il existe (au moins) un cycle autre que $1 \to 4 \to 2 \to 1$. L'idée est que dans ce cas l'ensemble C^I va contenir des entiers n qui apparaissent dans un ou plusieurs cycles disjoints ; on parle alors de *multi-cycle* fini.

Cet exercice ressemble à l'exemple de modélisation de la section 16.4 des notes de cours, mais attention : on travaille ici sur une signature plus restreinte, dans laquelle les formules données au début de l'énoncé comme *zero* ou *un*, ainsi que la formule *successeur* de la question 4, vont servir.

Notre formule va être $\varphi_1 \overset{\text{def}}{=} \varphi_{1,5} \wedge \varphi_{1,6} \wedge \varphi_{1,7} \wedge \varphi_{1,8} \wedge \varphi_{1,9}$ la conjonction des formules closes à définir ci-dessous.

[0,75] 5. Commençons par interdire zéro et éviter le cycle $1 \to 4 \to 2 \to 1$. Donner une formule close $\varphi_{1,5}$ telle que $(\mathbb{N}, +, C^I) \vDash \varphi_{1,5}$ ssi l'ensemble C^I ne contient que des entiers différents de 0 et de 1.

[0,75] 6. Pour que l'ensemble C^I soit un multi-cycle, il faut que si $n \in C^I$ et $n \to n'$, alors $n' \in C^I$. Donner une formule close $\varphi_{1,6}$ telle que $(\mathbb{N}, +, C^I) \vDash \varphi_{1,6}$ ssi cette condition est remplie.

[2] 7. Inversement, pour que l'ensemble C^I soit un multi-cycle, il faut que si $n' \in C^I$, alors il y ait *exactement* un $n \in C^I$ tel que $n \to n'$. Le mot « exactement » est important : par exemple, on a $5 \to 16$ et $32 \to 16$, mais si $16 \in C^I$ alors on doit avoir soit $5 \in C^I$ soit $32 \in C^I$ mais pas les deux. Donner une formule close $\varphi_{1,7}$ telle que $(\mathbb{N}, +, C^I) \vDash \varphi_{1,7}$ ssi cette condition est remplie.

[0,5] 8. Donner une formule close $\varphi_{1,8}$ telle que $(\mathbb{N}, +, C^I) \vDash \varphi_{1,8}$ ssi C^I n'est pas l'ensemble vide.

[1,5] 9. Enfin, donner une formule close $\varphi_{1,9}$ telle que $(\mathbb{N}, +, C^I) \models \varphi_{1,9}$ ssi C^I est un ensemble fini d'entiers naturels. Justifier votre raisonnement.

Exercice 2. Graphes bicoloriés

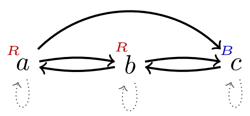
On se place dans cet exercice sur la signature $L \stackrel{\text{def}}{=} (\emptyset, \{E^{(2)}, =^{(2)}, R^{(1)}, B^{(1)}\})$ et dans la théorie axiomatique $\mathrm{Th}(S)$ définie par les axiomes suivants :

(irréflexivité de E)	$\forall x.$	$\neg E(x, x)$
(symétrie de E)	$\forall x \forall y.$	$E(x, y) \Rightarrow E(y, x)$
(partition des sommets)	$\forall x.$	$R(x) \Leftrightarrow \neg B(x)$
(2-coloriage)	$\forall x \forall y.$	$E(x, y) \Rightarrow (\neg R(x) \vee \neg R(y)))$
(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)	$\forall x_1 \forall x_2 \forall y_1 \forall y_2.$	$(x_1 = y_1 \wedge x_2 = y_2) \Rightarrow \big(E(x_1, x_2) \Rightarrow E(y_1, y_2)\big)$
(R-congruence)	$\forall x_1 \forall y_1.$	$(x_1 = y_1) \Rightarrow (R(x_1) \Rightarrow R(y_1))$
(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 $A_{\text{cgr}}(L)$.

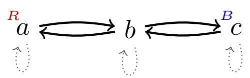
[3] 1. Pour chacune des interprétations suivantes (où les sommets représentent les éléments du domaine d'interprétation, les arcs pointillés représentent $=^I$, les arcs pleins représentent E^I, et les étiquettes R et B indiquent si l'élément du domaine est dans R^I ou B^I), dire si elle est un modèle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

(a)



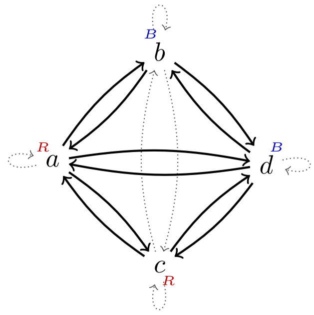
$D_I \stackrel{\text{def}}{=} \{a, b, c\}$
$E^I \stackrel{\text{def}}{=} \{(a, b), (a, c), (b, a), (b, c), (c, b)\}$
$=^I \stackrel{\text{def}}{=} \{(a, a), (b, b), (c, c)\}$
$R^I \stackrel{\text{def}}{=} \{a, b\}$
$B^I \stackrel{\text{def}}{=} \{c\}$

(b)



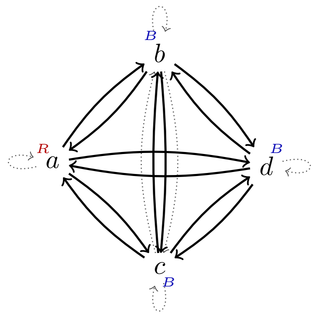
$D_I \stackrel{\text{def}}{=} \{a, b, c\}$
$E^I \stackrel{\text{def}}{=} \{(a, b), (b, a), (b, c), (c, b)\}$
$=^I \stackrel{\text{def}}{=} \{(a, a), (b, b), (c, c)\}$
$R^I \stackrel{\text{def}}{=} \{a\}$
$B^I \stackrel{\text{def}}{=} \{c\}$

(c)



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

(d)



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

[2,5] 2. Montrer que l'axiome de B-congruence se déduit des autres axiomes. Autrement dit, montrer que la formule $\forall x_1 \forall y_1.(x_1 = y_1) \Rightarrow (B(x_1) \Rightarrow B(y_1))$ appartient à la théorie $\text{Th}(S')$ où S' est l'ensemble des 9 premiers axiomes listés au début de l'exercice.

Exercice 3. Calcul des séquents

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

$$\forall x. R(x, x)$$
$$\big(\forall x. R(g(a), g(x)) \Rightarrow (\exists y. R(x, g(y)))\big)$$

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

$$\psi \stackrel{\text{def}}{=} \exists x. R(a, g(x))$$

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

[1,5] 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.

[1,5] 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 nnf(φ_3), ce qui montrera bien la validité de φ_3 par le théorème de correction.