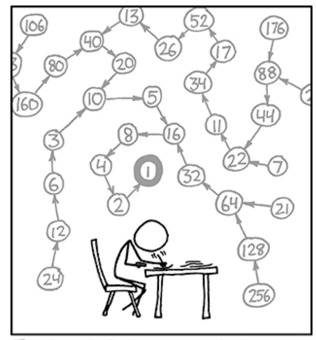
Devoir Maison 2

Devoir maison à rendre sur la page moodle du cours pour le 11 janvier 2021. Le barème sur 15 points donné dans la marge est indicatif.

Exercice 1. Conjecture de Collatz

Considérons le programme Java ci-dessous :

```java
public static void main(String[] args) {
    int n = Integer.parseInt(args[0]);
    assert (n > 0);
    while (n != 1)
        if (n % 2 == 0)
            n = n / 2;
        else
            n = 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

Ce programme prend en entrée un entier n strictement positif passé en argument de la ligne de commande, puis boucle tant que n n'a pas atteint la valeur 1 en effectuant la mise à jour suivante : soit n est pair, et on le divise par deux, soit il est impair, et on le multiplie par trois et on ajoute un.

La *conjecture de Collatz* énonce que ce programme termine pour toute valeur $n \in \mathbb{N}$ strictement positive passée en argument. Cette conjecture a maintenant un siècle et on ne sait toujours pas la démontrer ni l'infirmer. Le but de l'exercice est de modéliser cette conjecture 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 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 de cours donne des définitions similaires, mais sur $(\mathbb{N},+,\times)$, alors qu'ici nous n'avons pas le symbole de multiplication $\times^{(2)}$) :

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

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.

[0,5] 1. Définir une formule *divise2*(x, y) telle que $(\mathbb{N}, +), \rho \models$ *divise2*(x, y) ssi $\rho(x) = 2 \cdot \rho(y)$.

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

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

[0,25] 4. En déduire une formule *collatz*(x, y) telle que $(\mathbb{N}, +), \rho \models$ *collatz*(x, y) ssi soit $\rho(x)$ est pair et alors $\rho(x) = 2 \cdot \rho(y)$, soit $\rho(x)$ est impair et alors $\rho(y) = 3 \cdot \rho(x) + 1$.

Recherche de contre-exemple à la conjecture de Collatz. Passons maintenant dans la théorie Th$(\mathcal{K})$. Nous allons écrire une formule close φ_1 telle qu'il existe $I \in \mathcal{K}$ avec $I \models \varphi_1$ si et seulement si la conjecture de Collatz est *fausse*, c'est-à-dire si et seulement s'il existe au moins un entier $n > 0$ tel que le programme Java ne termine pas. L'idée est que C^I va contenir uniquement des entiers n qui sont de tels contre-exemples.

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* vont servir.

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

[1] 5. Donner une formule close $\varphi_{1,5}$ telle que $(\mathbb{N}, +, C^I) \models \varphi_{1,5}$ ssi C^I ne contient que des entiers strictement positifs.

[0,75] 6. Donner une formule close $\varphi_{1,6}$ telle que $(\mathbb{N}, +, C^I) \models \varphi_{1,6}$ ssi C^I ne contient pas l'entier 1.

[1] 7. Donner une formule close $\varphi_{1,7}$ telle que $(\mathbb{N}, +, C^I) \models \varphi_{1,7}$ ssi, pour tout $n \in C^I$, on a aussi $n' \in C^I$ où $n' = n/2$ si n est pair et $n' = 3n + 1$ si n est impair (votre formule devrait utiliser la formule *collatz* de la question 4).

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

[2 (bonus)] 9. Montrer que, si $(\mathbb{N}, +, C^I) \models \varphi_{1,6} \wedge \varphi_{1,7}$ et $n > 0$ est tel que le programme Java termine quand n est passé en argument, alors $n \notin C^I$.

Remarque : on pourrait (mais ça n'est pas demandé) écrire un fichier SMT-LIB qui correspond à la formule φ_1. N'espérez pas cependant résoudre la conjecture de Collatz comme cela : les solveurs SMT actuels n'arrivent pas à répondre à une telle formule.

Exercice 2. Graphes non orientés 2-réguliers

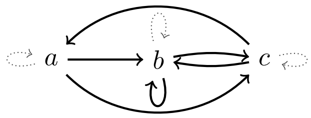
On se place dans cet exercice sur la signature $L_G \stackrel{\text{def}}{=} (\emptyset, \{E^{(2)}, =^{(2)}\})$ et dans la théorie axiomatique Th(A_G) définie par les axiomes suivants :

(irréflexivité de E)	$\forall x.$	$\neg E(x, x)$
(symétrie de E)	$\forall x \forall y.$	$E(x, y) \Rightarrow E(y, x)$
(2-régularité)	$\forall x \exists y_1 \exists y_2.$	$E(x, y_1) \wedge E(x, y_2) \wedge \neg(y_1 = y_2) \wedge \forall z. E(x, z) \Rightarrow (z = y_1 \vee z = y_2)$
(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)	$\forall x_1 \forall x_2 \forall y_1 \forall y_2.$	$(x_1 = y_1 \wedge x_2 = y_2) \Rightarrow (E(x_1, x_2) \Rightarrow E(y_1, y_2))$

Ces quatre derniers axiomes sont ceux de l'axiomatisation $A_{\text{cgr}}(L_G)$ définie dans l'exemple 15.3 des notes de cours.

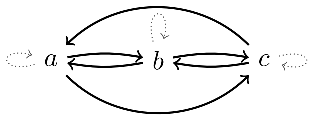
[2] 1. Pour chacune des interprétations suivantes, où les sommets représentent les éléments du domaine d'interprétation, les arcs pointillés représentent $=^I$ et les arcs pleins représentent E^I, dire si elle est un modèle de Th(A_G), et dans le cas contraire, montrer qu'au moins un axiome n'est pas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

(a)



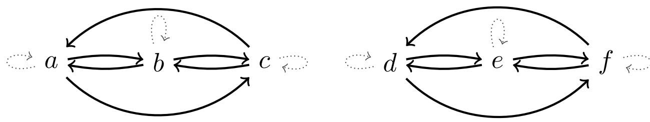
$$D_I \stackrel{\text{def}}{=} \{a,b,c\}$$
$$E^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(b,b),(b,c),(c,a),(c,b)\}$$
$$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(c,c)\}$$

(b)



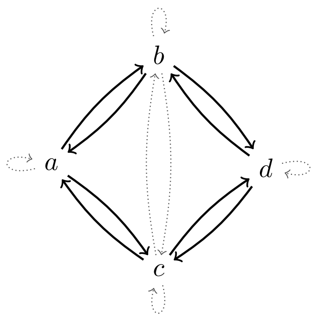
$$D_I \stackrel{\text{def}}{=} \{a,b,c\}$$
$$E^I \stackrel{\text{def}}{=} \{(a,b),(a,c),(b,a),(b,c),(c,a),(c,b)\}$$
$$=^I \stackrel{\text{def}}{=} \{(a,a),(b,b),(c,c)\}$$

(c)



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

(d)



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

[1,5] 2. Montrer que la formule suivante appartient à $\mathrm{Th}(A_G)$:

(2-régularité') $$\forall x \exists y_1 \exists y_2 . E(y_1,x) \land E(x,y_2) \land \neg(y_1 = y_2) \land \forall z . E(x,z) \Rightarrow (z = y_1 \lor z = y_2) \ .$$

[1,5] 3. Donner une interprétation normale de domaine infini qui est un modèle de $\mathrm{Th}(A_G)$.

Exercice 3. Calcul des séquents

On se place sur la signature $L \stackrel{\text{def}}{=} (\{f^{(1)}, g^{(1)}\}, \{P^{(1)}\})$. On travaille dans la théorie axiomatique $\mathrm{Th}(A)$ où A ne contient qu'un unique axiome

$$\forall x . P(f(g(x))) \Rightarrow P(f(x)) \ .$$

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

$$\big(\forall x . P(f(g(g(x))))\big) \Rightarrow \big(\forall x . P(f(x))\big)$$

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

[1,25] 1. Donner une formule φ_3 qui est valide si et seulement si la formule $\big(\forall x . P(f(g(g(x))))\big) \Rightarrow \big(\forall x . P(f(x))\big)$ appartient à $\mathrm{Th}(A)$.

[0,75] 2. Donner $\mathrm{nnf}(\varphi_3)$ la forme normale négative de φ_3.

[2,5] 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.