TD blabla, preuves par induction

1 Clôtures transitives et correspondance petits/grands pas

On considère des *expressions arithmétiques simples*, notées $a, a_1, \ldots$, et définies inductivement par la grammaire suivante (on se donne l'ensemble $\mathbb{Z}$ des entiers relatifs, notés k):

$$a \quad ::= \quad k \;\Big|\; a_1 + a_2 \;.$$

1. Proposez une définition pour la sémantique opérationnelle à grands pas pour les expressions arithmétiques.

2. On considère la sémantique opérationnelle à petits pas pour les expressions arithmétiques simples, notée $a \to a'$, et définie par les règles d'inférence suivantes:

   $$\frac{a_1 \to a_1'}{a_1 + a_2 \to a_1' + a_2} \qquad \frac{a_2 \to a_2'}{a_1 + a_2 \to a_1 + a_2'} \qquad \frac{}{k_1 + k_2 \to k}\; k = k_1 + k_2$$

   La relation $\to$ est-elle déterministe? Justifiez votre réponse.

3. Énoncez la correspondance entre sémantiques à grands et petits pas pour les expressions arithmétiques simples.

4. On considère les trois définitions suivantes pour la clôture réflexive et transitive de $\to$ (formellement, on fait trois définitions inductives de prédicats binaires sur E):

   Relation $\hookrightarrow$

   $$\frac{}{a \hookrightarrow a} \qquad \frac{a \to b \qquad b \hookrightarrow c}{a \hookrightarrow c}$$

   Relation $\twoheadrightarrow$

   $$\frac{}{a \twoheadrightarrow a} \qquad \frac{a \twoheadrightarrow b \qquad b \to c}{a \twoheadrightarrow c}$$

   Relation $\mapsto$

   $$\frac{}{a \mapsto a} \qquad \frac{a \to b}{a \mapsto b} \qquad \frac{a \mapsto b \qquad b \mapsto c}{a \mapsto c}$$

   Écrivez les preuves de la correspondance pour $\hookrightarrow$, $\twoheadrightarrow$ et $\mapsto$. Il vous est demandé à chaque fois de prouver la correspondance entre grands pas et petits pas, vous n'avez pas le droit de passer par des correspondances entre diverses versions de la clôture réflexive et transitive de $\to$.

   Laquelle des définitions de la clôture transitive est la plus adaptée, et pourquoi?

2 Petits et moyens pas pour les expressions arithmétiques **(partiel de l'an dernier)**

On reprend les notations de la partie précédente (expressions arithmétiques simples, sémantique à petits pas).

On considère, outre $\to$, la relation $\hookrightarrow$, définie *partiellement* par les règles d'inférence

$$\frac{}{k_1 + k_2 \hookrightarrow k}\; k = k_1 + k_2 \qquad \frac{a_1 \hookrightarrow a_1' \qquad a_2 \hookrightarrow a_2'}{a_1 + a_2 \hookrightarrow a_1' + a_2'}$$

1. Ajoutez une ou plusieurs règles d'inférence à celles-ci de façon à ce que $\hookrightarrow$ soit une relation *non réflexive*, *déterministe*, et satisfaisant les deux propriétés suivantes:

$$\forall a, a'.\ a \hookrightarrow a' \quad \Rightarrow \quad a \rightarrow^{+} a' \qquad (1) \quad \text{et}$$

$$\forall a, k.\ a \rightarrow^{*} k \quad \Rightarrow \quad a \hookrightarrow^{*} k \qquad (2)$$

   où l'on utilise la notation * pour représenter la clôture *réflexive et transitive* d'une relation, et la notation $^+$ pour représenter la clôture *transitive* d'une relation. On demande juste la ou les règles d'inférence pour cette question.

2. Démontrez *rigoureusement* que la relation $\hookrightarrow$ que vous avez définie satisfait la propriété (1).

3. Donnez la définition d'une fonction qui renvoie, étant donnée une dérivation δ d'un jugement de la forme $a \hookrightarrow a'$, le nombre d'additions entre entiers effectuées dans δ.

3 IMP parallèle — égalités entre programmes, atomicité (DM de l'an dernier)

On enrichit la grammaire de IMP avec une construction de *composition parallèle*, notée $\|$: à l'image de la composition séquentielle $(c_1; c_2)$, on dira que $c_1 \| c_2$ est une commande si c_1 et c_2 sont des commandes.

La sémantique opérationnelle des commandes héritées de IMP est inchangée par rapport à ce qui a été vu en cours. Le but de cette partie est de se poser des questions sur la sémantique opérationnelle de $c_1 \| c_2$.

Les programmes de IMP parallèle s'exécutent suivant un modèle de *mémoire partagée*: cela signifie que l'exécution des programmes peut être répartie sur plusieurs processeurs, qui ont tous accès à la même mémoire. On fait de plus un choix de modélisation, en décrétant que cet accès ne peut pas être simultané. Nous allons étudier, dans les parties qui suivent, diverses formes d'*atomicité* dans l'exécution des programmes, ce qui correspond à des disciplines différentes pour l'exécution des commandes que l'on lance en parallèle.

3.1 Le cas où $\|$ isole

Dans un premier temps, on s'intéresse à une approche assez élémentaire pour exécuter les programmes de IMP parallèle. Lorsqu'on doit exécuter une commande de la forme $c_1 \| c_2$, on exécute les deux composantes, c_1 et c_2, "en isolation", et successivement. En d'autres termes, tout se passe comme si soit c_1 est lancée en premier, soit c_2 est lancée en premier, l'exécution de l'autre commande démarrant lorsque l'exécution de la première a terminé. Lorsqu'une composante s'exécute, l'autre est bloquée.

Pour représenter cette façon d'exécuter les programmes, on reprend la sémantique opérationnelle à grands pas pour IMP vue en cours, et on ajoute deux règles d'inférence pour exécuter une commande de la forme $c_1 \| c_2$.

1. Donnez ces deux règles d'inférence, permettant de définir le jugement $\sigma, c \Downarrow \sigma'$ pour IMP parallèle (sémantique à grands pas).

2. Montrez que l'exécution des programmes IMP parallèle ainsi définie n'est pas déterministe.

3. On définit

$$c_1 \equiv c_2 \qquad\qquad \text{ssi} \qquad\qquad \forall \sigma, \sigma'.\ \sigma, c_1 \Downarrow \sigma' \ \text{ ssi } \ \sigma, c_2 \Downarrow \sigma' \ .$$

   (a) Montrez que $\|$ est commutatif pour $\equiv$, autrement dit que $c_1 \| c_2 \equiv c_2 \| c_1$, pour tous c_1, c_2 de IMP parallèle.

   (b) Montrez que $\|$ n'est pas associatif pour $\equiv$.

3.2 Instruction par instruction

Dans cette partie, on change la notion d'atomicité, en se fondant sur la sémantique opérationnelle à petits pas: à chaque pas de calcul, dans l'exécution d'un programme de la forme $c_1 \| c_2$, soit c_1 évolue en c_1' (et, ce faisant, c_2 ne bouge pas), soit c'est l'inverse qui se produit.

1. Donnez les trois règles d'inférence qu'il est nécessaire d'ajouter aux règles vues en cours pour la sémantique à petits pas de Imp, afin de définir une relation notée $\sigma, c \to \sigma', c'$ pour Imp parallèle.

2. On notera $\sigma, c \searrow \sigma'$ si $\sigma, c \to^* \sigma', \texttt{skip}$ (où $\to^*$ est la clôture réflexive et transitive[1]) de $\to$, et on définit

$$c_1 \approx c_2 \qquad\qquad \text{ssi} \qquad\qquad \forall \sigma, \sigma'.\, (\sigma, c_1 \searrow \sigma') \;\text{ ssi }\; (\sigma, c_2 \searrow \sigma')\ .$$

   (a) Montrez que les relations notées par $\searrow$ et $\Downarrow$ ne coïncident pas.

   (b) Comparez $\equiv$ et $\approx$ (prouvez une ou deux inclusions, ou montrez que ces relations sont incomparables).

   (c) Montrez que $\|$ est commutatif pour $\approx$. Donnez une preuve rigoureuse.

   (d) Montrez que $\|$ est associatif pour $\approx$. Donnez une preuve rigoureuse.

   (e) On dit que $\approx$ est *clos par* $\|$ *à droite* si pour tous c_1, c_2 de Imp parallèle, $c_1 \approx c_2$ implique que pour tout c, $c_1 \| c \approx c_2 \| c$.

   Montrez que $\approx$ n'est pas clos par $\|$ à droite.

   Note: ceci est regrettable, car on est habitué, en mathématiques, à ce qu'une égalité puisse être utilisée "partout": si $t = u$, alors je peux remplacer partout t par u.

3.3 Encore plus finement

On pourrait imaginer donner une sémantique "à grain encore plus fin" que pour les parties 3.1 et 3.2, en tenant compte du fait que les lectures et les écritures de variables Imp peuvent être entrelacées finement à l'exécution.

Ainsi, lorsqu'on exécute par exemple

$$X := Y + 1 \quad \| \quad Y := X + 2\ ,$$

il y a plusieurs exécutions possibles, dont en particulier celle où les valeurs lues pour Y et X correspondent aux valeurs avant qu'une quelconque affectation n'ait lieu. À noter que cette situation n'était pas possible suivant les sémantiques vues aux parties précédentes.

Décrivez comment on pourrait s'y prendre pour définir une sémantique opérationnelle de Imp parallèle qui corresponde à cette vision. Pour ce faire, expliquez comment s'écrit le jugement, sur quoi il porte, et donnez *des* règles d'inférence (pas forcément toutes).

A priori, beaucoup de règles d'inférence sont en effet nécessaires pour ce faire, il ne vous est pas demandé de toutes les écrire. Sélectionnez un sous-ensemble de règles que vous jugerez illustratif et convainquant.

[1] Vous pouvez adopter la définition que vous voulez pour $\to^*$, entre une définition "usuelle" faisant intervenir un nombre de pas suivant $\to$ (et ouvrant la voie, éventuellement, à une preuve par induction sur ce nombre), et une définition inductive.