Programmation 1

TD n°7

3 novembre 2020

$$\frac{}{\rho \vdash x := e \Rightarrow \rho[x \mapsto [\![e]\!]\rho]}\ (:=) \qquad \frac{}{\rho \vdash \texttt{skip} \Rightarrow \rho}\ (\texttt{Skip})$$

$$\frac{\rho \vdash c_1 \Rightarrow \rho' \quad \rho' \vdash c_2 \Rightarrow \rho''}{\rho \vdash c_1; c_2 \Rightarrow \rho''}\ (\texttt{Seq})$$

$$\frac{\rho \vdash c_1 \Rightarrow \rho'}{\rho \vdash \texttt{if}\ e\ \texttt{then}\ c_1\ \texttt{else}\ c_2 \Rightarrow \rho'}\ (\texttt{if}_1)\ \text{si } [\![e]\!]\rho \neq 0 \qquad \frac{\rho \vdash c_2 \Rightarrow \rho''}{\rho \vdash \texttt{if}\ e\ \texttt{then}\ c_1\ \texttt{else}\ c_2 \Rightarrow \rho'}\ (\texttt{if}_2)\ \text{si } [\![e]\!]\rho = 0$$

$$\frac{\rho \vdash c \Rightarrow \rho' \quad \rho' \vdash \texttt{while}\ e\ \texttt{do}\ c \Rightarrow \rho''}{\rho \vdash \texttt{while}\ e\ \texttt{do}\ c \Rightarrow \rho''}\ (\texttt{while})\ \text{si } [\![e]\!]\rho \neq 0 \qquad \frac{}{\rho \vdash \texttt{while}\ e\ \texttt{do}\ c \Rightarrow \rho}\ (\texttt{while}_{\text{fin}})\ \text{si } [\![e]\!]\rho = 0$$

FIGURE 1 – La sémantique opérationnelle à grands pas de IMP.

$$\begin{aligned}
(x := e \cdot C, \rho) &\to (C, \rho[x \mapsto [\![e]\!]\rho]) \\
(\texttt{skip} \cdot C, \rho) &\to (C, \rho) \\
(c_1; c_2 \cdot C, \rho) &\to (c_1 \cdot c_2 \cdot C, \rho) \\
(\texttt{if}\ e\ \texttt{then}\ c_1\ \texttt{else}\ c_2 \cdot C, \rho) &\to (c_1 \cdot C, \rho) \quad \text{si } [\![e]\!]\rho \neq 0 \\
(\texttt{if}\ e\ \texttt{then}\ c_1\ \texttt{else}\ c_2 \cdot C, \rho) &\to (c_2 \cdot C, \rho) \quad \text{si } [\![e]\!]\rho = 0 \\
(\texttt{while}\ e\ \texttt{do}\ c \cdot C, \rho) &\to (c \cdot \texttt{while}\ e\ \texttt{do}\ c \cdot C, \rho) \quad \text{si } [\![e]\!]\rho \neq 0 \\
(\texttt{while}\ e\ \texttt{do}\ c \cdot C, \rho) &\to (C, \rho) \quad \text{si } [\![e]\!]\rho = 0
\end{aligned}$$

FIGURE 2 – La sémantique opérationnelle à petits pas de IMP.

Théorèmes petit pas

Déterminisme la réduction est déterministe

Progrès les seules configurations ne possédant pas de successeur sont de la forme (ε, ρ)

$$\frac{}{(x,\rho) \rightarrow_{pp} (\widehat{\dot{\rho(x)}},\rho)}\ (\texttt{Var}) \qquad \frac{(e_1,\rho) \rightarrow_{pp} (e_1',\rho)}{(e_1 \dot{+} e_2,\rho) \rightarrow_{pp} (e_1' \dot{+} e_2,\rho)}\ (+_\ell)$$

$$\frac{(e_2,\rho) \rightarrow_{pp} (e_2',\rho)}{(\dot{n} \dot{+} e_2,\rho) \rightarrow_{pp} (\dot{n} \dot{+} e_2',\rho)}\ (+_r) \qquad \frac{}{(\dot{n} \dot{+} \dot{m},\rho) \rightarrow_{pp} (\widehat{\dot{n+m}},\rho)}\ (+_{\text{fin}})$$

$$\frac{(e,\rho) \rightarrow_{pp} (e',\rho)}{(\dot{-}e,\rho) \rightarrow_{pp} (\dot{-}e',\rho)}\ (-) \qquad \frac{}{(\dot{-}\dot{n},\rho) \rightarrow_{pp} (\widehat{\dot{-n}},\rho)}\ (-_{\text{fin}})$$

FIGURE 3 – Sémantique opérationnelle à petits pas des expressions arithmétiques.

Théorèmes grand pas

Déterminisme l'arbre de dérivation d'un jugement est guidé par la syntaxe et donc unique.

Correction s'il existe une dérivation $\rho \vdash c \Downarrow \rho_\infty$ alors il existe une dérivation $(c \cdot \varepsilon, \rho) \rightarrow^* (\varepsilon, \rho_\infty)$

Adéquation s'il existe une dérivation $(c \cdot \varepsilon, \rho) \rightarrow^* (\varepsilon, \rho_\infty)$ alors il existe une dérivation $\rho \vdash c \Downarrow \rho_\infty$

1 Operational semantics

Exercise 1 : Operational semantics

Let c be a program and ρ an environment. Show the equivalence between :

1. There exists an infinite derivation of $(c \cdot \varepsilon, \rho)$
2. There exists no ρ_∞ such that $\rho \vdash c \Downarrow \rho_\infty$.

Solution:

Infinite execution $\implies$ no derivation We do the contrapositive

— If there exists a big-step derivation of $\rho \vdash c \Downarrow \rho_\infty$, then by the *adequacy property* there is a finite and terminal derivation from $(c \cdot \varepsilon, \rho)$ to $(\varepsilon, \rho_\infty)$

— As the reduction $\rightarrow$ is *deterministic*, it is the only derivation starting from the configuration $(c \cdot \varepsilon, \rho)$

— This derivation being finite and terminal, there cannot be an infinite run.

No derivation $\implies$ infinite execution We do the contrapositive

— If there is no infinite execution, then there is necessarily a finite execution.

— By the theorem of *progress* it necessarily stops on $(\varepsilon, \rho_\infty)$.

— The *correction* theorem gives a derivation $\rho \vdash c \Downarrow \rho_\infty$.

Exercise 2 :

The operational semantics defined in exercise 1 may appear artificial. Indeed, it does not describe how the expressions are calculated.

We are interested in the small step operational semantics of expressions, like in figure 3.

1. Give a proof of

$$((x \dot{+} (\dot{-}y)) \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) \rightarrow^*_{pp} (\dot{3}, \rho[x \mapsto 3, y \mapsto 2])$$

2. State then prove the progress theorem (théorème de progrès)
3. State then prove the determinism theorem (théorème de déterminisme)
4. Show the correctness of denotational semantics
5. Show the adequacy of denotational semantics

Solution:
The general sketch is described below :

1. The reduction is as follows

$$\begin{aligned}((x \dot{+} (\dot{-}y)) \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) &\rightarrow^*_{pp} ((\dot{3} \dot{+} (\dot{-}y)) \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) \\ &\rightarrow^*_{pp} ((\dot{3} \dot{+} (\dot{-}2)) \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) \\ &\rightarrow^*_{pp} ((\dot{3} \dot{+} (\dot{-2})) \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) \\ &\rightarrow^*_{pp} (\dot{1} \dot{+} \dot{2}, \rho[x \mapsto 3, y \mapsto 2]) \\ &\rightarrow^*_{pp} (\dot{3}, \rho[x \mapsto 3, y \mapsto 2])\end{aligned}$$

2. The only expressions that cannot be reduced are of the form $(\dot{n}, \rho)$ where n is an integer. This is proved by case analysis on e.
3. If $(e, \rho) \rightarrow_{pp} (e_1, \rho)$ and $(e, \rho) \rightarrow_{pp} (e_2, \rho)$ then $e_1 = e_2$. By induction, and then case analysis.
4. We must show that if $[\![e]\!]_\rho = n$ then $(e, \rho) \rightarrow^*_{pp} n$. For this, we reason by induction on the expression e and analyse the cases. We need an intermediate lemma which says

$$(e_1, \rho) \rightarrow^*_{pp} (\dot{n}, \rho) \implies (e_1 \dot{+} e_2, \rho) \rightarrow^*_{pp} (\dot{n} \dot{+} e_2, \rho)$$

The base case and the case of $\dot{+}$ are largely sufficient to convey the proof idea.

5. We have to show that if $(e, \rho) \rightarrow^*_{pp} n$ then $[\![e]\!]_\rho = n$. For this, it is sufficient to show that all the rewriting rules preserve the semantics of expressions.

2 Lattices and orderings

Inf-demi-treillis complet

Un *inf-demi-treillis complet* est un ensemble ordonné $(X, \leq)$ non vide tel que toute famille $F \subseteq X$ a une borne inférieure $\bigwedge F$.

Exercise 3 : Complete lattices

1. Show that a complete inf-semi-lattice (called a complete meet-semilattice) is in fact a complete lattice.
2. Show that the set of all subsets of any set A (its powerset) is a complete lattice.
3. Justify that the set of open sets $\mathcal{O}$ of a topological space $(X, \mathcal{O})$ is a complete lattice. What is the sup of a family F of open sets ? What is its inf ?

Solution:

1. Let us show that every set F has an upper bound. This is obtained by considering $\inf \emptyset$.

   Now consider G the (non-empty) set of upper bounds of F, then $\inf G = \sup F$. It is clear that $\inf G$ is less than any upper bound of F, and it remains to be shown $\forall x \in F, \inf G \geq x$. However, this is evident by definition of G.
2. The infimum is the intersection, and the supremum is the union.
3. The open sets of a topological space are stable by arbitrary union, in particular, the union is going to be the sup. **Note !** The inf is not the intersection, because an arbitrary intersection of open sets need not necessarily be an open set. The infimum is given by the interior of the intersection.

Knaster-Tarski

Soit $(X, \leq)$ un treillis complet et $f : X \to X$ une fonction monotone. Alors l'ensemble des points fixes de f est un treillis complet non vide.

Exercise 4 : A proof of Knaster-Tarski

Let f be a monotonic function from X to X where X is a complete lattice.

1. Show that f has a greatest and least fixed point.
2. Deduce that the set of fixed points is a complete lattice.

Solution:

1. Let us consider the set $A \triangleq \{x \in X \mid x \leq f(x)\}$ and $B \triangleq \{x \in X \mid f(x) \leq x\}$. Let $a_\infty = \sup A$ and $b_\infty = \inf B$.
   - If $a \in A$ then $f(a) \in A$ (resp. b, B) because f is monotonic.
   - Since f is monotonic,
   $$f(b_\infty) \leq f(B) \wedge f(a_\infty) \geq f(A)$$
   - By definition of B and A we then obtain
   $$f(b_\infty) \leq \inf f(B) \leq \inf B \wedge f(a_\infty) \geq \sup f(A) \geq \sup A$$
   - Consequently, $a_\infty \in A$ and $b_\infty \in B$. Therefore a_∞ et b_∞ are fixed points.
   - By construction, if $f(x) = x$ then $x \in A \cap B$, therefore $a_\infty \geq x \geq b_\infty$. Those are, therefore, the greatest and the least fixed points.
2. Take a non-empty family F of fixed points of f, let $g : x \mapsto \sup F \cup \{f(x)\}$.
   - La function g is monotonic because f is monotonic. It, therefore, has a least fixed point u.
   - In particular, $f(u) \leq u$. Since F is composed of fixed points of f, $f(u)$ is also an upper bound of F.
   - Thus, since u is the smallest of the upper bounds of $F \cup \{f(u)\}$, we deduce $u \leq f(u)$. Which shows that u is a fixed point of f.
   - By construction, it is, therefore, the least fixed point of f which bounds F.
   - We can do the same construction for the inf.

Exercise 5 : Using Knaster-Tarski

Prove the Cantor-Schröder-Bernstein theorem : if A and B are two sets such that there exist

two injective functions f and g respectively from A to B and from B to A, then A is in bijection with B.
Hint (preserved in French for full effect) : faire un dessin avec deux patates, tout serait si beau si on pouvait trouver X tel que $f(X)^c$....

Solution:
We want to use f for one part, and g^{-1} for the other to define a bijection between A and B. But for that it is necessary that the image of g is disjoint from the set that we use for f.
We search for a subset X which verifies

$$g(f(X)^c) = X^c \tag{1}$$

This function is monotonic for the inclusion of the subsets of A, so it has a fixed point U. We can then set

$$h(x) \triangleq \begin{cases} f(x) & \text{if } x \in U \\ g^{-1}(x) & \text{if } x \notin U \end{cases} \tag{2}$$

And verify that h is well-defined and is a bijection.

3 DCPOs

Rappel sur les familles dirigées

Une famille D non vide d'un ensemble $(X, \leq)$ est dirigée si et seulement si

$$\forall (x,y) \in D, \exists z \in D, z \geq x \wedge z \geq y$$

Rappels sur les DCPOs

Un DCPO est un ensemble partiellement ordonné $(X, \leq)$ tel que toute famille dirigée possède un sup. Un DCPO est *pointé* s'il existe un élément minimal.

Exercise 6 : Which is which ?

Draw the following sets and indicate which are DCPOs, which are complete lattices, which are pointed, and justify.

1. $\mathbf{1} = \{\bot\}$.
2. $\mathbf{Bool}_\bot = \{0, 1, \bot\}$ with $x < y$ if and only if $x = \bot$ and $y \neq \bot$.
3. $\mathbb{N}$ with the usual ordering.
4. $\mathbb{N}_{\omega+1}$ with the usual ordering.
5. $\mathbb{N}^2$ with the product ordering.
6. $\{[x, y] \mid x, y \in I, x \leq y\}$ with the ordering $\supseteq$ where $I = [0, 1]$.
7. $\{[x, y] \mid x, y \in I \cap \mathbb{Q}, x \leq y\}$ with the ordering $\supseteq$ where $I = [0, 1]$.

Solution:

Number	**Complete lattice**	**DCPO**	**Pointed**
1	✔	✔	✔
2	✖	✔	✔
3	✖	✖	✔
4	✔	✔	✔
5	✖	✖	✔
6	✖	✔	✔
7	✖	✖	✔

Exercise 7 : Knaster-Tarski VS Scott

We endow $[0,1]$ with the usual ordering which makes it DCPO and complete as a lattice.

1. Show that a monotonic function $f : [0,1] \to [0,1]$ admits a fixed point.
2. Show that if $f : [0,1] \to [0,1]$ is a Scott-continuous function then it has a fixed point. Moreover, this fixed point is the limit of the sequence $x_i \triangleq f^i(0)$.
3. Show the equivalence between the two following propositions for a monotonic function $f : [0,1] \to [0,1]$.
   - f preserves the sup
   - f is left-continuous over $[0,1]$
4. Deduce that $\sup f^i(0)$ is not always a fixed point of f by giving a counter-example.

Solution:

1. Knaster-Tarski
2. Scott's unique least fixed point in a DCPO.
3. We must show the equivalence between $f(\sup x_i) = \sup f(x_i)$ for any sequence (x_i) and $y_i \to t$ implies $f(y_i) \to f(t)$.
4. There are monotonic and non-continuous functions on the left, for example

$$f : x \mapsto \begin{cases} 1/2 * x + 1/4 & \text{if } x < 1/2 \\ 1 & \text{else} \end{cases} \tag{3}$$

   We have $f([0,1/2[) \subseteq [0,1/2[$ therefore $\sup f^i(0) \leq 1/2$, but the only fixed point of f is 1.