Equivalence entre la sémantique naturelle et la sémantique operationnelle structurée

Stefano Guerrini
LIPN - Institut Galilée, Université Paris Nord 13
stefano.guerrini@univ-paris13.fr

Sémantique des Langages de Programmation
Sup Galillée Informatique, 1ère année

2 avril 2010

Le but est de démontrer que, pour toute commande S,

$$\mathcal{S}_{ns}[\![S]\!] = \mathcal{S}_{sos}[\![S]\!]$$

c'est-à-dire

$$\forall s \in \textsc{State}: \quad \langle S, s\rangle \to_{ns} s' \quad \text{et} \quad \langle S, s\rangle \to_{sos} s'' \qquad \Longrightarrow \qquad s' = s''$$

La preuve est par induction structurelle sur les termes du langage While. Dans certains cas on démontrera aussi des propriétés par récurrence sur la longueur de la démonstration en sémantique naturelle $\langle S, s\rangle \to_{ns} s'$ ou sur la longueur de la dérivation de $\langle S, s\rangle \to^*_{sos} s'$.

1 Les cas de base

Les cas de base sont les commandes qui ne sont pas définies par récurrence à partir de autres commande de While. Les cas de base sont le skip et l'affectation.

1.1 Skip

Par la règle `skip` de la sémantique naturelle et la règle `skip` de la SOS

$$\text{skip}\ \frac{}{\langle \texttt{skip}, s\rangle \to_{sos} s} \qquad\qquad \langle \texttt{skip}, s\rangle \to_{ns} s$$

pour tout s, et donc

$$\mathcal{S}_{ns}[\![\texttt{skip}]\!] = \mathcal{S}_{sos}[\![\texttt{skip}]\!]$$

1.2 Affectation

Par la règle `ass` de la sémantique naturelle et la règle `ass` de la SOS

$$\text{ass}\ \frac{}{\langle x := e, s\rangle \to_{ns} s[x \mapsto \mathcal{A}[\![e]\!](s)]} \qquad\qquad \langle x := e, s\rangle \to_{ns} s[x \mapsto \mathcal{A}[\![e]\!](s)]$$

pour tout s, et donc

$$\mathcal{S}_{ns}[\![x := e]\!] = \mathcal{S}_{sos}[\![x := e]\!]$$

2 Les cas inductifs

Ce sont les commandes définies par récurrence à partir de autres commandes de While. Dans ces cas là, pour démontrer la thèse

$$\forall s \in \textsc{State} : \langle S, s\rangle \to_{ns} s_1 \quad \text{et} \quad \langle S, s\rangle \to_{sos} s_2 \qquad \Longrightarrow \qquad s_1 = s_2$$

on peut utiliser l'hypothèse d'induction structurelle, c'est-à-dire que, si $S' \neq S$ est une sous-commande de S (comme par exemple S_1 et S_2 dans $S_1\,;S_2$), alors on a déjà

$$\mathcal{S}_{ns}[\![S']\!] = \mathcal{S}_{sos}[\![S']\!]$$

2.1 Composition

Les cas à analyser est $S = S_1\,;S_2$ et, par l'hypothèse d'induction structurelle, on a

$$\mathcal{S}_{ns}[\![S_1]\!] = \mathcal{S}_{sos}[\![S_1]\!] \qquad \text{et} \qquad \mathcal{S}_{ns}[\![S_2]\!] = \mathcal{S}_{sos}[\![S_2]\!]$$

Pour démontrer la thèse on utilisera le lemme suivant, qu'on démontrera après.

Lemme 1 (de la composition)**.**

1. *$\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) \neq \bot$ ssi $\mathcal{S}_{sos}[\![S_1]\!](s) \neq \bot$ et $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \mathcal{S}_{sos}[\![S_2]\!](\mathcal{S}_{sos}[\![S_1]\!](s)) \neq \bot$*
2. *$\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \bot$ ssi un des deux cas suivants est vrai*
   (a) $\mathcal{S}_{sos}[\![S_1]\!](s) = \bot$
   (b) *$\mathcal{S}_{sos}[\![S_1]\!](s) \neq \bot$ et $\mathcal{S}_{sos}[\![S_2]\!](\mathcal{S}_{sos}[\![S_1]\!](s)) = \bot$*

Démonstration. Voir la section A de l'appendice. □

Donné un état quelconque s, on considère trois cas distingués : le cas $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = s'$ avec $s' \neq \bot$; le cas $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = s'$ avec $s' \neq \bot$; les cas de non-terminaison $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = \bot$ ou $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \bot$.

1. $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = s'$ avec $s' \neq \bot$
   Dans ce cas là, on a une démonstration en sémantique naturelle de $\langle S_1\,;S_2, s\rangle \to_{ns} s'$. Donc, il existe un état s_1 t.q. la dernière règle de cette démonstration est

$$\text{comp}\ \frac{\langle S_1, s\rangle \to_{ns} s_1 \qquad \langle S_2, s_1\rangle \to_{ns} s'}{\langle S_1\,;S_2, s\rangle \to_{ns} s'}$$

   C'est-à-dire

$$\mathcal{S}_{ns}[\![S_1]\!](s) = s_1 \qquad \text{et} \qquad s' = \mathcal{S}_{ns}[\![S_2]\!](s_1) = \mathcal{S}_{ns}[\![S_2]\!](\mathcal{S}_{ns}[\![S_1]\!](s))$$

   Par l'hypothèse d'induction structurelle, $\mathcal{S}_{sos}[\![S_1]\!](s) = \mathcal{S}_{ns}[\![S_1]\!](s) = s_1$ et $\mathcal{S}_{sos}[\![S_2]\!](s_1) = \mathcal{S}_{ns}[\![S_2]\!](s_1) = s'$ et par conséquent

$$\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = s' = \mathcal{S}_{ns}[\![S_2]\!](\mathcal{S}_{ns}[\![S_1]\!](s)) = \mathcal{S}_{sos}[\![S_2]\!](\mathcal{S}_{sos}[\![S_1]\!](s))$$

   Finalement, par le lemme de la composition, $\mathcal{S}_{sos}[\![S_2]\!](\mathcal{S}_{sos}[\![S_1]\!](s)) = \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s)$ et donc

$$\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = s' = \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s)$$

2. $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = s'$ avec $s' \neq \bot$
   Dans ce cas là, par le lemme de la composition, il existe $s_1 \neq \bot$ t.q.

$$\mathcal{S}_{sos}[\![S_1]\!](s) = s_1 \qquad \text{et} \qquad s' = \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \mathcal{S}_{sos}[\![S_2]\!](s_1)$$

   Par l'hypothèse d'induction structurelle, $\mathcal{S}_{ns}[\![S_1]\!](s) = \mathcal{S}_{sos}[\![S_1]\!](s) = s_1$ et $\mathcal{S}_{ns}[\![S_2]\!](s_1) = \mathcal{S}_{sos}[\![S_2]\!](s_1) = s'$ et donc, en sémantique naturelle, on a une démonstration de $\langle S_1, s\rangle \to_{ns} s_1$ et une démonstration de $\langle S_2, s_1\rangle \to_{ns} s'$. En utilisant la règle de la composition de la sémantique naturelle on obtient finalement

$$\text{comp}\ \frac{\langle S_1, s\rangle \to_{ns} s_1 \qquad \langle S_2, s_1\rangle \to_{ns} s'}{\langle S_1\,;S_2, s\rangle \to_{ns} s'}$$

c'est-à-dire

$$\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = s' = \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s)$$

3. $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = \bot$ ou $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \bot$
   Une conséquence des cas qu'on vient de démontre c'est que
   (a) $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) \neq \bot$ implique $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) \neq \bot$ (premier point)
   (b) $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) \neq \bot$ implique $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) \neq \bot$ (deuxième point)
   C'est-à-dire
   $$\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) \neq \bot \qquad \iff \qquad \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) \neq \bot$$
   qui est équivalent a
   $$\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = \bot \qquad \iff \qquad \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \bot$$

On peut donc conclure que, pour tout état s, on a $\mathcal{S}_{ns}[\![S_1\,;S_2]\!](s) = \mathcal{S}_{sos}[\![S_1\,;S_2]\!](s)$, et donc

$$\mathcal{S}_{ns}[\![S_1\,;S_2]\!] = \mathcal{S}_{sos}[\![S_1\,;S_2]\!]$$

2.2 Conditionnel

Les cas à analyser est $S = \texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2$ et, par l'hypothèse d'induction structurelle, $\mathcal{S}_{ns}[\![S_1]\!] = \mathcal{S}_{sos}[\![S_1]\!]$ et $\mathcal{S}_{ns}[\![S_2]\!] = \mathcal{S}_{sos}[\![S_2]\!]$.

1. Si $\mathcal{B}[\![b]\!](s) = tt$, tout démonstration de $\langle \texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2, s\rangle \to_{ns} s'$ termine par une règle
   $$\text{if-tt}\ \frac{\langle S_1, s\rangle \to_{ns} s'}{\langle \texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2, s\rangle \to_{ns} s'}$$
   c'est-à-dire, $\langle \texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2, s\rangle \to_{ns} s'$ ssi $\langle S_1, s\rangle \to_{ns} s'$, et donc
   $$\mathcal{S}_{ns}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!] = \mathcal{S}_{ns}[\![S_1]\!]$$
   Au même temps, si $\mathcal{B}[\![b]\!](s) = tt$, par le règle if-tt de la SOS,
   $$\langle \texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2, s\rangle \to_{sos} \langle S, s\rangle$$
   et donc
   $$\mathcal{S}_{sos}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!] = \mathcal{S}_{sos}[\![S_1]\!]$$
   Par l'hypothèse d'induction structurelle, on obtient finalement
   $$\mathcal{S}_{ns}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!] = \mathcal{S}_{ns}[\![S_1]\!] = \mathcal{S}_{sos}[\![S_1]\!] = \mathcal{S}_{sos}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!]$$
2. Si $\mathcal{B}[\![b]\!](s) = ff$, en utilisant les règles if-ff et l'hypothèse d'induction structurelle on obtient
   $$\mathcal{S}_{ns}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!] = \mathcal{S}_{ns}[\![S_2]\!] = \mathcal{S}_{sos}[\![S_2]\!] = \mathcal{S}_{sos}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!]$$

En conclusion, pour toutes valeurs de $\mathcal{B}[\![b]\!](s)$ on a

$$\mathcal{S}_{ns}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!] = \mathcal{S}_{sos}[\![\texttt{if}\, b\, \texttt{then}\, S_1\, \texttt{else}\, S_2]\!]$$

2.3 Itération

Les cas à analyser est $S = \texttt{while}\, b\, \texttt{do}\, S_1$ et, par l'hypothèse d'induction structurelle, $\mathcal{S}_{ns}[\![S_1]\!] = \mathcal{S}_{sos}[\![S_1]\!]$.

Dans le cas de l'itération, la seul induction structurelle ne suffit pas à démontrer la thèse. En fait, dans le cas du commande while, si $\mathcal{B}[\![b]\!](s) = tt$, on verra que les valeurs de $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s)$ et $\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s)$ sont définies à partir des valeurs $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s_1)$ et $\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s_1)$, ou $\mathcal{S}_{ns}[\![S_1]\!] = s_1 = \mathcal{S}_{sos}[\![S_1]\!]$. Mais, l'hypothèse d'induction structurelle sur S ne dit rien à propos de $\mathcal{S}_{ns}[\![S']\!](s_1) = \mathcal{S}_{sos}[\![S']\!](s_1)$, vu que $S' = \texttt{while}\, b\, \texttt{do}\, S_1 = S$.

En fait, il faut analyser le cas $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = s'$ avec $s' \neq \bot$, et démontrer par récurrence sur la taille de la démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$ qu'il y a une dérivation (finie) de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, et le cas $\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = s'$ avec $s' \neq \bot$, et démontrer par récurrence sur la taille de la longueur de la dérivation de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$ qu'il y a une démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$.

Les bases de ces récurrences correspondent au cas $\mathcal{B}[\![b]\!](s) = ff$, dans lequel on voit tous de suite que

$$\text{while-ff}\ \frac{}{\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s}\ \mathcal{B}[\![b]\!](s) = ff$$

et que

$$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{sos} s \qquad \text{si } \mathcal{B}[\![b]\!](s) = ff$$

1. $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = s'$ avec $s' \neq \bot$

   On démontrera, par récurrence sur la taille de la démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$ que, pour tout s, il y a une dérivation (finie) de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$.

   La récurrence qu'on utilisera est complète ou forte :

   > Soit s un état t.q. $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$ est démontrable avec une démonstration de taille n (comme taille d'une démonstration on peut prendre le nombre de ses règles).
   >
   > On prend l'hypothèse de récurrence : pour tout état s_1 t.q. $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to_{ns} s'$ est démontrable avec une démonstration de taille $< n$, il y a une dérivation de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s'$.
   >
   > Si l'hypothèse de récurrence implique qu'il y a une dérivation de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, on conclut que $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$.

   Le cas $\mathcal{B}[\![b]\!](s) = ff$ a été déjà analysé. Si $\mathcal{B}[\![b]\!] = tt$, la démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$ termine par une règle

   $$\text{while-tt}\ \frac{\langle S_1, s\rangle \to_{ns} s_1 \qquad \langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to_{ns} s'}{\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'}$$

   et donc, $s_1 = \mathcal{S}_{ns}[\![S_1]\!](s)$. Au même temps, en SOS

   $$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{sos} \langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle$$

   Par l'hypothèse de récurrence sur la taille de la démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$, on a que

   $$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s'$$

   Par l'hypothèse d'induction structurelle on a $s_1 = \mathcal{S}_{ns}[\![S_1]\!](s) = \mathcal{S}_{sos}[\![S_1]\!](s)$, et

   $$\langle S_1, s\rangle \to^*_{sos} s_1$$

   Par le lemme de la composition, $\mathcal{S}_{sos}[\![S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s_1)$, et en conséquence

   $$\langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} \langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s'$$

   c'est-à-dire, $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, car

   $$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{sos} \langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} \langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s'$$

   On obtient ainsi que

   $$\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) \neq \bot \qquad \Longrightarrow \qquad \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s)$$

2. $\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = s'$ avec $s' \neq \bot$
   On démontrera, par récurrence sur la taille de la dérivation de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$ que, pour tout s, il y a une démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$.
   La récurrence qu'on utilisera c'est :

   Soit s un état t.q. $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$ avec une dérivation de longueur n.
   On prend la suivante hypothèse de récurrence : pour tout état s_1 t.q. $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s'$ avec une dérivation de longueur $< n$, il y a une démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to_{ns} s'$.
   Si l'hypothèse de récurrence implique qu'il y a une démonstration de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$, on conclut que $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$.

   Le cas $\mathcal{B}[\![b]\!](s) = ff$ a été déjà analysé. Si $\mathcal{B}[\![b]\!] = tt$, alors

$$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{sos} \langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle$$

   Vu qu'on est en train de analyser le cas $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, on a $\langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, et par le lemme de la composition

$$\langle S_1\, \texttt{;}\, \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} \langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to^*_{sos} s' \qquad \text{avec} \qquad \langle S_1, s\rangle \to^*_{sos} s_1$$

   Par l'hypothèse de récurrence sur la taille de la dérivation de $\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to^*_{sos} s'$, on a que

$$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to_{ns} s'$$

   Par l'hypothèse d'induction structurelle on a $\mathcal{S}_{ns}[\![S_1]\!] = \mathcal{S}_{sos}[\![S_1]\!]$ et donc

$$\langle S_1, s\rangle \to_{ns} s_1$$

   Et finalement, en utilisant la règle if-tt de la sémantique naturelle

$$\text{while-tt}\ \frac{\langle S_1, s\rangle \to_{ns} s_1 \qquad \langle \texttt{while}\, b\, \texttt{do}\, S_1, s_1\rangle \to_{ns} s'}{\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'}$$

   on conclut qu'il y a une démonstration de

$$\langle \texttt{while}\, b\, \texttt{do}\, S_1, s\rangle \to_{ns} s'$$

   En obtenant ainsi que

$$\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) \neq \bot \qquad \Longrightarrow \qquad \mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s)$$

3. $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \bot$ ou $\mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \bot$.
   Comme dans le cas du conditionnel, les deux cas précédents impliquent que

$$\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \bot \qquad \Longleftrightarrow \qquad \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \bot$$

Vu que les trois cas qu'on vient d'analyser couvrent toutes les possibilités, on peut conclure que, pour tout état s, $\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s) = \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!](s)$, c'est-à-dire

$$\mathcal{S}_{ns}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!] = \mathcal{S}_{sos}[\![\texttt{while}\, b\, \texttt{do}\, S_1]\!]$$

A Lemme de la composition

Lemme 2. *Pour tout* $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} \gamma$*, une des suivantes possibilités est vraie*

1. $\langle S_1, s\rangle \to^*_{sos} \langle S_1', s_1\rangle$ *et* $\gamma = \langle S_1' \,;\, S_2, s_1\rangle$
2. $\langle S_1, s\rangle \to^*_{sos} s_1$ *et* $\langle S_2, s_1\rangle \to^*_{sos} \gamma$

Démonstration. Par récurrence sur la longueur de la dérivation $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} \gamma$. La structure de la démonstration est :

Soit n la longueur de la dérivation $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} \gamma$, c'est-à-dire $\langle S_1 \,;\, S_2, s\rangle \to^n_{sos} \gamma$

1. On démontre que la propriété vaut dans le cas de base $n = 0$
2. On démontre la propriété pour le cas $n + 1$ à partir de l'hypothèse que la propriété vaut pour le cas n.

En conséquence des deux points précédents, on conclut que la propriété est valide pour tout n.

Voici donc les détails de la démonstration par récurrence.

1. Le cas de base est immédiat car, pour $n = 0$, on a $\langle S_1 \,;\, S_2, s\rangle \to^0_{sos} \langle S_1 \,;\, S_2, s\rangle$ et, pour $\gamma = \langle S_1, s\rangle$, on a $\langle S_1, s\rangle \to^0_{sos} \langle S_1, s\rangle$.
2. Si $\langle S_1 \,;\, S_2, s\rangle \to^{n+1}_{sos} \gamma$ est une dérivation de longueur $n+1$, alors $\langle S_1 \,;\, S_2, s\rangle \to^n_{sos} \gamma' \to_{sos} \gamma$. Par l'hypothèse de récurrence ($\langle S_1 \,;\, S_2, s\rangle \to^n_{sos} \gamma'$ est de longueur n) on a deux possibilités :
   (a) $\langle S_1, s\rangle \to^*_{sos} \langle S_1'', s_1'\rangle$ et $\gamma' = \langle S_1'' \,;\, S_2, s_1'\rangle$. Dans ce cas là,
      i. si $S_1'' = \texttt{skip}$, alors $\langle S_1'' \,;\, S_2, s_1'\rangle \to_{sos} \langle S_2, s_1'\rangle$ par une comp-2 règle, car $\langle S_1'', s_1'\rangle = \langle \texttt{skip}, s_1'\rangle \to_{sos} s_1'$. Donc, si on prendre $s_1 = s_1'$ et $\gamma = \langle S_2, s_1\rangle$, on a $\langle S_1, s\rangle \to^*_{sos} s_1$ et $\langle S_2, s_1\rangle \to^*_{sos} \gamma$, qui correspond a un des deux cas de la propriété qu'on est en train de démontrer ;
      ii. si $S_1'' = \texttt{skip}$, alors $\langle S_1'' \,;\, S_2, s\rangle \to_{sos} \langle S_1' \,;\, S_2, s_1\rangle$ par une comp-1 règle, car $\langle S_1'', s_1'\rangle \to_{sos} \langle S_1', s_1\rangle$. Donc, $\langle S_1, s\rangle \to^*_{sos} \langle S_1', s_1\rangle$ et $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} \langle S_1' \,;\, S_2, s_1\rangle = \gamma$, qui correspond a un des deux cas de la propriété qu'on est en train de démontrer.
   (b) Si $\langle S_1, s\rangle \to^*_{sos} s_1$ et $\langle S_2, s_1\rangle \to^*_{sos} \gamma'$, alors $\langle S_2, s_1\rangle \to^*_{sos} \gamma$, car $\gamma' \to_{sos} \gamma$. Donc, on obtient un des deux cas de la propriété qu'on est en train de démontrer.

□

Lemme 3. *Si un des deux cas suivants est vraie*

1. $\langle S_1, s\rangle \to^*_{sos} \langle S_1', s_1\rangle$ *et* $\gamma = \langle S_1' \,;\, S_2, s_1\rangle$ *;*
2. $\langle S_1, s\rangle \to^*_{sos} s_1$ *et* $\langle S_2, s_1\rangle \to^*_{sos} \gamma$*.*

alors $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} \gamma$*.*

Démonstration.

1. Par récurrence sur la longueur de la dérivation $\langle S_1, s\rangle \to^*_{sos} \langle S_1', s_1\rangle$.
2. Par récurrence sur la longueur de la dérivation $\langle S_2, s_1\rangle \to^*_{sos} \gamma$.

□

Corollaire 4. $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} s'$*, avec* $s' \neq \perp$*, ssi* $\langle S_1, s\rangle \to^*_{sos} s_1$ *et* $\langle S_2, s_1\rangle \to^*_{sos} s'$*, pour quelque* $s_1 \neq \perp$*.*

Démonstration. Si $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} s'$, avec $s' \neq \perp$, par le Lemme 2, $\langle S_1, s\rangle \to^*_{sos} s_1$ et $\langle S_2, s_1\rangle \to^*_{sos} s'$ (car on est certainement dans le cas 2 du lemme).

Si $\langle S_1, s\rangle \to^*_{sos} s_1$ et $\langle S_2, s_1\rangle \to^*_{sos} s'$, par le Lemme 3, on obtient (cas 2 du lemme) $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} s'$. □

Les précédente corollaire correspond en fait a une différente formulation du lemme de la composition (Lemme 1).

1. Pour le premier point du lemme, on observe que $\langle S_1 \,;\, S_2, s\rangle \to^*_{sos} s'$ correspond à $\mathcal{S}_{sos}[\![S_1 \,;\, S_2]\!](s) = s'$, tandis que $\langle S_1, s\rangle \to^*_{sos} s_1$ et $\langle S_2, s_1\rangle \to^*_{sos} s'$ correspondent à $s' = \mathcal{S}_{sos}[\![S_2]\!](s_1) = \mathcal{S}_{sos}[\![S_2]\!](\mathcal{S}_{sos}[\![S_1]\!](s))$.

2. Pour le deuxième point du lemme, on observe que $\mathcal{S}_{sos}[\![S_1\,;S_2]\!](s) = \bot$ ssi pour tout $\langle S_1\,; S_2, s\rangle \to^*_{sos} \gamma$ la configuration n'est pas un état final. Mais, pour le Corollaire 4, ça est possible seulement dans les deux cas suivants
   (a) pour tout $\langle S_1, s\rangle \to^*_{sos} \gamma$ la configuration γ n'est pas un état final, et donc $\mathcal{S}_{sos}[\![S_1]\!](s) = \bot$;
   (b) $\langle S_1, s\rangle \to^*_{sos} s_1$, mais pour tout $\langle S_2, s_1\rangle \to^*_{sos} \gamma$ la configuration γ n'est pas un état final, et donc $\mathcal{S}_{sos}[\![S_1]\!](s) = s_1$ mais $\mathcal{S}_{sos}[\![S_2]\!](s_1) = \bot$.