Preuve de programmes impératifs

David Delahaye
David.Delahaye@lirmm.fr

Université de Montpellier
Faculté des Sciences

Licence Informatique L3 2021-2022

Preuve de programmes impératifs

Principe

- Programmes fonctionnels : spécification sur un résultat ;
- Programmes impératifs :
  - Effets de bords sur un environnement (ensemble de variables) ;
  - Spécification sur l'évolution de l'environnement (les états) ;
  - Logique particulière : logique de Hoare.

Outils

- Beaucoup moins que pour le fonctionnel ;
- Deux outils assez connus :
  - Atelier B (industriel) : `http://www.atelierb.eu/` ;
  - Why (académique) : `http://why3.lri.fr/`.

De l'importance de la sémantique

Bilbo le Hobbit : un voyage inattendu (J. R. R. Tolkien, 1937)

Bilbon Sacquet :

- Bonjour !

Gandalf :

- Qu'entendez-vous par là ? dit-il. Me souhaitez-vous le bonjour ou constatez-vous que c'est une bonne journée, que je le veuille ou non, ou que vous vous sentez bien ce matin, ou encore que c'est une journée où il faut être bon ?

De l'importance de la sémantique

Bilbo le Hobbit : un voyage inattendu (J. R. R. Tolkien, 1937)

Bilbon Sacquet :

- Bonjour !

Gandalf :

- Qu'entendez-vous par là ? dit-il. Me souhaitez-vous le bonjour ou constatez-vous que c'est une bonne journée, que je le veuille ou non, ou que vous vous sentez bien ce matin, ou encore que c'est une journée où il faut être bon ?

Quelle est la bonne sémantique ?

De l'importance de la sémantique

Bilbo le Hobbit : un voyage inattendu (J. R. R. Tolkien, 1937)

Bilbon Sacquet :

- Bonjour !

Gandalf :

- Qu'entendez-vous par là ? dit-il. Me souhaitez-vous le bonjour ou constatez-vous que c'est une bonne journée, que je le veuille ou non, ou que vous vous sentez bien ce matin, ou encore que c'est une journée où il faut être bon ?

Quelle est la bonne sémantique ?

Bilbon Sacquet :

- Tout cela à la fois, je suppose.

Motivations pour formaliser les sémantiques

Définition rigoureuse de l'exécution

- Tout comportement est spécifié (même les cas d'erreurs) ;
- Plus d'ambiguïtés pour l'utilisateur (ordre d'évaluation).

Démonstration formelle de propriétés

- Équivalences sémantiques (si différentes sémantiques) ;
- Équivalences de programmes (syntaxiquement différents) ;
- Correction de transformations de programmes ;
- Propriétés relatives au typage :
  - Correction du typage vis-à-vis de la sémantique ;
  - Préservation du typage par la sémantique.

Principes

Syntaxe

- Définition préalable de la syntaxe (abstraite) du langage ;
- Utilisation d'une structure arborescente (AST).

Différentes sémantiques

- Sémantique opérationnelle naturelle (à grands pas) ;
- Sémantique opérationnelle structurée (à petits pas) ;
- Sémantique dénotationnelle (théorie des domaines) ;
- Sémantique axiomatique (logique de Hoare).

Dichotomie syntaxe et sémantique

- C. Strachey :
  « La sémantique est là pour ce que nous voulons dire et la syntaxe pour comment nous avons à le dire. »

Sémantique à grands pas d'un petit langage

Expressions arithmétiques

- $e ::= n \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$.

Sémantique à grands pas

- Valeurs : $v_e ::= n$, où $n \in \mathbb{Z}$;
- Sémantique : relation « $e \rightsquigarrow v_e$ » ;
- Règles en langage naturel :
  - Si $n \in \mathbb{Z}$, alors $n \rightsquigarrow n$;
  - Si $e_1 \rightsquigarrow v_1$ et $e_2 \rightsquigarrow v_2$, alors $e_1 + e_2 \rightsquigarrow v_1 +_{\mathbb{Z}} v_2$;
  - Si $e_1 \rightsquigarrow v_1$ et $e_2 \rightsquigarrow v_2$, alors $e_1 - e_2 \rightsquigarrow v_1 -_{\mathbb{Z}} v_2$;
  - Si $e_1 \rightsquigarrow v_1$ et $e_2 \rightsquigarrow v_2$, alors $e_1 \times e_2 \rightsquigarrow v_1 \times_{\mathbb{Z}} v_2$;
  - Si $e_1 \rightsquigarrow v_1$ et $e_2 \rightsquigarrow v_2$, alors $e_1/e_2 \rightsquigarrow v_1/_{\mathbb{Z}} v_2$.

Sémantique à grands pas d'un petit langage

Expressions arithmétiques

- $e ::= n \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$.

Sémantique à grands pas

- Règles d'inférence :

$$\frac{n \in \mathbb{Z}}{n \rightsquigarrow n}\,\mathbb{Z}$$

$$\frac{e_1 \rightsquigarrow v_1 \qquad e_2 \rightsquigarrow v_2}{e_1 + e_2 \rightsquigarrow v_1 +_{\mathbb{Z}} v_2}\,+ \qquad \frac{e_1 \rightsquigarrow v_1 \qquad e_2 \rightsquigarrow v_2}{e_1 - e_2 \rightsquigarrow v_1 +_{\mathbb{Z}} v_2}\,-$$

$$\frac{e_1 \rightsquigarrow v_1 \qquad e_2 \rightsquigarrow v_2}{e_1 \times e_2 \rightsquigarrow v_1 \times_{\mathbb{Z}} v_2}\,\times \qquad \frac{e_1 \rightsquigarrow v_1 \qquad e_2 \rightsquigarrow v_2}{e_1/e_2 \rightsquigarrow v_1/_{\mathbb{Z}} v_2}\,/$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques

- $e ::= n \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$.

Sémantique à grands pas

- Exemple d'évaluation :

$$\dfrac{\dfrac{\dfrac{4 \in \mathbb{Z}}{4 \rightsquigarrow 4}\,\mathbb{Z} \quad \dfrac{2 \in \mathbb{Z}}{2 \rightsquigarrow 2}\,\mathbb{Z}}{4 + 2 \rightsquigarrow 6}\,+ \quad \dfrac{\dfrac{9 \in \mathbb{Z}}{9 \rightsquigarrow 9}\,\mathbb{Z} \quad \dfrac{2 \in \mathbb{Z}}{2 \rightsquigarrow 2}\,\mathbb{Z}}{9 - 2 \rightsquigarrow 7}\,-}{(4 + 2) \times (9 - 2) \rightsquigarrow 42}\,\times$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques avec variables

- $e \ ::= \ n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1 / e_2$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Valeurs : $v_e \ ::= \ n \mid \mathrm{Err}$, où $n \in \mathbb{Z}$;
- Contextes d'exécution : $E = (x_1, v_1), (x_2, v_2), \ldots, (x_n, v_n)$;
- Sémantique : relation « $E \vdash e \rightsquigarrow v_e$ » ;
- Règles :

$$\frac{n \in \mathbb{Z}}{E \vdash n \rightsquigarrow n}\ \mathbb{Z} \qquad \frac{(x, v) \in E}{E \vdash x \rightsquigarrow v}\ \mathbb{V}$$

$$\frac{E \vdash e_1 \rightsquigarrow v_1 \qquad E \vdash e_2 \rightsquigarrow v_2}{E \vdash e_1 \ \mathrm{op} \ e_2 \rightsquigarrow v_1 \ \mathrm{op}_{\mathbb{Z}} \ v_2}\ \mathrm{op}, \text{ avec } \mathrm{op} \in \{+, -, \times, /\}$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques avec variables

- $e ::= n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Règles d'erreur (à ne pas oublier) :

$$\frac{x \notin \mathrm{dom}(E)}{E \vdash x \rightsquigarrow \mathrm{Err}}\ \mathbb{V}_{\mathrm{Err}}$$

$$\frac{E \vdash e_1 \rightsquigarrow \mathrm{Err}}{E \vdash e_1\ \mathrm{op}\ e_2 \rightsquigarrow \mathrm{Err}}\ \mathrm{op}_{\mathrm{Err}1},\ \text{avec op} \in \{+, -, \times, /\}$$

$$\frac{E \vdash e_1 \rightsquigarrow v_1 \qquad E \vdash e_2 \rightsquigarrow \mathrm{Err}}{E \vdash e_1\ \mathrm{op}\ e_2 \rightsquigarrow \mathrm{Err}}\ \mathrm{op}_{\mathrm{Err}2},\ \text{avec op} \in \{+, -, \times, /\}$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques avec variables

- $e ::= n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Exemple d'évaluation (succès) :

$$\dfrac{\dfrac{\dfrac{4 \in \mathbb{Z}}{E \vdash 4 \rightsquigarrow 4}\,\mathbb{Z} \qquad \dfrac{(x,2) \in E}{E \vdash x \rightsquigarrow 2}\,\mathbb{V}}{E \vdash 4 + x \rightsquigarrow 6}\,+ \qquad \dfrac{E \vdash 9 - x \rightsquigarrow}{}}{E = (x,2) \vdash (4+x) \times (9-x) \rightsquigarrow 42}\,\times$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques avec variables

- $e ::= n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Exemple d'évaluation (succès) :

$$\dfrac{\dfrac{\Pi}{E \vdash 4 + x \rightsquigarrow 6} \quad \dfrac{\dfrac{9 \in \mathbb{Z}}{E \vdash 9 \rightsquigarrow 9}\,\mathbb{Z} \quad \dfrac{(x,2) \in E}{E \vdash x \rightsquigarrow 2}\,\mathbb{V}}{E \vdash 9 - x \rightsquigarrow 7}\,-}{E = (x,2) \vdash (4 + x) \times (9 - x) \rightsquigarrow 42}\,\times$$

Sémantique à grands pas d'un petit langage

Expressions arithmétiques avec variables

- $e ::= n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1 / e_2$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Exemple d'évaluation (échec) :

$$\dfrac{\dfrac{\dfrac{4 \in \mathbb{Z}}{E \vdash 4 \rightsquigarrow 4}\,\mathbb{Z} \qquad \dfrac{y \notin \mathrm{dom}(E)}{E \vdash y \rightsquigarrow \mathrm{Err}}\,\mathbb{V}_{\mathrm{Err}}}{E \vdash 4 + y \rightsquigarrow \mathrm{Err}}\,+_{\mathrm{Err2}}}{E = (x, 2) \vdash (4 + y) \times (9 - x) \rightsquigarrow \mathrm{Err}}\,\times_{\mathrm{Err1}}$$

Sémantique à grands pas d'un petit langage

Instructions : affectation et séquence

- $i \ ::= \ x := e \mid i_1 ; i_2$
  où $x \in \mathbb{V}$ (ensemble de noms de variables).

Sémantique à grands pas

- Valeurs : $v_i \ ::= \ E \mid \mathrm{Err}$;
- Sémantique : relation « $E \vdash i \rightsquigarrow v_i$ » ;
- Règles :

$$\frac{x \in \mathrm{dom}(E) \qquad E \vdash e \rightsquigarrow v}{E \vdash x := e \rightsquigarrow E \leftarrow (x, v)} \ :=$$

$$\frac{E \vdash i_1 \rightsquigarrow E_1 \qquad E_1 \vdash i_2 \rightsquigarrow E_2}{E \vdash i_1 ; i_2 \rightsquigarrow E_2} \ ;$$

Sémantique à grands pas d'un petit langage

Instructions : conditionnelle

- $e ::= \ldots \mid \text{true} \mid \text{false} \mid \text{not}(e) \mid e_1 \text{ and } e_2 \mid e_1 \text{ or } e_2$
  $\mid e_1 = e_2 \mid e_1 != e_2 \mid e1 < e_2 \mid e_1 \leq e_2 \mid e_1 \geq e_2 \mid e_1 > e_2$;
- $i ::= \ldots \mid \text{if } e \text{ then } i_1 \text{ else } i_2$.

Sémantique à grands pas

- Valeurs (expressions) : $v_e ::= n \mid b \mid \text{Err}$, où $n \in \mathbb{Z}$, $b \in \mathbb{B} = \{\top, \bot\}$;
- Règles :

$$\frac{}{E \vdash \text{true} \rightsquigarrow \top}\ \text{if}_{\text{true}} \qquad \frac{}{E \vdash \text{false} \rightsquigarrow \bot}\ \text{if}_{\text{false}}$$

$$\frac{E \vdash e \rightsquigarrow b}{E \vdash \text{not}(e) \rightsquigarrow \neg b}\ \text{not}$$

Sémantique à grands pas d'un petit langage

Instructions : conditionnelle

- $e ::= \ldots \mid \text{true} \mid \text{false} \mid \text{not}(e) \mid e_1 \text{ and } e_2 \mid e_1 \text{ or } e_2$
  $\mid e_1 = e_2 \mid e_1 != e_2 \mid e1 < e_2 \mid e_1 \leq e_2 \mid e_1 \geq e_2 \mid e_1 > e_2$;
- $i ::= \ldots \mid \text{if } e \text{ then } i_1 \text{ else } i_2$.

Sémantique à grands pas

- Valeurs (expressions) : $v_e ::= n \mid b \mid \text{Err}$, où $n \in \mathbb{Z}$, $b \in \mathbb{B} = \{\top, \bot\}$;
- Règles :

$$\frac{E \vdash e_1 \rightsquigarrow b_1 \qquad E \vdash e_2 \rightsquigarrow b_2}{E \vdash e_1 \text{ and } e_2 \rightsquigarrow b_1 \wedge b2} \text{ and}$$

$$\frac{E \vdash e_1 \rightsquigarrow v_1 \qquad E \vdash e_2 \rightsquigarrow v_2}{E \vdash e_1 = e_2 \rightsquigarrow v_1 = v_2} =$$

Sémantique à grands pas d'un petit langage

Instructions : conditionnelle

- $e ::= \ldots \mid \text{true} \mid \text{false} \mid \text{not}(e) \mid e_1 \text{ and } e_2 \mid e_1 \text{ or } e_2$
  $\mid e_1 = e_2 \mid e_1 != e_2 \mid e1 < e_2 \mid e_1 \leq e_2 \mid e_1 \geq e_2 \mid e_1 > e_2$;
- $i ::= \ldots \mid \text{if } e \text{ then } i_1 \text{ else } i_2$.

Sémantique à grands pas

- Valeurs (expressions) : $v_e ::= n \mid b \mid \text{Err}$, où $n \in \mathbb{Z}$, $b \in \mathbb{B} = \{\top, \bot\}$;
- Règles :

$$\frac{E \vdash e \rightsquigarrow \top \qquad E \vdash i_1 \rightsquigarrow E'}{E \vdash \text{if } e \text{ then } i_1 \text{ else } i_2 \rightsquigarrow E'} \text{ if}_{\text{true}}$$

$$\frac{E \vdash e \rightsquigarrow \bot \qquad E \vdash i_2 \rightsquigarrow E'}{E \vdash \text{if } e \text{ then } i_1 \text{ else } i_2 \rightsquigarrow E'} \text{ if}_{\text{false}}$$

Sémantique à grands pas d'un petit langage

Instructions : boucle « while »

- $i ::= \ldots \mid \text{while } e \text{ do } i.$

Sémantique à grands pas

- Règles :

$$\frac{E \vdash e \rightsquigarrow \top \quad E \vdash i \rightsquigarrow E' \quad E' \vdash \text{while } e \text{ do } i \rightsquigarrow E''}{E \vdash \text{while } e \text{ do } i \rightsquigarrow E''} \text{ while}_\top$$

$$\frac{E \vdash e \rightsquigarrow \bot}{E \vdash \text{while } e \text{ do } i \rightsquigarrow E} \text{ while}_\bot$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\dfrac{r \in \mathrm{dom}(E_0) \qquad \dfrac{(x,2) \in E_0}{E_0 \vdash x \rightsquigarrow 2}\,\mathbb{V}}{E_0 \vdash r := x \rightsquigarrow E_1 = (x,2),(r,2),(i,0)} := \qquad E_1 \vdash \begin{array}{l} i := x; \text{while } i > 1 \text{ do} \\ (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1) \end{array}}{E_0 = (x,2),(r,0),(i,0) \vdash \begin{array}{l} r := x; i := x; \text{while } i > 1 \text{ do } (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1) \end{array}}\;;$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\dfrac{i \in \mathrm{dom}(E_1) \qquad \dfrac{(x,2) \in E_1}{E_1 \vdash x \rightsquigarrow 2}\,\mathbb{V}}{E_1 \vdash i := x \rightsquigarrow E_2 = (x,2),(r,2),(i,2)} := \qquad E_2 \vdash \begin{array}{l}\text{while } i > 1 \text{ do} \\ (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1)\end{array}}{E_1 = (x,2),(r,2),(i,0) \vdash \begin{array}{l} i := x; \text{while } i > 1 \text{ do } (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1)\end{array}}\ ;$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\begin{array}{c} E_2 \vdash i > 1 \rightsquigarrow \top \quad E_2 \vdash (r := r + x; i := i - 1) \rightsquigarrow E_3 = (x,2),(r,4),(i,1) \\ E_3 \vdash \text{while } i > 1 \text{ do } (r := r + x; i := i - 1) \rightsquigarrow (x,2),(r,4),(i,1) \end{array}}{E_2 = (x,2),(r,2),(i,2) \vdash \begin{array}{l} \text{while } i > 1 \text{ do } (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1) \end{array}} \text{while}_\top$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\dfrac{(i,2) \in E_2}{E_2 \vdash i \rightsquigarrow 2}\,\mathbb{V} \qquad \dfrac{1 \in \mathbb{Z}}{E_2 \vdash 1 \rightsquigarrow 1}\,\mathbb{Z}}{E_2 = (x,2),(r,2),(i,2) \vdash i > 1 \rightsquigarrow \top}\,>$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\dfrac{r \in \mathrm{dom}(E_2) \qquad \dfrac{\dfrac{(r,2) \in E_2}{E_2 \vdash r \rightsquigarrow 2}\,\mathbb{V} \qquad \dfrac{(x,2) \in E_2}{E_2 \vdash x \rightsquigarrow 2}\,\mathbb{V}}{E_2 \vdash r + x \rightsquigarrow 2}\,+}{E_2 \vdash r := r + x \rightsquigarrow E_4 = (x,2),(r,4),(i,2)}\,:= \qquad E_4 \vdash i := i - 1 \rightsquigarrow E_3}{E_2 = (x,2),(r,2),(i,2) \vdash \begin{array}{l}(r := r + x; i := i - 1) \rightsquigarrow \\ E_3 = (x,2),(r,4),(i,1)\end{array}}\,;$$

$$\dfrac{i \in \mathrm{dom}(E_4) \qquad \dfrac{\dfrac{(i,2) \in E_4}{E_4 \vdash i \rightsquigarrow 2}\,\mathbb{V} \qquad \dfrac{1 \in \mathbb{Z}}{E_4 \vdash 1 \rightsquigarrow 1}\,\mathbb{Z}}{E_4 \vdash i - 1 \rightsquigarrow 1}\,-}{E_4 \vdash i := i - 1 \rightsquigarrow E_3}\,:=$$

Sémantique à grands pas d'un petit langage

Exemple d'évaluation d'un programme (succès)

$$\dfrac{\dfrac{\dfrac{(i,1) \in E_3}{E_3 \vdash i \rightsquigarrow 1}\,\mathbb{V} \qquad \dfrac{1 \in \mathbb{Z}}{E_3 \vdash 1 \rightsquigarrow 1}\,\mathbb{Z}}{E_3 \vdash i > 1 \rightsquigarrow \bot}\,> }{E_3 = (x,2),(r,4),(i,1) \vdash \begin{array}{l}\text{while } i > 1 \text{ do } (r := r + x; i := i - 1) \rightsquigarrow \\ (x,2),(r,4),(i,1)\end{array}}\,\text{while}_\bot$$

Le langage (résumé)

Petit noyau impératif

- Expressions entières et booléennes ;
- Instructions d'affectation, de conditionnelle, et de boucle.

Expressions et instructions

- $e \ ::= \ n \mid x \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  $\mid \text{true} \mid \text{false} \mid \text{not}(e) \mid e \text{ and } e \mid e \text{ or } e$
  $\mid e = e \mid e \mathrel{!}= e \mid e < e \mid e \leq e \mid e \geq e \mid e > e$
  où $n \in \mathbb{Z}$ et $x \in \mathbb{V}$ (ensemble de noms de variables) ;
- $i \ ::= \ \text{skip} \mid x := e \mid i; i \mid \text{if } e \text{ then } i \text{ else } i \mid \text{while } e \text{ do } i.$

Sémantique opérationnelle à grands pas (résumé)

Sémantique des expressions

- Valeurs : $v_e ::= n \mid b \mid \mathrm{Err}$, où $n \in \mathbb{Z}$, $b \in \mathbb{B} = \{\top, \bot\}$;
- Contextes d'exécution : $E = (x_1, v_1), (x_2, v_2), \ldots, (x_n, v_n)$;
- Sémantique : relation « $E \vdash e \rightsquigarrow v_e$ » ;
- Règles :

$$\frac{n \in \mathbb{Z}}{E \vdash n \rightsquigarrow n}\ \mathbb{Z} \qquad \frac{(x, v) \in E}{E \vdash x \rightsquigarrow v}\ \mathbb{V}$$

$$\frac{E \vdash e_1 \rightsquigarrow v_1 \qquad E \vdash e_2 \rightsquigarrow v_2}{E \vdash e_1\ \mathrm{op}\ e_2 \rightsquigarrow v_1\ \mathrm{op}_{\mathbb{Z}}\ v_2}\ \mathrm{op},\ \text{avec } \mathrm{op} \in \{+, -, \times, /\}$$

$$\frac{}{E \vdash \mathrm{true} \rightsquigarrow \top}\ \mathrm{true} \qquad \frac{}{E \vdash \mathrm{false} \rightsquigarrow \bot}\ \mathrm{false}$$

$$\frac{E \vdash e \rightsquigarrow b}{E \vdash \mathrm{not}(e) \rightsquigarrow \neg b}\ \mathrm{not}$$

Sémantique opérationnelle à grands pas (résumé)

Sémantique des expressions

- Règles :

$$\frac{E \vdash e_1 \rightsquigarrow b_1 \qquad E \vdash e_2 \rightsquigarrow b_2}{E \vdash e_1 \text{ and } e_2 \rightsquigarrow b_1 \wedge b2} \text{ and}$$

$$\frac{E \vdash e_1 \rightsquigarrow b_1 \qquad E \vdash e_2 \rightsquigarrow b_2}{E \vdash e_1 \text{ or } e_2 \rightsquigarrow b_1 \vee b2} \text{ or}$$

$$\frac{E \vdash e_1 \rightsquigarrow v_1 \qquad E \vdash e_2 \rightsquigarrow v_2}{E \vdash e_1 \text{ op } e_2 \rightsquigarrow v_1 \text{ op}_{\mathbb{Z},\mathbb{B}} v_2} \text{ op, avec op} \in \{=, !=, <, \leq, \geq, >\}$$

Sémantique opérationnelle à grands pas (résumé)

Sémantique des instructions

- Valeurs : $v_i \ ::= \ E \mid \mathrm{Err}$;
- Sémantique : relation « $E \vdash e \rightsquigarrow v_i$ » ;
- Règles :

$$\frac{x \in \mathrm{dom}(E) \qquad E \vdash e \rightsquigarrow v}{E \vdash x := e \rightsquigarrow E \leftarrow (x, v)} \ :=$$

$$\frac{E \vdash i_1 \rightsquigarrow E_1 \qquad E_1 \vdash i_2 \rightsquigarrow E_2}{E \vdash i_1 ; i_2 \rightsquigarrow E_2} \ ;$$

$$\frac{E \vdash e \rightsquigarrow \top \qquad E \vdash i_1 \rightsquigarrow E'}{E \vdash \mathrm{if} \ e \ \mathrm{then} \ i_1 \ \mathrm{else} \ i_2 \rightsquigarrow E'} \ \mathrm{if}_\top$$

$$\frac{E \vdash e \rightsquigarrow \bot \qquad E \vdash i_2 \rightsquigarrow E'}{E \vdash \mathrm{if} \ e \ \mathrm{then} \ i_1 \ \mathrm{else} \ i_2 \rightsquigarrow E'} \ \mathrm{if}_\bot$$

Sémantique opérationnelle à grands pas (résumé)

Sémantique des instructions

- Règles :

$$\frac{E \vdash e \rightsquigarrow \top \quad E \vdash i \rightsquigarrow E' \quad E' \vdash \text{while } e \text{ do } i \rightsquigarrow E''}{E \vdash \text{while } e \text{ do } i \rightsquigarrow E''}\ \text{while}_\top$$

$$\frac{E \vdash e \rightsquigarrow \bot}{E \vdash \text{while } e \text{ do } i \rightsquigarrow E}\ \text{while}_\bot$$

Logique de Hoare

Triplet de Hoare

- Triplet noté : $\{P\}\ i\ \{Q\}$, où P et Q sont des assertions logiques, et i une instruction ;
- Assertions logiques : exprimées en logique du premier ordre, où les atomes sont les expressions de notre langage ;
- Un triplet de Hoare $\{P\}\ i\ \{Q\}$ est valide si pour tous états E_1 et E_2 tels que si P est vraie dans E_1 et $E_1 \vdash i \rightsquigarrow E_2$ (i termine), alors Q est vraie dans E_2.

Exemples de triplets de Hoare valides

- $\{x = 1\}\ x := x + 2\ \{x = 3\}$;
- $\{x = y\}\ x := x + y\ \{x = 2 \times y\}$.

Logique de Hoare

Règles

$$\frac{}{\{P\}\ \text{skip}\ \{P\}}\ \text{skip} \qquad \frac{}{\{P(e)\}\ x := e\ \{P(x)\}}\ :=$$

$$\frac{\{P\}\ i_1\ \{Q\} \qquad \{Q\}\ i_2\ \{R\}}{\{P\}\ i_1; i_2\ \{R\}}\ ;$$

$$\frac{\{P \wedge e\}\ i_1\ \{Q\} \qquad \{P \wedge \neg e\}\ i_2\ \{Q\}}{\{P\}\ \text{if}\ e\ \text{then}\ i_1\ \text{else}\ i_2\ \{Q\}}\ \text{if}$$

$$\frac{\{I \wedge e\}\ i\ \{I\}}{\{I\}\ \text{while}\ e\ \text{do}\ i\ \{I \wedge \neg e\}}\ \text{while}$$

$$\frac{\{P'\}\ i\ \{Q'\} \qquad P \Rightarrow P' \qquad Q' \Rightarrow Q}{\{P\}\ i\ \{Q\}}\ \text{Aff}$$

Logique de Hoare

Correction totale (avec terminaison)

- La sémantique précédente est partielle : elle suppose que le programme termine ;
- La sémantique peut être totale en imposant que le programme termine (par la pré-condition) ;
- Correction totale :
  Un triplet de Hoare $\{P\}\ i\ \{Q\}$ est valide si pour tous états E_1 et E_2 tels que si P est vraie dans E_1, alors $E_1 \vdash i \rightsquigarrow E_2$ (i termine), et Q est vraie dans E_2 ;
- Nouvelle règle pour le while :

$$\frac{\{I \wedge e \wedge v = n\}\ i\ \{I \wedge v \geq 0 \wedge v < n\}}{\{I\}\ \text{while}\ e\ \text{do}\ i\ \{I \wedge \neg e\}}\ \text{while}$$

où v est le variant (expression) et n une variable entière n'apparaissant pas dans i.

Exemples

Séquence

$$\dfrac{\dfrac{}{\{0+x\geq 0\}\ a:=0\ \{a+x\geq 0\}}:=\quad\dfrac{}{\{a+x\geq 0\}\ b:=x\ \{a+b\geq 0\}}:=}{\dfrac{\{0+x\geq 0\}\ a:=0;b:=x\ \{a+b\geq 0\}\qquad x\geq 0\Rightarrow 0+x\geq 0}{\{x\geq 0\}\ a:=0;b:=x\ \{a+b\geq 0\}}\ \text{Aff}}\ ;$$

Exemples

Conditionnelle

$$\dfrac{\dfrac{}{\{y = 0\}\ x := y\ \{x = 0\}}\ :=\qquad \dfrac{\neg(y = 0) \Rightarrow 0 = 0 \qquad \dfrac{}{\{0 = 0\}\ x := 0\ \{x = 0\}}\ :=}{\{\neg(y = 0)\}\ x := 0\ \{x = 0\}}\ \text{Aff}}{\{\}\ \text{if}\ y = 0\ \text{then}\ x := y\ \text{else}\ x := 0\ \{x = 0\}}\ \text{if}$$

Exemples

Boucle while

$$\dfrac{\dfrac{x \geq 0 \wedge x < 10 \Rightarrow x+1 \geq 0 \qquad \dfrac{}{\{x+1 \geq 0\}\ x := x+1\ \{x \geq 0\}}\ :=}{\{x \geq 0 \wedge x < 10\}\ x := x+1\ \{x \geq 0\}}\ \text{Aff}}{\{x \geq 0\}\ \text{while } x < 10 \text{ do } x := x+1\ \{x \geq 0 \wedge \neg(x < 10)\}}\ \text{while}$$