Sémantiques formelles

David Delahaye

Faculté des Sciences
David.Delahaye@lirmm.fr

Master M1 2017-2018

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 :
  - 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 :

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

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

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

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 « $E \vdash e \rightsquigarrow v_i$ » ;
- Règles :

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

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

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 :

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

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

Exercices

Programmes à évaluer

- $\text{if } x \geq 0 \text{ then } y := x \text{ else } y := -x$ dans les environnements $(x, 2), (y, 0)$ et $(x, -2), (y, 0)$;
- $\text{while } i < 3 \text{ do } (x := x + i; i := i + 1)$ dans l'environnement $(i, 1), (x, 0)$.

Boucle « for »

- Ajouter la boucle « for » à notre langage ;
- Évaluer le programme $\text{for } i := 1 \text{ to } 2 \text{ do } x := x + i$ dans l'environnement $(i, 0), (x, 0)$.

Mécanisation dans le système Coq

Encodage en Coq

- Utilisation des types inductifs (très bon support) ;
- Moyen idiomatique de formaliser en Coq ;
- Types de données inductifs pour la syntaxe (abstraite) ;
- Relations inductives pour la sémantique.

Mécanisation dans le système Coq

Encodage de la syntaxe

- $e ::= n \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 \times e_2 \mid e_1/e_2$
  où $n \in \mathbb{Z}$;
- Code Coq correspondant :

```
Inductive expr : Set :=
  | Cte : Z → expr
  | Plus : expr → expr → expr
  | Moins : expr → expr → expr
  | Mult : expr → expr → expr
  | Div : expr → expr → expr.
```

Mécanisation dans le système Coq

Encodage de la sémantique

- Règles :

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

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

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

Mécanisation dans le système Coq

Encodage de la sémantique

- Code Coq correspondant :

```
Inductive eval : expr → Z → Prop :=
  | ECte : forall c : Z, eval (Cte c) c
  | EPlus : forall (e1 e2 : expr) (v1 v2 : Z),
    eval e1 v1 → eval e2 v2 →
    eval (Plus e1 e2) (v1 + v2)
  | ...
```

Extraction d'interprètes

Interprète

- Code Coq correspondant :

```
Fixpoint f_eval (e : expr) : Z :=
  match e with
  | Cte c ⇒ c
  | Plus e1 e2 ⇒
    let v1 := f_eval e1 in
    let v2 := f_eval e2 in
    v1 + v2
  | ...
```

Correction et complétude

- Correction : soient une expression e et une valeur v, si $f_{\text{eval}}(e) = v$ alors $e \rightsquigarrow v$;
- Complétude : soient une expression e et une valeur v, si $e \rightsquigarrow v$ alors $f_{\text{eval}}(e) = v$.

Exercices

À faire en Coq en TP

- Modéliser la syntaxe abstraite du langage ;
- Donner des exemples de programmes ;
- Modéliser la sémantique du langage ;
- Donner des exemples d'évaluation (lemmes) ;
- Écrire une tactique qui démontre ces lemmes automatiquement ;
- Écrire directement la fonction d'évaluation ;
- Appliquer cette fonction à plusieurs programmes ;
- Démontrer les lemmes de correction et complétude ;
- Réaliser ces modélisations progressivement :
  1. Expressions arithmétiques ;
  2. Expressions arithmétiques avec variables ;
  3. Expressions arithmétiques et booléennes avec variables ;
  4. Expressions et instructions.