Modélisation - Résumé

October 20, 2023

THEVENET Louis

Table des matières

1. Logique propositionnelle

Définition 1.1:

La logique propositionnelle ne parle que de vérité :
- elle ne permet pas de faire référence à des objets, ou à des notions,
- elle ne permet pas de mettre objets ou notions en rapport.

2. Logique des prédicats

Définition 2.1:

C'est l'ajout des quantificateurs, des relations et des structures à la logique propositionnelle.

Extension de la logique des propositions :
- Univers $\mathcal{U}$ (objets mathématiques ou informatiques)
- Algèbre de termes (représentation des objets) : constantes et opérateurs sur $\mathcal{U}$
- Quantificateurs pour variables dans $\mathcal{U}$: $\forall, \exists$
- Relations sur $\mathcal{U}$ (permet aussi de représenter les termes)

Mais aussi :
- $\bot \; \top \neg \wedge \vee \rightarrow \leftrightarrow \mathcal{P}()$
- Ensembles dénombrables de symboles :
  - Variables $\mathcal{V}$
  - Relations (prédicats) $\mathcal{R}$ munie d'une arité $\in \mathbb{N}^*$
  - Propositions $\mathcal{P}$ (relations d'arité 0)
  - Fonctions $\mathcal{F}$ munie d'une arité $\in \mathbb{N}^*$

- Constantes $\mathcal{C}$ (fonctions d'arité 0)

- Lieurs : $\forall, \exists$
- Paramètres des relations et fonctions : (,)

2.1. Ordres de la logique des prédicats

Définition 2.1.1:

- Ordre supérieur : les lieurs peuvent quantifier des termes, des relations, des propositions, des fonctions, des constantes
- Premier ordre (First Order Logic, FOL) : Les lieurs ne peuvent quantifier que des termes
- Second ordre (SOL) : on peut quantifier sur des ensembles de termes

Exemple : du premier ordre avec $\mathcal{V} = \{m, n\}, \mathcal{R}_1 = \{\text{entier}\}, \mathcal{R}_2 = \{\text{egal}\}$

$\forall m.(\text{entier}(m) \rightarrow (\text{impair}(m) \leftrightarrow (\exists n.(\text{entier}(n) \land \text{egal}(m, \text{somme}(\text{produit}(\text{deux}, n), \text{un}))))))$

Exemple : du second ordre avec (g, o) est un groupe

$$\forall g.\forall o.\ \text{groupe}(g, o) \leftrightarrow \begin{cases} \forall x_1.\forall x_2.g(x_1)\land g(x_2)\rightarrow g(o(x_1,x_2)) \\ \land\exists e.g(e)\land \begin{cases} \forall x.g(x)\rightarrow \text{egal}(o(x,e),x)\land \text{egal}(o(e,x),x) \\ \land\forall x_1.\forall x_2.\forall x_3.g(x_1)\land g(x_2)\land g(x_3)\rightarrow \text{egal}(o(o(x_1,x_2),x_3),o(x_1,o(x_2,x_3))) \\ \land\forall x_1.g(x_1)\rightarrow\exists x_2.g(x_2)\land \text{egal}(o(x_1,x_2),e)\land \text{egal}(o(x_2,x_1),e) \end{cases} \end{cases}$$

3. Variables libres

Exemple :

$$\begin{aligned} & \text{VL}(\forall x.(\varphi \leftrightarrow \exists y.\psi)) \\ & = \text{VL}(\varphi \leftrightarrow \exists y.\psi) \setminus \{x\} \\ & = (\text{VL}(\varphi) \cup \text{VL}(\exists y.\psi)) \setminus \{x\} \\ & = (\text{VL}(\varphi) \cup (\text{VL}(\psi) \setminus \{y\})) \setminus \{x\} \end{aligned}$$

4. Substitution

Exemple :

$[f(x,y)/x]$: *$f(x,y)$ remplace x*

$$\begin{aligned}
&[f(x,y)/x]((x \to y) \land \exists y.(x \lor ((\forall x.\varphi) \to y))) \\
&= ([f(x,y)/x](x \to y)) \land [f(x,y)/x](\exists y.(x \lor ((\forall x.\varphi) \to y))) \\
&= ([f(x,y)/x](x) \to [f(x,y)/x](y)) \land [f(x,y)/x](\exists y.(x \lor ((\forall x.\varphi) \to y))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x][z,y](x \lor (((\forall x.\varphi) \to y)))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x]([z,y](x) \lor [z,y](((\forall x.\varphi) \to y)))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x](x \lor ((\forall x.[z/y](\varphi)) \to [z,y](y)))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x](x \lor ((\forall x.[z/y](\varphi)) \to [z,y](y)))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x](x \lor ((\forall x.[z/y](\varphi)) \to z))) \\
&= (f(x,y) \to y) \land (\exists z.[f(x,y)/x](x \lor ((\forall x.[z/y](\varphi)) \to z))) \\
&= (f(x,y) \to y) \land (\exists z.([f(x,y)/x](x) \lor [f(x,y)/x]((\forall x.[z/y](\varphi)) \to z))) \\
&= (f(x,y) \to y) \land (\exists z.(f(x/y) \lor [f(x,y)/x]((\forall x.[z/y](\varphi)) \to z))) \\
&= (f(x,y) \to y) \land (\exists z.(f(x/y) \lor ((\forall x.[z/y]\varphi) \to z)))
\end{aligned}$$

5. Preuves de programme

Exemple : spécification formelle (pré-condition, post-condition)

```
{0 ≤ N}
x := 0;
y := 0;
while x != N do
    y := y + 2 * x + 1;
    x := x + 1
od
{y = N²}
```

5.1. Preuve de correction

Théorème 5.1.1:

- Chaque étape intermédiaire est annotée par une propriété de l'état de la mémoire
- Chaque instruction I est
  - précédée d'une pré-condition φ
  - suivie d'une post-condition ψ
- Chaque instruction annotée doit satisfaire les règles de la logique de Hoare : $\{\varphi\}I\{\psi\}$
  - Correction partielle : φ est satisfaite et l'exécution termine alors ψ est satisfaite après exécution
  - Correction totale : φ est satisfaite alors l'exécution termine et ψ est satisfaite après exécution
- On représente les propriété sur l'état de la mémoire avec la **logique équationnelle** (i.e. premier ordre + spécifications algébriques)

5.1.1. Preuve de correction partielle

Exemple : Preuve de correction **partielle** de l'élevation au carré (invariant : $y = x^2$)

Si on veut que ψ_x soit vraie après avoir fait $(x \leftarrow E)$, il faut que qu'elle soit vraie pour E, i.e., on fait appraître E dans φ (*)

$$
\begin{array}{l}
\{0 \leq N\} \\
\{0 = 0^2\} \\
x := 0; \\
\{0 = x^2\} \\
y := 0; \\
\{y = x^2\} \\
\text{while } x \neq N \text{ invariant } y = x^2 \text{ do} \\
\qquad \{y = x^2 \land x \neq N\} \\
\qquad (*)\{y + 2 \times x + 1 = (x + 1)^2\} \\
\qquad y := y + 2 \times x + 1; \\
\qquad \left\{y = (x + 1)^2\right\} \\
\qquad x := x + 1; \\
\qquad \{y = x^2\} \\
\text{od} \\
\{y = x^2 \land \neg(x \neq N)\} \\
\{y = N^2\}
\end{array}
$$

5.1.2. Preuve de terminaison

Exemple : Preuve de correction **totale** de l'élevation au carré (invariant : $y = x^2$)

Elle sera totale car on a déjà prouvé la correction partielle. On pourrait combiner les preuves en remplaçant les ... par la preuve par invariant précédente.

$\{0 \leq N\}$
$\{... \wedge (N - 0) \in \mathbb{N}\}$
$x := 0;$
$\{... \wedge N - x \in \mathbb{N}\}$
$y := 0;$
$\{N - x \in \mathbb{N}\}$
while $x \neq N$ invariant $y = x^2$ variant $N - x$ do
    $\{... \wedge x \neq N \wedge (N - x) \in \mathbb{N} \wedge V = N - x\}$
    $y := y + 2 \times x + 1;$
    $\{... \wedge (N - (x + 1)) \in \mathbb{N} \wedge N - (x + 1) < V\}$
    $x := x + 1;$
    $\{... \wedge (N - x) \in \mathbb{N} \wedge N - x < V\}$
od
$\{...\}$
$\{y = N^2\}$

Puis

$$0 \leq N \to 0 = 0^2 \wedge (N - 0) \in \mathbb{N}$$

$$\begin{cases} y = x^2 \\ \wedge\, x \neq N \\ (N - x) \in \mathbb{N} \\ (N - x) = V \end{cases} \to \begin{cases} y + 2 \times x + 1 = (x + 1)^2 \\ (N - (x + 1)) \in \mathbb{N} \\ (N - (x + 1)) < V \end{cases}$$

$$y = x^2 \wedge \neg(x \neq N)) \to y = N^2$$