

Certification logicielle - CM

15 novembre 2018

1 Crise du logiciel

- Constat
 - Délais non-tenus
 - budget dépassé
 - qualité médiocre
- Il faut passer de l'artisanat au stade industriel
 - formation des "informaticiens"
 - concevoir des méthodes et des outils de développement

2 Spécifier, c'est difficile

- Spécifications informelles :
 - cahier des charges qui doit être précis, non ambigu, non redondant...
 - prévoir plein de scénarios pour que la correction ne devienne pas de la robustesse
 - est-ce que le logiciel répond au cahier des charges ?
- Spécifications formelles, plusieurs approches :
 - logique
 - algébrique (logique équationnelle avec conditions)
 - basées sur le modèle
 - on peut (essayer de) prouver que le programme répond bien à sa spécif.

3 Certification 2

3.1 Reprise de la logique de Hoare

Rappel : Logique de Hoare \Rightarrow mélange un langage de programmation et des spécifications logiques

Langage ? :

- langage des tant que (jouet - Turing complet)
- langages courants (C, JAVA, PHP, ...)

Définition du langage ;

- syntaxique - grammaire
- sémantique
 - de style sémantique dénotationnelle (mathématique pas trop formel)
 - intuitive
 - opérationnelles (vu tout à l'heure)

Syntaxe :

- id ou variable

— nombres entiers, flottants,

— booléens

Expressions : 2 types (arithmétiques, booléennes)

$$\begin{aligned} &E_a \rightarrow I_d | \\ &\quad Z | \\ &\quad -E_a | \\ &E_a + E_a | E_a - E_a | E_a * E_a | E_a / E_a \end{aligned}$$

Instructions :

$$\begin{aligned} &I \rightarrow skip | \\ &\quad I; I | \\ &if\ E_b\ then\ I\ else\ I | \\ &\quad I_d := E_a | \\ &while\ E_b\ do\ I \end{aligned}$$

Exemple :

$$\begin{aligned} &x := 3 \\ &x := x + 1 \\ &x := 0; x := x + 1 \\ &if\ x < y\ then\ m := x\ else\ m := y \end{aligned}$$

En principe, pour des langages jouets, la sémantique instruite est non ambiguë. Sinon c'est réglé par le manuel de référence ou par des normes.