Méthodes formelles

Daniel Sanz
Université de Fribourg,
daniel.sanz@unifr.ch

March 18, 2020

Abstract

Ceci est un résumé non officiel du cours de méthodes formelles du professeur Ultes Nietzche. Il s'agit principalement de ces slides traduites en français ainsi que quelques exos en guise d'exemple.

Introduction

Les formules logiques, les prédicats entre autres peuvent être utilisés afin d'éxprimer de l'information sur l'état d'un programme. $x = 10$; indique que x doit impérativement avoir la valeur 10.

Pré & post-condition

Définition Une précondition P nous indique ce qui peut être considéré comme vrai avant même l'execution d'une séquence d'instructions S.
Une postcondition Q nous indique ce qui sera vrai après l'execution des instructions S.

Notation On écrit : $\{P\}\ S\ \{Q\}$ qui veut dire que si P est vrai alors, après l'execution de S, Q est vrai. Il s'agit d'un triplet d'Hoarce.

Exemple

$$\{x = 2;\}\ x = x \cdot 3;\ \{x = 6;\}$$

On utilise $\hat{x}$ comme notation de la variable x pour indiquer la valeur de x après l'execution du programme et x avant l'execution.

Exemple

$$\{true\}\ x = x + 1;\ \{\hat{x} > x\}$$
$$\{true\}\ x = x + 1;\ \{\hat{x} = x + 1\}$$

Les assertions

Il est possible d'écrire des prédicats entre deux lignes de code. On présume alors que ce prédicats est la postcondition de la ligne de code précédente et qu'il est la précondition de la ligne suivante.

Définition De tels prédicats sont dits *assertions* ou *annotations*. Pour savoir si des triplets sont corrects il faut tout d'abord transformer le programme S en une formule ϕ_S. Ainsi il est possible de prouver l'exactitude d'un triplet:

$$\{P\}\ S\ \{Q\}$$

en verifiant la formule:

$$P \wedge \phi_S \rightarrow Q$$

ou de façon analogue:

$$\phi_S \rightarrow (P \rightarrow Q)$$

Exemple

$$\{true\}\ x = 10;\ \{x > 0\}$$
$$\phi_S \equiv x = 10$$

donc, $(true \wedge (x = 10)) \rightarrow (x > 10)$.

Exemple

$$\begin{aligned} \{x \neq 0\}\ & x = 1/x; \\ & x = 1/x;\ \{\hat{x} = x\} \end{aligned}$$

Soit $x'' = 1/x$ et $\hat{x} = 1/x''$ alors on vérifie:

$$(x \neq 0) \wedge (x'' = 1/x) \wedge (\hat{x} = 1/x'') \rightarrow \hat{x} = x$$

Ce qui est vrai par du calcul élémentaire. Biensûr, ici on ne tient pas compte de la précision limitée de *floats*.