La logique de Hoare

"Program testing can be used to show the presence of bugs, but never to show their absence !"
Edsger W. Dijkstra

"One does not need to give a formal proof of an obviously correct program ; but one needs a thorough understanding of formal proof methods to know when correctness is obvious."
John C. Reynolds

Schéma d'axiome et schémas de déduction

$$\textsc{Variable Declaration}\ \frac{\Gamma, x \in T \vdash_{\mathrm{TH}} P\,\{C\}\,Q}{\Gamma \vdash_{\mathrm{TH}} P\,\{T\ x; C\}\,Q}\ ^{1}$$

si x ne figure pas librement dans Γ

$$\textsc{Assignment}\ \frac{}{\Gamma \vdash_{\mathrm{TH}} [V/x]P\,\{x := V;\}\,P}$$

si V est librement substituable à x dans P

$$\textsc{Assignment'}\ \frac{}{\Gamma \vdash_{\mathrm{TH}} [V/x]P\,\{x := V;\}\,(P \wedge x = V)}$$

si V est librement substituable à x dans P et x ne figure pas librement dans V.

$$\textsc{Pre-Condition Strengthening}\ \frac{\Gamma \vdash_{\mathrm{TH}} P'\,\{C\}\,Q \qquad \Gamma \vdash_{\mathrm{JZ}} P \Rightarrow P'}{\Gamma \vdash_{\mathrm{TH}} P\,\{C\}\,Q}$$

$$\textsc{Post-Condition Weakening}\ \frac{\Gamma \vdash_{\mathrm{TH}} P\,\{C\}\,Q \qquad \Gamma \vdash_{\mathrm{JZ}} Q \Rightarrow Q'}{\Gamma \vdash_{\mathrm{TH}} P\,\{C\}\,Q'}$$

$$\textsc{Sequencing}\ \frac{\Gamma \vdash_{\mathrm{TH}} P\,\{C_1\}\,Q \qquad \Gamma \vdash_{\mathrm{TH}} Q\,\{C_2\}\,R}{\Gamma \vdash_{\mathrm{TH}} P\,\{C_1 C_2\}\,R}$$

$$\textsc{If-then-else}\ \frac{\Gamma \vdash_{\mathrm{TH}} (P \wedge B)\,\{C_1\}\,Q \qquad \Gamma \vdash_{\mathrm{TH}} (P \wedge \neg B)\,\{C_2\}\,Q}{\Gamma \vdash_{\mathrm{TH}} P\,\{\texttt{if}\ (B)\ \texttt{then}\ C_1\ \texttt{else}\ C_2\}\,Q}$$

$$\textsc{While}\ \frac{\Gamma \vdash_{\mathrm{TH}} (I \wedge B)\,\{C\}\,I}{\Gamma \vdash_{\mathrm{TH}} I\,\{\texttt{while}\ (B)\ C\}\,(I \wedge \neg B)}$$

[1] il en découle que toutes les variables locales doivent être *distinctes*

Commentaires

P, P' (« pre-conditions »), Q, Q', R, (« post-conditions ») et I (« loop invariant ») sont des méta-variables pour des *propositions* de L_{ens}.

C, C_1, et C_2 sont des méta-variables pour des morceaux de *programmes*.

x est une méta-variable pour une *variable de programme*.

T est une méta-variable pour un *type* (ensemble de valeurs).

V est une méta-variable pour une *valeur*.

B est une méta-variable pour une proposition de L_{prop}.

Γ est une méta-variable pour le *contexte* d'un morceau de programme.

$\vdash_{\mathrm{TH}}$ désigne la relation de déduction de la logique de (Tony) Hoare.

$\vdash_{\mathrm{JZ}}$ désigne la relation de déduction de la theorie des ensembles de Jacques Zahnd.

$P\,\{C\}\,Q$ est appelé un *triplet de Hoare*.

$\vdash_{\mathrm{TH}} P\,\{C\}\,Q$ est une assertion de la correction *partielle* (correction *sous l'hypothèse de terminaison*) de C.

La logique de Hoare s'applique à la vérification de la correction partielle des programmes *séquentiels*.

Ses hypothèses de base sont que les programmes à vérifier (1) *terminent* (à démontrer informellement), (2) sont *bien-typés*, (3) sont *correctement compilés*, et (4) sont *correctement exécutés* (système d'exploitation correct, machine correcte).