部分的正当性に関する Hoare論理の体系

割当公理(代入公理)(assignment axiom)

$$\langle\!\langle \phi[E/x] \rangle\!\rangle x=E \langle\!\langle \phi \rangle\!\rangle$$

ただし $\phi[E/x]$は ϕ 中のxをEで置き換えて得られる命題

backward substitution

実行前のxの値をx_I, 実行後をx_Oとする（I: input, O: output）

$\phi[x_O/x]$かつ$x_O=E[x_I/x]$ならば $\phi[E[x_I/x]/x]$

$\phi[E[x_I/x]/x]$かつ$x_O=E[x_I/x]$ならば $\phi[x_O/x]$

すなわち ⟪ $\phi[E/x]$ ⟫ x=E ⟪ ϕ ⟫

例

⟪ 5=5 ⟫x=5 ⟪ x=5 ⟫

⟪ x+3=10 ⟫ x=x+3 ⟪ x=10 ⟫

⟪ x+y>y ⟫ x=x+y ⟪ x>y ⟫

$x_O>y_I \wedge x_O=x_I+y_I \supset x_I+y_I>y_I$

$x_I+y_I>y_I \wedge x_O=x_I+y_I \supset x_O>y_I$

割当公理の健全性

⟪ ϕ[E/x] ⟫x=E⟪ ϕ ⟫に対して,

論理変数に対するどのような附値 ρ^{L} および,

プログラム変数に対するどのような状態(附値)ρ, ρ'に対しても

$\rho^{L},\rho \models \phi[E/x]$かつ$\mathrm{Exec}_{M}(x{=}E, \rho, \rho')$ならば $\rho^{L},\rho' \models \phi$

を示せばよい.

$\rho^{L},\rho \models \phi[E/x]$とする. 実行関係の定義より$\mathrm{Exec}_{M}(x{=}E, \rho, \rho[M[E]_{\rho}/x])$となる.

ところが $\rho^{L},\rho \models \phi[E/x]$と $\rho^{L},\rho[M[E]_{\rho}/x] \models \phi$は同値.

(∵)どちらも ϕ中のxを ρで解釈したEの値で代入した式を解釈している

したがって $\rho^{L},\rho[M[E]_{\rho}/x] \models \phi$がいえるので正しい.

（参考）割当公理(assignment axiom) forward substitution

$\langle\!\langle \phi \rangle\!\rangle$ x=E $\langle\!\langle \exists y(\phi[y/x] \wedge x=E[y/x]) \rangle\!\rangle$

R. W. Floyd (1967), “Assigning meanings to programs”,
Proceedings of the American Mathematical Society Symposia on Applied Mathematics 19: 19–31.
https://people.eecs.berkeley.edu/~necula/Papers/FloydMeaning.pdf

代入文は数学では$x_O=E[x_I/x]$の意味. したがって，$\phi[x_I/x] \wedge x_O=E[x_I/x]$

例

$\langle\!\langle x=3 \rangle\!\rangle$ x=x+4 $\langle\!\langle \exists y(y=3 \wedge x=y+4) \rangle\!\rangle$

postconditionは$x=3+4$と同値

連結規則 (composition rule)

前件(antecedent)

$$\dfrac{\langle\!\langle \phi \rangle\!\rangle C_1 \langle\!\langle \phi_1 \rangle\!\rangle \quad \langle\!\langle \phi_1 \rangle\!\rangle C_2 \langle\!\langle \phi_2 \rangle\!\rangle \quad \ldots \quad \langle\!\langle \phi_{n-1} \rangle\!\rangle C_n \langle\!\langle \psi \rangle\!\rangle}{\langle\!\langle \phi \rangle\!\rangle C_1; \ldots ; C_n \langle\!\langle \psi \rangle\!\rangle}$$

後件(consequent)

演習問題

以下を証明せよ.

ただし変数は全て自然数を領域とするプログラム変数とする.

$$\vdash_{par} (\!(x=a \wedge y=b)\!)\ z=x;\ x=y;\ y=z\ (\!(y=a \wedge x=b)\!)$$

条件規則(conditional rule)

$$\frac{⟪ B\land\phi ⟫\, C1\, ⟪ \phi ⟫ \qquad \neg B\land\phi\supset\phi}{⟪ \phi ⟫\ \text{if } B\ \{C1\}\ ⟪ \phi ⟫}$$

$$\frac{⟪ B\land\phi ⟫\, C1\, ⟪ \phi ⟫ \quad ⟪ \neg B\land\phi ⟫\, C2\, ⟪ \phi ⟫}{⟪ \phi ⟫\ \text{if } B\ \{C1\}\ \text{else}\ \{C2\}\ ⟪ \phi ⟫}$$

例

$⟪ -x=x_0 ⟫\ x=-x\ ⟪ x=x_0 ⟫$

?↓

$$\frac{⟪ |x|=x_0\land x<0 ⟫\ x=-x\ ⟪ x=x_0 ⟫ \qquad |x|=x_0\land x\geq 0\supset x=x_0}{⟪ |x|=x_0 ⟫\ \text{if } (x<0)\ \{x=-x\}\ ⟪ x=x_0 ⟫}$$

帰結規則(consequence rule)

$$\frac{\phi_1 \supset \phi_2 \quad \langle\!\langle \phi_2 \rangle\!\rangle P \langle\!\langle \phi_1 \rangle\!\rangle \quad \phi_1 \supset \phi_2}{\langle\!\langle \phi_1 \rangle\!\rangle P \langle\!\langle \phi_2 \rangle\!\rangle}$$

$\phi_1 \supset \phi_2$, $\phi_1 \supset \phi_2$ 検証条件 (verification conditions)

例

$$\frac{\langle\!\langle -x=x_0 \rangle\!\rangle\ x=-x\ \langle\!\langle x=x_0 \rangle\!\rangle}{\langle\!\langle |x|=x_0 \wedge x<0 \rangle\!\rangle\ x=-x\ \langle\!\langle x=x_0 \rangle\!\rangle}$$

(∵ $|x|=x_0$ かつ $x<0$ ならば $-x=x_0$)

ϕがψより弱い(weaker)とは ψから ϕが導出できる, つまり$\psi \supset \phi$が成り立つ
(または, ここで用いている論理と数学で証明できる)ことである.
このとき ψは ϕより強い(stronger).

弱いとはより一般的(general)な表明であり,
強いとはより特殊(specific)な表明のことである。

最弱前条件 weakest precondition
最強後条件 strongest postcondition

演習問題

以下を証明せよ.

ただし変数は全て自然数を領域とするプログラム変数とする.

$$\vdash_{par} ⦇ a=x+1 ⦈ \mathrm{if}(a-1==0)\{y=1\}\mathrm{else}\{y=a\} ⦇ y=x+1 ⦈$$

while規則(while rule)

$$\frac{⦅\eta \wedge B⦆\ C\ ⦅\eta⦆}{⦅\eta⦆\ \text{while } B\ \{C\}\ ⦅\eta \wedge \neg B⦆}$$

このような η をループ不変表明(loop invariant assertion)という

演習問題

以下を証明せよ.

ただし変数は全て自然数を領域とするプログラム変数とする.

$$\vdash_{par} (\!|\ y=1 \wedge z=0 |\!) \texttt{while (z!=x) \{z=z+1;y=y*z \}} (\!|\ y=x!\ |\!)$$

演習課題

以下を証明せよ.

ただしx, yは全て自然数を領域とするプログラム変数

x_0は自然数を領域とする論理変数とする.

$$\vdash_{par} \llparenthesis x=x_0 \wedge y=1 \rrparenthesis \text{while } (x!=0)\ \{y=y*x;\ x=x-1\} \llparenthesis y=x_0! \rrparenthesis$$

演習課題

以下を証明せよ.

ただし変数は全て自然数を領域とするプログラム変数とする.

$$\vdash_{par} ⦇a=0 \wedge z=0⦈ \mathrm{while}\ (a!=y)\ \{z=z+x;\ a=a+1\} ⦇z=x \cdot y⦈$$

Hoare論理の健全性

定理

Hoare論理がモデルMに対して健全である ⇔

帰結規則で用いた全ての命題(検証条件) $\phi_1 \supset \phi_2$, $\phi_1 \supset \phi_2$がMによって充足可能である.

Hoare論理の証明能力

whileプログラムに対するHoare論理の相対完全性

部分正当性の意味での正しい表明付きwhileプログラムは, whileプログラムのHoare論理で証明できる.

完全正当性についても同様である.

但し, 正しい数学の定理ならばどんなものでも

帰結規則で用いる第1, 第3の前提(検証条件 A⊃B, C⊃D)として用いても良い(相対性)

Hoare論理の証明能力

Clarkeの不完全性定理

- Algol-likeなプログラム言語に対しては,
- 健全かつ相対完全なHoare論理を作ることができない
  - Algol-like:
    - 手続きが定義できる, 局所手続きもできる
    - 手続きを手続きの引数として渡せる
    - 再帰呼出しができる
    - 静的スコープルールが使える
    - 大域変数が使える

レポート問題

以下を証明せよ.

ただしx, yは全て自然数を領域とするプログラム変数

x_0は自然数を領域とする論理変数とする.

$$\vdash_{par} ⦅y=0 \wedge x=x_0⦆ \mathrm{while}\ (x>0)\ \{y=y+x;\ x=x-1\} ⦅y=x_0(x_0+1)/2⦆$$

締切　7月30日(水)15:15

提出先　manaba