完全正当性の形式的理論THL(PV, AV, I)

PV, AV: PHLのときと同じ

I: 論理式の解釈(interpretation)

定数, 関数記号, 述語記号に意味を与える

例：$I(\leq)$=”≤”, $I(+)$=”+”, $I(\cdot)$=”・”, $I(0)$=”0”, ...

ρ: 変数への値の割当(assignment)

例：$\rho(x)$=”3”, $\rho(y)$=”2”, ...

項tの解釈 $I_\rho[t]=$

$I(t)$	tが定数のとき
$\rho(t)$	tが変数のとき
$I(f)(I_\rho[t_1], \ldots, I_\rho[t_n])$	tが$f(t_1, \ldots, t_n)$のとき

論理式の解釈

$I_\rho[F]=$

$I(p)\ (I_\rho[t_1], \ldots, I_\rho[t_n])$	Fが$p(t_1, \ldots, t_n)$ (原子論理式)のとき
$\wedge\cdot(I_\rho[F_1], I_\rho[F_2])$	Fが $F_1 \wedge F_2$のとき $\wedge\cdot$: $\wedge$の真理関数
$\forall\cdot(\{I_{\rho[a/x]}[F_1] \mid a \in D\})$	Fが$\forall x\ F_1$のとき
... (以下同様)	

論理式の解釈

$I_\rho[F]=$ $I(p)\,(I_\rho[t_1], \ldots, I_\rho[t_n])$ Fが$p(t_1, \ldots, t_n)$ (原子論理式)のとき

$\wedge\cdot(I_\rho[F_1], I_\rho[F_2])$ Fが $F_1 \wedge F_2$のとき $\wedge\cdot$: $\wedge$の真理関数

$\forall\cdot(\{I_{\rho[a/x]}[F_1] \mid a \in D\})$ Fが$\forall x\ F_1$のとき

... (以下同様)

整礎表明(well-founded assertion)

集合B上の2項関係W(x, y)が**整礎(well-founded)**である

⇔ W(x_i, x_{i+1})であるような無限列x_0, x_1, ..., x_i, ...(無限降下列)が

存在しない

例:　集合N上の2項関係>は整礎である.

集合Z上の2項関係>は整礎でない.

Rが**整礎表明(well-founded assertion)**である

⇔Rが, 整礎であるようなW(x, y)を含む解釈Iで成立つ

※「解釈Iで成立つ」のかわりに

「非論理的公理Sをもつ形式的理論で証明できる」として理論を構成することは困難

問題

集合N×N上の2項関係$<_2$を

$(x_1, y_1)<_2(x_2, y_2) \Leftrightarrow y_1< y_2$または $(y_1= y_2$かつ $x_1< x_2)$

(ここで“<”は自然数上の通常の不等号)

と定義するとこれは整礎である.

このことを証明せよ.

(ヒント:無限降下列が存在しない(存在すると矛盾する)

ことを示す)

THL(PV, AV, I)の公理と推論規則

while文の規則以外の公理と推論規則はPHLのときと同じ

R_{wh}は以下のR_{twh}に変更

$$\frac{< t_1=p_1 \wedge \ \ldots \ \wedge t_n=p_n \wedge C \wedge A > P < R[t_1/p'_1, \ldots, t_n/p'_n] \wedge A >}{<A>\text{while } C \text{ do } P \text{ od}<\neg C \wedge A>}$$

ただし,

- Rは$<p_1, \ldots, p_n>, <p'_1, \ldots . p'_n>$に対して整礎表明
- $t_1, \ldots, t_n$はプログラム変数を含んだ項
- $p_1, \ldots, p_n, p'_1, \ldots . p'_n$は論理変数, A, C, $t_1, \ldots, t_n$に出現しない

演習

<y=1∧z=0> while z≠x do begin z:=z+1;y:=y*z end <y=x!>

の形式的証明をせよ

プログラムの意味

形式化されたHoare論理PHL(PV, AV, S), THL(PV, AV, I)の性質(完全性, 健全性等)を考える際に

対象となるプログラムの「意味」(semantics)を与えなければならない.

プログラムの実行
(Execution)

ρ: 状態(state)

プログラム変数xから値 ρ(x) への関数

プログラムの実行でρが変化する　ρ→ρ': 遷移

プログラムの実行(execution)

$\rho_0 \rightarrow \rho_1 \rightarrow \rho_2 \rightarrow \rho_3 \rightarrow \ldots \rightarrow \rho_i \rightarrow \rho_{i+1} \ldots$

ρ_0 : 初期状態

プログラムの実行関係
(Execution Relation)

関係$Exec_I(P, \rho, \rho')$でプログラムPの実行によるρからρ'への遷移を与える

$Exec_I(skip, \rho, \rho') \quad \Leftrightarrow \rho'=\rho$

$Exec_I(x:=t, \rho, \rho') \quad \Leftrightarrow \rho'=\rho[I\rho[t]/x]$

すなわち

$$\rho'(y)= \begin{cases} \rho(y) & \text{if yが変数xでないとき} \\ I\rho[t] & \text{if yがxのとき} \end{cases}$$

ここで$I\rho[t]$は解釈Iおよび状態ρのもとでのtの値

$Exec_I(\text{if C then P else P' fi}, \rho, \rho') \Leftrightarrow$

$$\begin{cases} I, \rho I=C \Rightarrow ExecI(P, \rho, \rho'), & \text{ここで } I, \rho I=C\text{は解釈Iと状態}\rho\text{のもとでCが成立つ} \\ I, \rho I \neq C \Rightarrow ExecI(P', \rho, \rho') \end{cases}$$

$Exec_I(\text{begin P1; ... ; Pn end}, \rho, \rho') \quad \Leftrightarrow$

ある$\rho_1,..., \rho_{n-1}$が存在して $ExecI(P1, \rho, \rho_1), ... , ExecI(P_n, \rho_{n-1}, \rho')$

$Exec_I(\text{while C do P od}, \rho, \rho') \Leftrightarrow$

ある$m>0$および$\rho_1,..., \rho_m$が存在して，$\rho=\rho_1, \rho'=\rho_m$,

$I, \rho_m I \neq C$，m未満の全てのiで $I, \rho_i I=C$かつ $ExecI(P, \rho_i, \rho_{i+1})$

プログラムの実行関係
(Execution Relation)

関係 $Exec_I(P, \rho, \rho')$でプログラムPの実行によるρからρ'への遷移を与える

$Exec_I$(begin P1; ... ; Pn end, ρ, ρ') ⇔

ある$\rho_1,..., \rho_{n-1}$が存在して $Exec_I(P_1, \rho, \rho_1), ... , Exec_I(P_n, \rho_{n-1}, \rho')$

$Exec_I$(while C do P od, ρ, ρ') ⇔

ある$m>0$および$\rho_1,..., \rho_m$が存在して, $\rho=\rho_1$, $\rho'=\rho_m$,

I, ρ_mI⊭C, m未満の全てのiで I, ρ_iI=Cかつ $Exec_I(P, \rho_i, \rho_{i+1})$

表明付きプログラムの意味

{A}P{B}の解釈 I に対する部分的正当性は

　　どんなρ, ρ’に対してもI, ρI=AかつExec$_I$(P, ρ, ρ’)ならばI, ρ’I=B

と定義する.

これを　I I= {A}P{B}　と表す.

解釈Iが明らかな場合はIを省略する.

健全性と完全性

PHL(PV, AV, S)が解釈Iに対して**健全(sound)**

⇔

PHL(PV, AV, S) |- {A}P{B}ならば必ずI |= {A}P{B}

(証明可能ならば正しい)

PHL(PV, AV, S)が解釈Iに対して**完全(complete)**

⇔

I |= {A}P{B}ならば必ず PHL(PV, AV, S) |- {A}P{B}

(正しいならば証明可能)

部分的正当のHoare論理の健全性

定理

PHL(PV, AV, S)が解釈Iに対して健全である ⇔ Sの任意の表明AについてI I= A

証明

(⇒)AがSの要素ならばSI-true⊃A.　よってPHL(PV, AV, S)I-{true}skip{A}.

したがってPHL(PV, AV, S)が健全ならばII={true}skip{A}.

{true}skip{A} の意味より

どんなρについてもI, ρI=trueかつ$Exec_I$(skip, ρ, ρ)ならばI, ρI=A

がいえるのでどんなρについてもI, ρ I= A.　すなわちI I= A.

(<=)証明の長さの帰納法による.

1行目からn-1行目までの表明付きプログラムが正しいとし,

n行目の表明付きプログラム {A}P{B} が正しいこと，すなわち

どんなρ, ρ'に対してもI, ρI=AかつExec$_I$(P, ρ, ρ')ならばI, ρ'I=B

を示す.

{A}P{B}の場合分けを行う.

・n行目が代入公理{A[t/x]}x:=t{A}のとき

ρ I= A[t/x]とする．実行関係の定義よりExec(x:=t, ρ, ρ[I$_ρ$[t]/x])となる.

ところが ρ I= A[t/x]と ρ[I$_ρ$[t]/x]I=Aは同値.

(∵)どちらもA中のxをρで解釈したtの値で代入した式を解釈している

したがってρ[I$_ρ$[t]/x]I=Aがいえるので正しい.

・n行目がwhile規則で導出された{A} while C do P od {¬C ∧ A}のとき

ρ I= A ... (1)
および

Exec(while C do P od , ρ, ρ') ... (2)
よりρ' I= ¬C ∧ Aを示す.

帰納法の仮定よりn-1行目以前に{C∧A}P{A}が証明されていて正しい. すなわち

I I= {C∧A}P{A} ... (3).
(2)より ρ=ρ_1, ρ'=ρ_m, ρ'I=¬C, m未満の全てのiで ρ_iI=Cかつ $Exec_I(P, \rho_i, \rho_{i+1})$

なる状態列ρ_1,..., ρ_mが存在する.

これと(1)(3)よりm以下の全てのiでρ_iI=Aとなる.

したがって ρ'I=¬C∧Aである.

・他の公理, 規則の場合も同様.

(証明終)

演習

n行目が {A} if C then P_1 else P_2 fi {B} (条件文の規則)

の場合について示せ.

・n行目が条件文の規則で導出された {A} if C then P_1 else P_2 fi {B} のとき

ρ I= A ... (1)
および

Exec(if C then P_1 else P_2 fi, ρ, ρ') ... (2)
よりρ' I= B を示す.

帰納法の仮定よりn-1行目以前に{C∧A} P_1{B}および {¬C∧A} P_2{B} が証明されていて
正しい. すなわち
I I= {C∧A} P_1{B} ... (3), I I= {¬C∧A} P_2{B} ... (4).

(2)より ρI=C ならば $Exec_I(P_1, ρ, ρ')$... (2'), および ρI=¬C ならば $Exec_I(P_2, ρ, ρ')$... (2")
一方(3)より ρI=C∧Aかつ $Exec_I(P_1$ ρ, ρ') ならば ρ'I=B... (3')
(4)より ρI=¬C∧Aかつ $Exec_I(P_2, ρ, ρ')$ ならば ρ'I=B... (4')
よって(1)(2')(3')より ρI=C ならば ρ'I=B, (1)(2")(4')より ρI=¬C ならば ρ'I=B
したがって ρ'I=B.

部分的正当のHoare論理の完全性

Hoare論理PHL(PV, AV, I)は充分な記述能力を持てば解釈Iに対して完全である.

すなわち, I I= {A}P{B}ならばPHL(PV, AV, I) I- {A}P{B}である.

ただし,

最弱前条件(weakest precondition) $pwp_I(P, B)$

$pwp_I(P, B) = \{\rho \mid Exec_I(P, \rho, \rho')$なるどんな$\rho'$に対しても, $I, \rho' I=B \}$

表明Aが状態集合Sを**表現できる(representable)**⇔

与えられた語彙の範囲でS={ρ I I, ρI=A}なる表明Aが存在する

PHL(PV, AV, I)が**十分な記述能力を持つ(expressive)**⇔

どんなプログラムPと表明Bに対しても$pwp_I(P, B)$を表現できる表明が存在する

なお,

φがψより**弱い(weaker)**とは, ψからφが導出できる, つまりψ⊃φ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.

定理

Hoare論理PHL(PV, AV, I)は充分な記述能力を持てば解釈Iに対して完全である.

すなわち, I I= {A}P{B}ならばPHL(PV, AV, I) I- {A}P{B}である.

証明

PHL(PV, AV, I)が十分な記述能力を持つと仮定する.

最弱前条件の特性

$$I \models \{A\}\ P\ \{B\} \Leftrightarrow \text{すべての}\rho\text{に関して}(\ I\ ,\ \rho \models A \Rightarrow \rho \in pwp(P, B)\ )$$

(ただし $pwp_I(P, B) = \{\rho \mid Exec_I(P, \rho, \rho')$なるどんなρ'に対しても, I, ρ'I=B $\}$)

と実行関係$Exec_I(P, \rho, \rho')$の特徴

$$Exec_I(skip, \rho, \rho') \Leftrightarrow \rho'=\rho$$

$Exec_I$(while C do P od, ρ, ρ') ⇔あるm>0および$\rho_1,\ldots, \rho_m$が存在して,

$\rho=\rho_1$, $\rho'=\rho_m$, I, ρ_mI=C, m未満の全てのiで I, ρ_iI=Cかつ $Exec_I(P, \rho_i, \rho_{i+1})$

など

を用いて, Pの構造による帰納法を用いて I= {A}P{B}ならばI- {A}P{B} を示す.

Pが代入文のとき

仮定は$\models \{A\}x:=t\{B\}$. したがって $\rho \models A \Rightarrow \rho \in pwp(x:=t, B)$.

ところがpwpとExecの関係, および代入の性質により

$$\rho \in pwp(x:=t, B) \Leftrightarrow \rho[I_\rho[t]/x] \models B \Leftrightarrow \rho \models B[t/x]$$

したがって,

$$\models A \supset B[t/x]$$

よって, 代入公理 $\vdash \{B[t/x]\}x:=t\{B\}$と帰結規則より $\vdash \{A\}x:=t\{B\}$も導ける.

Pがskip文のとき

同様.

Pが複合文 begin P_1; P_2 end のとき

仮定は$\models$ {A} begin P_1; P_2 end {B}.

最弱前条件の性質から

$\models$ {pwp(P_1, pwp(P_2, B))}P_1{pwp(P_2, B)} および $\models$ {pwp(P_2, B)}P_2{B}

がいえる.

帰納法の仮定より

$\vdash$ {pwp(P_1, pwp(P_2, B))P_1{pwp(P_2, B)} および $\vdash$ {pwp(P_2, B)}P_2{B}

が成り立つ.

したがって複合文の規則より

$\vdash$ {pwp(P_1, pwp(P_2, B))} begin P_1; P_2 end{B}

ここで, Exec(begin P_1; P_2 end, ρ, ρ')とpwpの定義より

ρ$\models$pwp(begin P_1; P_2 end, B)⇔ρ$\models$ pwp(P_1, pwp(P_2, B))

がいえる.

したがって

$\models$ A⊃pwp(P_1, pwp(P_2, B))

となるため. 帰結規則より $\vdash$ {A} begin P_1; P_2 end {B}もいえる.

Pがif, whileの場合も同様である.

完全正当性の意味論

状態ρを初期状態とするPの実行列が必ず有限になるとき

ρからPの実行は**停止(terminate)する**という.

I, ρI={A}P{B}が成り立ち，ρからPの実行が停止するとき,

<A>P<B>は解釈Iと状態ρに対して正しいといい,

I，ρI=<A>P<B>

と表す.

任意のρに対して<A>P<B>が正しいとき，<A>P<B>は解釈Iに対して正しいといい,

I I=<A>P<B>

と表す.

完全正当のHoare論理の健全性

THL(PV, AV, I)が健全であるとは,

THL(PV, AV, I) |- <A>P<B> ならば I |= <A>P<B> となることである.

定理

THL(PV, AV, I)は解釈Iに対して健全である.

完全正当のHoare論理の完全性

Hoare論理THL(PV, AV, I)は相対完全であるとは，THL(PV, AV, I)が十分な記述能力を持つとき，
以下のことが成り立つときをいう.

$I \models \langle A\rangle P\langle B\rangle$ならばTHL(PV, AV, I) $\vdash \langle A\rangle P\langle B\rangle$

ただし，

最弱前条件(weakest precondition) $twp_I(P, B)$

$twp_I(P, B) = \{\rho \mid \exists\rho' Exec_I(P, \rho, \rho') \wedge \rho \in pwp_I(P, B)\}$

これは

$I \models \langle A\rangle P\langle B\rangle \Leftrightarrow \forall\rho'(I, \rho' \models A \supset (\rho' \in twp_I(P, B)))$

を満たす.

THL(PV, AV, I)が**十分な記述能力を持つ(expressive)**⇔

どんなプログラムPと表明Bに対しても$twp_I(P, B)$を表現できる表明が存在する

定理

THL(PV, AV, I)は充分な記述能力を持てばそれはIに対して完全である.

すなわち

I |= <A>P<B>ならばTHL(PV, AV, I) |- <A>P<B>

である.