Hoare 論理 (2)

- プログラム証明と構築のための手法と論理 -

東京大学計数工学科
胡 振江
hu@mist.i.u-tokyo.ac.jp

復習：部分正当性の証明

部分的正当性の表明例

```
{N>=0}
i := 1;
f := 1;
While i<=N Do
  f := f*i;
  i := i+1
End
{f=N!}
```

部分的正当性の証明

プログラムにかかわる公理と推論規則：
* 代入文の公理
* 複合文の規則
* if 文の規則
* while 文の規則
* 帰結の規則

第一階述語論理の拡張

復習：代入文の公理

{Q[e/x]} x := e {Q}

復習：複合文の推論規則

{P} S1 {R}   {R} S2 {Q}

{P} S1; S2 {Q}

復習：if 文の規則

{P and B} S1 {Q}   {P and not B} S2 {Q}

{P} If B Then S1 Else S2 End {Q}

復習：while 文の規則

{P and B} S {P}

{P} While B Do S End {P and not B}

復習：帰結の規則

P ➔ P1　{P1} S {Q1}　Q1 ➔ Q

{P} S {Q}

言語の拡張：配列要素への代入文

S ::= x := e　　　　代入文
　| a(e1) := e2　　　配列要素への代入文
　| S1 ; S2　　　　複合文
　| If B Then S1 Else S2 End　　if 文
　| While B do S End　　while文

問題点

配列変数を使うと，複雑になる.

{x(1)=1 and x(2)=3}

x(x(1)) := 2

{x(x(1))=2}

No!!!

代入によってx(1)も変わるので，結果は3である.

配列要素への代入文の公理

{ Q[(if z=e1 then e2 else a(z) end)/a(z)] }

a(e1) := e2

{Q}

配列要素に対する置換処理

2段階置換：
tに対する置換;
配列要素a[t]に対する置換

a(t)[(if z=e1 then e2 else a(z) end)/a(z)]

= (if z=e1 then e2 else a(z) end)

[t[(if z=e1 then e2 else a(z) end)/a(z)]/z]

例題1：配列要素への代入

{ j=i or a(j)=1 }　a(i) := 1　{ a(i)=a(j) }　を証明せよ

{ j=i or a(j)=1 }

➔

{(a(i)=a(j))[(if z=i then 1 else a(z) end)/a(z)]}

(a(i)=a(j))[(if z=i then 1 else a(z) end)/a(z)]

↔

a(i)[(if z=i then 1 else a(z) end)/a(z)]

= a(j)[(if z=i then 1 else a(z) end)/a(z)]

↔

(if z=i then 1 else a(z) end)[i[(if z=i then 1 else a(z) end)/a(z)]/z]

= (if z=i then 1 else a(z) end)[j[(if z=i then 1 else a(z) end)/a(z)]/z]

↔

(if z=i then 1 else a(z) end)[i/z] = (if z=i then 1 else a(z) end)[j/z]

(if z=i then 1 else a(z) end)[i/z] = (if z=i then 1 else a(z) end)[j/z]
←→
(if i=i then 1 else a(i) end) = (if j=i then 1 else a(j) end)
←→
1 = (if j=i then 1 else a(j) end)
←→
(j=i => 1=1) and (j<>i => 1=a(j))
←
j=i or a(j)=1

例題2

配列要素への代入 a(a(2)):=1 に対する部分的正当性の表明

{ a(2)<>2 or a(1)=1 } a(a(2)) := 1 { a(a(2))=1 }

を示す。公理より、

{(a(a(2))=1)[(if z=a(2) then 1 else a(z) end)/a(z)]}

a(a(2)) := 1

{a(a(2))=1}

すると、

{ a(2)<>2 or a(1)=1 }

→ (a(a(2))=1)[(if z=a(2) then 1 else a(z) end)/a(z)]

を示せればよい。

(a(a(2))=1)[(if z=a(2) then 1 else a(z) end)/a(z)]
←→ a(a(2))[(if z=a(2) then 1 else a(z) end)/a(z)] = 1
←→ (if z=a(2) then 1 else a(z) end)
[a(2)[(if z=a(2) then 1 else a(z) end)/a(z)] /z] = 1
←→ (if z=a(2) then 1 else a(z) end)
[((if z=a(2) then 1 else a(z) end)
[2[(if z=e1 then e2 else a(z)end)/a(z)]/z]) /z] = 1
←→ (if z=a(2) then 1 else a(z) end)
[((if z=a(2) then 1 else a(z) end)[2/z])/z] = 1

←→ (if z=a(2) then 1 else a(z) end)
[((if z=a(2) then 1 else a(z) end)[2/z])/z] = 1
←→ (if z=a(2) then 1 else a(z) end)
[(if 2=a(2) then 1 else a(2) end)/z] = 1
←→ (if 2=a(2) then (if 1=a(2) then 1 else a(1) end)
else (if a(2)=a(2) then 1 else a(a(2)) end) end) = 1
←→ (if 2=a(2) then (if 1=a(2) then 1 else a(1) end) else 1 end) = 1
←→ if 2=a(2) then a(1)=1 else 1=1 end
← a(2)<>2 or a(1)=1

Dijkstra's WP

- Weakest Precondition (WP)

Total correctness

wp(S,Q):

the set of initial states that this guarantee termination of S in a state satisfying Q

$$\frac{P \Rightarrow wp(S,Q)}{\{P\}\ S\ \{Q\}}$$

WPの定義

wp(x:=e, Q) ≡ Q(e/x)
wp(S1;S2, Q) ≡ wp(S1, wp(S2, Q))
wp(If B Then S1 Else S2 End, Q)
≡ (B→wp(S1,Q)) and (not B → wp(S2,Q)
wp(While B do S End, Q) ≡ ∃k:k>=0. P_k
where P_0 = (not B) and Q
P_k = B and wp(S,P_{k-1})

例

wp(x:=x+1; y:=y+1, x=y)
≡ wp(x:=x+1, wp(y:=y+1, x=y))
≡ wp(x:=x+1, x=y+1)
≡ x+1=y+1
≡ x=y

例

wp(If i=j Then m:=k else j:=k End, k=j=m)
= (i=j ➔ wp(m:=k,k=j=m)) and
(i/=j ➔ wp(j:=k, k=j=m))
= (i=j ➔ k=j=k) and (i/=j ➔ k=k=m))
= (i=j ➔ k=j) and (i/=j ➔ k=m))

例

次のWPを求めよ.
wp(W, Q)
where W = While n<>m do S End
S = j:=j*i; k:=k+j; n:=n+1
Q = k=(i^(m+1)-1)/(i-1) and j=i^m
ただし，i<>0 and i<>1.

P0 ≡ not (n<>m) and Q
≡ n=m and k=(i^(m+1)-1)/(i-1) and j=i^m

P1 ≡ n<>m and wp(S,P0)
≡ n<>m and n+1=m and
k+j*i=(i^(m+1)-1)/(i-1) and j*i=i^m
≡ n=m-1 and k=(i^m-1)/(i-1) and j=i^(m-1)
≡ n=m-1 and k=(i^m-1)/(i-1) and j=i^n

P2 ≡ n=m-2 and k=(i^m-1)/(i-1) and j=i^n
...
Pr ≡ n=m-r and k=(i^m-1)/(i-1) and j=i^n

従って:
wp(W,Q)
≡ ∃r:r>=0. Pr
≡ n=m-r and k=(i^m-1)/(i-1) and j=i^n

演習問題3

次のWPを計算せよ.
wp(While i<>n do i:=i+1;s:=s+i End,
s=n*(n+1)/2)

WP's Healthiness Conditions

wp(S, Q and R) ≡ wp(S,Q) and wp(S,R)
wp(S, Q or R) ≡ wp(S,Q) or wp(S,R)
wp(S, not Q) ≡ not wp(S,Q)

wp(S, false) ≡ false
wp(S, true) = all states that guarantee termination of S

演習問題4

次のことを証明せよ.

wp(S,Q➔R) ➔ (wp(S,Q) ➔ wp(S,R))