Hoare 論理 (3)

- プログラム証明と構築のための手法と論理 -

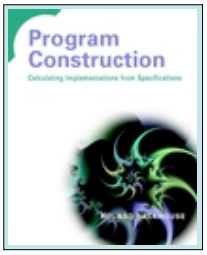
東京大学計数工学科
胡 振江
hu@mist.i.u-tokyo.ac.jp

参考書

Program Construction : Calculating Implementations from Specifications

Roland Backhouse, ISBN: 0-470-84882-0, 352 pages, May 2003, US $45.00

9章，10章，13章



（正しい）プログラムの構成

Given P,Q, construct a program S such that

{P} S {Q}

仕様: {P} S {Q}, Sは未知

実現: Sの導出

仕様の例

- {true} S {i=j}
- {i<5} S {i<10}
- {i+j=C} i:=i+1; S {i+j=C}
- {s=n^2} S; n:=n+1 {s=n^2}
- {true} S {z=max(x,y)}
- {0<m=M} S {m=M÷2}
- {0<N} S {s=∑i|0<=i<N:a[i]}
- {0<N} S {s=∑i|0<=i<N:a[i]*X^i}

(C,M,N,Xは定数)

復習：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})

代入文の導出

- 問題:
  仕様{P} x:=e {Q}を満たすeを導出せよ.
- 方法:
  Match wp(x:=e,Q) with P to obtain the definition for e.

代入文の導出:例1

仕様: {true} i := e {i=j}

wp(i:=e,i=j) ≡ e=j
P ≡ true ≡ j=j

match

e = j

代入文の導出:例2

仕様:{i+j=C} i:=i+1; j:=e {i+j=C}

wp(i:=i+1; j:=e, i+j=C) ≡ i+1+e=C
P ≡ i+j=C ≡ i+1+j-1=C

match

e = j-1

演習問題5

以下の仕様を満たすeを求めよ.
(1) {i<5} i:=e {i<10}
(2) {s=n^2} s:=e; n:=n+1 {s=n^2}

条件文の導出

- 問題:
  仕様{P} If B Then S1 Else S2 End {Q} を満たすB,S1,S2を求めよ.
- 方法:
  - Bを決める
  - {P and B}S1{Q}を満たすS1を求める.
  - {P and not B}S2{Q}を満たすS2を求める.

条件文の導出:例

仕様:{true} If B then S1 else S2 End {z=max(x,y)}

導出

Step 1: B ≡ x >= y (creative step)

Step 2: {x >= y} S1 {z=max(x,y)}
を満たすS1を求める.
性質:max(x,y)=x ≡ x>=y
max(x,y)=y ≡ x<=y

Step 2 (Cont.): Sを代入文で実現したい.

{max(x,y)= x} z:=e {z=max(x,y)}

➔ e ≡ x

Step 3: {not (x >= y)} S2 {z=max(x,y)}

を満たすS2を求める.

➔ S2 ≡ z:=y

Why?

複合文の導出

問題:{0<=m=M} S {m=M÷2}を満たすSを導出せよ.

注: ÷が使えない. ただし, mが偶数の時にm÷2=rot(m)が成立する.

{0<=m=M}

S1;

{0<=m=M and even(m) and P}

m:=rot(m)

{m=M÷2}

P, S1?

Pの導出:

0<=m=M and even(m) and P ➔ rot(m)= M÷2

P ≡ m÷2 = M÷2

S1の導出:条件文の導出法を利用する.

{0<=m=M}

If even(m) Then S1' Else S2' End

S1',S2' は?

{0<=m=M and even(m) and m÷2 = M÷2}

While文の導出

- 問題:
  仕様{P} S; While B do T End {Q} を満たす S,B,Tを求めよ.
- ループ不変条件invとbound関数bf
  - {B and inv} T {inv}
  - bf >=0
  - Tが実行すると, bfが必ず減少

- 方法:
  1. not B and inv ➔ Q
     inv ➔ bf >=0
     によりBとinvを求める.
  2. {P} S {inv}によりSを求める.
  3. {inv and B and bf=C} T {inv and bf<C}
     を満たすTを求める.

配列要素和を求めるプログラムの導出

仕様:

{0<N}

S; While B do T End

{s = ∑i|0<=i<N:a[i]}

Step 1:

s = ∑i|0<=i<N:a[i]

≡ 0<=k<=N and s = ∑i|0<=i<k:a[i] and k>=N

inv

Not B

bf = N-k

19

Step 2:

{0<N} S {0<=k<=N and s = ∑i|0<=i<k:a[i] }

k:=0;
s:=0

20

Step 3:

{k<N and 0<=k<=N and

s = ∑i|0<=i<k:a[i] and N-k=C}

T

{0<=k<=N and s = ∑i|0<=i<k:a[i] and N-k<C}

k:=k+1;
s:=e

eは？

21

演習問題6

次の仕様を満たすプログラムを導出せよ.

{0<N}

S; While B do T End

{s = ∑i|0<=i<N:a[i]*X^i}

22

レポートの提出について

- 演習問題1－6を解いて，6月27日（月）までに，レポートを提出してください.
- 提出先：胡のポスト
- 氏名と学生証番号を記入すること.

23