Hoare論理の拡張

「古典的な」Hoare論理では扱えなかったプログラム構成要素

- 配列等のデータ構造
- goto文
- 変数宣言
- 手続き,関数 – 再帰的呼出し

ここでは配列の取扱いについて述べる.

配列

配列とは

変数に通し番号がついているものの様にも見える

a[0], a[1], a[2], ... ←比較→ a_0, a_1, a_2, ...

{A[t/a[2]]} a[2]:=t{A} ←比較→ {A[t/a_2]} a_2:=t{A}

{4=4} a[2]:=4 {a[2]=4} ←比較→

{a[2]=3} a[1+1]:=4 {a[2]=3}　これはおかしい

∵ (a[2]=3)[4/a[1+1]] ≡ a[2]=3　代入できない!

配列

配列aに対してa(t; i)という表記を導入

配列aのi番目の要素a[i]をtに変更して得られる配列全体

$$a(t;\ i)[j] = \begin{cases} t & \text{if } i=j \\ a[j] & \text{if } i \neq j \end{cases}$$

配列の代入公理

$$\{A[a(t;\ i)/a]\}\ a[i]:=t\ \{A\}$$

$$(\text{cf. } \{A[t/a]\}a:=t\{A\})$$

演習

$\{i=0\}$ while $i \neq n$ do begin $b[i]:=a[i]$; $i:=i+1$ end $\{\forall j(0 \leq j < n \supset a[j]=b[j])\}$

を検証せよ.

$$\frac{\{\forall j(0\leq j<i+1\supset a[j]=b(a[i];i)[j])\wedge i+1\leq n\}\ b[i]:=a[i]\{\forall j(0\leq j<i+1\supset a[j]=b[j])\wedge i+1\leq n\}}{\{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\wedge i\neq n\}\ b[i]:=a[i]\{\forall j(0\leq j<i+1\leq n\supset a[j]=b[j])\wedge i+1\leq n\}}$$

$$\{\forall j(0\leq j<i+1\supset a[j]=b[j])\wedge i+1\leq n\}\ i:=i+1\{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\}$$

$$\frac{\qquad}{\{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\wedge i\neq n\}\ \mathrm{begin}\ b[i]:=a[i];\ i:=i+1\ \mathrm{end}\ \{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\}}$$

$$\frac{\qquad}{\{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\}\ \mathrm{while}\ i\neq n\ \mathrm{do\ begin}\ b[i]:=a[i];\ i:=i+1\ \mathrm{end}\ \{\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\wedge i=n\}}$$

$$\frac{\qquad}{\{i=0\}\ \mathrm{while}\ i\neq n\ \mathrm{do\ begin}\ b[i]:=a[i];\ i:=i+1\ \mathrm{end}\ \{\forall j(0\leq j<n\supset a[j]=b[j])\}}$$

検証条件 $i=0\supset \forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n$

$$\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\wedge i=n\supset\forall j(0\leq i<n\supset a[i]=b[i])$$

$$\forall j(0\leq j<i\supset a[j]=b[j])\wedge i\leq n\wedge i\neq n\supset\forall j(0\leq j<i+1\supset a[j]=b(a[i];i)[j])\wedge i+1\leq n$$

特に，$j=i$のとき$b(a[i];i)[j]=a[i]$

$j<i$のとき$b(a[i];i)[j]=b[j]$

演習

配列要素の入替(バブルソートの一部)

$\{a[i+1] \le a[i] \wedge \forall k<i.a[k] \le a[i]\}$

begin

t1:=a[i]; a[i]=a[i+1]; a[i+1]:=t1

end

$\{\forall k<i+1.a[k] \le a[i+1]\}$

$$\dfrac{\dfrac{S0}{S1} \qquad S2 \qquad S3}{\{a[i+1]\le a[i] \land \forall k<i.a[k]\le a[i]\}\ \textbf{begin}\ t1:=a[i];\ a[i]=a[i+1];\ a[i+1]:=t1\ \textbf{end}\{\forall k<i+1.a[k]\le a[i+1]\}}$$

S0: $\{\forall k<i+1.(a(a[i];\ i+1))(a[i+1];\ i)[k]\le(a(a[i];\ i+1))(a[i+1];\ i)[i+1]\}$

$t1:=a[i]$

$\{\forall k<i+1.(a(t1;\ i+1))(a[i+1];\ i)[k]\le(a(t1;\ i+1))(a[i+1];\ i)[i+1]\}$

S1: $\{a[i+1]\le a[i]\land\forall k<i.a[k]\le a[i]\}$

$t1:=a[i]$

$\{\forall k<i+1.(a(t1;\ i+1))(a[i+1];\ i)[k]\le(a(t1;\ i+1))(a[i+1];\ i)[i+1]\}$

S2: $\{\forall k<i+1.a(t1;\ i+1)(a[i+1];\ i)[k]\le a(t1;\ i+1)(a[i+1];\ i)[i+1]\}$

$a[i]=a[i+1]$

$\{\forall k<i+1.a(t1;\ i+1)[k]\le a(t1;\ i+1)[i+1]\}$

S3: $\{\forall k<i+1.a(t1;\ i+1)[k]\le a(t1;\ i+1)[i+1]\}\ a[i+1]:=t1\ \{\forall k<i+1.a[k]\le a[i+1]\}$

$a[i+1] \leq a[i] \land \forall k<i. a[k] \leq a[i]$ ... (1)と

$\forall k<i+1. (a(a[i]; i+1))(a[i+1]; i)[k] \leq (a(a[i]; i+1))(a[i+1]; i)[i+1]$ ... (2)との関係

$(a(a[i]; i+1))(a[i+1]; i)$は

配列aのi+1番目の要素をa[i]に，i番目の要素をa[i+1]に置換えたもの

これをa*と表すことにする.

すなわちa*[i]=a[i+1]，a*[i+1]=a[i]，jがiでもi+1でもないときはa*[j]=a[j]

(2)式は「i+1未満のkについて$a^*[k] \leq a^*[i+1]$」を主張.

すなわち「i未満のkについて$a[k] \leq a[i]$，かつ$a[i+1] \leq a[i]$」である.

(1)式は「i未満のkについて$a[k] \leq a[i]$かつ$a[i+1] \leq a[i]$」を示している.

したがって，検証条件 (1)$\supset$ (2) が得られる.

証明

まずループ不変証明を考える．　それは

$$\forall i(0<i\leq z \supset y[i]=i!) \wedge \forall i(z<i\leq x \supset y[i]=1) \wedge y[0]=1$$

であろう．これをS0とおく，

$$\{S0 \wedge z\neq x\} \text{ begin } z:=z+1; y[z]:=y[z-1]*z \text{ end } \{S0\} \qquad (1)$$

を検証する．

配列への代入公理により，

$$\{S1\}\ y[z]:=y[z-1]*z\ \{S0\}$$

ただし

$$S1 \equiv \forall i(0<i\leq z \supset y(y[z-1]\cdot z\,;\,z)[i]=i!) \wedge \forall i(z<i\leq x \supset y(y[z-1]\cdot z\,;\,z)[i]=1) \wedge y(y[z-1]\cdot z\,;\,z)[0]=1$$

となる．一方，　$\{S1[z+1/z]\}\ z:=z+1;\ \{S1\}$となる．ただし

$$S1[z+1/z] \equiv \forall i(0<i\leq z+1 \supset y(y[z]\cdot(z+1)\,;\,z+1)[i]=i!) \wedge \forall i(z+1<i\leq x \supset y(y[z]\cdot(z+1)\,;\,z+1)[i]=1)$$
$$\wedge\, y(y[z]\cdot(z+1)\,;\,z+1)[0]=1$$

である．　ここで，$y(y[z]\cdot(z+1)\,;\,z+1)[i]$を考えると

$$y(y[z]\cdot(z+1)\,;\,z+1)[i]=\begin{cases} y[i] & \text{if } i\neq z+1 \\ y[z]\cdot(z+1) & \text{if } i=z+1 \end{cases}$$

である．したがって，

$$\forall i(0<i\leq z \supset y[i]=i!) \wedge \forall i(z<i\leq x \supset y[i]=1) \wedge y[0]=1 \wedge z\neq x \supset S1[z+1/z]$$

が成り立つので，帰結規則より(1)が証明された．

証明(続き)

(1)が証明できたので，while規則より

$$\{S0\}\ \text{while } z=x \text{ do begin } z:=z+1; y[z]:=y[z-1]*z \text{ end od } \{S0 \wedge z=x\} \qquad (2)$$

が導出される

最終的に証明したい式は

$$\{\forall i(0 \leq i \leq x \supset y[i]=1) \wedge z=0\}\ \text{while } z \neq x \text{ do begin } z:=z+1; y[z]:=y[z-1]*z \text{ end } \{\forall i(0 \leq i \leq x \supset y[i]=i!)\}$$

であるので,

$$\forall i(0 \leq i \leq x \supset y[i]=1) \wedge z=0 \supset S0 \qquad (3)$$

$$S0 \wedge z=x \supset \forall i(0 \leq i \leq x \supset y[i]=i!) \qquad (4)$$

を示せばよい(ただし，$S0 \equiv \forall i(0<i \leq z \supset y[i]=i!) \wedge \forall i(z<i \leq x \supset y[i]=1) \wedge y[0]=1$).

これらは自明である.

したがって,

$$\{\forall i(0 \leq i \leq x \supset y[i]=1) \wedge z=0\}\ \text{while } z \neq x \text{ do begin } z:=z+1; y[z]:=y[z-1]*z \text{ end } \{\forall i(0 \leq i \leq x \supset y[i]=i!)\}$$

が証明された.

$$\frac{\dfrac{\dfrac{\{S1[z+1/z]\}\ \text{begin } z:=z+1;\ \{S1\}}{\{\forall i(0\le i\le z\supset y[i]=i!)\wedge\forall i(z<i\le x\supset y[i]=1)\wedge z\ne x\}\ \text{begin } z:=z+1\{S1\}} \quad \{S1\}y[z]:=y[z-1]*z\ \{S0\}}{\{\forall i(0\le i\le z\supset y[i]=i!)\wedge\forall i(z<i\le x\supset y[i]=1)\wedge z\ne x\}\text{begin } z:=z+1;y[z]:=y[z-1]*z \text{ end } \{S0\}}}{\begin{array}{c}\{\forall i(0\le i\le z\supset y[i]=i!)\wedge\forall i(z\le i\le x\supset y[i]=1)\}\ \text{while } z\ne x \text{ do begin } z:=z+1;y[z]:=y[z-1]*z \text{ end}\\ \{\forall i(0\le i\le z\supset y[i]=i!)\wedge\forall i(z\le i\le x\supset y[i]=1)\wedge z=x\}\end{array}}}{\{\forall i(0\le i\le x\supset y[i]=1)\wedge z=0\}\ \text{while } z\ne x \text{ do begin } z:=z+1;y[z]:=y[z-1]*z \text{ end } \{\forall i(0\le i\le x\supset y[i]=i!)\}}$$

$$S0:\ \forall i(0\le i<z\supset y[i]=i!)\wedge\forall i(z<i\le x\supset y[i]=1)\wedge y[0]=1$$

$$S1:\ \forall i(0<i\le z\supset y(y[z-1]\cdot z\ ;\ z)[i]=i!)\wedge\forall i(z<i\le x\supset y(y[z-1]\cdot z\ ;\ z)[i]=1)\wedge y(y[z-1]\cdot z\ ;\ z)[0]=1$$

$$S1[z+1/z]:\ \forall i(0<i\le z+1\supset y(y[z]\cdot(z+1)\ ;\ z+1)[i]=i!)\wedge\forall i(z+1<i\le x\supset y(y[z]\cdot(z+1)\ ;\ z+1)[i]=1)$$
$$\wedge y(y[z-1]\cdot z\ ;\ z)[0]=1$$

検証条件　$\forall i(0<i\le z\supset y[i]=i!)\wedge\forall i(z<i\le x\supset y[i]=1)\wedge y[0]=1\wedge z\ne x\supset S1[z+1/z]$

$\forall i(0\le i\le x\supset y[i]=1)\wedge z=0\supset S0$

$S0\wedge z=x\ \supset\ \forall i(0\le i\le x\supset y[i]=i!)$

演習

次のバブルソートプログラムを検証せよ.

{∀i≤n.a[i]=b[i]} P {A0(a, b, n, 0)}

```
P::
begin
    j:=n;
    while j>0 do begin
            i:=0;
                while i<j do begin
                        if a[i+1]<a[i] then begin t1:=a[i]; a[i]:=a[i+1]; a[i+1]:=t1end fi;
                        i:=i+1 end od;
            j:=j-1;
            end od
end
```

A0(a, b, n, j)は以下の条件が成立つことを示す.

1. b[0], ... , b[n]はa[0], ... , a[n]の置換になっている. (bは論理変数:実行開始時の配列の値)
2. a[j+1], ... , a[n]の範囲はソートされている.
3. 0≤h≤j, j+1≤k≤nなるh, kに対して, a[h]≤a[k].

ヒント： 外側のwhile文のループ不変表明は A0(a, b, n, j),

内側のwhile文のループ不変表明は i≤j∧A0(a, b, n, j)∧∀k<i.a[k]≤a[i]

```
{ ∀i≤n.a[i]=b[i] }  ◀······ A0(a, b, n, n)
begin
    j:=n;
    { A0(a, b, n, j) }
    while j>0 do
    { j>0∧A0(a, b, n, j) }
        begin
            i:=0;
            {i≤j∧A0(a, b, n, j)∧∀k<i(a[k]≤a[i])}
            while i<j do
            { i<j∧A0(a, b, n, j)∧∀k<i(a[k]≤a[i]) }
                begin
                    if a[i+1]<a[i] then
                        { a[i+1]<a[i]∧i<j∧A0(a, b, n, j)∧∀k<i(a[k]≤a[i]) }
                        begin t1:=a[i]; a[i]:=a[i+1]; a[i+1]:=t1end
                        { i<j∧A0(a, b, n, j)∧∀k<i+1(a[k]≤a[i+1]) }
                        fi;
                    i:=i+1 end
                { i≤j∧A0(a, b, n, j)∧∀k<i(a[k]≤a[i]) }
            od;
            {A0(a, b, n, j)∧∀k<j(a[k]≤a[j]) }
            j:=j-1;
        end
    {A0(a, b, n, j)}
    od
end
```

局所変数宣言

変数xのスコープがプログラムPであるような局所変数宣言を以下の形で与えるとする.

new x; P

例： {a=1∧b=2} **new** a; **begin** a:=7; b:=a+b **end** {a=1∧b=9} (postconditionでa=7ではない!)

{a=1∧b=2} **new** n; **begin** a:=7; b:=n+b **end** {a=1∧b=9}　でも同じ

局所変数宣言の規則

$$\frac{\{A\}\ P[n/x]\ \{B\}}{\{A\}\ \text{new}\ x;\ P\ \{B\}}$$

ただしnはA, B, Pに現れない新しい変数

例

$$\frac{\{a=1 \wedge b=2\}\ \mathbf{begin}\ n:=7;\ b:=n+b\ \mathbf{end}\ \{a=1 \wedge b=9\}}{\{a=1 \wedge b=2\}\ \mathbf{new}\ a;\ \mathbf{begin}\ a:=7;\ b:=a+b\ \mathbf{end}\ \{a=1 \wedge b=9\}}$$