向井研: ホーア論理によるプログラム検証に関するメモ

酒井政裕

2003年5月16日

1　検証したいプログラム

```
begin
  i = 0
  s = 0
  while (i != 10) do
    begin
      s = s + i
      i = i + 1
    end
end
```

このプログラムを実行した後に $s = \sum_{j=0}^{9} j$ となっている事を証明したい。

2　証明

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{(s+i)+(i+1)=\sum_{j=0}^{i+1} j\}\ s=s+i\ \{s+(i+1)=\sum_{j=0}^{i+1} j\}}\text{(代入規則)}}{\{(i\neq 10)\wedge(s+i=\sum_{j=0}^{i} j)\}\ s=s+i\ \{s+(i+1)=\sum_{j=0}^{i+1} j\}}\text{(帰結規則)}\qquad \dfrac{}{\{s+(i+1)=\sum_{j=0}^{i+1} j\}\ i=i+1\ \{s+i=\sum_{j=0}^{i} j\}}\text{(代入規則)}}{\{(i\neq 10)\wedge(s+i=\sum_{j=0}^{i} j)\}\ \text{begin}s=s+i;i=i+1;\text{end}\ \{s+i=\sum_{j=0}^{i} j\}}\text{(複合文の規則)}}{\{s+i=\sum_{j=0}^{i} j\}\ \text{while}(i\neq 10)\text{do}\ldots\ \{(i=10)\wedge(s+i=\sum_{j=0}^{i} j)\}\ \cdots(1)}(\mathit{while}\text{ 規則})$$

$$\dfrac{\dfrac{\dfrac{}{\{0=\sum_{j=0}^{0} j\}\ i=0;s=0;\ \{s+i=\sum_{j=0}^{i} j\}}\text{(代入規則)}\qquad \begin{matrix}(1)\\ \vdots\\ \{s+i=\sum_{j=0}^{i} j\}\ \text{while}(i\neq 10)\text{do}\ldots\ \{(i=10)\wedge(s+i=\sum_{j=0}^{i} j)\}\end{matrix}}{\{0=\sum_{j=0}^{0} j\}\ \text{begin}\ldots\text{end}\ \{\{(i=10)\wedge(s+i=\sum_{j=0}^{i} j)\}}\text{(複合文の規則)}}{\{\}\ \text{begin}\ldots\text{end}\ \{s=\sum_{j=0}^{9} j\}}\text{(帰結規則)}$$