Hoare 論理(1)

- プログラム証明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

参考文献

• 1969年, C.A.R Hoareは, プログラム が仕様に関して部分正当であることを 証明するための公理的手法を導入した.

C.A. R. Hoare, An Axomatic Basis for Computer Programming, CACM 12 (10), 1969, 576-580.

計算機科学においてもっとも広く引用されている文献の一つ

部分的正当性の表明(定義) (Partial Correctness Assertion)

{P} S {Q}

事前条件 P を満足する時に、 プログラムSを実行すると、 その実行後には、事後条件 Q を満足する。

プログラムSが終了すれば、プログラム実行の効果として、事前条件と事後条件との対によって表現した意図通りの結果が得られる。

簡単な言語

代入文 S ::= x := e複合文 | S1; S2 | If B Then S1 Else S2 End if 文 | While B do S End while文

部分正当性の証明

部分的正当性の表明例

部分的正当性の証明

{N>=0} i := 1; f := 1; While i<=N Do

 $f := f^*i;$ i := i+1

End {f=N!}

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

代入文の公理

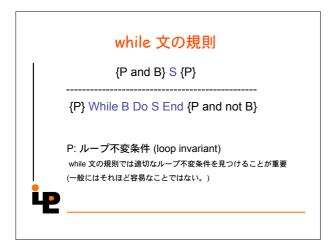
 ${Q[e/x]} x := e {Q}$

代入文 x := e の実行後に事後条件 Q が成 り立つには事前条件としてQ[e/x] が成り立 つ必要がある。

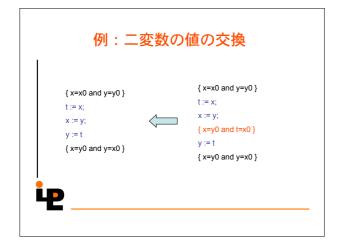
例: $\{x>9\} x := x+1 \{x>10\}$

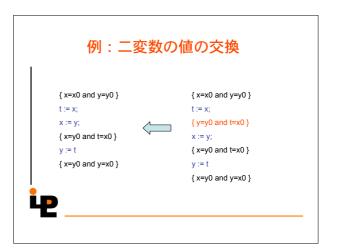








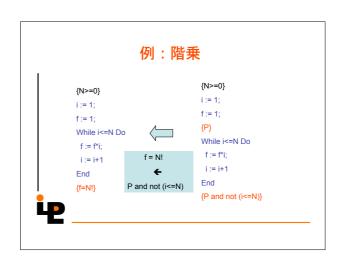


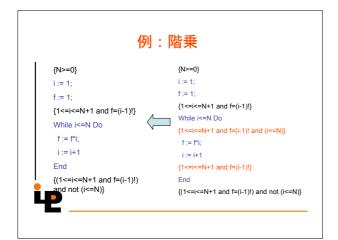


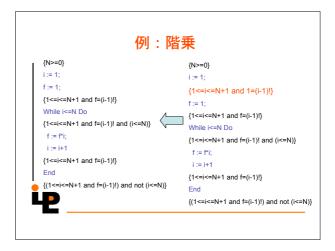
証明手法のまとめ 所望の部分的正当性の表明を目標として、 topdown向きに証明を構成

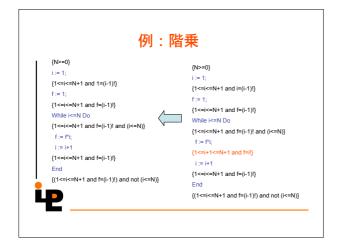
- 目標となる部分的正当性の表明を導出するため、どの推論規則を用いる?
- また、その場合の前提として成り立つ必要がある論理式はどのようなもの?

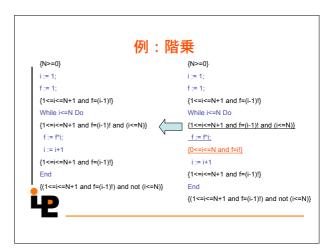












```
掛算
{ x>0 }
                                      { x>0 }
z := y;
                                      z := y;
u := x - 1:
                                      u := x - 1:
While u<>0 Do
                                      While u<>0 Do
z := z + y;
                                       z := z + y;
u := u - 1
                                       u := u - 1
End
                                      End
\{z = x * y\}
                                      \{ x>0 \text{ and } z = x * y \}
```

