形式的理論としてのHoare論理

形式的理論 (formal theory)

- 推論規則 (inference rules)
- 論理的公理 (logical axioms)
  - ここまで「論理」(logic)を構成する
- 非論理的公理 (non logical axioms)
  - これを追加することにより「理論」(theory) を構成する
    - 数学を構成する公理など　例: Peanoの自然数論の公理

Hoare論理は広義の形式的理論と看做すことができる

Hoare論理の形式的理論PHL(PV, AV, S)

Hoare論理の言語

まず語彙(vocabulary)を定める

語彙: 変数, 定数, 関数記号, 述語記号の集合

Hoare論理の語彙　<PV, AV>

PV: プログラムの語彙 (program vocabulary)

プログラム中の式(expression)およびブール式(boolean expression)

ブール式には量記号(quantifier: ∀, ∃)を含まない

AV: 表明の語彙 (assertion vocabulary)

一階述語論理の語彙, PVの語彙の拡張

(PVで表記できるものは全てAVで表記できる)

非論理的公理の集合S

AVを語彙とする論理式Fml(AV)の部分集合

プログラム言語Minの定義

PVだけに依存(AV, Sとは無関係)

Min(PV)と表記する

変数　　::=　PVの変数

式　　::=　PVから定義される項

ブール式 ::=　PVから定義される原子論理式 | ブール式∧ブール式

ブール式∨ブール式 | ブール式⊃ブール式 | ¬ブール式

文　　::=　skip | 変数:=式 | begin 文 { ; 文 } end |

if ブール式 then 文 else 文 fi |

while ブール式 do 文 od

プログラム:= 文

表明,　表明付きプログラム

表明::=　AVから定義される論理式

表明付きプログラム::= {表明}プログラム{表明}

表明付きプログラムが**形式的に証明可能 (formally provable)**

　　形式的証明によってその表明付きプログラムが証明されたとき

PHL(PV, AV, S)⊢F

　　Hoareの形式的理論PHL(PV, AV, S)で表明付きプログラムFが証明可能

証明の**結論 (conclusion)**

　　形式的証明の最後の表明付きプログラム

PHL(PV, AV, S)の公理と推論規則

公理

A_{as}(代入文の公理)

$\{A[t/x]\}x:=t\{A\}$

A_{sk}(スキップ文の公理)

$\{A\}skip\{A\}$

推論規則

R_{if}(条件文の規則)

$$\frac{\{C \wedge A\}P\{B\}\{\neg C \wedge A\}Q\{B\}}{\{A\}\text{if } C \text{ then } P \text{ else } Q \text{ fi}\{B\}}$$

R_{cp}(複合文の規則)

$$\frac{\{A\}P1\{S1\} \ldots \{Sn\text{-}1\}Pn\{B\}}{\{A\}\text{begin } P1; \ldots ; Pn \text{ end}\{B\}}$$

R_{wh}(while文の規則)

$$\frac{\{C \wedge A\}P\{A\}}{\{A\}\text{while } C \text{ do } P \text{ od}\{A \wedge \neg C\}}$$

R_{cs}(帰結規則)

$$\frac{\{B\}P\{C\}}{\{A\}P\{D\}}$$

但しSl-A⊃B,　Sl-C⊃D

PHL(PV, AV, S)の形式的証明(formal proof)

$<1, AP1, C_1>, \ldots, <i, AP_i, C_i>, \ldots, <n, AP_n, C_n>$

i : 行番号

AP_i: 表明付きプログラム

C_i: コメント，以下のいずれかである

公理名

AP_iは公理

$<R_i, j_1, \ldots j_n>$ 但し$j_1, \ldots j_n < i$

R_i: 推論規則名

AP_iは$AP_{ji}, \ldots, AP_{jn}$から推論規則R_iによって推論される.

すなわち

$$R_i \ \frac{AP_{ji} \quad \ldots \quad AP_{jn}}{AP_i}$$

例

1. {S0} a:=a **mod** b{S1}, A_{as}

2. {b≠0∧gcd(a, b)=gcd(x, y)} a:=a **mod** b{S1}, <R_{cs}, 1>

3. {S1} c:=a {S2}, A_{as}

4. {S2} a:=b {S3}, Aas

5. {S3} b:=c{gcd(a, b)=gcd(x, y)}, A_{as}

6. {b≠0∧gcd(a, b)=gcd(x, y)} **begin** a:=a **mod** b; c:=a; a:=b; b:=c **end**{gcd(a, b)=gcd(x, y)}, <Rcp, 2, 3, 4, 5>

但し　　S0 : gcd(b, a mod b)=gcd(x, y)

S1 : gcd(b, a)=gcd(x, y)

S2 : gcd(b, c)=gcd(x, y)

S3 : gcd(a, c)=gcd(x, y)

また,　S ⊢ b≠0∧gcd(a, b)=gcd(x, y)⊃S0

$b \neq 0 \wedge gcd(a, b)=gcd(x, y) \supset S0 \quad \{S0\}\ a:=a\ \textbf{mod}\ b\{S1\}$

$\{b \neq 0 \wedge gcd(a, b)=gcd(x, y)\}\ a:=a\ \textbf{mod}\ b\{S1\} \quad \{S1\}\ c:=a\ \{S2\} \quad \{S2\}\ a:=b\ \{S3\} \quad \{S3\}\ b:=c\{gcd(a, b)=gcd(x, y)\}$

$\{b \neq 0 \wedge gcd(a, b)=gcd(x, y)\}$ **begin** $a:=a$ **mod** $b;\ c:=a; a:=b; b:=c$ **end**$\{gcd(a, b)=gcd(x, y)\}$

$$S3 : \ gcd(a, c)=gcd(x, y)$$

$$S2 : \ gcd(b, c)=gcd(x, y)$$

$$S1 : \ gcd(b, a)=gcd(x, y)$$

$$S0 : \ gcd(b, a \bmod b)=gcd(x, y)$$

検証条件 (verification condition)

帰結規則で用いる S ⊢ A⊃B, S ⊢ C⊃Dのこと

Hoare論理はプログラムの正しさを検証条件の正しさに

帰着させるものと考えられる

Hoare論理の完全性も検証条件を証明するための数学(S)の

完全性に帰着できる(相対完全性)

演習

$\{y=1 \wedge z=0\}$ while $z \neq x$ do begin $z:=z+1; y:=y*z$ end $\{y=x!\}$

の形式的証明をせよ