数理解析研究所講究録
494巻 1983年 203-214

プログラムの検証と完備な述語のクラス

名古屋大学工学部　村上　昌己　稲垣　康善
豊橋技術科学大学　本多　波雄

1　まえがき　Apt[1]らは，プログラムの検証における述語のクラスについての重要な概念として，完備性(completeness)の概念を導入した．直観的には，ある述語のクラス$\mathcal{A}$が完備であるとは，プログラムのクラスを$\mathcal{S}$とするとき，任意の$P, Q \in \mathcal{A}$, $S \in \mathcal{S}$について$P\{S\}Q$が成立するならば，すべての中間表明を$\mathcal{A}$から選んで証明が可能であることをいう．Apt[1]では$\mathcal{S}$としてwhileプログラムのクラスを選び，帰納的述語，帰納的可算述語等のクラスの完備性について議論をした．

さらにApt[2]では$\mathcal{S}$として条件付臨界領域によって制御されるcobegin−coend文を許す並行プログラムを選び，帰納的述語のクラスの完備性について議論した．

以上の結果は，扱うプログラムの性質が部分的正当性に限られるHoare流の公理系，あるいはそれを拡張したOwicki[6]の公理系をもとに得られたものである．

一方，並行プログラムの正当性検証体系としてOwickiらの

方法の他に，Flon-Suzukiの公理系[4]が提案されている．Flon-Suzukiの公理系では部分的正当性，停止性等の他にさらに一般的なプログラムの性質も取り扱えるようにしている．

本稿ではFlon-Suzukiの体系をもとに，完備性の概念を一般的なプログラムの性質に拡張して議論する．Flon-Suzukiの体系の特徴として，次のような点があげられる．すなわち，そこで扱える性質は特定のものに固定されておらず，任意のプログラムSの構文からつくられる連続ないしは単調な述語関数の最小あるいは最大不動点で表現される性質ならば，取り扱うことが一般的に可能であることである．また一般にプログラムの性質は，ある述語関数の不動点を用いて表わすことができることが知られている．[3)]

従って，プログラムの多様な性質の証明について考える際，個々の正当性についてそれぞれ公理系を個別に与え，それらを個々に議論する必要はなく，一般的な取り扱いが可能である．そこで本稿では，不動点によって表現されたプログラムの性質の証明についての完備性を一般的に定義し，算術的階層の各クラスの完備性についていくつかの結果を示す．

2．被防護命令　本稿では自然数の集合N上の並行プログラムを被防護命令によって表わす．被防護命令は非決定性プロ

グラムの一種で次のようなものである．

$$\underline{do}\ B_1 \to A_1 \,\|\, B_2 \to A_2 \,\|\, \cdots \,\|\, B_n \to A_n\ \underline{od}$$

ここで，各A_i $(i=1,\cdots,n)$は作用(action)で，N上の代入文の並びである．また，B_iは防護(guard)と呼ばれ，N上の帰納的述語である．上のステートメントの実行は次のようにして行なわれる．すなわちB_i $(i=1,\cdots,n)$を評価し，その値が真であるもののうちから１つを非決定的に選び，対応するA_iを実行する．そして同様の動作を繰返し，すべてのB_iが偽になった時に停止する．

cobegin－coend文から被防護命令への変換については文献[3]に示されている．

プログラムの意味を形式的に与えるために計算木(computation tree)を導入する．

<u>定義１</u>　状態iは各プログラム変数からN上の値への写象である．

<u>定義２</u>　プログラムSと初期状態iに対して，計算木$\mathcal{T}(s,i)$を次のように定義する．木の各節点は状態によってラベル付けられている．各節点から出る枝は，その節点にラベルとして付けられている状態で真となる防護でラベル付けられており，その先に続く節点は各枝に付けられた防護に対応する命令を実行した結果の状態でラベル付けられている．

$\mathcal{T}(s,i)$の根から子孫に向う各道は，sをiから実行したときの実行系列に対応している．プログラムの性質は，それをある初期状態の集合から実行した時の計算木の性質として表わすことができる．例えば「プログラムSを状態iから実行したとき，実行中は常にRが成立しつづける．」という性質は，「$\mathcal{T}(s,i)$ のすべての節点はRの成立する状態でラベルづけられている．」と表わすことができる．

3．プログラムの性質と不動点理論　N上の述語全体からなる領域は次のような半順序⊑のもとで完備束となることが知られている．

$$P \sqsubseteq Q \quad \text{iff} \quad \pi(P) \subset \pi(Q)$$

N上のプログラムの性質は，一般にN上の述語がなす領域がなす完備束の上の関数(述語関数)の不動点として表わされる．[3] すなわち，次の命題が成り立つ．

命題1 (Emerson－Clarke[3])　プログラムSの性質pre(s, R)について計算木$\mathcal{T}(s,i)$についての表現から，SとRの構文からつくられる述語関数の不動点を使った表現に変換するアルゴリズムがある．

例えば，プログラムS

$$\underline{\text{do}}\ B_1 \rightarrow A_1 \parallel B_2 \rightarrow A_2 \parallel \cdots \parallel B_n \rightarrow A_n\ \underline{\text{od}}$$

に対し，A_i の実行後 P が成立するための最弱前条件(weakest precondition) を $A_i^{-1}P$ と書くことにすると「S の実行中 R が成立しつづける.」という性質は

$$\Phi_R^S(X) = R \wedge \bigwedge_i^n (B_i \Rightarrow A_i^{-1} X)$$

の最大不動点と一致する.

又，次の命題により，不動点によって特徴づけられた性質については，その証明のための公理系を容易に得ることができる.[4]

<u>命題 2 (Flon-Suzuki)</u>[4] プログラム S の性質 pre(S, R) がある単調な述語関数 $\Phi_R^S(X)$ の最大不動点 gfp $X.\Phi_R^S$ と等価であり，かつ次の 2 つの条件:

1) gfp $X.\Phi_R^S(X)$ と等価な述語が存在し，表明として与えることが出来る.

2) 述語 P, Q に対して $P \Rightarrow \Phi_R^S(X)$ という形の式を証明する公理系がある.

以上を満す時,

$$\frac{P \Rightarrow \Phi_R^S(P)}{P \Rightarrow pre(S, R)}$$

という推論規則をつけ加えることによって完全かつ無矛盾な $Q \Rightarrow pre(S, R)$ の証明体系が得られる.

<u>命題 3 (Flon-Suzuki)</u> プログラム S の性質 pre(S, R) がある連

統な述語関数$\Phi_R^s(X)$の最小不動点$\mathit{lfp}\, X\,\Phi_R^s$と等価であり，かつ次の２つの条件:

1) $\models \Phi_R^{s\,i}(\mathit{false}) \equiv J(i)$ となるN上の述語$J(i)$を中間表明として与えることができる．

2) 述語P, Q に対して$P \Rightarrow \Phi_R^s(Q)$という形の式を証明する公理系が存在する．

以上を満す時,

$$\frac{J(n+1) \Rightarrow \Phi_R^s(J(n)) \quad , \quad \neg J(0)}{J(n) \Rightarrow pre(s, R)}$$

という推論規則をつけ加えることによって完全かつ無矛盾な$Q \Rightarrow pre(s, R)$の証明体系が得られる．

4．完備性　完備性の定義は，プログラムの性質に対して，それを証明するそれぞれの公理系の形に依存する．しかし前節の命題2.3より，不動点で特徴づけられた性質については証明体系の一般的な形がわかっているので，それに基づいて次のように完備性を一般的に定義できる．

定義３　述語のクラス$\mathcal{A}$が，ある単調な述語関数Φ_R^sの最大不動点と等価な性質$pre(s, R)$の証明について完備であるとは，任意のs，任意の$Q, R \in \mathcal{A}$に対して$\models Q \Rightarrow pre(s, R)$ならば，$Q \Rightarrow P$，$P \Rightarrow \Phi_R^s(P)$となる$P \in \mathcal{A}$が存在することである．

同様に，ある連続な述語関数Φ_R^sの最小不動点と等価な性質pre(s, R)の証明について完備であるとは，任意のs，任意のQ，R∈$\mathcal{A}$に対して$\models Q \Rightarrow pre(s,R)$ならば，$Q \Rightarrow \exists i J(i)$, $J(i+1) \Rightarrow \Phi_R^s(J(i))$, $\neg J(0)$ である$\exists i J(i) \in \mathcal{A}$が存在することである．

5　算術的階層　N上の述語は，それが定義するN上の関係の複雑さによって階層構造をなす．

定義4　　$r \geq 0$について

i) $\Sigma_0^0 = \Pi_0^0 =$ {帰納的に決定可能なN上の関係を定義する述語のクラス.}

ii) $\Sigma_{r+1}^0 = \{P(x_1, \cdots, x_n) \mid P(x_1, \cdots, x_n) \equiv \exists y Q(x_1, \cdots, x_n, y),$
$Q(x_1, \cdots, x_n, y) \in \Pi_r^0\}.$

iii) $\Pi_{r+1}^0 = \{P(x_1, \cdots, x_n) \mid P(x_1, \cdots, x_n) \equiv \forall y Q(x_1, \cdots, x_n, y),$
$Q(x_1, \cdots, x_n, y) \in \Sigma_r^0\}.$

iv) $\Delta_r^0 = \Sigma_r^0 \cap \Pi_r^0$

Σ_1^0は帰納的可算述語のクラスに，またΠ_1^0は有限反証的(否定をとると帰納的可算)述語のクラスに一致する.[5)]

図1は算術的階層全体を表わしたものである.

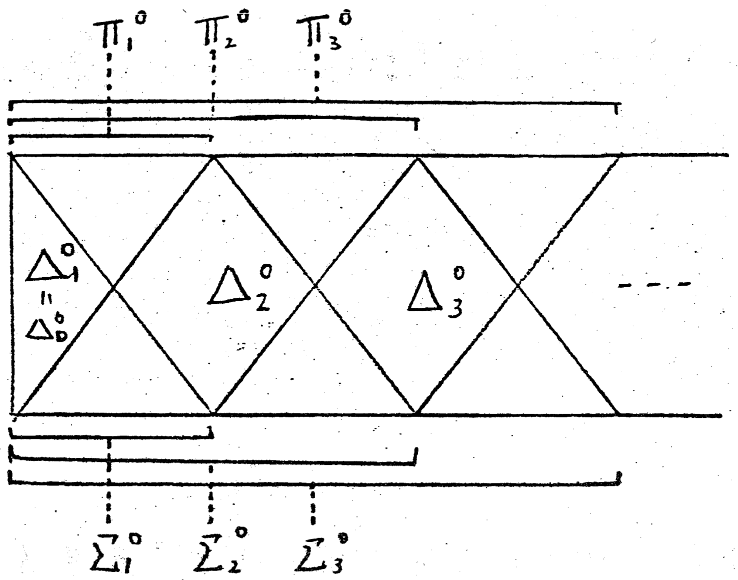

図1　算術的階層

6. 結果　任意の $r>0$ について，

定理1　Φ_R^s が下記の条件 i), ii), iii) を満す述語関数であるとき，Φ_R^s の最小不動点と等価な pre(s, R) の証明について Σ_r^0 は完備である．

i) $\Phi_R^s(X)$ は X について連続．

ii) $P \in \Sigma_r^0$ ならば $\Phi_R^s(P) \in \Sigma_r^0$．

iii) ${\Phi_R^s}^i(\mathrm{false}) \equiv J(i)$ となる $J(i) \in \Sigma_r^0$ が存在する．

証明)　$\models Q \Rightarrow \mathrm{pre}(s, R)$ のとき，Φ_R^s の連続性より，

$$\mathrm{l.f.p}\, X . \Phi_R^s(X) = \sqcup_i {\Phi_R^s}^i(\mathrm{false})$$

$J(i) \equiv {\Phi_R^s}^i(\mathrm{false})$ より $\models J(0) \equiv \mathrm{false}$，ゆえに $\vdash \neg J(0)$．

$\models J(i+1) \equiv \Phi_R^s(J(i))$ より，$\vdash J(i+1) \Rightarrow \Phi_R^s(J(i))$．

また，$\models Q \Rightarrow \mathrm{lfp}\, X \Phi_R^s(X)$ より　$Q \sqsubseteq \sqcup_i {\Phi_R^s}^i(\mathrm{false})$

ある m が存在して，$Q \sqsubseteq \Phi_R^{s^m}(\mathrm{false})$．すなわち $Q \sqsubseteq J(m)$．

ゆえに，$\vdash Q \Rightarrow \exists i J(i)$ となる．

$\exists i J(i) \in \Sigma_r^0$ であることは，$J(i) \in \Sigma_r^0$ かつ

Σ_r^0 が $\exists$ について閉じていることより明らか．　証明終)

定理２　Φ_R^s が下記の条件 i) ii) iii) を満す述語関数であるとき，Φ_R^s の最大不動点と等価な $pre(s, R)$ の証明について Π_r^0 は完備である．

i) $\Phi_R^s(X)$ は X について連続．

ii) $P \in \Pi_r^0$ ならば $\Phi_R^s(P) \in \Pi_r^0$．

iii) $\Phi_R^{s^i}(\mathrm{true}) \equiv J(i)$ となる $J(i) \in \Pi_r^0$ が存在する．

証明)　$\models Q \Rightarrow pre(s, R)$ のとき

$\vdash Q = P$, $\vdash P \Rightarrow \Phi_R^s(P)$ となる P を次のように与える．

$$P \equiv \sqcap_i \Phi_R^{s^i}(\mathrm{true})$$

Φ_R^s の連続性より P は $gfp\, X.\Phi_R^s(X)$ と等しくなる．

ゆえに $\vdash Q \Rightarrow P$，$\vdash P \Rightarrow \Phi_R^s(P)$ は明らか．

$P \in \Pi_r^0$ であることは次のようにして示される．

P は，鎖 $\mathrm{true} \sqsupseteq \Phi_R^s(\mathrm{true}) \sqsupseteq \Phi_R^{s^2}(\mathrm{true}) \sqsupseteq \Phi_R^{s^3}(\mathrm{true}) \sqsupseteq \cdots$ の下限である．条件より $\Phi_R^{s^i}(\mathrm{true}) \equiv J(i)$ なる $J(i) \in \Pi_r^0$ が存在する．鎖 $J(0) \sqsupseteq J(1) \sqsupseteq \cdots$ の下限は $\forall i J(i)$ となり $P \equiv \forall i J(i)$．

Π_r^0 は $\forall$ について閉じているので $\forall i J(i) \in \Pi_r^0$．　証明終)

以下の結果については紙面の都合上，証明は省略する．

定理3　Π_r^0 は Φ_R^s の最小不動点と等価なpre(s,R)の証明について完備でない．

定理4　Φ_R^s が定理1と同様の条件を満す述語関数であるとき，Φ_R^s の最小不動点と等価なpre(s,R)について，$\models Q \Rightarrow pre(s,R)$，$Q, R \in \Pi_r^0$ ならば中間表明を Σ_{r+1}^0 から選んで証明が可能である．

定理5　Φ_R^s が定理2と同様の条件を満す述語関数であるとき，Φ_R^s の最大不動点と等価なpre(s,R)について，$\models Q \Rightarrow pre(s,R)$，$Q, R \in \Sigma_r^0$ ならば，中間表明を Π_{r+1}^0 から選んで証明が可能である．

定理6　Δ_r^0 は，Φ_R^s の最小不動点と等価なpre(s,R)の証明について完備でない．

定理7　Δ_r^0 は，Φ_R^s の最大不動点と等価なpre(s,R)の証明について完備である．

定理8　$r \geq 0$ について $\Pi_r^0 \cup \Sigma_r^0$ は Φ_R^s の最小不動点と等価なpre(s,R)の証明について完備でない．

定理9　$\Delta_\omega^0 (= \bigsqcup_r (\Sigma_r^0 \cup \Pi_r^0))$ は定理1の条件を満す Φ_R^s の最小不動点の証明について完備である．

定理10　Δ_ω^0 は定理2の条件を満す Φ_R^s の最大不動点の証明について完備である．

以上の結果をまとめると次の表のようになる．ここで○印

は完備であることを，X印は完備でないことを．？は未解決であることを表わす．

	Σ_r^0	Π_r^0	Δ_r^0	$\Pi_r^0 \cup \Sigma_r^0$	Δ_ω^0
最大不動点	?	O	X	?	O
最小不動点	O	X	X	X	O

7　謝辞　日頃御指導下さる本学福村教授，並びに御討論下さる研究室の皆様に感謝致します．

文献

1) Apt. K. R, J. A. Bergstra, and L. G. L Meertens: "Recursive Assertions Are Not Enough - Or Are They?" Theort. Comp. Sci. 8 (1979) 73-87

2) Apt. K, R, "Recursive Assertions and Parallel Programs" Acta Informatica 15. (1981) 219-232

3) Emerson E. A. and E. M. Clarke "Characterizing Correctness Properties of Parallel Programs Using Fixpoints" Proc. of ICALP 80 (1980)

4) Flon. L. and N. Suzuki "The Total Correctness of Parallel Programs" SIAM. J. Comput. Vol 10. No2 May (1981) 227-246

5) Hinman P.G.: "Recursion-Theoretic Hierarchies" Springer-Verlag Berlin (1978)

6) Owicki S. and D. Gries; "Verifying Properties of Parallel Programs: An Axiomatic Aprroachi" CACM 19 (1976) 279-285