報告番号	※甲第 1773 号

主論文の要旨

題名 並列プログラムの検証体系に関する
論理学的研究

氏名 村上昌己

主論文の要旨

報告番号	※甲第　　号	氏名	村上昌己

本論文は，並列性を含むプログラムの形式的意味記述のための論理学的手法について述べたものである．

第1章では，本研究の背景，動機及び問題の位置づけについて述べている．

プログラムの意味を形式的に記述し，取り扱うことは，プログラムを見通しよく設計するために重要である．プログラムの形式的意味記述のためには，計算の適当な数学的モデルが必要である．

近年，論理型プログラミング，関係データベースなどに見られるように，プログラムや情報システムを扱う場面において，数理論理学的な手法が注目をあつめている．そこで，プログラムの形式的モデルを論理学的対象として与える公理的意味論，即ちプログラム正当性の検証の理論が，意味記述法として有用であると考えられる．

また近年，計算機システムの並列化に伴い，並列プログラムの生産性，信頼性を向上させるための工学的手法として，並列計算の数学的モデルに関する議論の重要性がたかまっている．

しかし並列計算と呼ばれるものは，その形態，レベルも様々であり，それぞれの場合によって関心のある問題は異なったものとなる．この章では，並列計算の種類とそれぞれのモデルにおいて扱う問題についてまとめ，公理的意味論，即ちプログラム正当性の検証の理論が特に有効であろうと思われる並列プログラムの種類として，ユーザレベルでの並列プログラミングを想定し，そこで使用される言語のモデルとして，次のような特徴を上げる．

主論文の要旨

報告番号	※甲第　　号	氏名	村上　昌己

(1). 原則として，プログラムの実行は下位のレベルでは非決定性の逐次型になっているものとする．

(2). すべてのプロセスは有限時間内に計算を終了し，計算結果を出力するものとする．

(3). プロセス間の情報の交換は共有変数による場合と，通信による場合がある．

(4). 並列に走るプロセスの数は有限個に固定されている．

次に，従来のプログラムの公理的意味論を並列プログラムに適用する際の問題点についてふれている．

第2章では，共有変数によって情報の交換を行うような並列プログラムの正当性の検証体系を，Harelによって提案された非決定性プログラムの検証体系である第一階ダイナミックロジック（ＲＧ－ＤＬ）を拡張することによって与える．

この章では，まず共有変数型の並列プログラムのモデルとして，正規並行プログラム（ＲＧＣ）を導入する．ＲＧＣは先に述べた(1)，(2)，(4)に加えて，次のような特徴をもつものである．即ち，すべてのプロセスは，分岐，連接，及び脱出条件が書かれた繰り返しの組合わさった構造により，計算を行う．また，各プロセス間の同期の条件は，許される実行系列の集合を表す正規表現として与えられる．ここでは，ＲＧＣのシンタックスを，基本命令をアルファベットとし，シャッフル演算と共通部分をとる演算をもつ正規表現として定義する．またＲＧＣのセマンティクスとして状態集合の上の二項関係及び，計算履歴集合を定義する．

主論文の要旨

報告番号	※甲第　　号	氏名	村上　昌己

次に，ＲＧ－ＤＬにいくつかの論理記号，公理，及び推論規則を付け加えることにより，共有変数型の並列プログラムの性質として証明すべき速度独立部分的正当性，デッドロックフリー性，相互排除性についての検証体系ＲＧＣ－ＩＬを与える．そして，この体系が，先に定義したセマンティクスの上で無矛盾性かつ完全であることを示す．

ここで提案した体系は，従来の共有変数型の並列プログラムの検証体系の持つ問題点であった，デッドロックフリー性，相互排除性等のプログラムの制御に関する性質の検証について，プログラムを検証に先立って非決定性プログラムに変換する等の操作を必要とせず，直接的に扱うことを可能とするものである．

第３章では，通信型の並列プログラムの検証体系について述べる．この章では通信型の並列プログラムのモデルとして，Hoareの相互通信逐次型プロセス系(communicating sequential processes:ＣＳＰ）を採用する．ＣＳＰは，共有変数を含まずプロセス間の情報の交換及び動機を通信命令という機能によっておこなう．

ここでは，ＲＧＣの場合と同様に，まず与えられたＣＳＰプログラムに対し状態の集合を考え，その上の二項関係を定義することによって，プログラムの実行中の詳細を無視し入出力関係のみに着目したセマンティクスを与える．このセマンティクスを定める際に，多くの類似の論文で行われているような，個々のプロセスについてそれぞれの意味を定め，後にそれらをもとに，全体の

主論文の要旨

報告番号	※甲第　　号	氏名	村上昌己

意味を定めるといった方法をとらず，プログラム全体について，ある１ステップの実行の効果と，続いて実行されるプログラムの残りの部分の意味から，全体の意味をきめるという方法をとる．このような方法は，(Elrad Francez 82)のcentralized approachと同じものであり，また，表示的意味論における接続法(continu-ation)の拡張とも考えられる．このセマンティクスをもとに，ＣＳＰの部分的正当性を証明する公理系を提案し，その無矛盾性を示す．この体系は，セマンティクスを定義したときと同様に，centralized approachに沿った推論の手順をふんだ証明を可能とするものである．

この章では次に，プログラムの実行中に現れる命令及び途中の状態に関する情報をも記録したセマンティクスとして，計算履歴集合を，やはり同様にして，centralized approachによって定義する．続いて，これをもとに，ＣＳＰの部分的正当性とデッドロックフリー性を，同時に検証する公理系を与え，その無矛盾性(soundness)を示す．

従来のＣＳＰの検証体系は，推論規則が複雑であり，プログラムの一部の働きを理解するのに，証明全体を見渡す必要があるなど，証明をドキュメントとして用いる際に問題点があった．ここで与えた体系は，そのような点を改善するものである．

第４章では，並列プログラムの検証体系について，その数学的性質を議論する．Apt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(completness)の概念を

主論文の要旨

報告番号	※甲第　　号	氏名	村上昌己

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は$\mathcal{S}$としてwhile プログラム及び条件付臨界領域によって制御されるcobegin-coend 文を許す並列プログラムのクラスを選び，帰納的述語，帰納的可算述語，有限反証的述語等のクラスの完備性についていくつかの結果を示した．以上の結果は，プログラムの性質のうち取扱いが可能であるもの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Owikiの公理系をもとにして得られたものである．一方，並列プログラムの正当性検証体系として第1章に述べたようにOwikiらの方法の他に，Flon，Suzuki の公理系，即ち並列プログラムを非決定性プログラムとして検証を行う体系が提案されている．この体系の特徴としては，そこで扱える性質は特定な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大ないしは最小不動点で表現される性質ならば，一般に取扱うことが可能である．また一般に並列プログラムの性質は，ある述語関数の不動点を用いてあらわすことができることが，Emerson- Clarke によって知られている．

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，個々の性質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，一般的な取扱いが可能である．

主論文の要旨

報告番号	※甲第　　号	氏名	村上昌己

そこでこの章では，並列プログラムを被防護命令によって表し，プログラムから作られるある述語関数の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，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次のような結果を示している．

即ち，ある条件をもつ連続な述語関数の最大不動点で表される性質の証明について，Π^0_r は $r > 0$ で完備である．

また，ある条件をもつ連続な述語関数の最小不動点で表される性質の証明について，Σ^0_r は $r > 0$ で完備である．

さらに，連続な述語関数の最大不動点で表される性質のうち，不変的性質と呼ばれるものについて，Σ^0_r は $r > 0$ で完備であること等を示している．

最後に，あとがきとして，今後の研究の方向について述べている．