審 査 の 結 果 の 要 旨

氏 名　　末 永　幸 平

本論文は、オペレーティングシステム等を構成する現実的な並行プログラムの信頼性の向上を目的として、並行プログラムの型システムに基づく静的検証手法を提案している。特に本論文では、デッドロックと資源使用という二つの安全性問題に対処するための型システムを構築している。

本論文の第一章では、本研究の背景と概要について述べられている。

本論文の第二章では、デッドロック検証手法について詳述されている。本手法によって、(1) 入れ子構造をとらないロックプリミティブ (2) 破壊的代入が可能なロックへの参照 (3) 割り込みという三つの特徴を備えた並行プログラムを扱うことができる。ネットワークプロトコル等の現実的な並行プログラムの多くがこれらの特徴を有しているにもかかわらず、既存のデッドロック解析手法ではこれらの特徴を有するプログラムを扱うことができなかった。本研究では、これらの特徴を備えた計算体系が構築され、その計算体系で記述されたプログラムのための型システムが提案されている。さらに、この型システムに基づいて、ネットワークプロトコルの実装の一部に対して行った検証実験の結果が報告され、本手法の有効性が示されている。

本論文の第三章では、パイ計算のための資源使用法解析手法が提案されている。資源使用法解析は、逐次プログラムに対して非常に多くの研究がなされて来たが、並行プログラムに対する研究は少なく、特に資源や通信チャネルを実行時に生成してアクセスするような現実的な並行プログラムに対する検証手法は研究されていなかった。本研究では、そのような並行プログラムに対する資源使用法解析手法を構築するために、パイ計算に資源の生成やアクセスを行うプリミティブを追加し、その計算体系のための型システムを定義している。この型システムは、禁じられているアクセスを行わないという通常の資源安全性に加えて、プログラムが正常終了すれば、必要なアクセスは全て行われているという部分活性を保証する。さらに、プログラマが型に関する複雑な記述をしなくても済むように、健全な型推論アルゴリズムが設計され、このアルゴリズムに基づいてパイ計算に対する資源使用法解析器のプロトタイプが実装された。

本論文の第四章では、関連研究との比較が述べられている。

以上で述べたように、本研究は、現実的な並行プログラムにおいて従来扱うことが困難であった安全性問題に対して型システムに基づく検証手法を与えており、本論文は博士（情報理工学）の学位請求論文として合格と認められる。