審 査 の 結 果 の 要 旨

氏 名　マーティ　ニコラ

本論文は、オペレーティングシステムカーネルにおけるメモリ領域の保護に関する性質を形式的に検証するための新しい技術に関して述べている。近年、組込みシステムのソフトウェア等、ハードウェアに近い低レベルのソフトウェアの形式的検証の研究が活発である。しかし、低レベルソフトウェアは複雑であり、しばしば複数のプログラミング言語で記述され、しかも難解な制御フローを実装しているため、その検証は極めて困難である。本研究では、そのような低レベルソフトウェアにおける最も基本的な性質であるメモリ領域の保護に関して、分離論理と呼ばれる枠組みのもとで、正当性が保証されしかも効率のよい検証系を構築し、C 言語および機械語で書かれたプログラムの検証に成功した。しかも、本研究は、ネットワークデバイスのための組み込みオペレーティングシステムである Topsy を形式的検証の具体的な対象としている。

本論文の第 1 章では本研究の背景とアプローチについて概説されている。本論文の以下の部分は第一部と第二部から成り立っている。

第一部では、まず第 2 章において、Hoare 論理の拡張である分理論理、Coq 証明支援系、Topsy に関する背景知識が説明された後、第 3 章において、Coq 上で分離論理の公理化が行われたうえで、Coq のタクティクを用いて、リスト操作を行う C 言語風のプログラムの検証が行われている。第 4 章においては、有限長の整数理論の上で、コンテキストスイッチングを行う MIPS 風の機械語のプログラムの検証が行われている。

第二部では検証ツールについて述べられている。第 5 章において、形式的検証を効率化するために、Coq 上に効率のよい検証系が構築され、その正当性が形式的に検証されたうえで、形式的証明から取り出された Caml のプログラムによって実際に検証が効率よく行えることが示されている。第 6 章では、C 言語風のプログラムから機械語のプログラムへの翻訳系の正当性が形式的に検証され、検証済みの C プログラムから検証済みの機械語プログラムが得られることが示されている。

第 7 章では本論文の貢献についてまとめられている。

以上で述べたように、本研究は低レベルソフトウェアの形式的検証の技術を大きく進展させており、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。