審 査 の 結 果 の 要 旨

氏　　名　　住 井　英 二 郎

本論文は、情報隠蔽形式に関わるプログラムの等価性に対する二つの証明方式について報告している。二つの証明方式とは、論理関係と双模倣である。また、本論文が対象としている情報隠蔽形式とは、型抽象と完全な暗号化（動的封印）の二つの形式である。

本論文は５章から成り、第１章では、本研究の背景と目的について述べられている。型抽象はプログラミング言語において最も基本的な情報隠蔽形式であり、型抽象について論じる主要な方式として論理関係（logical relation）が知られている。暗号化はもう一つの基本的な情報隠蔽形式であり通信システムにおいて支配的であるが、暗号化に似た操作はプログラミング言語においても有用であり動的封印と呼ばれている。本章では、二つの情報隠蔽形式の間に形式的な関連を確立し、一方の理論を他方へ応用する重要性について指摘されている。

第２章では、型抽象に対する理論を動的封印に適用している。具体的には、動的封印のためのプリミティブにより拡張された単純型つきラムダ計算に対して、論理関係が定義されている。この理論の応用の実例として、いくつかのセキュリティプロトコルの安全性が証明されている。

第３章では、動的封印のための双模倣（bisimulation）の理論が構築されている。論理関係と異なり、この理論は再帰関数や再帰型のある言語、もしくは、まったく型のない言語へ容易に拡張できる。本章では、動的封印のある型なしラムダ計算が定義され、様々な抽象データ構造の実装の等価性や、複雑な暗号プロトコルの正しさを証明することにより、この理論の強力さが示されている。

第４章では、前章の双模倣の理論が動的封印から型抽象へと逆移入され、総称型・存在型および再帰型のあるラムダ計算における、健全・完全なおかつ初等的な型抽象の理論が得ることに成功している。例として、抽象データ型、生成的関手、オブジェクトのエンコーディングについて論じされている。この成果は、以上のようなラムダ計算が定式化されて20年を経て、その文脈等価性に関する初等的な証明方式をはじめて与えたという点において、大きな意義がある。

本論文の最後の章では、型抽象から動的封印への型誘導変換の完全抽象の予想と、抽象性を損なわずに、静的検査・動的検査・無検査のコードを同時にサポートする言語環境への応用の方向の可能性について述べられている。

本論文は、以上に述べたように、情報隠蔽形式に関わるプログラムの等価性の証明方式を究めたものであり、理論的な深さと同時に実際的なプログラムの等価性を議論するための実用的な枠組みを与えている。よって、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。