

|              |                                                                               |
|--------------|-------------------------------------------------------------------------------|
| Title        | 定理証明器HOLにおけるオブジェクト指向理論の構築                                                     |
| Author(s)    | 矢竹, 健朗                                                                        |
| Citation     |                                                                               |
| Issue Date   | 2006-03                                                                       |
| Type         | Thesis or Dissertation                                                        |
| Text version | author                                                                        |
| URL          | <a href="http://hdl.handle.net/10119/975">http://hdl.handle.net/10119/975</a> |
| Rights       |                                                                               |
| Description  | Supervisor:片山 卓也, 情報科学研究科, 博士                                                 |

# 定理証明器 HOL におけるオブジェクト指向理論の構築

矢竹健朗

北陸先端科学技術大学院大学 情報科学研究科

2006 年 1 月 10 日

## 論文の内容の要旨

オブジェクト指向開発法の上流工程では、UML に代表されるモデリング言語により、分析モデルが構築される。分析モデルは図解ベースの表現であるため、解釈が曖昧であり、矛盾や誤りを含みやすいという問題がある。システムの欠陥を早期発見するという意味で、分析モデルに形式的な意味論を与え、検証を行うことは重要である。本研究の検証対象はオブジェクトの属性に関する不変表明である。属性は、一般に整数やリストなどのデータ型により表現されており、これを検証するためには定理証明器を用いることが妥当である。

本研究では、分析モデル検証の意味論として、定理証明器 HOL にオブジェクト指向理論を実装した。分析モデルは抽象型や問題領域に特化した型によって高度に抽象化されるという特徴がある。本研究では、このような分析モデルの特徴に対応するために、オブジェクトが任意の型の属性を持つことを可能とした。HOL の単純一階型システムにおいては、任意の型の属性を任意の数だけ格納するオブジェクトを一般的な型として表現するのは困難である。そこで本研究では、オブジェクト指向理論をアプリケーションの型情報に特化して自動生成するというアプローチをとる。アプリケーションに出現する型が予め与えられれば、一階の型システムでもオブジェクトを表現することが可能となる。

理論の健全性は definitional extension により保証する。これは、既存の健全な理論から定義の導入または健全な推論規則による導出のみを許して新しい理論を構築する手法であり、HOL において理論を構築する際の標準的な手法である。具体的には、リストや組の理論を用いてオブジェクトを格納するためのヒープメモリ構造を定義し、その操作的意味論からオブジェクト指向の公理を導出する。

不変表明の検証法としてコラボレーションに基づく手法を提案する。この手法においては、コラボレーションをオブジェクト指向理論により与えられる基本的な演算子を用いた関数適用列として定義し、不変表明をシステムの初期状態からの遷移列に関する帰納法により証明する。状態遷移図と比較して、コラボレーションはクラスに横断する概念であり、複数のオブジェクトにまたがる不変表明の検証に有効である。

キーワード： オブジェクト指向、定理証明、HOL、不変表明、コラボレーション