

|              |                                                                                 |
|--------------|---------------------------------------------------------------------------------|
| Title        | 高階述語論理定理証明器HOLのための問題領域ライブラリの構築                                                  |
| Author(s)    | 矢竹, 健朗                                                                          |
| Citation     |                                                                                 |
| Issue Date   | 2002-03                                                                         |
| Type         | Thesis or Dissertation                                                          |
| Text version | author                                                                          |
| URL          | <a href="http://hdl.handle.net/10119/1539">http://hdl.handle.net/10119/1539</a> |
| Rights       |                                                                                 |
| Description  | Supervisor:片山 卓也, 情報科学研究科, 修士                                                   |

# 高階述語論理定理証明器 HOL のための 問題領域ライブラリの構築

矢竹 健朗 (010118)

北陸先端科学技術大学院大学 情報科学研究科

2002 年 2 月 15 日

キーワード: HOL, 問題領域, オブジェクト指向.

## 1 背景

オブジェクト指向開発法は大規模システムの開発に非常に有効であり、実際のシステム開発でも採り入れられつつある。

オブジェクト指向開発法の上流工程では、分析モデルが構築される。この分析モデルでは、対象とする概念が非常に抽象的なものであるため、曖昧になりがちであり、それゆえ、矛盾や誤りを含みやすいという問題がある。この誤りが開発の下流工程で発見された場合、修復には非常に大きなコストがかかってしまう。また、発見されない場合はシステムに大きな欠陥をもたらすことになる。

この問題の解決法として、定理証明技術の分析工程への応用手法が提案されている。この手法では、UML で提案されている複数のモデルを形式化し、統合写像と呼ばれる概念により、それらを一つのモデルに統合する。統合したモデルから公理系を自動生成し、証明すべき命題を定理証明器 HOL で証明することにより、複数のモデル間の一貫性を保証する。

## 2 問題点

現状は、HOL での証明は開発者にとって負担が大きい。これは、HOL には、自然数、リスト、文字列といった原始的な理論しか定義されていないことが原因である。式の中に原始的な要素が多く含まれる場合、その式がアプリケーションレベルでどういった意味を持つのが理解しにくく、証明の方向性がつかみにくい。また、原始的であればそれだけ事実の積み重ねが足りないということであり、証明には非常に多くのステップを要してしまう。HOL での証明を効率化することは、開発を円滑に進める上で極めて重要である。

### 3 目的

これを解決する方法として、現実世界のある問題領域に特化した、高級なデータ型、オペレータ、定理を含む定理モジュールを準備しておくというものがある。この高級定理モジュールを用いれば、証明ステップが削減されるとともに、式の意味の理解が容易になり、開発者のもつ問題領域に関する知識を生かした直感的な証明が行えるようになる。式の意味を理解しながら証明を進めることは、その問題領域の本質を理解することにもつながる。

本研究では、あらゆる領域に適用可能な定理モジュールの構築法を提案する。この方法では、あらゆる領域に適用可能とするために、オブジェクト指向分析モデルを基礎として定理モジュールを構築する。また、オブジェクト指向分析モデルは人間の思考の自然な表現であり、このモデルから定理モジュールを生成することにより、思考の単位となるような定理を得ることが可能である。

### 4 研究内容

まず、あらゆる領域を扱うためのオブジェクト指向の枠組みを HOL に実装した。

- 領域の考え方

領域を協調動作するオブジェクトの集合と考える。領域の状態は、個々のオブジェクトの属性と、オブジェクト間に張られているリンクによって表現する。オブジェクトは関数を持ち、属性の変更、リンクの張替えを行うことができる。あるオブジェクトの関数呼出しを起点に、複数のオブジェクトが関数を呼び出しあい、領域の状態を変化させる。

- クラスモデル

本研究で導入するオブジェクト指向分析モデルは、単純にするためにクラスモデルのみとする。クラスは、属性、リンク集合、関数を持つ。リンク集合はその値がオブジェクトの集合である特別な属性である。

- 領域の理論

クラスモデルの意味付けはモデルを領域の理論に対応付けることによって行う。公理系は、次の要素から構成される。

- 領域の型
- 領域の初期値を表す定数
- 基本関数の集合
- オブジェクト生成関数の集合
- 存在検査述語の集合

- 複合関数の集合
- 公理の集合

基本関数は、属性操作関数とリンク集合操作関数に分類される。属性操作関数はモデルにおける属性に対応して与えられる関数であり、属性の取得、更新の機能を持つ。リンク集合操作関数はモデルにおけるリンク集合に対応して与えられる関数であり、リンク集合の取得、初期化、リンクの追加、削除の機能を持つ。オブジェクト生成関数、存在検査述語はモデルにおけるクラスに対応して与えられる関数、述語であり、オブジェクト生成関数は領域内にオブジェクトを生成する機能を持ち、存在検査述語はオブジェクトが領域内に存在するかどうかを検査する機能を持つ。複合関数はモデルにおける関数に対応して与えられる関数であり、その式は関数の意味記述をもとに定義される。公理はこれらのオペレータに関する関係を示すものである。

#### ● HOL への実装

領域の公理系をHOLの既存の理論を用いて作成する。まず、一般的なクラスのオペレータの定義と定理を格納した定理モジュール `obj_ax` を用意した。これはリストに対する要素の追加と削除を基礎として構築される。特定の領域が与えられたとき、まず、クラスごとに `obj_ax` を継承した定理モジュールを作成する。各定理モジュールにおいて `obj_ax` のオペレータをそのクラスの情報をもとに詳細化し、それらの間の関係を証明する。得られた各クラスの定理モジュールに対し、それを継承する一つの定理モジュールを作成し、異なるクラスのオペレータの関係を証明する。

定理モジュールの構築は以下の手順で行う。

1. オブジェクト指向分析モデルによる領域分析
  - (a) 領域分析によりクラスモデルを生成する。
  - (b) クラスモデルが決定すると関数を定義するための基本関数、オブジェクト生成関数が与えられる。これを用いて関数を定義する。これは模式言語を利用して行う。
  - (c) モデルに制約を与える。これは、関数に事前条件、事後条件を与えることによって行う。条件は参照関数から構成される論理式である。
2. モデルを HOL に実装した公理系に変換する。
3. 模式言語で記述された関数定義を HOL の関数定義に変換する。
4. 制約記述を命題に変換し、生成された公理系の上で証明する。
5. 他のシステムから利用できるような型を生成する。

例題として、貸出システムについて定理モジュールを構築した。その結果をもとに、定理モジュールの再利用可能性について検討した。