JAIST Repository
https://dspace.jaist.ac.jp/

Title	オブジェクト指向方法論のための検証フレームワークに関する研究
Author(s)	花田，真樹
Citation	
Issue Date	1999-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/1221
Rights	
Description	Supervisor:片山 卓也，情報科学研究科，修士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

オブジェクト指向方法論のための検証フレームワークに関する研究

花田 真樹

北陸先端科学技術大学院大学 情報科学研究科

1999 年 2 月 15 日

キーワード： オブジェクト指向, 形式的モデル.

現在、多くのオブジェクト指向方法論が提案されている。それらの方法論の１つにOMT法がある。OMT 法では対象システムを記述するために３つのモデル (オブジェクトモデル、動的モデル、機能モデル) を用いる。この３つのモデルは、対象システムを直交する３つの視点に分割して記述する。しかし、ここで用いられるモデルは形式的取扱いが十分でないため、計算機による支援を困難にしている。

以上の問題点から、オブジェクト指向方法論のための形式的モデル (以下、形式的モデル) が提案されている。このモデルは OMT 法を基礎として形式化を行ったものであり、集合と関数の概念を用いて定義されている。

本論文では、形式的モデルに基づいた検証を計算機により支援する手法を提案する。

検証を計算機上で支援するソフトウェアのことを検証アプリケーションと呼ぶ。本論文では、まず、データの流れに注目した一貫性検証、不変表明を用いた一貫性検証、状態に注目した属性の値に関する検証に関してどのような支援が行えるかの考察を行った。データの流れに注目した一貫性検証は公理と推論規則による公理系より機能モデル記述されているデータフローを証明する形式で行われる。不変表明を用いた一貫性検証はクラスに対して高階述語論理を用いて不変表明を与え、アクションが実行されても不変表明を満たしているかどうか検証するものである。状態に注目した属性の値に関する検証は、ある状態における属性の値がどのような性質を持つかを高階述語論理を用いて検証するものである。この結果、データの流れに注目した一貫性検証に関しては決まったアルゴリズムにしたがって自動証明できることがわかった。残りの２つの検証法に関しては高階述語論理を用いているため自動証明は不可能であり、基礎となる理論や証明ステップを定理証明系を用いて支援できることがわかった。

Copyright © 2000 by Masaki Hanada

形式的モデルを用いた検証法は、これらの他にも無数にある。そこで本論文では、検証フレームワークという概念を提案する。検証フレームワークでは、検証アプリケーションをフローズンスポットとホットスポットに分解する。フローズンスポットは複数の検証アプリケーションに共通な部分であり、あらかじめ実装しておく。ホットスポットは検証アプリケーション毎に異なる部分がある。検証アプリケーションを作成する場合はホットスポットの部分だけを実装して実現できる。これにより、検証アプリケーション作成のコストを削減され、柔軟に計算機上で検証を行うことができる。

検証フレームワークは ML と HOL を基礎とした計算機環境に実装した。検証フレームワークでは、構築された形式的モデルや付加情報は ML の参照型変数に格納される。これは、モデルの選択/加工といった操作は ML のほうが HOL より扱い易いためである。構築されたモデルには HOL の概念が割り当てられ、特定の検証を支援するのに適した HOL における環境を生成する。このことは、割り当て関数、翻訳関数、生成関数により実現する。割り当て関数は、構築された形式的モデルや付加情報のおのおのの要素に HOL における要素を対応づける。翻訳関数は、形式的モデルや付加情報の HOL における解釈を与える。生成関数は、構築された形式的モデルや付加情報に基づいて HOL における環境を生成する。これらの関数のうち形式的モデルに固有なものは、その意味定義に基づいてフローズンスポットとして実装される。検証アプリケーションは、追加する概念に基づいたこれらの関数をホットスポットとして実装することにより実現される。