オブジェクト指向方法論ための検証支援環境に関する研究

立石 孝彰

北陸先端科学技術大学院大学 情報科学研究科

2000年2月15日

キーワード: オブジェクト指向方法論、分析モデル、検証、状態遷移図、計算機支援.

近年、計算機の急速な発展と計算機利用の増加に伴い、開発するシステムが大規模になってきている。そのようなシステム開発に対して、様々なオブジェクト指向方法論が提案されてきた。オブジェクト指向方法論では、オブジェクトを用いて、開発システムの分析と設計を行なう。分析では、開発システムの論理的な振舞を示すために、分析モデルを構築する。分析モデルに基づいて、開発システムの設計と実装を行なうため、分析されたモデルが正しくないと、そのモデルは、設計と実装にまで悪影響を及ぼす。医療システムや航空システムなどのように、安全性を最も重要視するシステムを開発する場合がある。このようなシステムでは、テストツールやシミュレーション環境などを利用した妥当性の確認だけでは不十分であり、分析モデルに対する正当性を保証する必要がある。現在までに提案されたオブジェクト指向方法論において、分析モデルの振舞に関する正当性まで触れたものは少ない。

オブジェクト指向方法論では、開発システムに表れるオブジェクトを、クラス図を用いて表わし、互いに並行して協調動作を行なうオブジェクトの振舞を、属性評価を含む状態遷移図を用いて表わす方法が一般的に用いられる。状態遷移図の振舞を検査するために、**モデルチェッキング**と呼ばれる検証方法が提案されている。この手法では、到達可能なすべての状態を探索することで、モデルの検査を行なう。このため、状態爆発という問題が起こる。そこで、*BDD(Binary Decision Diagram)* と呼ばれる効率的なデータ表現で、状態遷移図を表現する方法が提案されている。この方法を用いることで、探索する状態数を減らし、検証を効率的に行なうことができる。しかし、オブジェクトが持つ属性は、無限の値を持ち得る。属性が無限の値を持つ時、モデルチェッキングでは、探索する状態数は無限となり、属性に関する性質を検証できない。故に、本論文では、数学的な証明を用いて、状態遷移図によって振舞が表わされるオブジェクトの属性についての検証方法を提案

する。この検証方法を用いることで、属性に関する公理と定理を用いて証明を行なうため、無限の値を持ち得るオブジェクトの属性に関する検証を行なうことができる。

本論文の構成は、以下の通りである。2 章では、本論文で用いる例題モデルを挙げる。これには、エアコンのシステムを用いる。このエアコンのシステムは、3 つのクラスから構成される。そして、それらのクラスには、それぞれのクラスから実体化したオブジェクトの振舞を表わす状態遷移図がある。

3 章では、*F-Model*の概要について触れる。F-Model は OMT 法と呼ばれるオブジェクト指向方法論に基づく形式的モデルである。本研究では、F-Model に基づく分析モデルを、関数型言語 SML を用いて、計算機上で取り扱った。F-Model は、SML のデータ型として取り扱い、開発システムに対する分析モデルは、SML のデータとして定義する。SML のデータとして定義したエアコンの例題モデルを例として挙げる。

そして 4 章では、分析モデルに対して、ある性質が常に成立することを検証するための公理系と、検証における証明方法について述べる。このことを証明するためには、すべての状態において、ある性質が成立することを示せば十分である。ここで、証明したい性質のことを**大域表明**と呼ぶ。大域表明を証明する為には、個々の状態で必ず成り立って欲しい性質をあらかじめ定める。これを**局所表明**という。本論文では、局所表明の妥当性を、状態遷移図に関する帰納法を用いて導く。こうして妥当性が証明された局所表明を、**局所不変表明**と言う。そして、各々の局所不変表明表明を用いて大域表明を導く。

分析モデルに誤りがあると、再び分析を行ない、分析モデルを設計し直す。このような分析モデルの構築において、変更と検査は繰り返し行なわれる可能性がある。このため、モデルが変更される度に公理系を定義し直さなければならない。公理系の定義には、多くのコストを費やすため、公理系は分析モデルに対して自動的に生成するべきである。本論文で提案する公理系は、F-Model に基づく様々な分析モデルに対して適用できるように定義する。このため、本論文で提案する検証方法は、オブジェクト指向方法論を用いて分析されたモデルすべてに対して適用できる。こうして定義した公理系を、エアコンの例題モデルに対して適用して、検証を行なうことで、具体的な検証方法を示す。

5 章では、4 章で示した公理系についての考察を行なう。考察には、提案した公理系と検証方法を用いて、検証可能な性質についてのべる。

検証には、通常多くの証明ステップと、検証のための前準備が必要となる。さらに、分析モデルは、変更が頻繁に行なわれる。分析モデルに対する検証を、効率的に行なうために、6 章と 7 章では、計算機による支援を提案し、HOL を用いた検証の方法を示す。計算機による支援には、SML と、高階述語論理に基づく定理証明器 HOL を用いる。本論文で提案した公理系は、F-Model に基づく様々な分析モデルに対して適用可能な形式で定義されているため、計算機によって分析モデルから、分析モデルを検証するための公理系と証明戦略を自動生成できる。本研究では、この検証支援のための環境を開発する。