演繹的検証法と探索的検証法の組み合わせについての研究

川崎　恵久 (0610027)

北陸先端科学技術大学院大学 情報科学研究科

2009 年 2 月 05 日

キーワード: 形式手法, CafeOBJ, 対話的検証, モデル検査.

背景と目的

近年，ソフトウェアや情報システムにおいて，高信頼性や安全性を重要視するようになり，それらの性質を十分に検証する必要がある．現在，ソフトウェアや情報システムにおける検証方法は大きく分けて二つある．一つはモデル検査を用いた探索的な検証法で，もう一つは推論ベースの演繹的な検証法である．二つの検証法にはそれぞれ異なる特徴やメリット・デメリットを持っている．例えば，無限の状態をとるシステムをモデル検査する場合には，何らかの方法で有限状態に抽象化しなければならない．しかし，推論による検証は，無限の状態でも検証が可能である，一方では，推論による検証は，人の手による労力がモデル検査よりも必要である，などである．

そこで本研究では，演繹的な検証法と探索的な検証法の利点を上手く組み合わせ，従来の検証法よりもより効率的な検証法を提案することを目的とする．

1　研究の手法

代数仕様記述言語 CafeOBJ は，順序ソート項書換理論に基づいた代数仕様言語であり，等式を書換規則として解釈し，計算機上で実行することが可能である．また，CafeOBJ には演繹的な検証法と探索的な検証法に相当する二つの検証法を持つ．それぞれ証明譜による検証，Search コマンドを用いたモデル検査による検証がそれに当たる．CafeOBJ は OTS（観測遷移システム）に基づいて記述することが出来る．CafeOBJ/OTS 法に基づいて記述された仕様は，証明譜の検証が可能で，また，Search コマンドによる検証が可能である．それにより，両検証間を同時に扱う場合，仕様の変換や仕様が同一であることを示すための証明などの必要がない．

CafeOBJ において Search コマンドを用いて全探索のモデル検査を実行する場合，withStateEq と観測等価関数を用いて全探索する方法がある．また，もう一つの方法として，等式によって状態を有限化・抽象化する方法がある．withStateEq と観測等価関数によるモデル検査は，ある二つの状態において観測等価関数に基づき探索枝が一致したと判断された場合，その状態を等価とみなし，状態の削減を随時行いながら探索する方法である．等式によって状態を有限化・抽象化する手法は，証明譜により正当性が証明された”状態の抽象化を行うような等式”を宣言してあらかじめ状態を縮退させ，モデル検査にかける方法である．後者の方法は，演繹的な検証と探索的な検証の組み合わせと考えられる．

以上の方法は，相互排除プロトコル QLOCK で検証の有効性を示している．QLOCK においては，等式を用いる検証法は，withStateEq と観測等価関数を用いる検証よりも探索時間が短いことが示されている．

しかし，他のプロトコルに対し有効性が確かめられていないため，QLOCK とは性質の異なるプロトコルに対し有効性を求める必要があると考えられる．また，等式を用いた状態の有限化・抽象化する手法に関して，等式の発見に関しての指針が示されていないため，等式の発見が困難であると考えられる．そこで本研究は以下のことを行う．

- 通信プロトコル SCP に対して検証法を適用する
- 等式の発見法や分類の体系化

QLOCK とは異なる性質を持つプロトコルに対して検証を行うことで，有効性を高め，等式の発見や分類の分析を行い体系化することで，検証の効率化を目指す．

2　結論と今後の課題

通信プロトコル SCP に対して，等式による状態の有限化・抽象化手法を適用した．その結果，withStateEq と観測等価関数をもちいた検証よりも探索時間が大幅に短くなったことが分かった．等式の発見法や分類，いくつかのパターンを発見し体系化することができた．また，等式を導入する際，追加する等式の種類によっては探索時間が追加しない場合よりかかってしまうことも発見した．今後の課題としては，SCP より複雑な通信プロトコル ABP に関して適用を実験してみる，どのような等式が追加すべき等式なのかを検証していくといったことがあげられる．