平成20年度 情報工学コース卒業研究報告要旨

高木 研究室	氏　　名	尾 野　紀 博
卒業研究題目	順序回路の形式的検証における回路変換による フォールスネガティブ削減手法	

近年、設計される論理回路の大規模化や複雑化に伴い、設計段階で誤りを犯す危険性が高まっている。設計段階で可能な限り早く誤りを発見することが重要になってきており、設計された順序回路が正しく動作するかどうかを数学的に検証する形式的検証の研究がなされている。形式的検証手法の一つとして、有限サイクル分にの動作を完全に保証する限定モデル検査がある。

初期状態から多くの状態を遷移して初めて発現するような設計誤りを検出する検証では、初期状態からの到達可能性を考慮しない限定モデル検査を用いた検証が行われる。そのような検証の一つとして、多段限定モデル検査がある。多段限定モデル検査は、仕様違反が見つかるか仕様違反がないことが示されるまで、初期状態を考慮しない限定モデル検査を繰り返し行う。このような検証では、到達不能状態に起因するフォールスネガティブが発生することが知られている。ここで、フォールスネガティブとは、検証アルゴリズムが、本来、初期状態から到達不能であるため仕様違反ではない動作を誤ってバグと判定してしまうことである。このような形式的検証において、フォールスネガティブを削減することは、誤検出されたバグの対応に費やされる検証時間を削減する上で重要な問題である。

本研究では、回路変換を行うことにより、到達不能状態における動作を、誤検出されないような動作に変更することで、フォールスネガティブを削減する手法を提案する。本手法では、回路が正しい動作をしている間は常に成り立っている不変条件が成り立たない到達不能状態において、誤検出が発生することに着目する。これにより、誤検出が減ることで、検証の高速化が期待できる。

提案するフォールスネガティブの削減手法では、設計された回路をそのまま検証対象とせず、回路変換を行った後の回路を検証対象とする。また、それに伴い検証仕様も変換し、変換後の検証仕様を用いて検証を行う。回路変換では、RTL(Register Transfer Level) で設計された回路を解析し、到達不能状態においてフォールスネガティブにならないような動作を回路に追加する。仕様の変換では、LTL(Linear Temporal Logic) 式で記述された仕様を、回路変換を考慮した仕様に変換する。ここで、回路に追加する動作は、不変条件が成り立たなければエラー状態に遷移するというものである。仕様の変換は、エラー状態では仕様は満たされているという仕様を追加するものである。変換後の回路が変換後の仕様を満たすことが示されれば、変換前の回路が仕様を満たすことが保証される。

提案手法を実装し、2つのベンチマーク回路に対して回路変換を行い、多段限定モデル検査による実験を行った。その結果、回路変換によるフォールスネガティブの減少と検証の高速化が確認できた。