発表概要

証明支援系Coqを用いた有界モデル検査アルゴリズムの検証

藤井 采人[1,a)]　石井 大輔[1]

2019年3月18日発表

有界モデル検査（bounded model checking，BMC）は，システム（状態遷移系）と性質を述語論理式にエンコードし，その充足性をSAT/SMTソルバーで判定することにより，システムの安全性を示したり，不具合を見つけたりするための方法である．さまざまなBMCアルゴリズム（BMC法）が提案されているが，それぞれの方法は，実行パスのunrolling，実行パスに関する帰納法，状態の抽象表現など煩雑な考察に基づいて設計されている．BMC法の設計や実装にあたっては，背景の考察を理解して正確に行わなければ，検査器の信頼性が損なわれてしまう．そこで本研究では，高信頼なBMCツールの実現を目標に，BMC法および背景となる考察を証明支援系を用いて記述・検証し，さらに前記BMC法の記述をそのまま用いて検査を実施可能にする．具体的には，証明支援系Coq上にSheeranらが提案したBMC法を実装し，その健全性を証明し，プラグインされたSMTソルバーを利用して検査を実施可能にした．本研究の貢献は，(1) Sheeranらが提案した複数のBMC法とその健全性の証明をCoqで記述・形式化するとともに，一般的なBMC法へ流用可能な関数や定理を同定・整備したこと，(2) システム，性質，BMC法，その健全性の証明，SMTソルバーの入出力等をCoq上で記述し，検査対象システムの記述，システムの検査，BMC法の正しさの検証といった作業を統合したこと，の2点である．

Presentation Abstract

Verification of Bounded Model Checking Algorithm Using Coq

Saito Fujii[1,a)]　Daisuke Ishii[1]

Presented: March 18, 2019

Bounded model checking (BMC) is a formal method for verifying safety properties of systems modelled as transition systems. In a verification process, it encodes a system and its property into a predicate logic formula and checks the satisfiability of the formula. Various BMC algorithms have been proposed, each of which is carefully designed by e.g., unrolling of execution paths, inductions on execution paths, and abstract representation of states. To provide a reliable BMC tool, we need to understand their background consideration and design/implement a BMC algorithm correctly. In this research, to provide a reliable BMC tool, we describe BMC methods and verify their soundness using a proof assistant; then, the same BMC method description is utilized for model checking on top of the proof assistant. Our contributions are as follows: (1) We describe several BMC algorithms proposed by Sheeran et al. using Coq; then, we formalize the proof of the soundness of the algorithms; also, we identify/prepare functions and theorems that can be applied to generic BMC methods. (2) We describe various objects related to BMC on top of Coq, e.g., target systems, properties, BMC algorithms, their soundness proofs, and inputs/outputs of SMT solvers. Accordingly, several operations are integrated such as modeling of target systems, model checking, and verification of the underlying algorithms.

This is the abstract of an unrefereed presentation, and it should not preclude subsequent publication.

[1] 福井大学
University of Fukui, Fukui 910–8507, Japan
[a)] donn2005s@gmail.com