発表概要

手続きを含む命令型プログラムを検証するための証明戦術の提案

小島 裕登[1,a)]　山田 俊行[1]

2021年1月13日発表

近年，プログラムの大規模化と複雑化にともない，プログラムの安全性は様々な分野でますます重要となってきている．大規模なプログラムの正しさを検証する際，人の手による証明だけでは膨大な時間を要するため，自動証明は必要不可欠である．しかし，大規模で複雑なプログラムに対して完全な自動化はほぼ不可能であり，人の手による証明は避けられない．そこで，重要な課題となるのが，部分的な自動証明は可能なため，人の手による証明の負担をできる限り削減する自動証明が期待される．そこで本発表では，Hoare 論理を用いて手続きを含む命令型プログラムの検証の自動化を提案する．我々は定理証明支援系 Coq を用いて自動証明を行うタクティクを開発した．本手法は，非再帰手続きのプログラムの正当性を証明する場合は，最弱事前条件を用いて検証条件を自動的に生成する．また，再帰手続きのプログラムの正当性を証明する場合は，最弱事前条件と最強事後条件を組み合わせることで検証条件を自動的に生成する．本手法のタクティクを用いることで，事前条件と事後条件とループ不変条件から，検証条件を自動的に生成できる．これにより，人の手による証明を検証条件に関する表明の正当性の検証のみにする．また，検証条件に関する表明についても簡易的な正当性の検証を自動化する戦術を開発した．

Presentation Abstract

Proof Tactics for Verifying Imperative Programs with Procedures

Hiroto Kojima[1,a)]　Toshiyuki Yamada[1]

Presented: January 13, 2021

In recent years, as programs have grown in size and complexity, program security has become increasingly important in many areas. Automatic proof is essential for verification of large scale programs since the huge amount of time required for manual proofs only. However, fully automated verification of complex programs is almost impossible to achieve and manual verification is inevitable. Therefore, the important issue is that automated proofs are expected to reduce the burden of manual proofs as much as possible since partially automated proofs are possible. In this presentation, we propose automatic proof to verify imperative programs with procedures by using Hoare logic. We develop automated proof tactics in Coq. Our method automatically generates verification conditions using the weakest preconditions in a non-recursive procedure. In a recursive procedural program, the verification conditions are automatically generated by combining the weakest preconditions and the strongest postconditions. By using the tactics of our method, we can automatically generate verification conditions. These tactics reduce manual proofs to only verifying the validity of assertions about verification condition. We also develop tactics to automatically prove simple correctness of assertions about verification condition.

[1] 三重大学工学研究科情報工学専攻
Department of Information Engineering, Graduate School of Engineering, Mie University, Tsu, Mie 514–8507, Japan
[a)] kojima@cs.info.mie-u.ac.jp