発表概要

定理証明支援系 Coq における余帰納的証明のガード条件の漸進的検査

小澤 祐也[1,a)]　中野 圭介[2,b)]

2018年10月31日発表

定理証明支援系 Coq では，無限に続くリストのような余帰納的構造を持つデータについての証明を，タクティクと呼ばれるコマンドを用いて進めることができる．ただ，Coq では無限のデータや証明をそのまま扱うことはできないため，再帰的な表現による有限の形で表している．このような無限のデータや証明は再帰関数として表現されるため，意味のないループの形でないという，ガード条件の検査（guardedness check）が証明の最後に行われている．このため証明全体を走査するために時間がかかってしまうという問題や，途中でガード条件が成立しなくなっていてもユーザは証明の最後の検査まで気づくことができないという問題がある．Coq には証明途中でガード条件の検査を行う Guarded コマンドが存在するが，これもそれまでの証明全体を走査するために，タクティクごとに実行すると時間効率が悪い．そこで本発表では，Coq における余帰納的証明のガード条件の検査を証明中に少しずつ行い，ガード条件が成立しなくなった際，即座にユーザに知らせることができるような手法を提案する．本手法ではタクティクの実行ごとに新しく作られた部分の証明のみを取得し，その部分的な証明に対してガード条件の検査を行う．検査を行った後は，その時点での環境やゴールの ID などの情報を保持しておき，次回のタクティク実行時のガード条件の検査に用いる．

Presentation Abstract

Incremental Guardedness Check of the Co-recursive Proof in Coq Proof Assistant

Yuya Ozawa[1,a)]　Keisuke Nakano[2,b)]

Presented: October 31, 2018

In the proof assistant Coq, we can manipulate a proof of co-inductive structure data, such as infinite lists, using a command called tactic. Coq handles infinite data and infinite proofs by representing them in a finite form with (co-)recursion. To justify this approach, Coq checks that the guardedness of infinite data and proofs in which no co-recursive expressions are invalid like the non-productive infinite loop, when every proof is completed. Hence, there are problems that the check takes time since it scans the whole proof, and the user can not notice the guardedness became unsatisfied in the middle of the proof until the final guardedness check finished. Although Coq provides a Guarded command that checks the guardedness in the middle of the proof, it is inefficient for users to execute the command by each tactic during a proof. In this presentation, we propose a method to check the guardedness of the co-recursive proof incrementally and notify the user immediately when the guardedness condition gets violated. In our approach, we only observe a newly-generated part of the proof and check the guardedness condition every time applying a tactic. At that time, we also store some information such as the proof environment and the identifier of the current goal.

[1] 電気通信大学大学院情報理工学研究科情報・ネットワーク工学専攻
Graduate School of Informatics and Engineering, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan

[2] 東北大学電気通信研究所
Research Institute of Electrical Communication Tohoku University, Sendai, Miyagi 980–8577, Japan

[a)] ozawa@ipl.cs.uec.ac.jp

[b)] ksk@tohoku.ac.jp