定理証明と検証

平成２５年度シラバス

２０１３年1月４日

国立情報学研究所

トップエスイープロジェクト

代表者　本位田　真一

1. 科目名

定理証明と検証

2. 担当者

今井 宜洋

3. 本科目の目的

本科目では証明支援器 Coq を用いたプログラミング検証を扱う。

証明支援器の持つ強力な表現力について理解し、関数型プログラミング言語

と組み合わせて実践できる技術を習得することを目的とする。

4. 本科目のオリジナリティ

証明支援器を使ったシステム検証に関する科目はこれまでなかった。

本科目では証明支援器 Coq を使って対話的に証明を構築する技術について学ぶことができる。

5. 本科目で扱う難しさ

高階述語論理を扱うことのできる対話的証明器は、高度な仕様記述能力と

強力な検証を可能とするが、証明の方針を人間が指示して構築する必要がある。

証明支援器 Coq にはタクティックと呼ばれる機構があり、この操作を

半自動化する。高度な検証を行うためには高階述語論理の扱いと

タクティックの習得が必要となる。

また、関数型スタイルのアルゴリズムの記述は、静的検証に適しており、

再帰関数や高階関数を使ったプログラムを理解する能力も重要となる。

6. 本科目で取得する知識・技術

証明支援器 Coq を使ってアルゴリズムを検証する上で必要となる技術を学ぶ。

具体的には、本科目では以下の項目について扱う。

- タクティックを使った証明の構築

- 高階述語論理で表現する高度な仕様記述
- 実際のプロジェクトで証明されたコードを使う

また、これらを学ぶことを通じて、Coq の表現能力の強力さを理解し、

的を絞った検証技法を意識できるようになる。

7. 前提知識

とくに必須となる前提知識は仮定しないが，ML や Haskell などの関数型言語の知識があれば理解の助けになる。

8. 講義計画

概要

- 第 1 回: 概要
- 第 2 回: Coq の基礎と Coq によるプログラミング
- 第 3 回: Coq の論理と仕様記述
- 第 4 回: 演習: 会計システムの検証
- 第 5 回: 停止性、証明の自動化
- 第 6 回: Java との連携
- 第 7 回: 事例紹介: 最短経路探索問題

詳細(予定、変更の可能性あり)

第 1 回: 概要

- 証明支援器(対話的定理証明器)とは
- Coq とは
- Coq の利用例
- Coq の導入について
- ファイルへの保存
- Definition コマンドによる定義
- Check, Print, Eval compute in
- モジュールのインポート
- Extraction コマンド

第 2 回: Coq の基礎と Coq によるプログラミング

- Coq の原理
- Inductive によるデータ型の定義
- 自然数

- リスト
- 練習問題

第 3 回: Coq の論理と仕様記述

- Coq での仕様記述
- 初めての証明
- 等式に関する証明
- 場合分けによる証明
- 帰納法を使った証明
- 演習問題

第 4 回: 演習: 会計システムの検証

- 問題設定
- 定義
- 演習

第 5 回: 停止性、証明の自動化

- 再帰関数と停止性
- Function コマンドによる高度な再帰関数の定義
- CoInductive による無限のデータ構造の扱い
- 証明付きデータ構造
- 自動証明を行うタクティック
- 独自タクティックの定義

第 6 回: Java との連携

- Coq2Scala とは

- Coq2Scala の導入について
- Java からの呼び出し
- サンプル

第 7 回: 事例紹介: 最短経路探索問題

- 問題設定
- アルゴリズムの定義
- 検証事項とその証明
- Extraction オプション
- 実行例とその結果

9. 教育効果

Coq を使って簡単なアルゴリズムの定義、証明事項の定式化とその証明ができるようになる。

また、Coq でどのような検証が可能なのか、検証したアルゴリズムをどのように

利用できるかについて理解する。

10. 使用ツール

- edubase Cloud および関連ツール
- 証明支援器 Coq
- Coq2Scala
- Scala, JDK

11. 実験及び演習

テキストで演習問題を設定している。これらに順次取り組むことによって、

実際の検証に必要な基本的な技術を習得する。

12. 評価

課題レポート、出席日数を総合して評価する。

13. 教科書/参考書

講師が作成したテキストを使用する。