「計算と論理」
Software Foundations
その0

五十嵐 淳
cal14@fos.kuis.kyoto-u.ac.jp
igarashi@kuis.kyoto-u.ac.jp

京都大学

October 7, 2014

担当教員について

- **名前**: **五十嵐 淳 (いがらし あつし)**
- **所属**: **情報学研究科 通信情報システム専攻 計算機ソフトウェア分野**
- **オフィス**: **総合研究 7 号館 224 号室 (火曜日の** 13:30 **〜**15:00 **は在室予定)**
- **講義についての質問・連絡**: `cal14@fos.kuis...`
  - TA **にも届くのでできるだけこちらを使ってください**
- **講義** WWW **ページ**: `http://www.fos.kuis.kyoto-u.ac.jp/~igarashi/class/cal/`

TA

- 奥村 健太郎 (おくむら けんたろう)
- 村井 涼 (むらい りょう)
- 所属: 情報学研究科 通信情報システム専攻 計算機ソフトウェア分野
- オフィス: 総合研究 7 号館 227 号室

講義内容

シラバスより

数理論理学の基礎と，数理論理学を用いた**計算機プログラムの検証**について講述する．また，講義を補完するため，証明支援系 (計算機上で数学的証明を行うシステム) である Coq **を用いた演習**を行う．

数理論理学

判断 (judgment) について (数理的手法で) 考える学問

判断 (命題ということもある)
真偽を考えることが可能な文

- **命題論理: 単純な判断を組み合わせて複合的な判断を構成する「接続詞」の理論**
  - **「かつ」「または」「ならば」「〜ではない」**
- **述語論理: 量化を伴なう判断の理論**
  - **「任意の○○について〜である」「ある○○が存在して〜である」**
- **(様相論理: 真偽を修飾する副詞の理論)**
  - **「必然的に〜である」「〜である可能性がある」「未来永劫〜である」**

数理論理学: 意味論と証明論

- 意味論…与えられた判断が「真である」とはどういうことかを考える
  - 真理値表 (論理関数) は命題論理の意味論のひとつ
- 証明論…与えられた命題の「証明」とは何か,「証明が同じ・違う」とはどういうことかを考える
  - 様々な証明 (記述) 体系: 自然演繹，シーケント計算，ヒルベルト流公理
  - 証明の構造について考える
    - 証明の等しさ，簡単さ

数理論理学: 意味論と証明論

- 意味論…与えられた判断が「真である」とはどういうことかを考える
  - 真理値表 (論理関数) は命題論理の意味論のひとつ
- 証明論…与えられた命題の「証明」とは何か,「証明が同じ・違う」とはどういうことかを考える
  - 様々な証明 (記述) 体系: 自然演繹，シーケント計算，ヒルベルト流公理
  - 証明の構造について考える
    - 証明の等しさ，簡単さ

計算機プログラムの検証

「計算機プログラム」の正しさの証明を与える

- **「正しさ」の基準 $\Rightarrow$ 判断として書かれた仕様** (specification)
- **例**:

リストを反転させる Scheme 関数 `rev` の仕様

任意のリスト `xs` について `(rev (rev xs))` $=$ `xs`

Q. **これだけで仕様として十分といえるだろうか？**
(他にも `rev` が満たすべき仕様はないだろうか？)

- c.f. **単体** (unit) **テスト**

証明支援系 Coq を用いた演習

証明支援系: 計算機で数学をするためのソフトウェア

- **数学的対象 (数，リスト，木などのデータ) 定義とその対象を操作するプログラムの記述言語**
  - Scheme のような関数型プログラミング
  - ただし静的に型がついている
  - そして文法がちょっと変わっている
- **(対象の性質を述べる) 判断の記述言語**
- **判断の証明の記述言語**
- **証明の検査機能**
- **(自動証明機能)**

を使って，色々なプログラムや，それが正しいことの証明を書く

Coq について

- フランス INRIA で開発されている証明支援系
- 2013 年に ACM SIGPLAN Programming Languages Software Award と ACM Software System Award を受賞
- 大規模な応用例も:
  - ソフトウェア安全性・正しさの保証
    - ★ レピダム社による OpenSSL のバグ発見
    - ★ C コンパイラ の検証 (CompCert プロジェクト)
  - 数学の証明の正しさのチェック

    ⇒ 例) 四色問題，ケプラー予想

講義内容

シラバスより

数理論理学の基礎と，数理論理学を用いた**計算機プログラムの検証**について講述する．また，講義を補完するため，証明支援系 (計算機上で数学的証明を行うシステム) である Coq **を用いた演習**を行う．

講義の (裏) テーマ

$$\text{証明} = \text{プログラム}$$

(Curry–Howard 同型対応としても知られる論理と計算の関係)

教科書

Benjamin C. Pierce, et al. Software Foundations.
http://www.cis.upenn.edu/~bcpierce/sf/

- **注意: オンライン・テキストで予告なく内容が変わる可能性あり**
- **本講義では 2014 年 10 月時点でのスナップショットを使う**
  - **講義 WWW ページから「ダウンロード用」のリンクあり**
  - **ユーザ名**: cal2014
  - **パスワード**: cookadoodledoo

成績評価

- **宿題** 30%
  - **宿題提出システムへの登録が必要 (次週紹介)**
- **期末試験** 70%
- **随意課題によりさらに加点**

宿題：10/14 午前10:30まで

- テキスト Preface, Basics.v の予習
- Coq 環境の構築
- Preface, Basics を予習し，今日配る質問用紙に，予習時に生じた質問と自分なりの予想回答を記入
  - (提出は授業開始時)

Coq 環境の構築

1. Coq 8.4pl4 のインストール
2. Emacs 使いの人は proofgeneral のインストール
   - Emacs から証明支援系を使うための elisp ソフトウェア
3. そうでない人は CoqIDE のインストール
   - Gtk を使った Coq 専用の証明統合開発環境

Coq 環境構築 (Ubuntu 編)

- opam (OCaml パッケージマネージャ) のインストール
- Coq 8.4pl4 (と CoqIDE) のインストール
  - opam install coq
  - opam install coqide
    - ★ (コンパイラは 4.01 以前を使ってください)
- (Ubuntu の) proofgeneral パッケージをインストール
  - ~/.emacs (など) に

    ```
    (setq coq-prog-name
      "~/.opam/4.01.0/bin/coqtop")
    ```

    が必要 (4.01.0 は適宜置き換え)
  - コマンド名は (emacs でなく) proofgeneral

Coq 環境構築 (MacOS X 編)

- Coq 8.4pl4 (と CoqIDE) のインストール
  - `http://coq.inria.fr/download` から `coqide-8.4pl4.dmg` をダウンロード・インストール
  - CoqIDE もいっしょに入る
- Emacs と proofgeneral のインストール
  - 頑張れ! :-)

Coq 環境構築 (Windows 編)

- Coq 8.4pl4 (と CoqIDE) のインストール
  - `http://coq.inria.fr/download` から `coq-installer-8.4pl4.exe` をダウンロード・インストール
  - CoqIDE もいっしょに入る
- Emacs, proofgeneral のインストール
  - 頑張れ!超頑張れ!:-)

Coq 環境構築 (メディアセンター端末編)

Coq, proofgeneral はインストール済.

- Linux 環境にログイン
- 環境変数 PGHOME の値を `/usr/share/emacs/site-lisp/ProofGeneral` に設定する:
  - (デフォルトの) bash の場合: `~/.bashrc` に
    ```
    export PGHOME=/usr/share/emacs/site-lisp/ProofGeneral
    ```
    の一行を追加
  - (`source ~/.bashrc` を実行して上の設定を反映させる.)
  - 他のシェルの場合: 自分でできますね? :-)

Coq の動作確認 (Proof General 編)

Proof General 起動方法

```
% cd <教科書のディレクトリ>
% proofgeneral Basics.v
```

- 軍人さん (Proof General) が現れた後，ファイルの内容が表示される
- C-c C-n で，ファイルの内容が少しずつ (決まった単位で) Coq に送られ，処理済部分の背景が青くなる
- C-c C-u は逆 (undo)
  - ツールバーの左右矢印でも操作可能

蛇足

軍人さんが怖い，という人は表示される画像を「じぇねらるたん」©苅山春馬に差し替えてください

Coq の動作確認 (CoqIDE 編)

- Basics.v を ファイル → 開く，で開く
- ツールバーの下矢印で，ファイルの内容が少しずつ (決まった単位で) coq に送られ，処理済部分の背景が緑になる
- 上矢印は逆で undo する．
  - ショートカットキーもあります

教科書のダウンロード・解凍・展開

- 前のページにある URL から教科書の .zip ファイルをダウンロード
- 適当なディレクトリに解凍・展開
- `sf` というディレクトリができる
  - index.html をブラウザで読み込む
  - *.v が各章の Coq ファイル

受講上の注意

- ノート PC 持込受講を歓迎します
- 実際に証明を書いてみないと身につきません
- 書かれている記号の意味をよくよく考えましょう
  - みようみまねでいつの間にか証明ができるのは危険な徴候