2019年度後期・数理解析・計算機数学II

理学部数理学科4年・大学院多元数理科学研究科

講義担当: Jacques Garrigue

講義の内容

今回のテーマは「計算機が支援する数学の証明」である.

講義の目的

証明の正しさとはどうやって保証されるものなのか。自分が書いた証明に自信が持てないことはないだろうか。多くの人が確認すれば、少し安心できるようになるが、証明が非常に大きくなるとそれも困難である。人間と違い、正しくプログラムされた計算機は絶対に間違わない。計算機に論理の基礎を教えると、証明に間違いや不足がないことをチェックしてもらえる。定理証明支援系のCoqはそういうプログラムの一つである。また、証明が必要なのは数学だけではない。特に、計算機のプログラムも間違いが起きやすく、その正しさを保証するのはまた証明である。プログラムが大きくなると必然的に証明が大きくなるので、ここでも計算機による証明が期待される。

この講義ではCoqを使い、数学の証明や証明付きプログラムを書く方法を習う。同時にその裏付けである関数型プログラミングと型理論にも触れることになる。

Coqは型理論に基づいた論理を基礎とし、同じ言語の中でプログラムと証明が表現できる。証明も人間が書くが、正しさがコンピュータに保証される。プログラム抽出機能により、証明されたプログラムを普通にコンパイルできる形に変換でき、高速に実行することもできる。

証明対象はプログラムに限定されるわけではなく、通常の数学の定理も証明できる。有名なものとして、4色定理や群論のFeit-Thompson定理がCoqで証明された。型理論の表現力を活用し、数論・代数学や解析学も扱える。なお、今回の講義では、この二つの定理に使われたMathCompというライブラリーを最初から使う。

授業の進め方

基本的には，1時限目を講義，2時限目をその実習とする．ただし，1・2時限目両方を講義にあてることや，実習開始時間を変えることもありうる．実習には，情報メディア教育センターの「理学部サテライトラボ」を利用する予定である．

実習について　基本的には計算機数学I・IIIと同じように実習を行なう．プログラムの制作と実行のためにemacsとCoqを利用するが，それ以外のソフトウェアはサポートしない．

出席について　講義に関して，毎回出席を取るが成績には一切関係しない．授業後には「感想・その他」を下記メールアドレスに送って下さい.

評価の方法

学期途中と学期末にCoqのプログラミングと証明課題をもとに評価する．どちらも授業の応用であり，実習時間内に質問もできる.

レポートはプログラムと理論があり、後者は授業中に学んだ理論について，いくつかの課題を与え，解いていただく．それほど難しい課題ではないが，証明能力を重視する.

採点方針として，それぞれの課題が部分的に解ければ可とし，レポートのでき次第でそれ以上の点数を与える.

どちらもメールで出して下さい.

連絡先

講義に関するメール	comp2-2019@math.nagoya-u.ac.jp
それ以外	garrigue@math.nagoya-u.ac.jp
Office hour	水曜日 13 時〜14 時 多元棟-405 号室

教科書

教科書を使わない．参考書として

- 萩原学, アフェルト・レナルド, 「Coq/SSReflect/MathComp による定理証明:フリーソフトではじめる数学の形式化」, 森北出版, 2018.
- Ilya Sergey, *Programs and Proofs: Mechanizing Mathematics with Dependent Types*, https://ilyasergey.net/pnp/, 2014–2017.
- Yves Bertot, Pierre Castéran, *Interactive Theorem Proving and Program Development.* Springer, 2004.

を挙げておく．また，講義資料は以下の URL から入手できる．

http://www.math.nagoya-u.ac.jp/~garrigue/lecture/2019_SS/index.html

講義予定

以下の予定で講義を行なう．しかし，これは「現在での予定」であって，変更がありうる．

第 1〜4 回 (4/17・23・5/8・15)
定理証明支援系 Coq と SSReflect の基礎

- Coq/SSReflect の論理
- 述語論理と帰納法
- 帰納的な定義
- 自己反映による証明

第 5・6 回 (5/22・29)
Coq/SSReflect によるプログラムの証明

第 7〜9 回 (6/5・12・19)
MathComp による数学の証明

第 10〜14 回 (6/26・7/3・10・20・24)
応用: 例えば，論理学や代数学の証明