コンピュータサイエンス入門（2012年度）

照井一成
京都大学数理解析研究所
terui@kurims.kyoto-u.ac.jp
http://www.kurims.kyoto-u.ac.jp/~terui

平成 24 年 4 月 12 日

ソフトウェア科学の階層性：

計算　–　計算モデル　–　プログラミング言語　–　プログラミング技法

本講義で論じるのは、計算の一般論および計算モデルの理論まで。**個別のプログラミング言語やプログラミング技法については論じない。**

本講義の目的：　１９世紀末に台頭した数学基礎論から、いかにしてコンピュータの概念が生まれ、２０世紀後半に計算機科学が成立するに至ったのか、その過程を現代的な観点から再考すること。歴史的事実や技術的詳細ではなく、大まかな概念的な流れを理解することを目標とする。

内容（予定）:

- 論理学（一階述語論理、直観主義論理）
- 計算論（テューリング機械、決定不能性）
- 算術（ペアノ算術、不完全性定理）
- ラムダ計算（多相型、カリーハワード対応、正規化定理、表示的意味論）

３分の２はテクニカルな内容（定義–定理–証明･計算）、３分の１はインフォーマルな説明。適宜演習を行う。昨年度の内容については http://www.kurims.kyoto-u.ac.jp/~ cs/lecturesj.html を参照。

評価：　学期末のレポートによる（簡単な中間レポートを課す可能性もあり）。

テキスト：　毎回資料を配布。また、ウェブサイト

http://www.kurims.kyoto-u.ac.jp/~terui/cs2012

にて講義録を公開し、随時更新していく予定。

教室：　４月中は 420 号室、**5 月 10 日からは 110 号室。**

数学基礎論とは：　「数学すること」について数学すること。

$$\begin{array}{ccc} \text{証明する} & \Longrightarrow & \textbf{証明論} \\ \text{例をつくる} & \Longrightarrow & \textbf{モデル論} \\ \text{計算する} & \Longrightarrow & \textbf{計算論} \end{array}$$

日本では、これに**集合論**と**非古典論理**を加えた５分野に分類されることが多い。

素朴集合論：　集合は数学理論を展開する上で必要不可欠な道具として用いられてきたが、カントールはこの集合、特に無限集合を数学的対象としてはっきりと認識し、集合そのものについての数学理論を展開した（１８８０年代 $\sim$）。最も根本的なのは

包括原理　“性質”$P(x)$ が与えられたとき、それを満たすもの全てからなる集合 $\{x|P(x)\}$ が存在する。つまり、

$$a \in \{x|P(x)\} \quad \Longleftrightarrow \quad P(a).$$

しかし、安易に包括原理を適用すると即座に矛盾が生じてしまう。

ラッセルのパラドックス：　包括原理を「x は自分自身を要素として含まない」という性質、つまり $\neg(x \in x)$ に適用すると、集合 $R = \{x \mid \neg(x \in x)\}$ が得られる。しかし

$$R \in R \quad \Longleftrightarrow \quad \neg(R \in R). \qquad (1902\text{ 年})$$

このパラドックスを回避するために、包括原理の使用を制限する二つのアプローチが提起された。

公理的集合論：　どのような集合が存在するのか、また各集合はどのような性質を満たすのかを公理によって規定する（ツェルメロ、フレンケル、フォンノイマン、1900 年代 $\sim$）。

型理論：　対象を型により分類する。それにより $x \in x$ のような表現は意味をなさないものとして排除する（ラッセル、1900 年代 $\sim$）。数学の基礎としては公理的集合論が主流となったが、やがて計算機科学の台頭とともに型理論の重要性も再認識されることになる。

集合論におけるパラドックスの発見は、数学全体に対して根本的な疑問を投げかけることになった。数学において無限を実無限として扱ったり、抽象的な論法を用いたりすることは、本当に “安全” なのだろうか？

直観主義数学：　数学を制限し、構成的な論法しか用いないことにする（ブラウワー、1900 年代 $\sim$）。ここで用いられる推論法則は、後にハイティングにより**直観主義論理**として公理化される。ブラウワーの主張は、その特異性により数学の主流とはなりえなかったが、直観主義は後に計算機科学の台頭とともに再び脚光を浴びることになる。

ヒルベルトのプログラム：　数学における抽象的な論法の使用を有限主義的な立場から正当化する（ $\sim$ 1925 年)。

1. 各数学理論を形式化する。
2. 形式化された数学理論において矛盾が導出されないことを、“有限主義的に” 証明する。

これにより、数学理論の無矛盾性の問題は “証明の幾何学” すなわち証明論に帰着することになる。ヒルベルトの提案は、数学の無矛盾性の問題をあくまでも “数学的に” 解決しようとする試みであり、他の論者の主張とは一線を画する。

ゲーデルの不完全性定理：　ゲーデルは１９３１年の論文で有名な第一および第二不完全性定理を証明した。これらはヒルベルトのプログラムに対するカウンターアタックとみなすことができる。

1. （算術を含む理論の）形式化は完全には遂行できない。すなわちどんな “リーズナブルな” 形式化を考えても、証明不能な真命題が存在してしまう。
2. 一般に無矛盾性証明は有限主義的には遂行できない。それどころか、“リーズナブルな” 理論の無矛盾性はその理論自体を用いてすら証明できない。

ゲンツェンの無矛盾性証明：　ペアノ算術（中学レベルの数学）の無矛盾性は、有限主義をほんのちょっと拡大解釈すれば証明できる。このことを示すために、ゲンツェンは都合のよい証明体系（自然演繹、シークエント計算）を考案し、以下のように論じた（1936 年)。

1. 仮に矛盾の複雑な証明が与えられたとしたら、それはより単純な証明に書き換えることができるはずである。
2. この書き換えは有限ステップで停止し、それ以上書き換えることのできない超単純な証明が得られるはずである。
3. しかしそのような超単純な証明が存在しないことは明らかである。
4. ゆえに矛盾の証明はそもそも存在しえない。

この中で 2 の部分がペアノ算術（したがって厳密な意味での有限主義）をほんのわずかに超え出ている。以後の証明論は、ゲーデル的な手法とゲンツェン的な手法を車軸の両輪として展開していくことになる。

様々な計算モデル：　ヒルベルトの形式化、ゲーデル不完全性の強い影響下で、1930 年代には様々な計算モデルが提起された。

- **再帰的関数**（ゲーデル、エルブラン、クリーニ)。関数を「再帰的に呼び出す」操作に着目し、計算可能な関数を特徴づけたもの。

- **ラムダ計算**（チャーチ）「関数を作る」「関数を値に適用する」などの操作を抽象化したもの。後に関数型プログラミング言語（LISP, SCHEME, ML）の核心部分となる。
- **テューリング機械**（テューリング）「紙に文字を書く」「過去に書いた文字を参照する」など、人間が計算をする際に行う基本動作を抽象化したもの。後に（フォンノイマンによる改良を経て）ハードウェアとしてのコンピュータの基礎となる。

これらは一応独立に考案されたものであるが、いずれも同じクラスの関数（計算可能関数）を定義することが後々でわかり、個々の計算モデルに依存しない普遍的な計算論（**計算可能性理論**）が確立された。

カリー・ハワード同型対応：　定理—証明の関係と仕様—プログラムの関係は本質的に同じである（ハワード、1969 年)。さらに言えば、ゲンツェン流の証明論とラムダ計算の間にも深い対応関係がある。極言すれば**証明論＝計算論**である。

高階論理と多相型ラムダ計算：　竹内は高階算術（解析学）の無矛盾性が高階論理のカット除去に帰着することを示した上で、高階論理についてカット除去定理が成り立つことを予想した（**竹内の基本予想**、1953 年)。この予想は後に多相型ラムダ計算の強正規化定理（ジラール、1971 年）へと結実する。これは、数学の基礎をめぐる様々な主義主張やその副産物たち（型理論、直観主義論理、証明論、非可述的論法）たちが一点に集約された見事な具体例であると言ってよい。数学基礎論的な発想によって理論計算機科学の強固な基盤が形成されたのである。

計算機科学の論理的基盤：

- PCF と領域理論（スコット、1960 年代 ～ ）
- 限定算術と計算量（バス、1985 年）
- 線型論理と相互作用の幾何（ジラール、1986 年）
- 古典論理と制御演算（1990 年代）
- 様相論理とプロセス計算（1980 年代 ～ ）

日本語で読める参考文献：

- 新井敏康, 数学基礎論. 岩波書店, 2011.
- 小野寛晰, 情報科学のための論理. 情報科学セミナー, 日本評論社, 1994.
- 鹿島亮, 数理論理学. 現代基礎数学 15, 朝倉書店, 2009.
- 高橋正子, 計算論：計算可能性とラムダ計算. コンピュータサイエンス大学講座 24, 近代科学社, 1991.
- 田中一之 (編著), 数学基礎論講義—不完全性定理とその発展. 日本評論社, 1997.
- 萩谷 昌己, 西崎 真也, 論理と計算のしくみ. 岩波書店, 2007.
- Michael Sipser, 計算理論の基礎 (原著第二版). 太田和夫, 田中圭介監訳, 共立出版, 2008.
- Raymond M. Smullyan, ゲーデルの不完全性定理. 高橋昌一郎訳, 丸善, 1996.