

キミのスマホやゲーム機が今日もきちんと動くのは 背景に膨大な知識と技術の積み重ねがあるから。

【研究テーマ】

コンピュータを用いた論理的な推論の
自動化(定理自動証明)と、そのソフトウェア検証への応用

【キーワード】ソフトウェア

研究

社会の至る所で活用され
セキュリティやプライバシーも
ますます大きな問題になるからこそ
ソフトウェアの安全を守るために。

効率良く証明を考えるため、人間とコンピュータが協調

いつも使っているスマートフォンやゲーム機のソフトウェアが、突然動かなくなった経験はありませんか？そうしたことを防止するための基礎的な技術に関わる分野が、研究のテーマです。ソフトウェアが社会の至る所で活用されている今、安全性の保証は重要です。そのために、ソフトウェアが期待される性質を持つことを厳密に証明する「形式的検証」の技術がより使いやすくなるように、基礎となるコンピュ

ータによる定理自動証明の研究をしています。ソフトウェアが正しく安全に動作するかどうか、人間がきちんと論理的に一生懸命考えることは重要ですが、それをコンピュータがなるべく自動的にやってくれれば効率上がり、コストも抑えられます。コンピュータには難しいところを人間が補助し、人間とコンピュータが協調して効率良く証明できるシステムを考えています。

形式検証の応用例： 車両制御システムの検証

パリ地下鉄14号線の車両制御 (1998年, Siemens・パリ交通公団)

- ▶開発期間4年間(50名)、システム20万行、証明2万7千件
- ▶形式検証による初の大規模な開発例であり、証明実施後の動作テスト・実際の運用において問題は発生していない

ニューヨーク地下鉄カナーシ線の車両制御 (2005年, Siemens)

- ▶開発期間1年(4名)、システム25万行、証明8万件
- ▶パリ14号線の経験・ツールの改善により開発効率が改善

シャルルドゴール空港のシャトル制御 (2006年, Siemens・ClearSy他)

- ▶証明4万3千件のうち97%が自動証明(残りは対話的に証明)
- ▶証明に要した工数は全体の27%

ソフトウェアの欠陥による事故や障害を少なくしたい

研究では、自動的に証明することが難しそうな数学の定理やソフトウェアの性質に対して、私たち人間が考える解き方をコンピュータで実現するにはどんな仕組みが必要かを検討し、プログラムを書いて実験します。さまざまな定理証明システムが開発・公開されていますが、実際の開発現場ではまだ十分に活用されているとは言えません。つまり、現状多くのソフトウェ

アが厳密に検査されないまま使われているともいえます。幸運にも多くの人はあまり影響を受けずに済んでいます。ソフトウェアの欠陥による大きな事故や障害を少なくするためには厳密な検証が本質的に必要であると考えられるため、こうした形式的検証のシステムをより手軽に利用できるようにすることを目指しています。

対話的証明システム

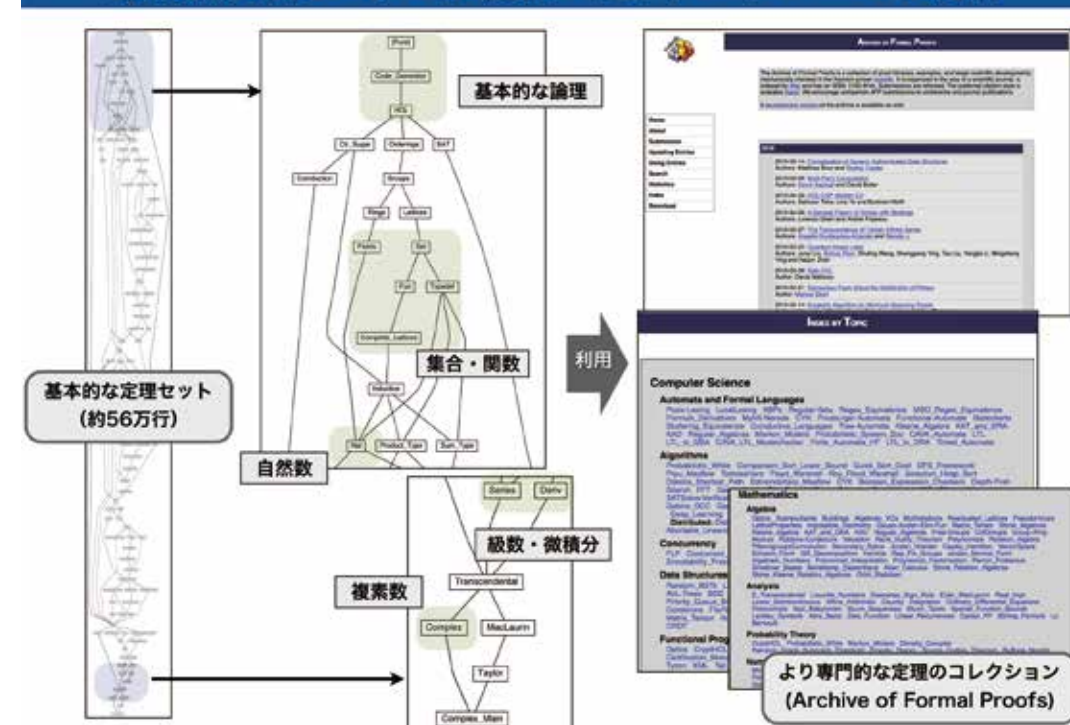
対話的証明システム (証明アシスタント)

- 機械が検証可能な証明(形式証明)の作成を支援するシステム
- 以下のような機能を提供する
 - 証明を記述するための言語
 - 証明の正しさのチェック
 - 証明の自動生成(自動証明)
 - 利用可能な定理のデータベース

- 対話的証明システムの例
 - Isabelle (ケンブリッジ大・ミュンヘン工大)
 - Coq (フランス国立情報学自動制御研究所)
 - Mizar (ピャウィストク大・アルバータ大・信州大)



対話的証明システムの機能：定理データベースの提供



授業

計算機言語学Ⅱ

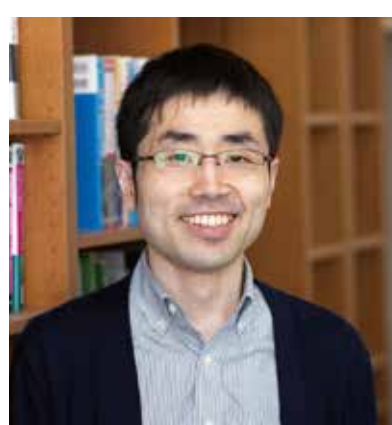
「コンパイラ」の仕組みを学ぶことで
コンピュータの本質的な理解を深めます。



今、役立つ技術だけではなく、長く使える基礎的な考え方を

プログラミング言語の使い方を「計算機言語学Ⅰ」で学んでから、「Ⅱ」ではより専門的に「計算とはそもそも何なのか」「コンピュータの限界とは」といったことを深く考察してもらいます。具体的には、プログラミング言語で書かれたものを実際にコンピュータが動かす機械語に変換するコンパイラについて、講義と演習を通して学びます。プログラミングには、コンパ

イラの仕組みの理解がとても重要です。実用的な技術に直結するだけでなく、コンパイラが動く背後には「計算とは何か」といった計算機科学の基礎的で重要な内容が密接に関わっているため、コンピュータに対する深い理解と視野を広げることができ、長期的に役立つ教養としてみなさんの財産になります。



工学部電子情報工学科
准教授

さとう はる ひこ

佐藤 晴彦

実は、コンピュータは思った通り動いてくれないことばかり。一方で、思いもよらない実験結果が出てくる面白さがあります。情報系の研究はパソコン1台あれば手軽にでき、アイデアを打ち込むと結果をすぐに確認できるのも魅力です。

〈専門分野〉
情報工学
(ソフトウェア工学)

〈主な担当科目〉
計算機言語学Ⅰ・Ⅱ、計算機実習Ⅰ、
情報工学基礎Ⅱ、
オペレーティングシステム



北海学園大学

工学部