寺内研
研究室紹介

教員紹介

寺内 多智弘(てらうち たちお)

- 1978年生まれ
  - 本籍：栃木県宇都宮市
- 14-28歳を米国で過ごす
  - コロンビア大学(学士号)　カリフォルニア大学バークレー校(博士)
- 2007.1～2011.3 東北大学 助教
- 2011.4～2014.3 名古屋大学 准教授
- 2014.4～2017.9 北陸先端科学技術大学院大学 教授
- 2017.10～現在　早稲田大学 教授

研究内容 (cf. ホームページ)

専門分野：プログラミング言語

- **主な研究テーマ**
  - **先進的プログラミング言語機能の研究**
    - 依存型(dependent type)、篩型(refinement type)といった先進的型システムや代数的エフェクト(algebraic effects)といった先進的言語機能の研究など
  - **プログラム検証**
    - 静的コード解析によるプログラムの正しさの自動検証
  - **プログラム合成**
    - 仕様や入出力例などから正しいプログラムを自動生成
  - **自動定理証明**
    - SAT/SMT/CHCソルバ等の自動定理証明・制約解消の研究など
  - **セキュリティに関する研究**
    - プログラム検証による脆弱性の検出やプログラム合成による脆弱性の修正など

背景：ソフトウェアバグによる社会問題

近年の事例

- ソフトウェアバグによる衛星喪失(2016)
- ソフトウェアバグによる1000名以上の従業員個人情報流出(2017)
- コロナ接触確認アプリの不具合(2020)
- 金融機関システム不具合によるATMの機能停止(2021)

損害は急増傾向：600億ドル(2002 NIST)→**1.1兆ドル**(2016 Tricentis)

テスト実行など従来のソフトウェア開発手法だけでは複雑化するソフトウェアの品質の担保が困難

研究のねらい：コンピュータアルゴリズムにより、自動的に(かつ理論的に正しさの保証が得られる形で)プログラムの正しさの検証や正しいプログラムの合成をしよう

例題1：ReDoS脆弱性の修正

- ReDoS (Regular-expression Denial of Service)
  - 正規表現を用いた文字列処理の振る舞いを悪用したDoS攻撃
  - 著名サイトがサービス停止になる等、現代社会における深刻な脅威
- ReDoS脆弱な正規表現の例：**<(.*)>.*</¥1>**
  - **<><>< … ></>**という形の長い文字列を入力として与えるとマッチング処理に膨大な時間がかかりサービス停止を起こす

- 近年の成果 **[千田@寺内研D3/NTT研,寺内 S&P2022]**
  - Programming-by-Examplesという考え方に則り、例を用いて脆弱な正規表現を非脆弱なものに修正するアルゴリズムを提案
  - 例えば、上記の正規表現は**<([^>]*)>[^<]*</¥1>**という非脆弱なものに修正される

例題2：代数的エフェクトの型システム

- 代数的エフェクト (Algebraic Effects)
  - 副作用(破壊的代入、例外、継続など)を代数的に扱うための先進的なプログラミング言語機能
  - 最新バージョンのOCamlに取り入られるなど、実用的な言語でも導入されはじめている

  - 例えば、下のプログラム断片は$x \geq y$かつ$v \geq w$のとき$x - w$を出力する

```
with { decide (_, k) ↦ max (k true, k false) } handle
  let a = if decide () then x else y in
  let b = if decide () then v else w in
  a - b
```

例題2：代数的エフェクトの型システム(続き)

- 代数的エフェクトのための新しい型システムを作っている
  - 目的：**型によるプログラムの正しさの保証**
- 近年の成果
  - 時相仕様検証のための型エフェクトシステム
    [川俣@寺内研M1,寺内 PPL2022(論文賞)]
  - Answer type modificationの仕組みを取り入れた依存篩型システム
    [川俣@寺内研M1,関山@NII,海野@筑波,寺内 投稿中]
    - 例えば、前頁のプログラム断片の動作を正確に表す型付けが可能：

      $\Gamma \vdash$ **前頁のプログラム断片：{u:int | u=x−w}**

      ただし、$\Gamma =$ **x:int,y:{u:int | x≥u},v:int,w:{u:int | v≥u}**

その他の近年の研究 (cf. ホームページ)

一階不動点論理の自動定理証明とプログラム検証への応用
- POPL 2023 (Distinguished Paper Award)

拡張正規表現の形式言語理論
- FSCD 2022, PPL 2023 (論文賞)

述語制約解消による関係性仕様の検証
- CAV 2021

プログラム検証・合成によるタイミング攻撃の検出・防衛
- Journal of Computer Security 2020, POST 2019, PLDI 2017

循環証明のカット除去性についての研究
- Computer Software 2020

など

どんな人に来てほしいか

- **理論(特に”形式理論”)に根ざした研究がしたい人**
  - 形式検証
  - 型システム
  - 数理論理と(特に自動)定理証明
  - 形式言語理論とオートマトン理論
  - プログラム意味論
  - など
- 理論に強くないかもしれないけど興味がある人も歓迎

より詳しくは個別面談で

- 面談希望日時を書いたメールを送ってください

- メールアドレス： terauchi@waseda.jp
- 場所：62号館 209B
  - オンラインでの面談も受け付けます