SOFTWARE TECHNOLOGY GROUP

Seminar

Foundations of Static Analysis
Winter Semester 25/26

TuCan-No: 20-00-1028-se

Course Type: 2SWS / 3 CPs

Prof. Dr.-Ing. Mira Mezini

Process

- **By Friday, October 17th, 23:59 :** Send an e-mail with your three preferred papers and why you are the right person for these topics to: **julius.naeumann@tu-darmstadt.de**
  - Subject: "**FoSA Topic**"
  - If you register as a team, send a **single email** with all members (include their mat-nr and email addresses)
- **Wednesday, October 22nd:** Assignment of topics
- **Next:** *Contact your supervisor* to discuss details of your topic,
  - 4 Pages (per student)
- **TBD:** Paper Draft Submission
- **TBD:** Final Paper Submission
- **TBD:** Presentation (10 minutes per student)

Scalable Propagation-Based Call Graph Construction Algorithms

Frank Tip
IBM T.J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
tip@watson.ibm.com

Jens Palsberg
Dept. of Computer Science
Purdue University
West Lafayette, IN 47907
palsberg@cs.purdue.edu

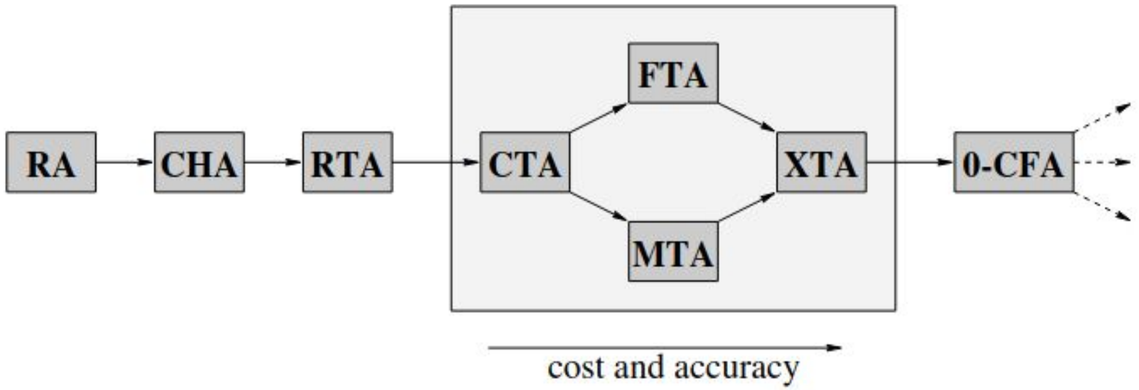


Figure 1: Schematic overview of the algorithms studied in this paper, and their relationship to several previous algorithms.

https://web.cs.ucla.edu/~palsberg/paper/oopsla00.pdf

Precise Interprocedural Dataflow Analysis via Graph Reachability

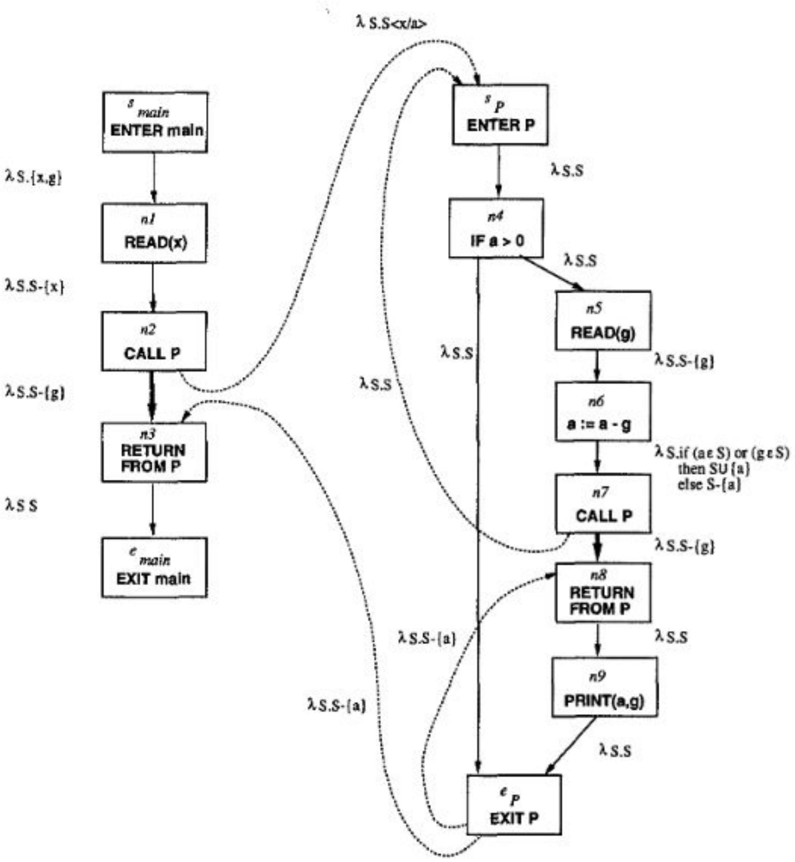
Thomas Reps,[†] *Susan Horwitz,*[†] *and Mooly Sagiv*[†, ‡]
University of Wisconsin

```
declare g: integer

program main
begin
  declare x: integer
  read(x)
  call P (x)
end

procedure P (value a : integer)
begin
  if (a > 0) then
    read(g)
    a := a − g
    call P (a)
    print(a, g)
  fi
end
```

(a) Example program



(b) Its supergraph G^*

Figure 1. An example program and its supergraph G^*. The supergraph is annotated with the dataflow functions for the "possibly-uninitialized variables" problem. The notation S<x/a> denotes the set S with x renamed to a.

https://dl.acm.org/doi/pdf/10.1145/199448.199462

Boomerang: Demand-Driven Flow- and Context-Sensitive Pointer Analysis for Java

Johannes Späth[1], Lisa Nguyen Quang Do[*2], Karim Ali[3], and Eric Bodden[†4]

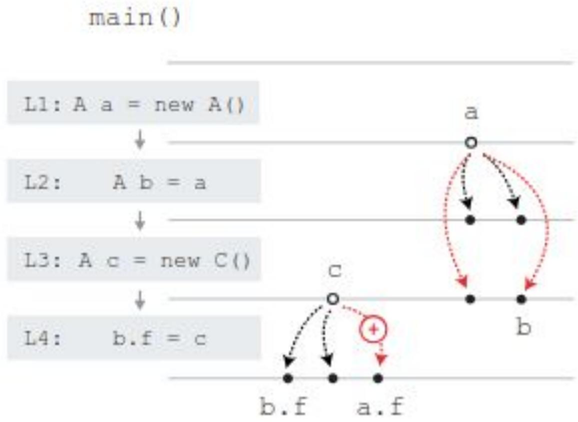


Figure 5 Handling field writes in BOOMERANG.

https://www.bodden.de/pubs/sna+16boomerang.pdf

Explorative: LLM-Assisted Static Analysis

Perform a survey of current techniques for configuring Static Analysis using LLMs.

Starting Point: IRIS https://openreview.net/forum?id=9LdJDU7E91

5 papers per student

Reminder

Please register for the TUCAN course 20-00-1028-se

Positions & Theses

If you are interested in **HiWi Positions** or **Bachelor- or Master theses** contact: julius.neumann@tu-darmstadt.de