Seminar: Modular Static Analysis

Prof. Dr. Reinhard Wilhelm
Jan Reineke, M.Sc.
Dipl.-Inform. Björn Wachter
Modular Static Analysis

- Static Analysis
- Shape Analysis
- Modularity
Static Analysis

- Statically determine invariants
- Examples:
  - $x \in [3,8]$  $\Rightarrow$  $2/x$ is safe
  - $x \neq$ null  $\Rightarrow$  $x->next = y$ is safe
Static Analysis - How?

\[
x := 1;
\]
\[
x := x + y;
\]
\[
x := 2/x;
\]

Abstract Domain: Intervals
+ Abstract Semantics on Intervals
Static Analysis - How?

\[ x \in [-\infty, \infty], \quad y \in [3,7] \]

\[ x := 1; \]
\[ x := x + y; \]
\[ x := 2/x; \]

Abstract Domain:
Intervals
+
Abstract Semantics on Intervals
Static Analysis - How?

\[ x \in [-\infty, \infty], y \in [3,7] \]

\[ x := 1; \]
\[ x := x + y; \]
\[ x := \frac{2}{x}; \]

Abstract Domain: Intervals
+ Abstract Semantics on Intervals
Static Analysis - How?

\[ x \in [\infty, \infty], \ y \in [3,7] \]

\[ x := 1; \]

\[ x \in [1, 1], \ y \in [3,7] \]

\[ x := x + y; \]

\[ x \in [4, 8], \ y \in [3,7] \]

\[ x := \pi/x; \]

Abstract Domain: Intervals + Abstract Semantics on Intervals
Static Analysis - How?

\[ x \in [-\infty, \infty], y \in [3, 7] \]
\[ x := 1; \]
\[ x \in [1, 1], y \in [3, 7] \]
\[ x := x + y; \]
\[ x \in [4, 8], y \in [3, 7] \]
\[ x := 2/x; \]
\[ x \in [0.25, 0.50], y \in [3, 7] \]
Shape Analysis

• Statically determine invariants regarding the shape of the heap:

• Examples:
  • No memory leaks!
  • List library: lists remain acyclic
  • ...

• Very complex abstract domains
  → VERY expensive analyses
Class-Level Modularity

- Class Invariants as Abstract Interpretation of Trace Semantics
- Using History Invariants to Verify Observers
- Modular Shape Analysis for Dynamically Encapsulated Programs
Class-Level Modularity

- Class Invariants as Abstract Interpretation of Trace Semantics
- Using History Invariants to Verify Observers
- Modular Shape Analysis for Dynamically Encapsulated Programs
Interprocedural Analysis

- Computing Procedure Summaries for Interprocedural Analysis
- Interprocedural Shape Analysis with Separated Heap Abstractions
- Footprint Analysis: A Shape Analysis that Discovers Preconditions
- Componentized Heap Abstraction
- Polymorphic Predicate Abstraction
Thread-Modular Analysis

- Thread-Modular Shape Analysis
- Modular Verification of a Non-Blocking Stack
Requirements

- Presentation: 45-60 minutes, summary of current research paper in English
  - send presentation to tutor at least two weeks prior to talk (strict)
  - meet tutor to discuss presentation

- Summary of paper: ~5 pages
  - cover important aspects in your own words in German or English
  - due four weeks after talk
Organizational Issues

• Regular meeting: Wednesdays **2pm or 4pm**?

• Dates:
  • April, 18th: Kick-Off Meeting
  • April, 25th: Assignment of Papers
  • May, 30th: First two talks