Context-Insensitive Interprocedural Analysis & Context-Sensitive Pointer Analysis

(Purple Dragon book – Chapter 12.5 & 12.6)

Method invocation

- **What are effects of method invocation?**
- **What is to be determined**

- **Points-to relation**
- Dynamically determine the type of **receiver**
- Assignment of parameters

  (formal – actual; this – 0^{th})
- Type of returned object

Context-Insensitivity

Parameters and returned values by **copy** statements

? How to determine the type of receiver?

It **has to be** done dynamically

Discovering call targets „on the fly“

C-iS Interprocedural Analysis

- **3 EDB predicates in Datalog**

- **actual (S, I, V)**

  V – Ith actual parameter • in call site S

- **formal (M, I, V)**

  • in method M

- **cha(T, N, M)**

  class hierarchy analysis

Call graph discovery

- **Edges** – IDB predicates **invokes**
- **Nodes** – call targets & call sites

- **points-to** relations are created

Dynamic loading

- Especially in **Java** (everything is **Object**)

- Static analysis – only approximation
- Possibility of thinning and narrowing

- *Analysis on **bytecode** level*

Pointer analysis

- **Context sensitivity**

  (interprocedural an.)

  - **cloning-based**
  - **summary-based**

- **Copy** method for each use

- Many possible **contexts** of interest

Context

- **What** is context?
- **How** to handle it?

- Logically – context-insensitive algorithm on cloned call-graph

- In practise – how to represent large contexts?
  (exponentially many; 10^{14})

Call string

- Distinguish context a method is called in
- Described by **regular expression** or **finite automaton**

Call graph modifications

- **derived from context-insensitive points-to analysis**

- Find all mutually recursive sets of functions
  - **Strongly connected components in the graph**
  - *trivial = single nonrecursive functions*
  - *nontrivial = (mutually) recursive functions*
- All call strings for **RE**

- **Call string ≈ context**

Cloned call graph

- **Input:** Call graph & methods & context

- Adding context to Datalog rules

- Context sensitivity in the naming of objects

- Object sensitivity

Thank You

(Ondřej Horníček, xhorni09)