Xisa: Precise Program Analysis with Data Structures

University of California, Berkeley

Bor-Yuh Evan Chang, Xavier Rival, and George Necula

http://xisa.cs.berkeley.edu

Problem

Program analysis tools are being increasingly adopted to improve the security, reliability, and overall quality of software because they can rule out entire classes of errors. Yet, almost all of today's tools have difficulty when objects of interest are put into data structures.

Approach

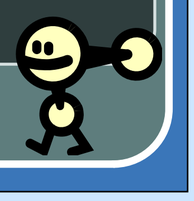
Reasoning about data structures typically requires sophisticated and burdensome logical invariant specifications from the user. We propose a novel way to involve the user in guiding the analysis by extracting both the necessary invariants and reasoning rules from executable assertions in the code.

```
dllist(x) =
  if (x!next == null) then true
  else
    x!next!prev == x  and
    dllist(x!next)
```

data structure validation code

Examines validation code to turn it into a specification for static analysis

Analyzes program using "whiteboard-level" abstraction given by the developer



the Xisa shape analyzer

Approach and Impact

New Approach

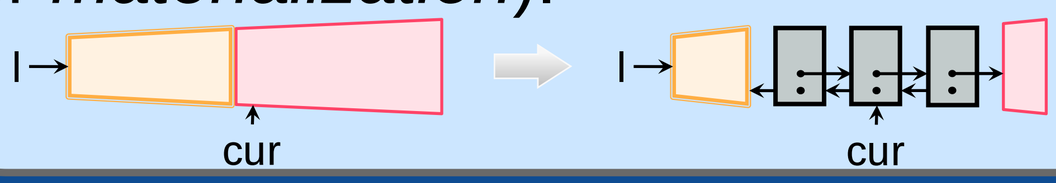
- User-centric approach
- Utilize run-time checking code as specification for static analysis

Research Impact

- Toward practical analyses even with data structures
  - 10-100x speed-up over generic approaches
  - Extensible with developer-oriented specifications

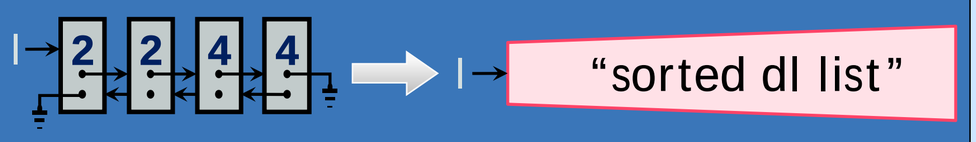
Technical Description

Xisa is a shape analysis parametric in "code-like" inductive data structure descriptions. Two key innovations are an abstraction that generalizes these descriptions to apply even when the data structure invariant only partially holds and a pre-analysis on these descriptions to derive reasoning rules (for *materialization*).



Example

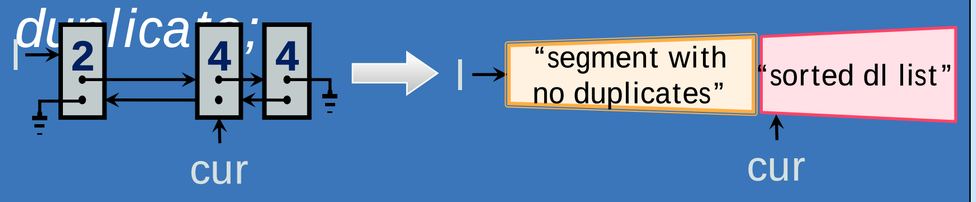
Example



// l is a sorted doubly-linked list

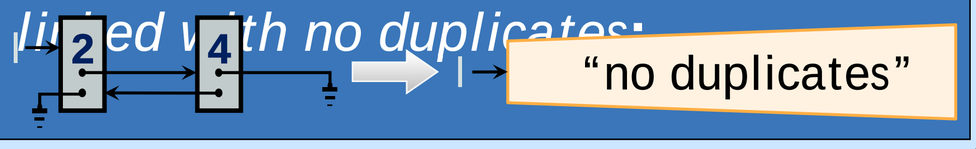
for each node cur in list l {

remove cur if duplicate;



}

assert l is sorted, doubly-linked with no duplicates;



Abstraction

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

CT-ISG: Collaborative Research: Open Software Security: Principles and Systems, PIs George Necula and Martin Abadi. Number: CCF-0524784.