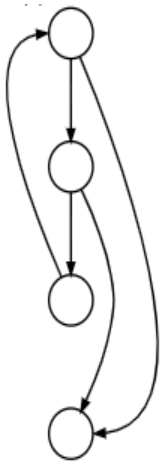
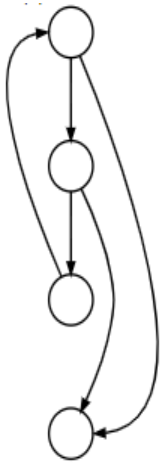


Program Analysis

Venkatesh Vinayakarao

venkateshv@cmi.ac.in
Mar – Apr, 2018
Chennai Mathematical Institute



"The supply of grand challenges … shows little sign of drying up."

– Harman and O'Hearn in "Opportunities and Open Problems for Static and Dynamic Program Analysis", Madrid, Spain, 2018.

Agenda

- What is Program Analysis?
- Why Study Program Analysis?
- In this Course…
- Course Logistics

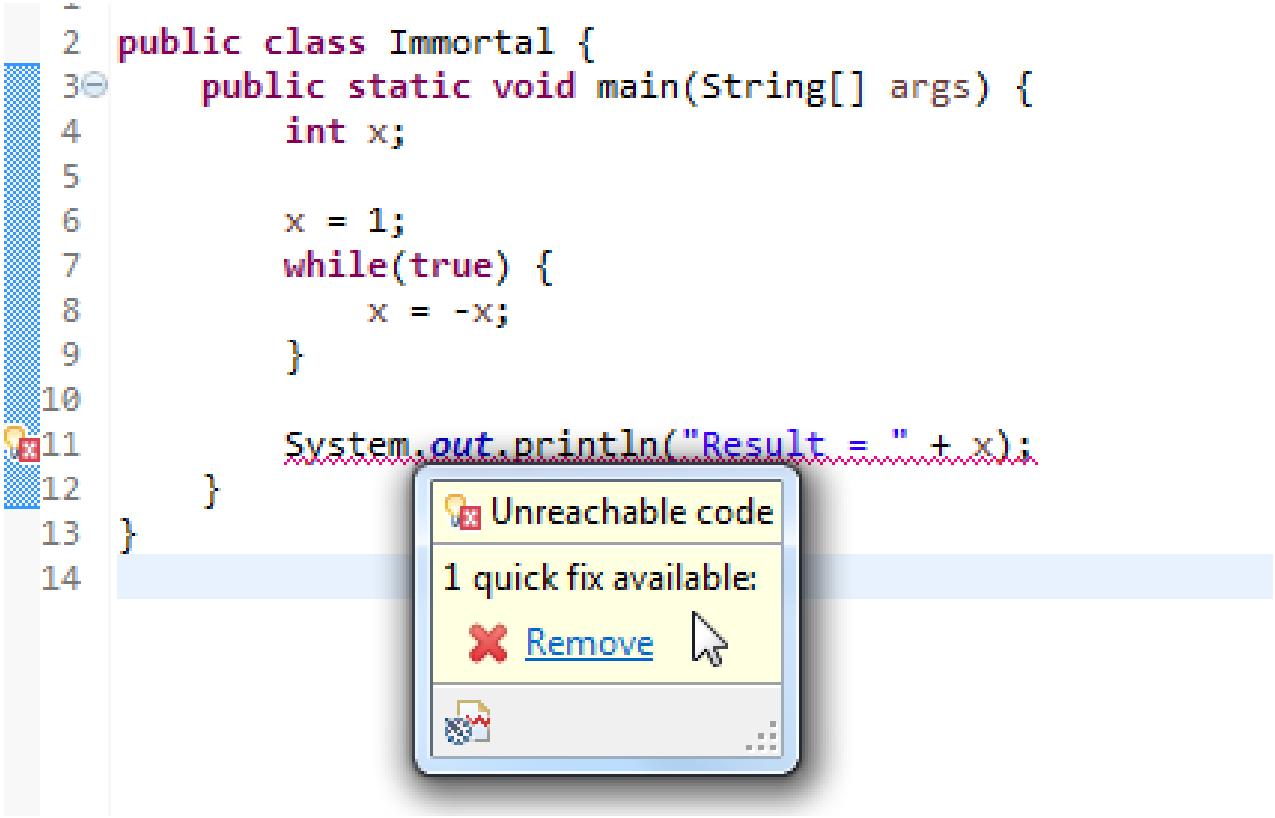
What is Program Analysis?

Quiz

```
class Immortal {
  public static void main(String[] args) {

    int x;

    x = 1;
    while(true){
          x = -x;
    }

    System.out.println("Result = " + x);
  }
}
```

Any problem in this code?

Built into Eclipse

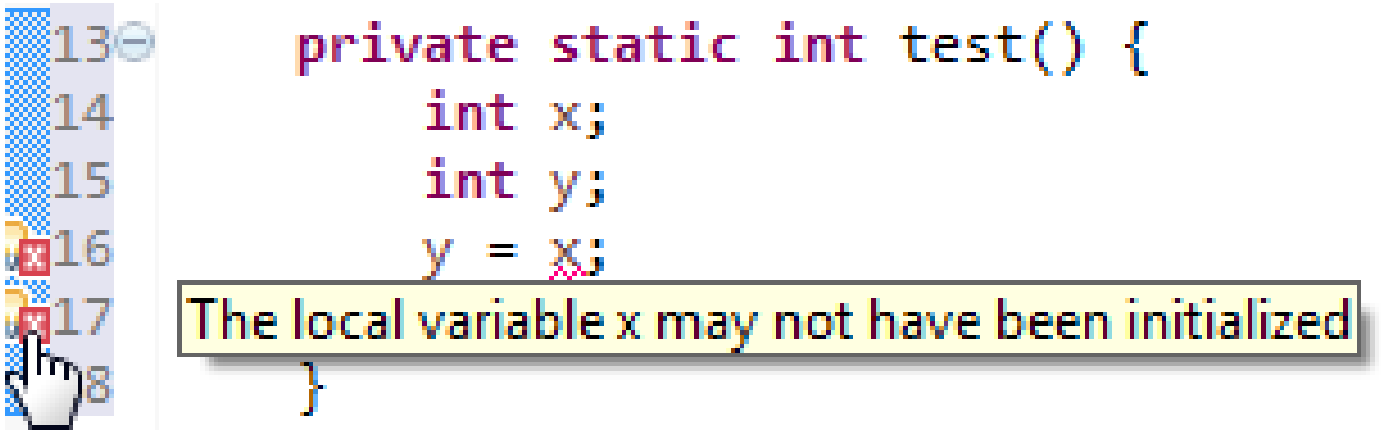


Quiz

```
private static int test() {
    int x;
    int y;
    y = x;
    return x;
}
```

Any problem in this code?

IDE Catches Some!



Source Code Optimization

- How to optimize this?

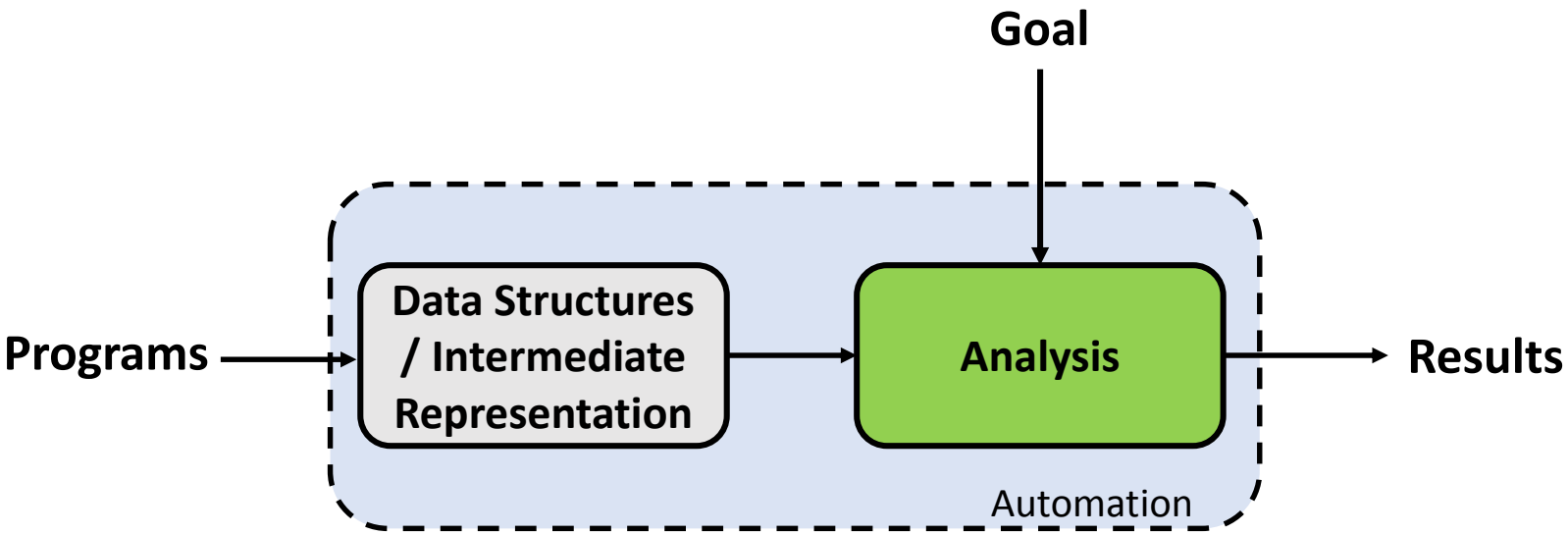
```
if (x != 5) x = 5;
```

- Simply,

```
x = 5;
```

http://icps.u-strasbg.fr/~bastoul/local_copies/lee.html

Program Analysis



Why Study Program Analysis?

Everyone is in a hurry…

Picture Courtesy: Web.

Software Reliability: An Issue

For more, visit http://www.cs.tau.ac.il/~nachumd/horror.html

Mars Orbiter Crash

- Primary Cause: Results reported in wrong units
- ”Various officials at NASA have stated that NASA itself was at fault **for failing to make the appropriate checks and tests** that would have caught the discrepancy.”

https://spectrum.ieee.org/aerospace/robotic-exploration/why-the-mars-probe-went-off-course

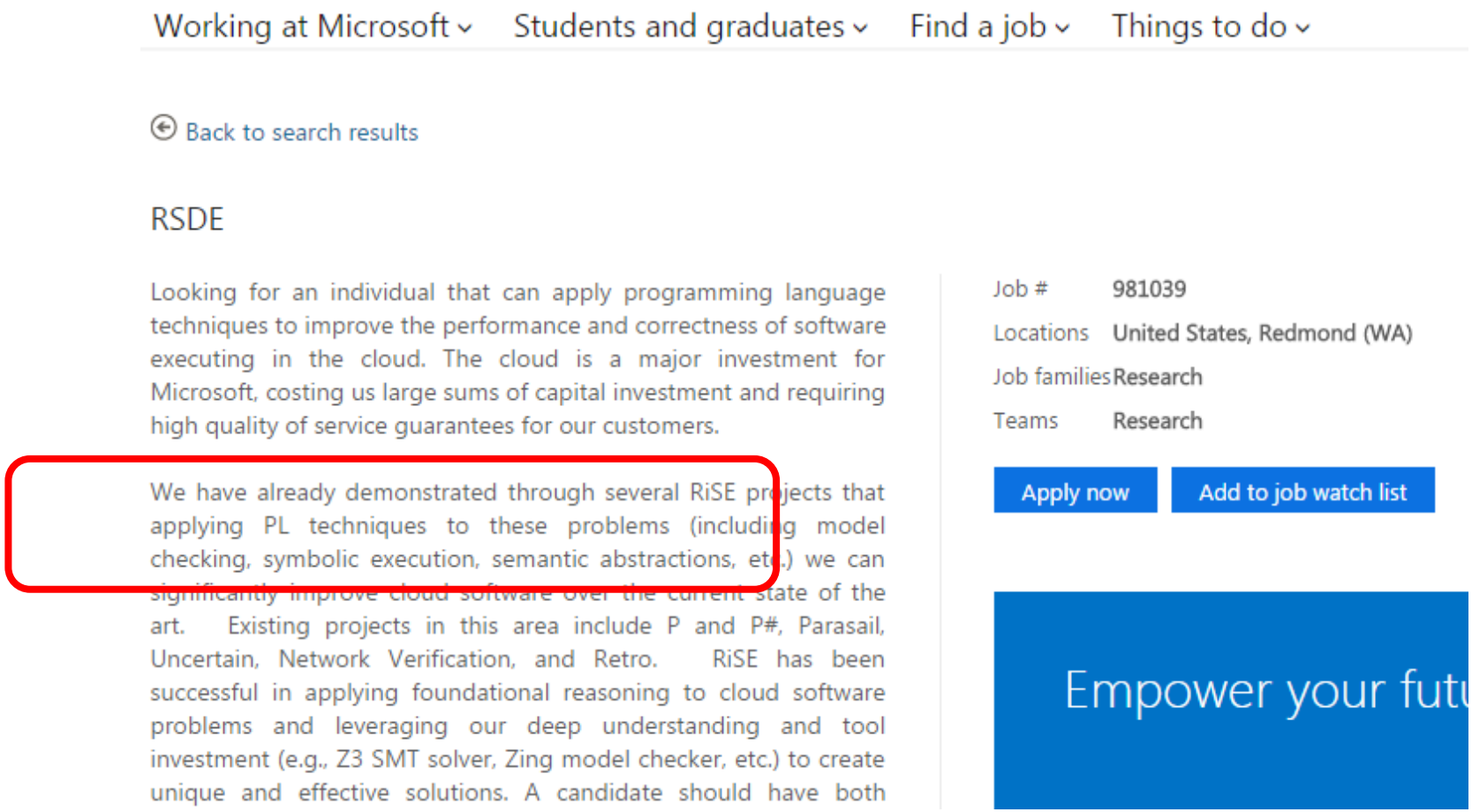
Security Breaches

Aadhaar details leaked after TRAI chief throws breach challenge

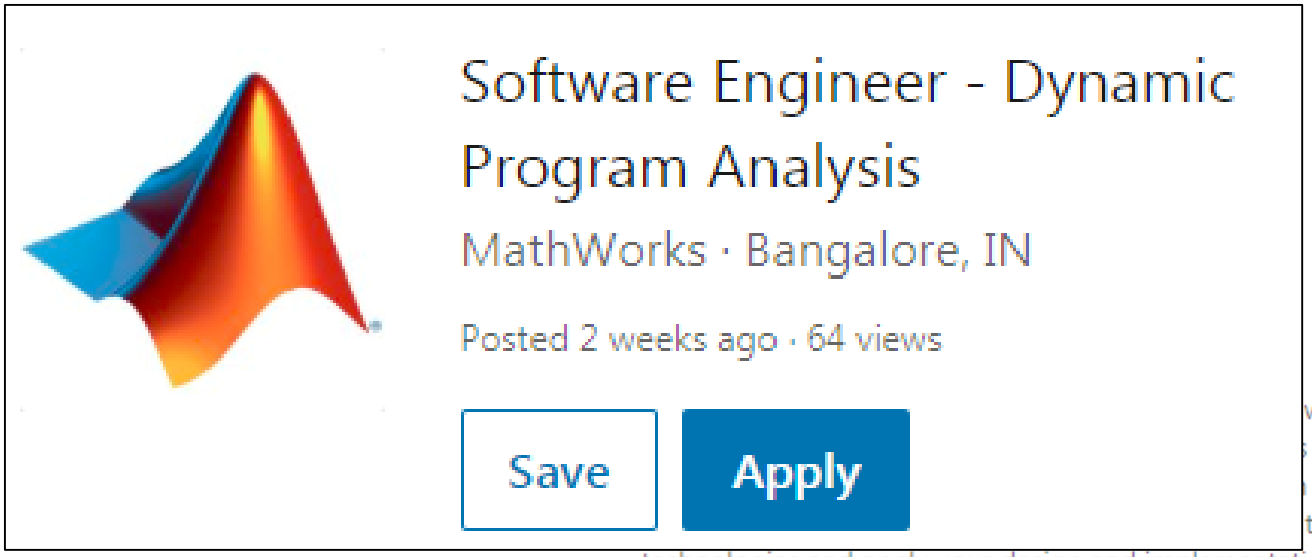
Alleged personal details of Indias telecom watchdog chief R.S. Sharma were leaked on Saturday after the TRAI chairman threw a challenge and tweeted his 12-digit Aadhaar asking if it had made him vulnerable to any security risk.

IANS | Updated: July 29, 2018, 08:47 IST

Microsoft Research



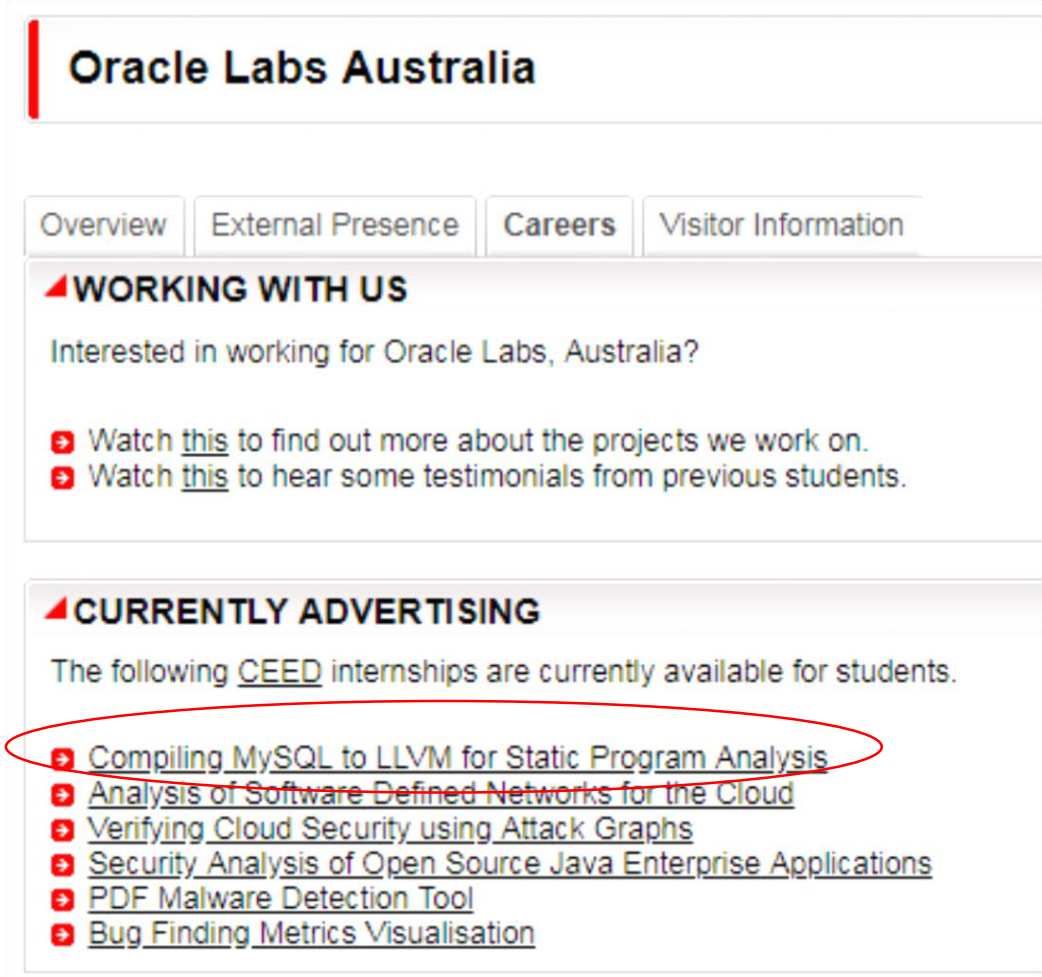
MathWorks



who is good at abstract thinking
is a plus. You will join a dynamic
and debugging capabilities to
to learn many of our core
technologies and apply your design and implementation skills to build parts of our product from ground up.

- Design data-structures and algorithms for data-flow analysis of Simulink/Stateflow models and generated code
- Build customer visible UIs for configuring and invoking analysis and transformation engines

Oracle Labs



Oracle Labs Australia

Overview | External Presence | **Careers** | Visitor Information

WORKING WITH US

Interested in working for Oracle Labs, Australia?

- Watch this to find out more about the projects we work on.
- Watch this to hear some testimonials from previous students.

CURRENTLY ADVERTISING

The following CEED internships are currently available for students.

- Compiling MySQL to LLVM for Static Program Analysis
- Analysis of Software Defined Networks for the Cloud
- Verifying Cloud Security using Attack Graphs
- Security Analysis of Open Source Java Enterprise Applications
- PDF Malware Detection Tool
- Bug Finding Metrics Visualisation

IBM IRL

Productive Parallel Programming

Current object-oriented languages have revealed several drawbacks with respect to parallel/concurrent programming at the level of unstructured threads with lock-based synchronization. IBM Research is developing X10, a modern object-oriented programming language designed for high performance with explicit programmer defined parallelism for realizing high productivity programming of parallel computer systems. The key features of X10 include explicit reification of locality in the form of places, support for a partitioned global address space (PGAS) across places, and lightweight activities embodied in async, future, foreach, and ateach constructs which subsume communication and multithreading operations in other languages. Our current focus is on static program analysis (for example, May-Happen-in-Parallel analysis, Bad Place Analysis), compilation for C/C++, debugging for X10, and assessment and semi-automated migration of domain-specific serial code to emerging multi-core architectures, leveraging productive programming models and their variants (such as OpenMP, OpenCL).

More…

CodeSearch - Senior Software Engineer - Program Analysis

Elastic · Yokohama-shi, JP

Posted 2 weeks ago · 207 views

Save Apply

Principal Researcher - Phd/Program Analysis

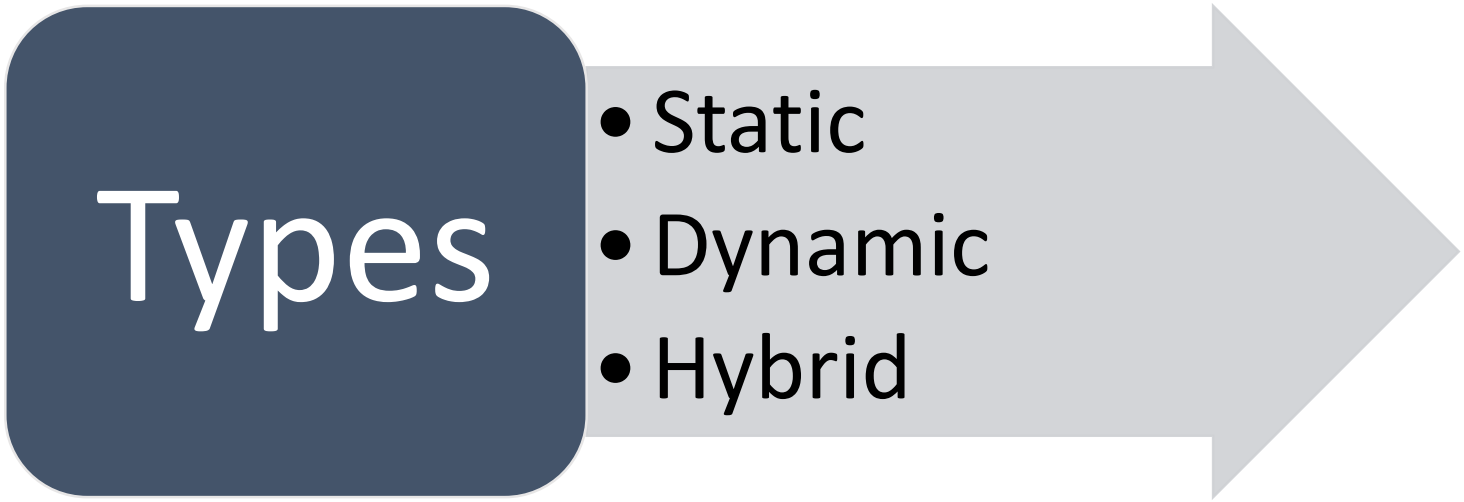
Oracle · Brisbane, Australia

Posted 6 days ago · 79 views

Save Easy Apply

In This Course…

Analysis



Static Analysis

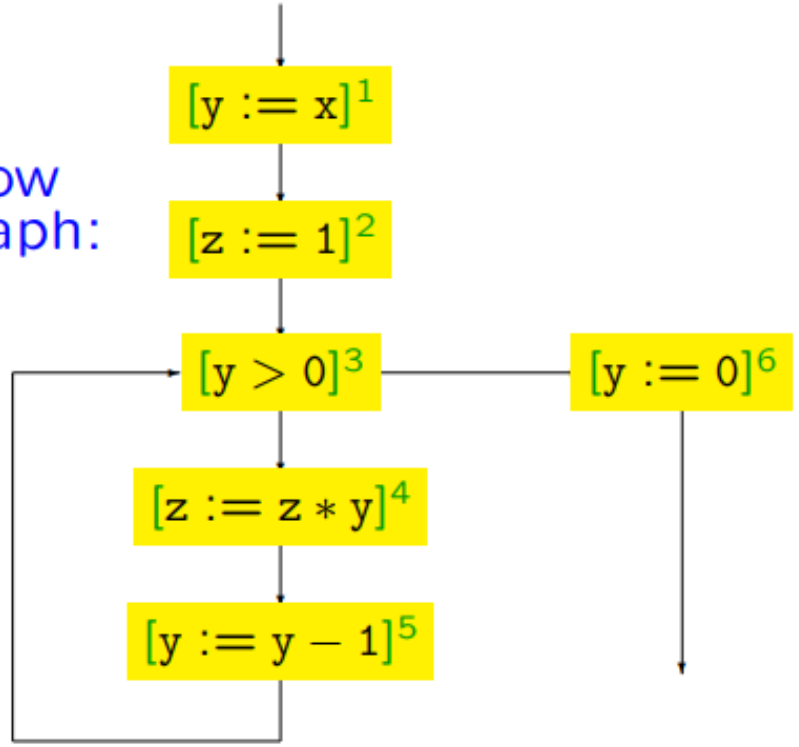
Analysis without executing the program

In this course, we will learn…

Reaching Definitions (RD) Analysis

```
y = x;
z = 1;
while (y > 0) {
      z = z * y;
      y = y – 1;
}
y = 0
```

Flow graph:



The assignment $[x := a]^{\ell}$ reaches ℓ' if there is an execution where x was last assigned at ℓ. Does $[z := 1]^2$ reach 5?

RD Analysis

ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2		
3		
4		
5		
6		

(y,?) ➔ y is undefined. (y,1) ➔ y is defined in line 1.

Labeled Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
    $[z = z * y]^4$;
    $[y = y - 1]^5$;
}
$[y = 0]^6$

RD Analysis

ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2	(x,?),(y,1),(z,?)	(x,?),(y,1),(z,2)
3		
4		
5		
6		

Labeled
Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
    $[z = z * y]^4$;
    $[y = y - 1]^5$;
}
$[y = 0]^6$

RD Analysis

ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2	(x,?),(y,1),(z,?)	(x,?),(y,1),(z,2)
3	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,2),(z,4),(y,5)
4		
5		
6		

Labeled
Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
    $[z = z * y]^4$;
    $[y = y - 1]^5$;
}
$[y = 0]^6$

RD Analysis

ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2	(x,?),(y,1),(z,?)	(x,?),(y,1),(z,2)
3	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,2),(z,4),(y,5)
4	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,4),(y,5)
5		
6		

Labeled
Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
    $[z = z * y]^4$;
    $[y = y - 1]^5$;
}
$[y = 0]^6$

RD Analysis

ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2	(x,?),(y,1),(z,?)	(x,?),(y,1),(z,2)
3	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,2),(z,4),(y,5)
4	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,4),(y,5)
5	(x,?),(y,1),(z,4),(y,5)	(x,?),(y,5),(z,4)
6		

Labeled Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
    $[z = z * y]^4$;
    $[y = y - 1]^5$;
}
$[y = 0]^6$

RD Analysis

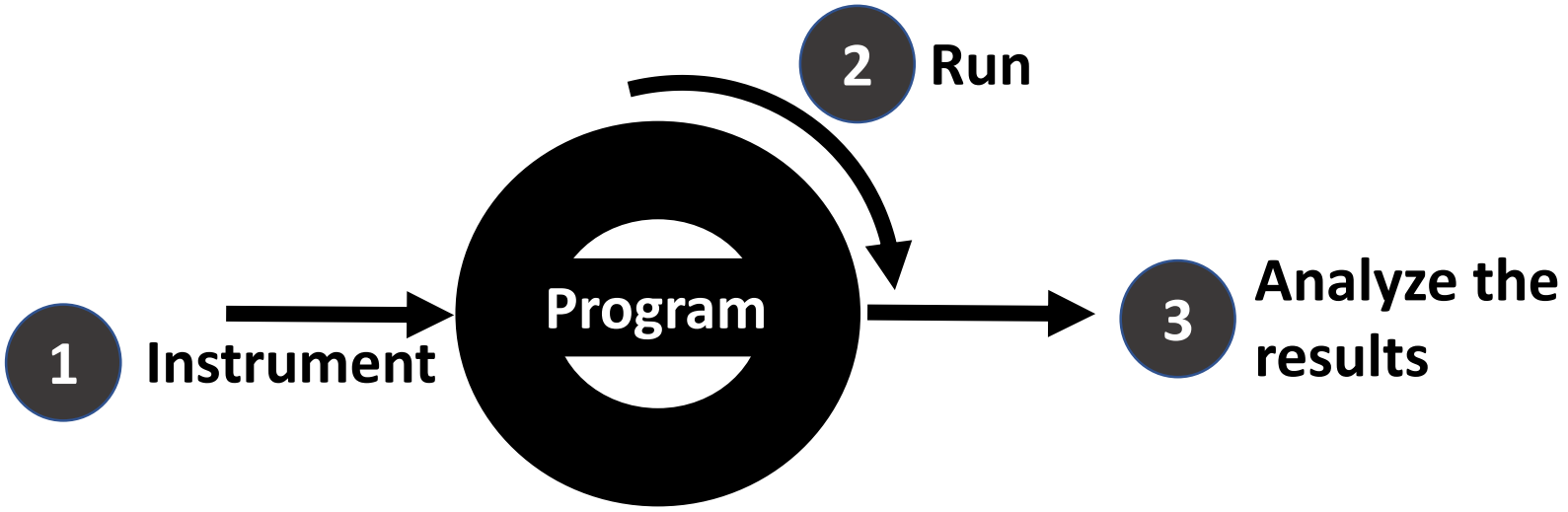
ℓ	$RD_{entry}(\ell)$	$RD_{exit}(\ell)$
1	(x,?),(y,?),(z,?)	(x,?),(y,1),(z,?)
2	(x,?),(y,1),(z,?)	(x,?),(y,1),(z,2)
3	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,2),(z,4),(y,5)
4	(x,?),(y,1),(z,2)(z,4),(y,5)	(x,?),(y,1),(z,4),(y,5)
5	(x,?),(y,1),(z,4),(y,5)	(x,?),(y,5),(z,4)
6	(x,?),(y,1),(z,2),(z,4),(y,5)	(x,?),(y,6),(z,2),(z,4)

This table answers all RD questions.

Labeled Input Program

$[y = x]^1$;
$[z = 1]^2$;
while $[(y > 0)]^3$ {
  $[z = z * y]^4$;
  $[y = y - 1]^5$;
}
$[y = 0]^6$

Dynamic Analysis



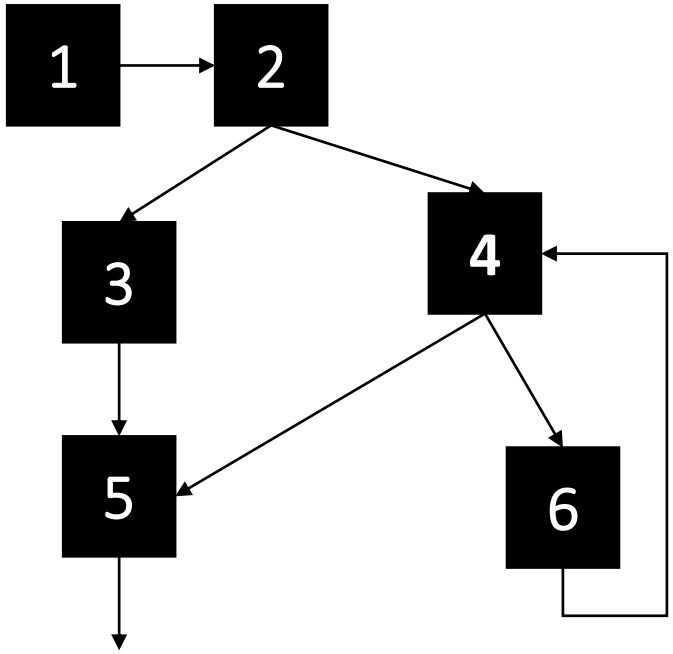
In this course, we will learn…

Introduction to Runtime Verification

Monitor Oriented Programming (Using JavaMOP)

Example: Path Profiling

- Count the paths taken during actual execution
  - consider them for optimization, distribution (with better hardware support) and test coverage



Path	Frequency
1 2 3 5	100
1 2 4 6 4 5	2000
1 2 4 6 4 6 4 5	10
1 2 4 5	10

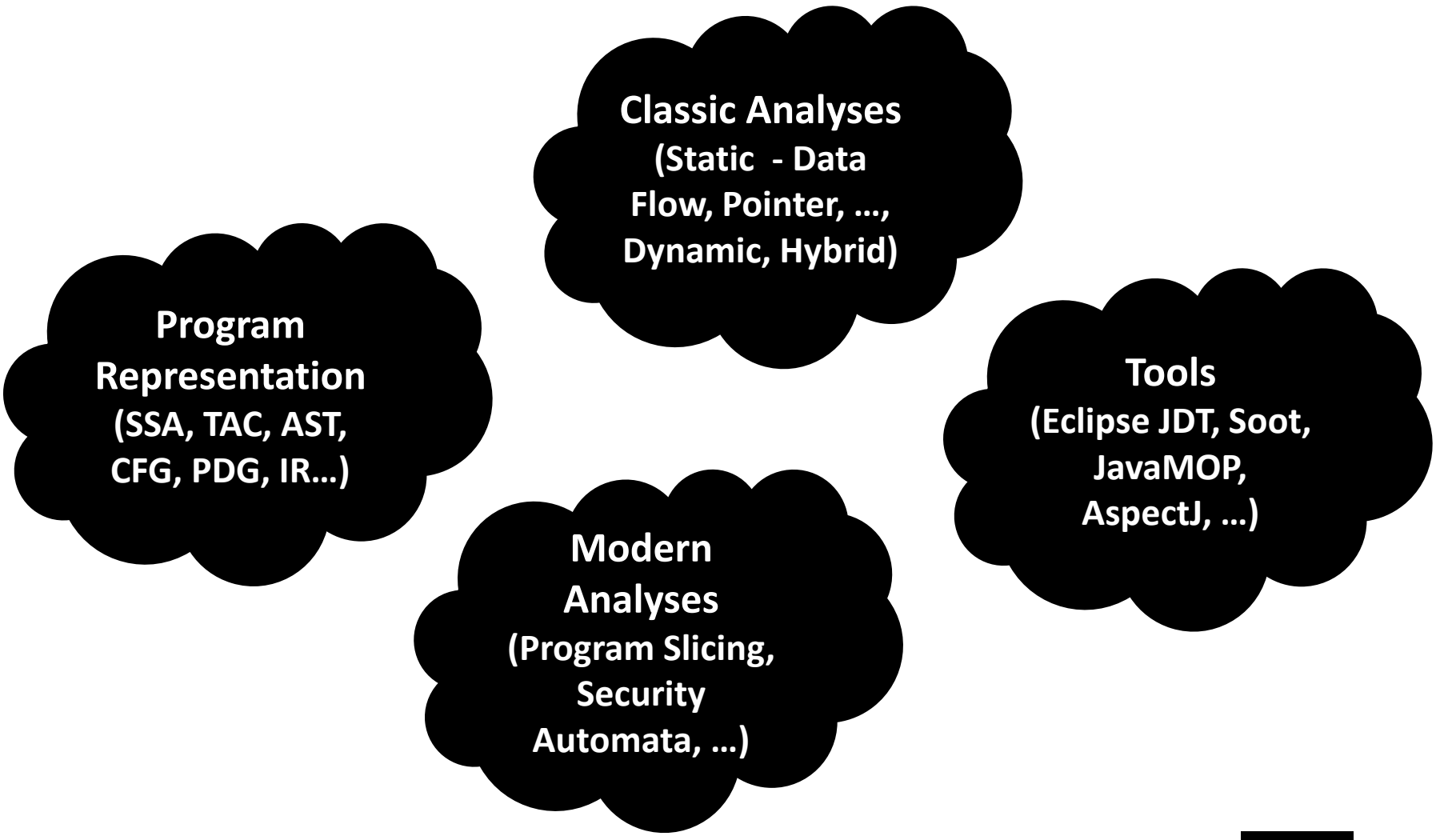
Hybrid Analysis

- Often, we hit limitations with pure static or dynamic analysis.
- Hybrid = Static + Dynamic

In this course, we will learn…

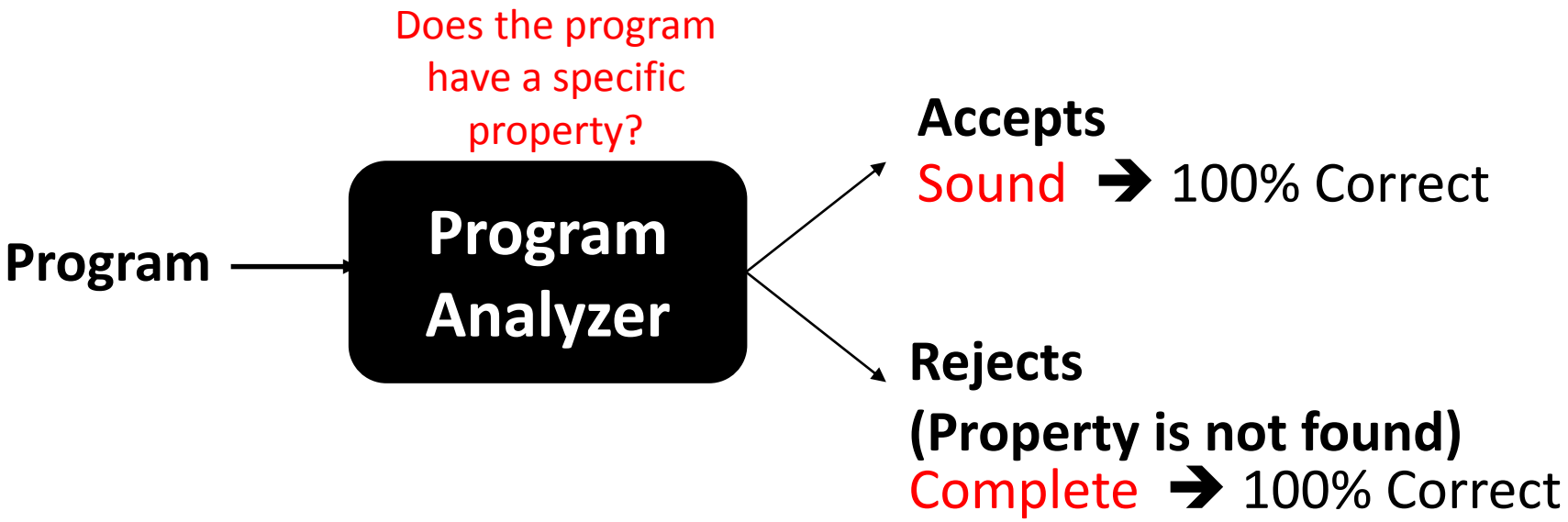
Symbolic Execution and Concolic Execution (Overview of KLEE and JavaPathFinder if time permits)

Course Overview



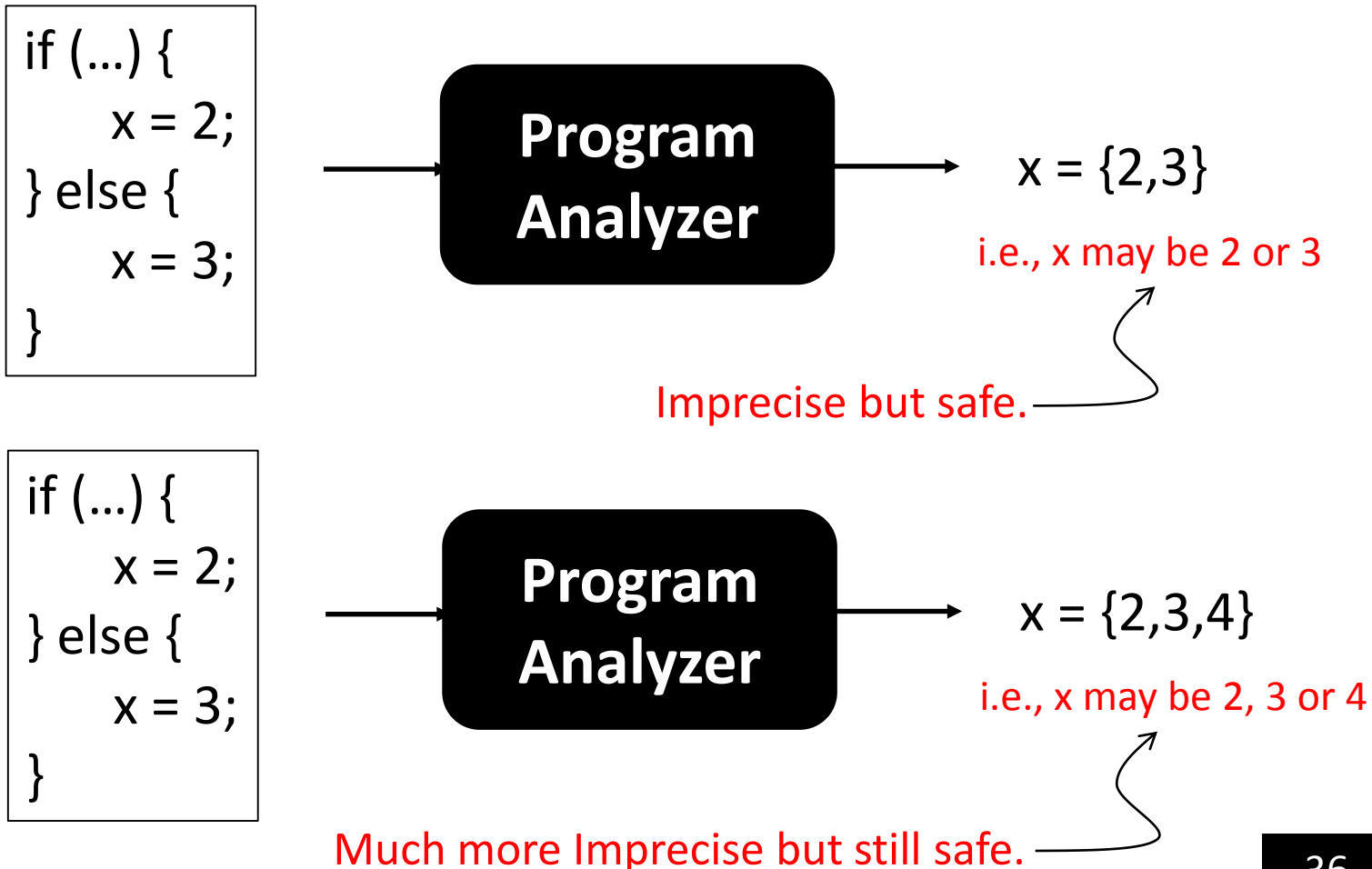
Is Our Analysis Good?

Soundness and Completeness



May not halt as well! The Don't Know result.

Safe Approximation and Precision



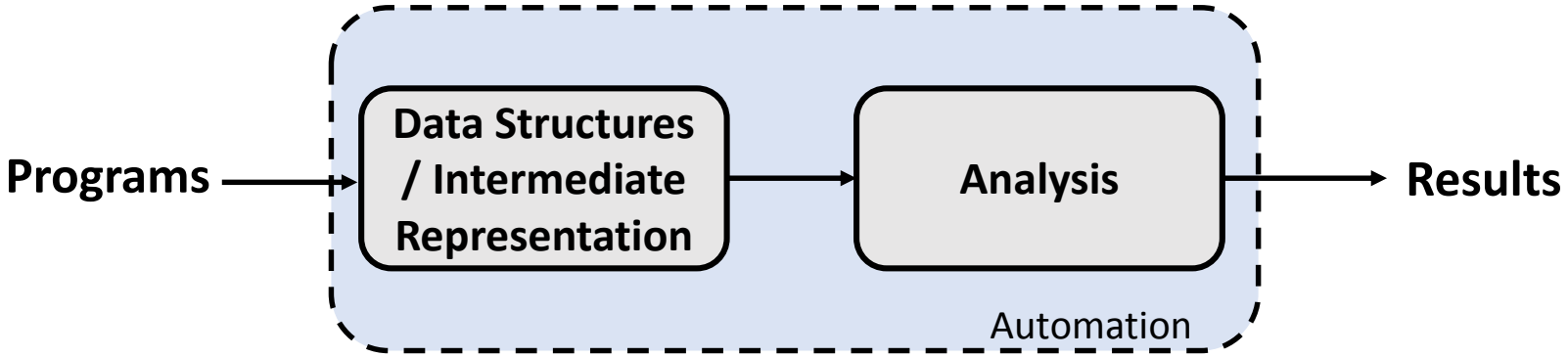
Analysis Quality

- Soundness
- Completeness
- Scalability
- Applicability
- …

Note: Many other terminologies can be found in the literature such as Correctness and Completeness, Precision and Recall, Safety and Precision, …

Summary

- What is Program Analysis?



- Why Study Program Analysis?
  - Analyzing programs is important for various reasons including optimization and verification.
- In this Course
  - **Static**, Dynamic and Hybrid Analyses