

ALLOY ANALYSIS

CURT CLIFTON

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

GOALS FOR TODAY

- **THINK ABOUT HOW ALLOY WORKS INTERNALLY.
IT'S JUST ANOTHER PROGRAM AFTER ALL.**
- **CLEAR UP ANY CONFUSION REGARDING THE
PROJECT**

HOW DOES COMPUTER
PROGRAMMING WORK?

MAGIC.



全
玄
漫

ALLOY ANALYSIS

A PEEK UNDER THE HOOD

EQUIVALENT PROBLEMS

- CHECKING ASSERTIONS IS EQUIVALENT TO RUNNING PREDICATES
- FIND SOME ASSIGNMENT OF RELATIONS TO VARIABLES THAT MAKES CONSTRAINTS TRUE
- PREDICATES:
SIGS + FIELDS + FACTS + **PREDICATE CONSTRAINTS**
- ASSERTIONS:
SIGS + FIELDS + FACTS + **NOT(ASSERTION CONSTRAINTS)**

THE PROBLEM

- **ALLOY'S LOGIC IS UNDECIDABLE**
- **IMPOSSIBLE TO BUILD A TOOL THAT CAN CHECK EVERY ASSERTION**
- **MUST MAKE SOME COMPROMISES**

**ANY LOGIC STRONG ENOUGH
TO MODEL SOFTWARE SYSTEMS
IS (PROBABLY) UNDECIDABLE**

TRADITIONAL COMPROMISE

- **USE AUTOMATED THEOREM PROVING**
 - TRIES TO BUILD PROOF THAT ASSERTION HOLDS
 - REQUIRES GUIDANCE FROM USER
- **SUCCESS? – ASSERTION DEFINITELY HOLDS**
- **FAILURE? – ASSERTION MAY OR MAY NOT HOLD**

HARD TO TELL
WHICH IS THE CASE!

ALLOY'S COMPROMISE

- **USE INSTANCE FINDING**
 - **LOOKS FOR A “REFUTATION” BY CHECKING AGAINST A HUGE SET OF TEST CASES**
- **SUCCESS? – PRODUCES COUNTEREXAMPLE**
- **FAILURE? – ASSERTION MAY HOLD, OR THERE MAY BE A LARGER COUNTEREXAMPLE THAN WAS CHECKED**

WHY INSTANCE FINDING?

- DURING EXPLORATORY MODELING MOST ASSERTIONS WILL BE INVALID
- SPECIFIC COUNTEREXAMPLES ARE HELPFUL
- INVALID ASSERTIONS CAN BE FOUND QUICKLY



CAN STOP AFTER FIRST
COUNTEREXAMPLE

TRACTABLE INSTANCE FINDING

- LIMIT SCOPE OF EACH SIGNATURE TO CONTROL SIZE OF SEARCH SPACE
- STILL HANDLES HUGE NUMBER OF TEST CASES
- MY P1 SOLUTION:
 - 1 LIFT, 5 FLOORS, 25 MOMENTS IN TIME, 2 DIRECTIONS, 2 DOOR STATES:
 - CURRENT FLOOR RELATION: 25 X 5 POSSIBILITIES
 - REQUESTS RELATION: 25 X 2⁵ POSSIBILITIES
 - DIRECTION INDICATOR RELATION: 25 X 3 POSSIBILITIES
 - PLANNED DIRECTION RELATION: 25 X 3 POSSIBILITIES
 - DOORS RELATION: 25 X 2 POSSIBILITIES

**MORE THAN 28 BILLION
INSTANCES CHECKED IN 103 MS!**

**PROGRAM TESTING CAN BE USED
TO SHOW THE PRESENCE OF BUGS,
BUT NEVER TO SHOW THEIR ABSENCE.**

DIJKSTRA

**IT CAN'T USUALLY SHOW
THEIR PRESENCE EITHER.**

– JACKSON

THE SMALL SCOPE HYPOTHESIS

**MOST BUGS HAVE SMALL
COUNTEREXAMPLES**

P1 QUESTIONS