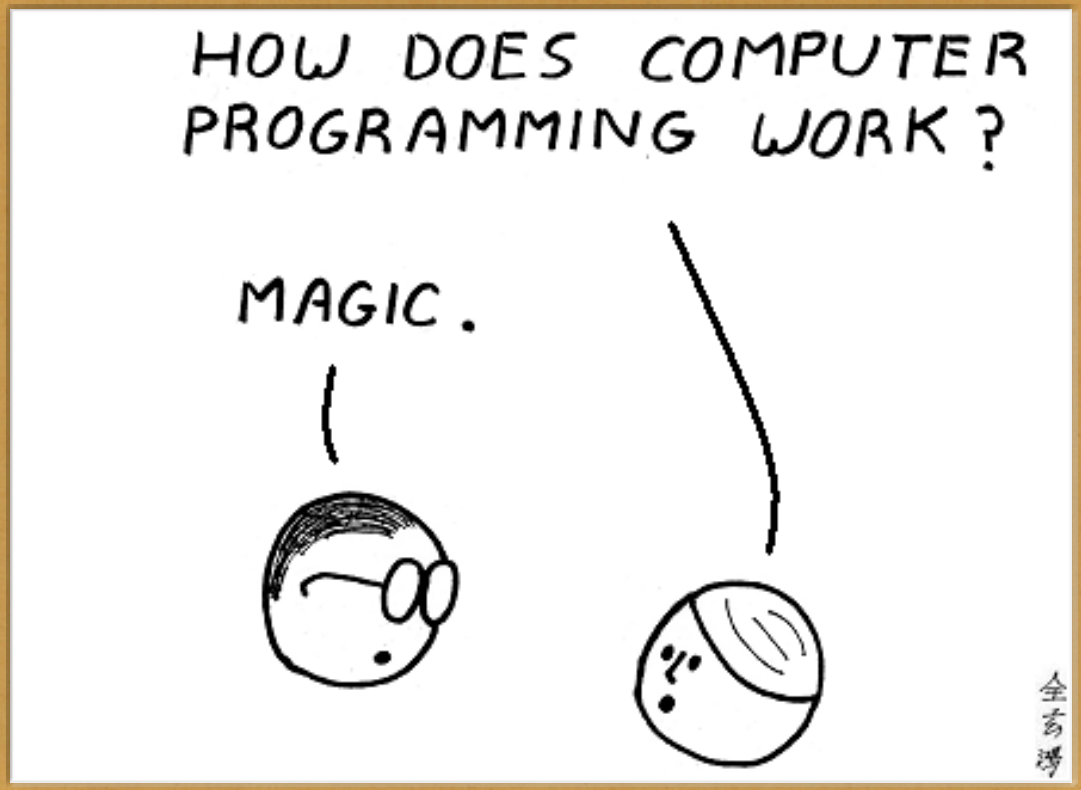
Alloy Analysis

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



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)**

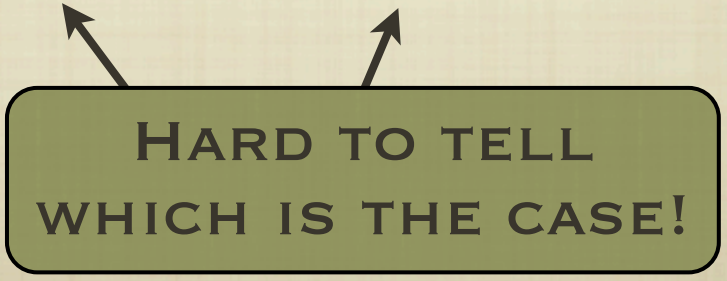
The Problem

- 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



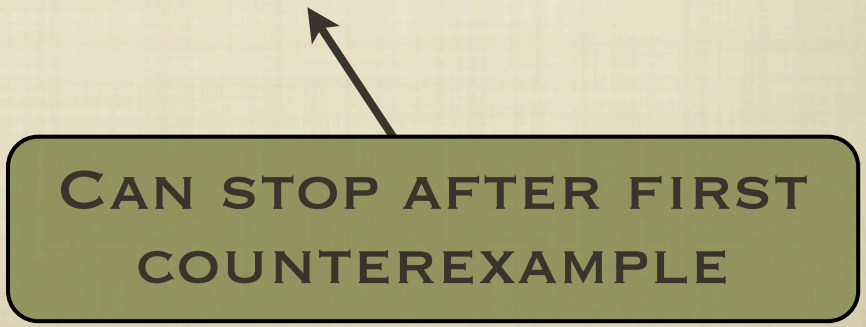
Q2

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

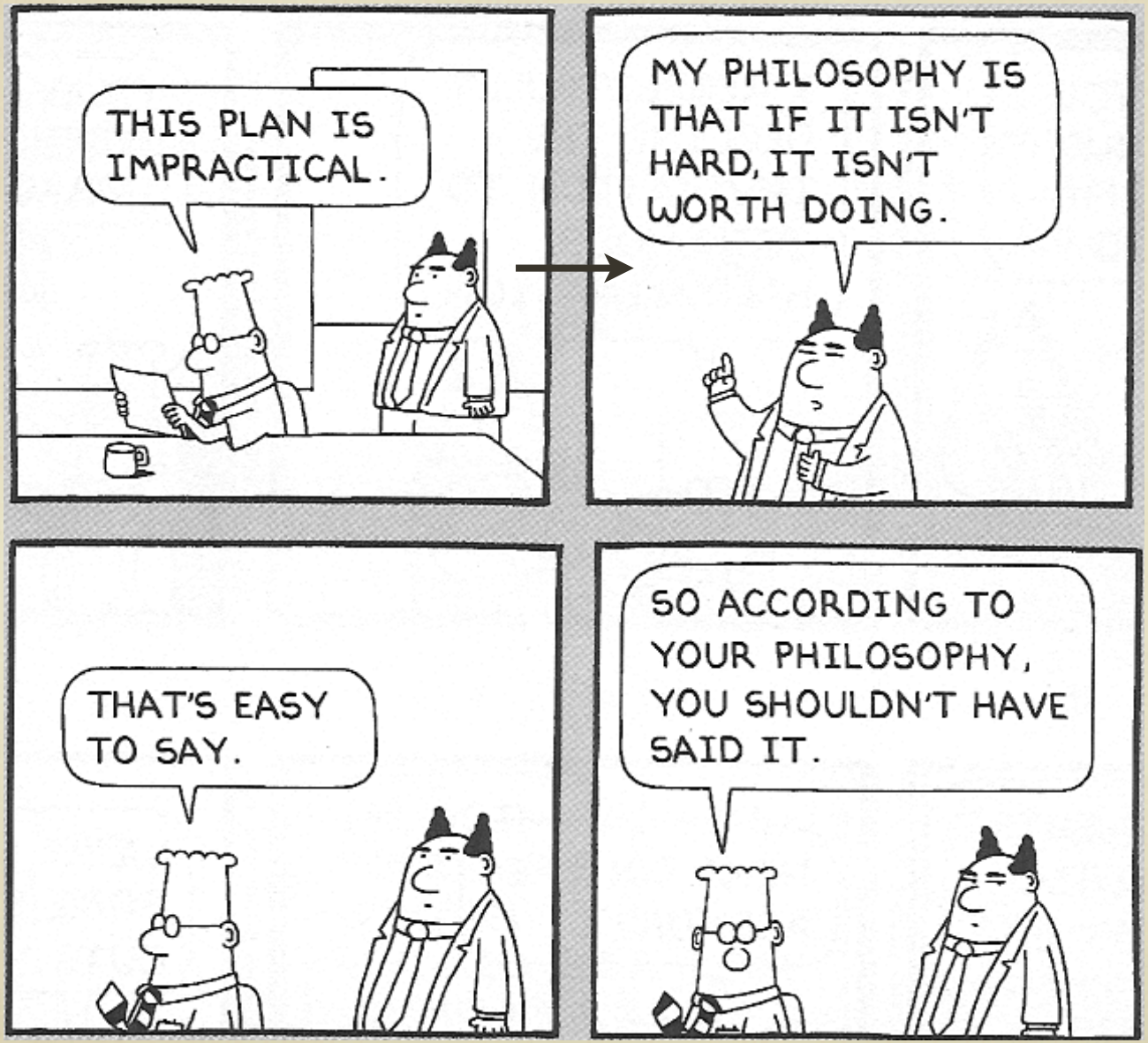
Why Instance Finding?

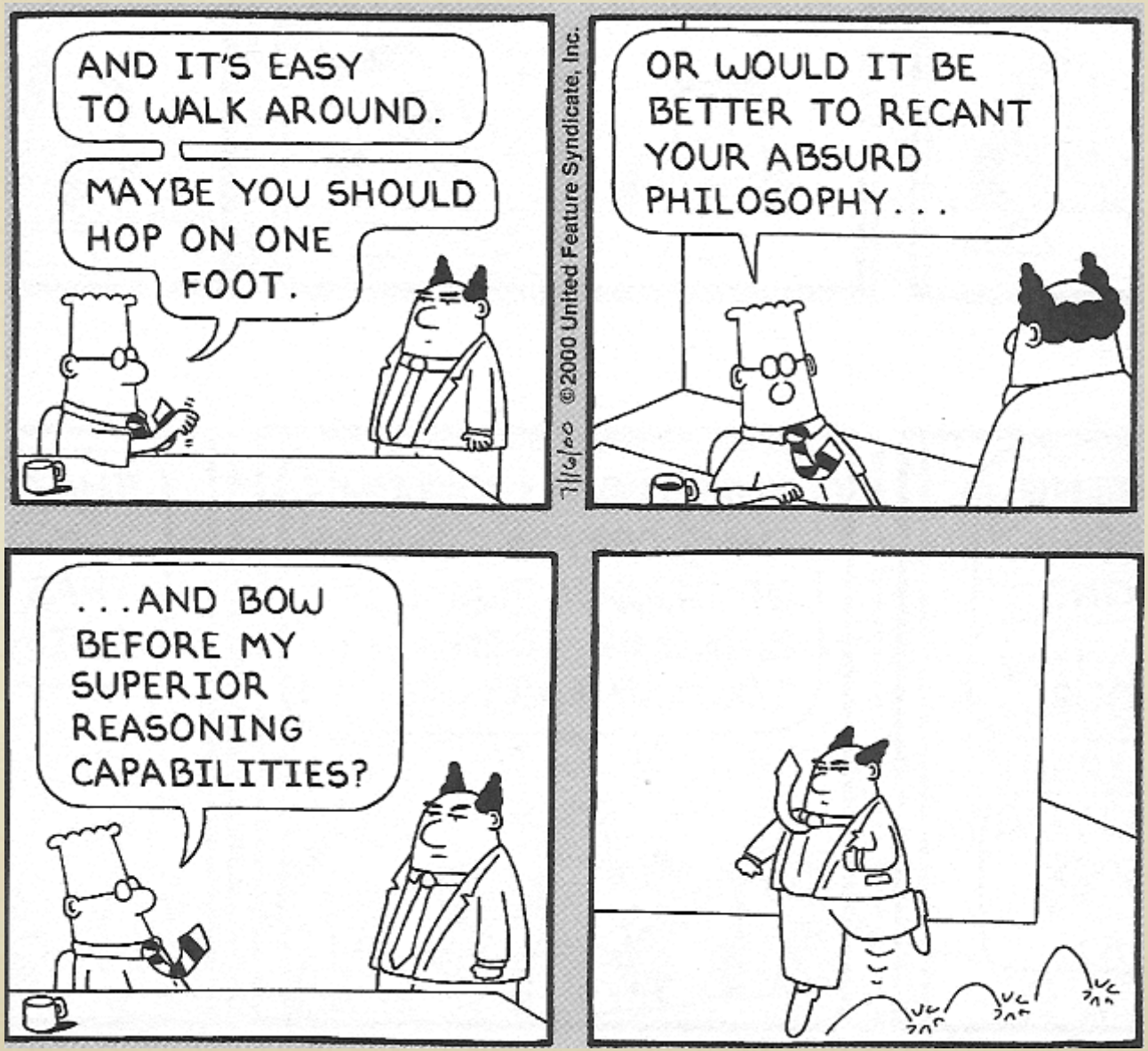
- During exploratory modeling most assertions will be invalid
- Specific counterexamples are helpful
- Invalid assertions can be found quickly



Q3

Cartoon of the Day




AND IT'S EASY TO WALK AROUND.
MAYBE YOU SHOULD HOP ON ONE FOOT.
7/6/00
©2000 United Feature Syndicate, Inc.
OR WOULD IT BE BETTER TO RECANT YOUR ABSURD PHILOSOPHY...
...AND BOW BEFORE MY SUPERIOR REASONING CAPABILITIES?

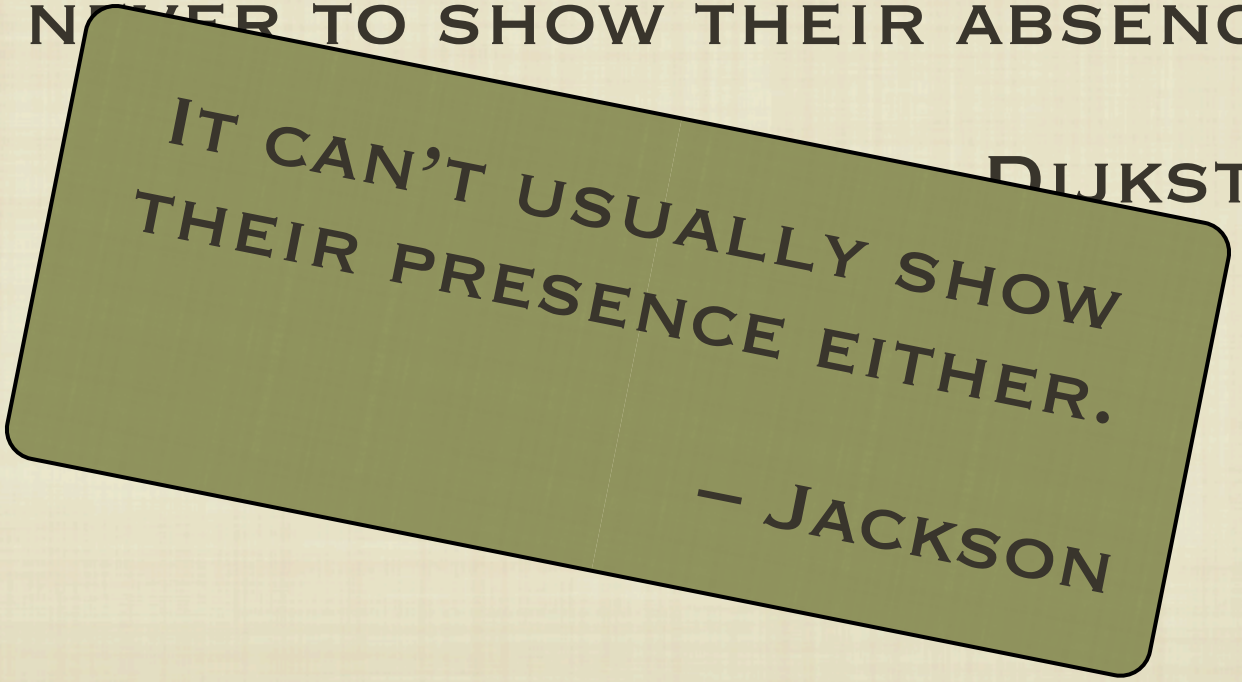
Tractable Instance Finding

- 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 possibilities
    - requests relation: 25 x 2^5 possibilities
    - direction indicator relation: 25 x 3 possibilities
    - planned direction relation: 25 x 3 possibilities
    - doors relation: 25 x 2 possibilities

More than 5.6 billion instances checked!

Program testing can be used
to show the presence of bugs,
but never to show their absence.

Dijkstra



The Small Scope Hypothesis

Most bugs have small counterexamples

Q4,5

P1 Questions