Alloy Paragraphs and Commands

Curt Clifton
Rose-Hulman Institute of Technology

Goals for Today

- Increase our understanding of Alloy constraints by looking at a couple of examples in detail
- Understand when to use facts, predicates, assertions, and functions

Paragraphs

Facts, Assertions, Predicates, Functions

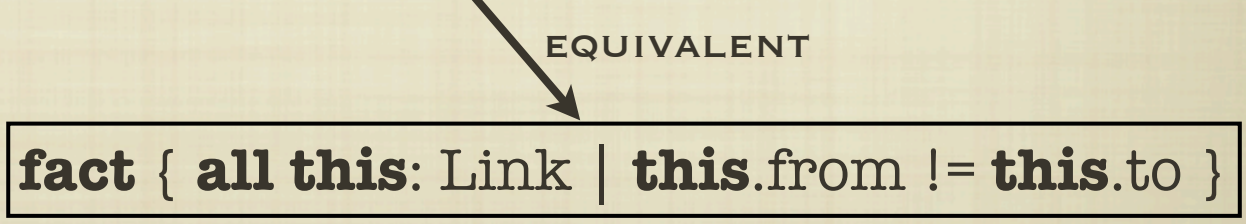
Facts

- Always assumed to hold
- Example...

Signature Facts

- Can give simple facts about a signature after its declaration:

- **sig** Host { }
  sig Link { from, to: Host } { from != to }



Functions & Predicates

- For reuse and clarity:
  - Functions are named expressions
  - Predicates are named constraints
- Example...

More OO-like Notation

- Instead of:
  - ```
    fun redLights[s: LightState]: set Light { s.color.Red }
    pred mostlyRed[s: LightState, i: Intersection] {
        lone i.lights - redLights[s]
    }
    ```
- Can write:
  - ```
    fun LightState.redLights[]: set Light { this.color.Red }
    }
    pred LightState.mostlyRed[i: Intersection] {
        lone i.lights - this.redLights[]
    }
    ```

Facts vs. Predicates

- Small models:
  - Favor facts – more succinct, easy to change into predicates if needed
- Large models:
  - Use helper predicates to define properties
  - Use other predicates or facts to package properties together

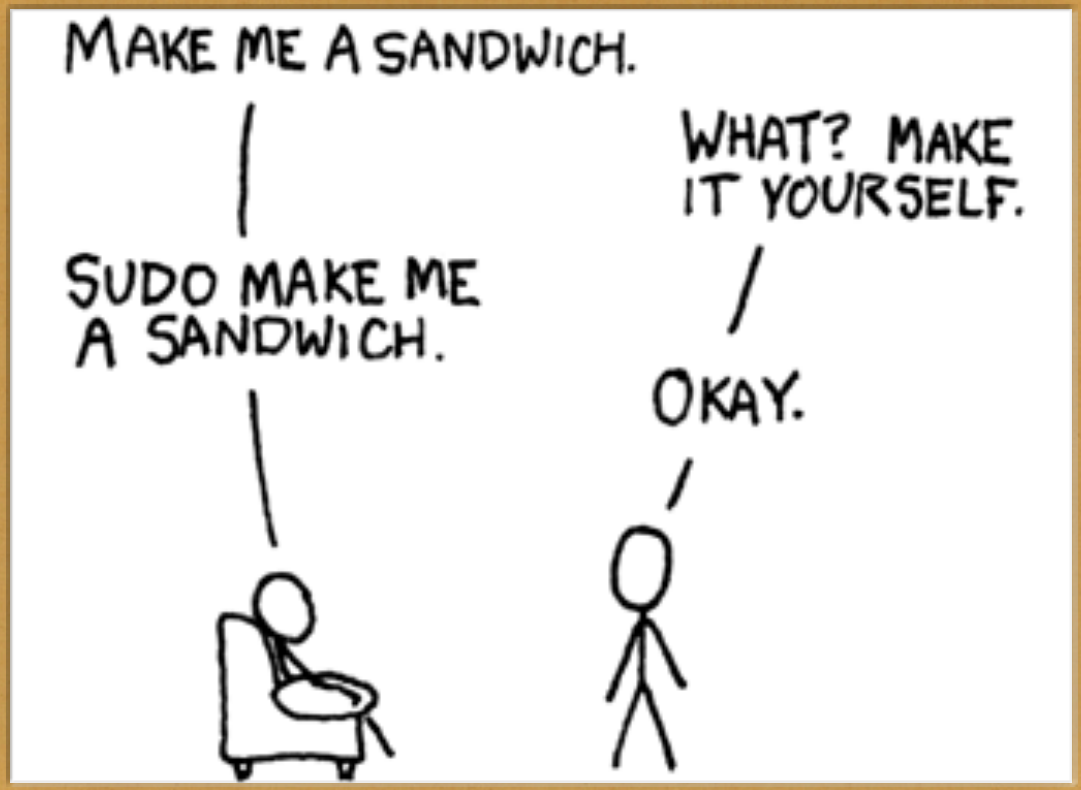
Assertions

- Constraints that are intended to follow from the facts
- Alloy looks for counterexamples
  - Think "bug reports"
- Example...

Typical Assertions...

- ...Express mundane properties
  - Used to detect flaws in our thinking
  - "elevator has only one choice of next move"
- ...or Express essential properties
  - "Elevator eventually services all requests"

Q2,3



http://xkcd.com/149/

Commands & Scope

Two Commands

- **run** — search for an instance of a predicate
- **check** — search for a counterexample for an assertion

Scope

- Not specified?
  - Command uses default:
    3 of each **top-level** signature
- Can bound mix of top-level and sub-signatures
  - As long as bounds are complete...

Choosing the Scope

- Small system? Scope might match real world
  - E.g., exactly 3 elevators, exactly 5 floors
- Larger systems
  - Scope is set large enough for confidence
  - Small enough for speed

Goals for Today

- Increase our understanding of Alloy constraints by looking at a couple of examples in detail
- Understand when to use facts, predicates, assertions, and functions

Next Time

- Discuss project milestone P1
- Reuse in Alloy
- Sample HW problems if time permits