Alloy as an Introduction to Formal Methods
**SIMPLE**: Minimal Essential Complexity

**CONVENIENT**: Minimal Accidental Complexity
Convenience Hypothesis

People prefer a convenient but imperfect tool over a perfect but inconvenient one.
Alloy is convenient
What are the “easiest” improvements?
“Easiest” Improvements

• No centralization
• No organization
• No language extensions
• No programming
• Online Reference
Hillel Wayne
• Online Reference
• Online Documentation
INTRODUCTION

Note

If you want a video introduction, come watch my Strange Loop talk on TLA+!

What is TLA+?

TLA+ is a *formal specification language*. It’s a tool to design systems and algorithms, then programmatically verify that those systems don’t have critical bugs. It’s the software equivalent of a blueprint.

Why should I use it?

Here’s a simple TLA+ specification, representing people trading unique items. Can you find the bug?

```plaintext
People == {"alice", "bob"}
Items == {"ore", "sheep", "brick"}
(algorithm trade
  variable owner_of \in [Items -> People]
process giveitem \in 1..3 /* up to three possible trades made
  variables item \in Items,  Hillel Wayne
  owner = owner_off[item],
```

• Online Reference
• Online Documentation
• Recipe Books
• (Identity of set) $A \triangleleft \text{idem}$
• (Is symmetric) $\sim r \in r$
• (Rest of cycle) $a. (^\text{succ} + ^\sim\text{succ})$
• Traces
• Stuttering
• etc
• Online Reference
• Online Documentation
• Recipe Books
• Directed Labs
@Hillelogram Inspired by your blog posts, I attempted to model a work project in Alloy.

I discovered that there are huge number of invariants that we believe our data model has but that are enforced only accidentally. Now thinking about enforcing them more explicitly.

2:00 AM - Mar 23, 2018