Specifications need refinement

- To handle special cases
- To guide designers
- To V&V the spec
Toward more formalism

- **Language and style**
  - “may” / “should” / “must”
  - condition → response
  - state × action → response

- **Still English, at end**
- **OK to specify in the background**
Formal Methods

- Specification & Design
  - bleed into implementation & testing
- Many possible styles
  - UML / OOD (formal?)
  - Data Flow Diagrams
  - Finite State Machines
Fundamental ideas

- **Systematize work**
  - Can prove sound & complete
  - High precision possible
- **Focus worker**
  - Small steps
  - Checkable by anyone
Formal Methods
supernaturns

- It's too hard
- It's too slow
- It's unnecessary
- “The kind I know is bad, so surely all kinds are bad”
How to get quality SW

• Three techniques
  – Inspection
  – Testing
  – Formal Methods

• Probably in that order

• Synergy: solve different problems
Formal spec as *oracle*

- **Testing w/ formal method**
  - Can check test cases
  - Can work inputs to outputs
  - Can work outputs to inputs

- **Synchronizes spec with tests = good for requirements change**
Where we use formal methods

- “Formal methods are used today only in safety-critical applications.” — humbug
  - transportation / aerospace
  - simulation

- Use formal methods when confused and worth fixing
Example: Cut/Copy/Paste

- Use Alloy spec language
- Allows constructing model
  - of state
  - of user actions
  - of responses
- Succinct, checkable
- Still need English spec
Specifications need refinement

- To handle special cases
- To guide designers
- To V&V the spec
Toward more formalism

- Language and style
  - “may” / “should” / “must”
  - condition → response
  - state × action → response

- Still English, at end

- OK to specify *in the background*
Formal Methods

- **Specification & Design**
  - bleed into implementation & testing
- **Many possible styles**
  - UML / OOD (formal?)
  - Data Flow Diagrams
  - Finite State Machines
Fundamental ideas

- **Systematize work**
  - Can prove sound & complete
  - High precision possible
- **Focus worker**
  - Small steps
  - Checkable by anyone
Formal Methods superstitions

- It's too hard
- It's too slow
- It's unnecessary
- “The kind I know is bad, so surely all kinds are bad”
How to get quality SW

- Three techniques
  - Inspection
  - Testing
  - Formal Methods
- Probably in that order
- Synergy: solve different problems
Formal spec as *oracle*

- **Testing w/ formal method**
  - Can check test cases
  - Can work inputs to outputs
  - Can work outputs to inputs

- **Synchronizes spec with tests** = good for requirements change
Where we use formal methods

- “Formal methods are used today only in safety-critical applications.” — humbug
  - transportation / aerospace
  - simulation
- Use formal methods when confused and worth fixing
Example: Cut/Copy/Paste

- Use *Alloy* spec language
- Allows constructing model
  - of state
  - of user actions
  - of responses
- Succinct, checkable
- Still need English spec