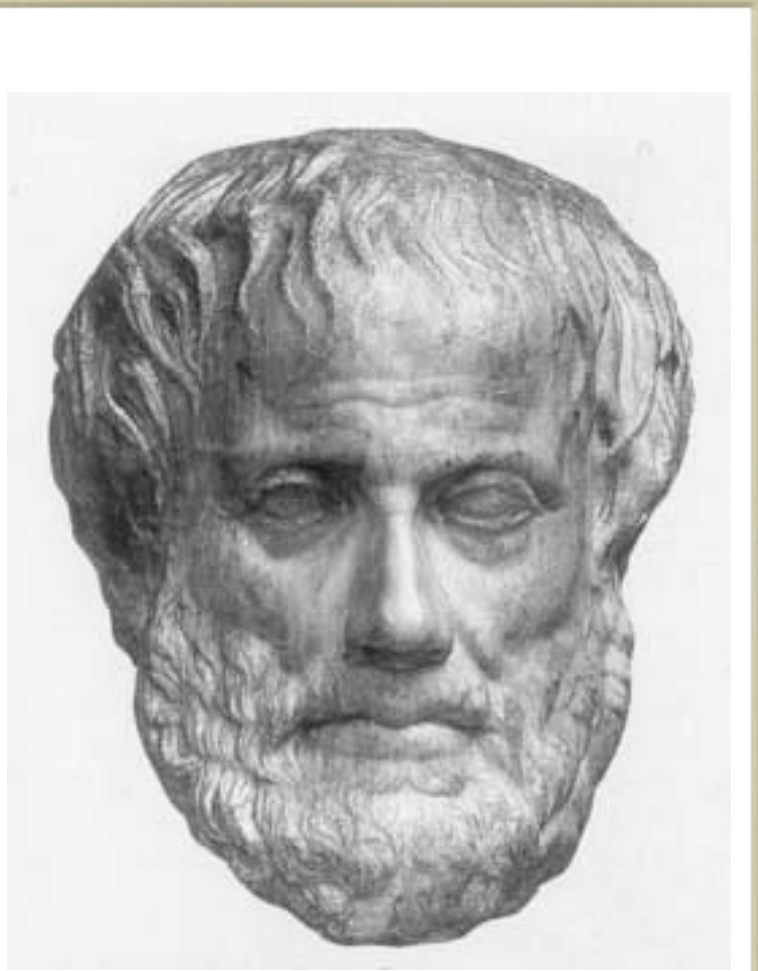
What are Formal Methods?

CSSE 373, Formal Methods

Curt Clifton

What are formal methods? (1/2)

- Formal methods are methods that use formal language.
- Formal methods use formal logic.



$$\forall M \in Men \cdot M \in Mortal; S \in Men; \therefore S \in Mortal$$

What are formal methods? (2/2)

- Formal methods use formal specification languages. That is, they use languages that have a mathematically-defined static semantics.
- Formal methods employ analysis that is mathematically sound.

When are formal methods most useful?

- When you have to get it right
- When you cannot test it adequately
- Examples:
  - safety-critical applications
    - aviation
    - medical equipment
  - economically-critical applications
    - Stock Exchange
    - ATMs

Jackson on Design

- "Such massive failures [Denver airport baggage handling, etc.] occur because crucial design flaws are discovered too late."

- "No amount of refactoring, bar starting from scratch, can rescue a system built on flawed concepts."

- "When good abstractions are missing from the design, or erode as the system evolves, the resulting program grows barnacles of complexity."

Possible Ways to get the abstraction right

- Evolve the design
- Formal specification and theorem proving
- Model checking
- SAT Solving

Benefits of SAT Solving

- No test cases
- Automatically discovers counterexamples
- "A kind of exploration therefore becomes possible that combines the incrementality and immediacy of extreme programming with the depth and clarity of formal specification"

Fallacies about Software – 1

- Software is too complicated to get completely right.
- The only way to know whether software works is to test it.
- Users don't know what they want—only trial and error will lead to the right solution.

Fallacies about Software – 2

- Everything has bugs in it, so there is no point in making anything better.
- It costs too much to make highly-reliable software.
- Computing is still too immature to be reliable.

Installing Alloy

- On campus:
  - http://www.rose-hulman.edu/class/csse/binaries/Alloy
- Off campus:
  - http://alloy.mit.edu/alloy4
- **Next time, Monday:**
  - **Bring Laptop and text book!**