Lecture 11: Introduction to Formal Software Engineering

Kenneth M. Anderson

Foundations of Software Engineering

CSCI 5828 - Spring Semester, 1999

Today's Lecture

- Present Introduction to Formal Software Engineering
  - Discuss Models
  - Discuss Formal Notations

Software Engineering

- Software

  Computer programs and their related artifacts

- Engineering

  The application of scientific principles in the context of practical constraints

Formal Software Engineering

- Software

  Computer programs and their related artifacts

- Engineering

  The application of scientific principles in the context of practical constraints

- Formal

  The use of models, techniques, and tools that are grounded in mathematics

Some Important Points

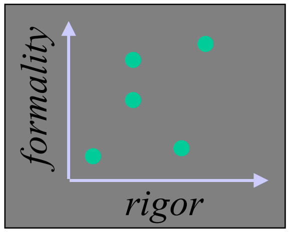
- *Formal* does not mean *Hard*
- *Formal* does not mean *Good*
- *Informal* does not mean *Bad*

… unless it means *ad hoc*

Some Important Points

- *Formal* does not mean *Hard*
- *Formal* does not mean *Good*
- *Informal* does not mean *Bad*

… unless it means *ad hoc*



What Are "Formal Methods"?

❶*Writing* a formal specification

❷*Proving* properties about the specification

❸*Constructing* a program by mathematically manipulating the specification

❹*Verifying* the program by mathematical argument

Formal SE is Broader

Not just specification and verification of programs…

- Architecture
- Analysis/Testing
- Reliability and Performance Engineering
- Configuration Management
- Process Management
- And More…

Model/Specification/Formalism

- Model

  An abstract representation
- Specification

  A formal expression of a model or of a property of a model
- Formalism

  A mathematical notation for writing specifications; a specification language

Specification and the Lifecycle

- Requirements
- Design

  High level and low level
- Implementation
- Test

Specification and the Lifecycle

- Requirements
- Design

  High level and low level
- Implementation
- Test

Specification is used in All Activities

Specification/Modeling Styles

- Operational
- Declarative
  - Axiomatic
  - Algebraic
- Structural/Relational

Specification/Modeling Styles

- Operational
- Declarative
  - Axiomatic
  - Algebraic
- Structural/Relational

Choice of style dictated by focus of concerns

Logical Foundations

- Predicate logic
- Modal logic
- Lambda calculus

Mathematical Foundations

- Set theory
- Graph theory
- Automata theory
- Abstract algebra
- Probability and statistics

Analysis of Specifications

- Static Analysis

  Examines specification text to reveal properties
- Dynamic Analysis

  Executes specification text to reveal properties

Analysis of Specifications

- Static Analysis

  Examines specification text to reveal properties

- Dynamic Analysis

  Executes specification text to reveal properties

Choice of analysis dictated by focus of concerns and choice of specification style