SE4033 Formal Methods in Software Engineering

Course Outline

Program Learning Outcomes

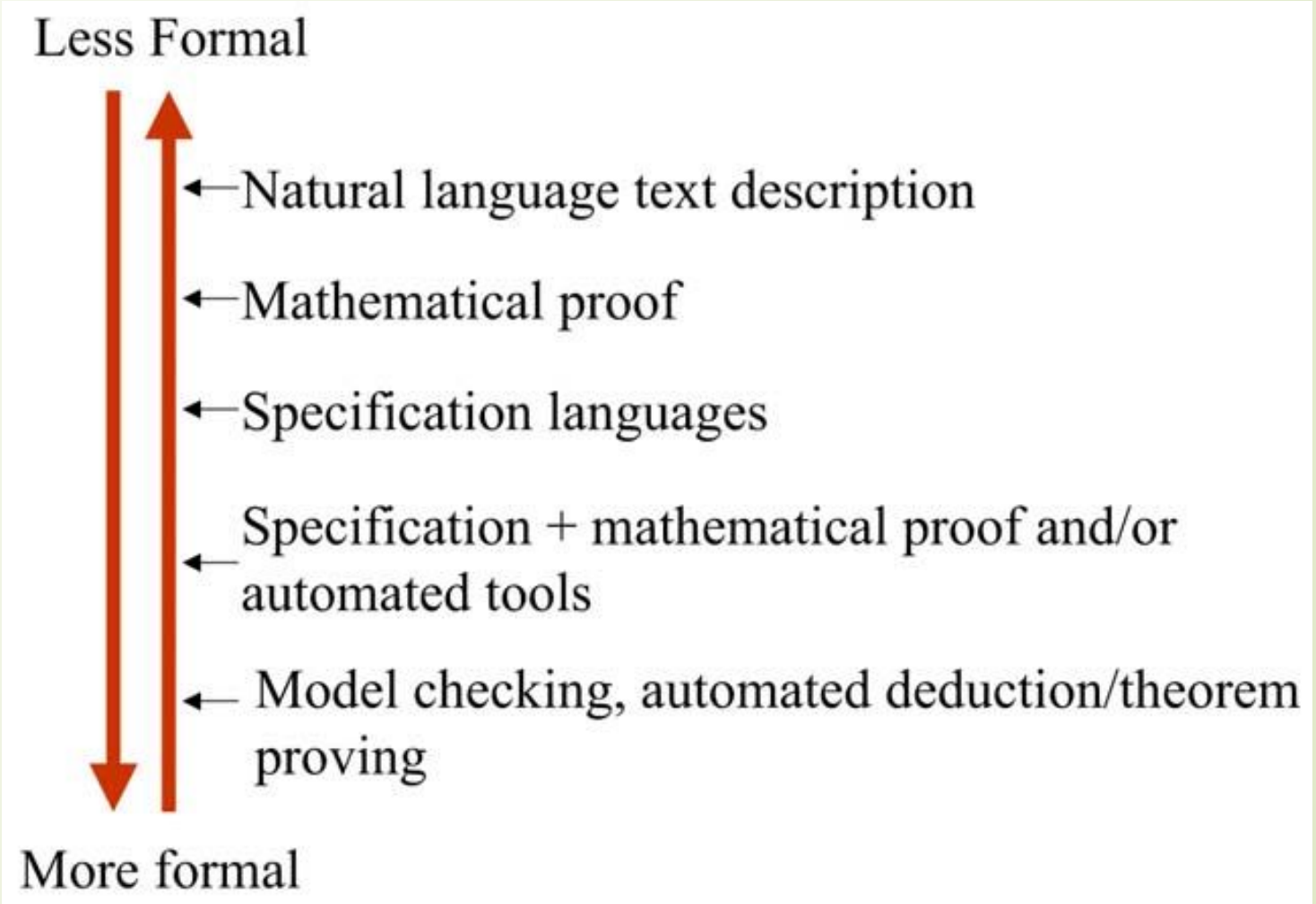
- Problem Analysis
  - Identify, formulate, research literature, and analyze complex computing problems, reaching substantiated conclusions using first principles of mathematics, natural sciences, and computing sciences.
- Design/Develop Solutions
  - Design solutions for complex computing problems and design systems, components, and processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal, and environmental considerations.
- Investigation & Experimentation
  - Conduct investigation of complex computing problems using research-based knowledge and research-based methods.

Course Learning Outcomes (CLOs)

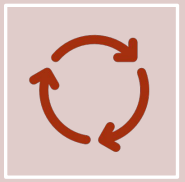
- Describe the costs and benefits of formal methods’
- Construct formal models of sequential
- software systems Implement sequential software systems based on formal models
- Verify attributes of formal models
- Demonstrate formal correctness of simple procedure

Formalization Spectrum

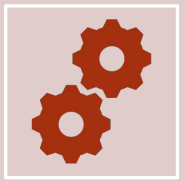
- From Less to more formal



Outline



Software Development Life Cycle (SDLC) Revision

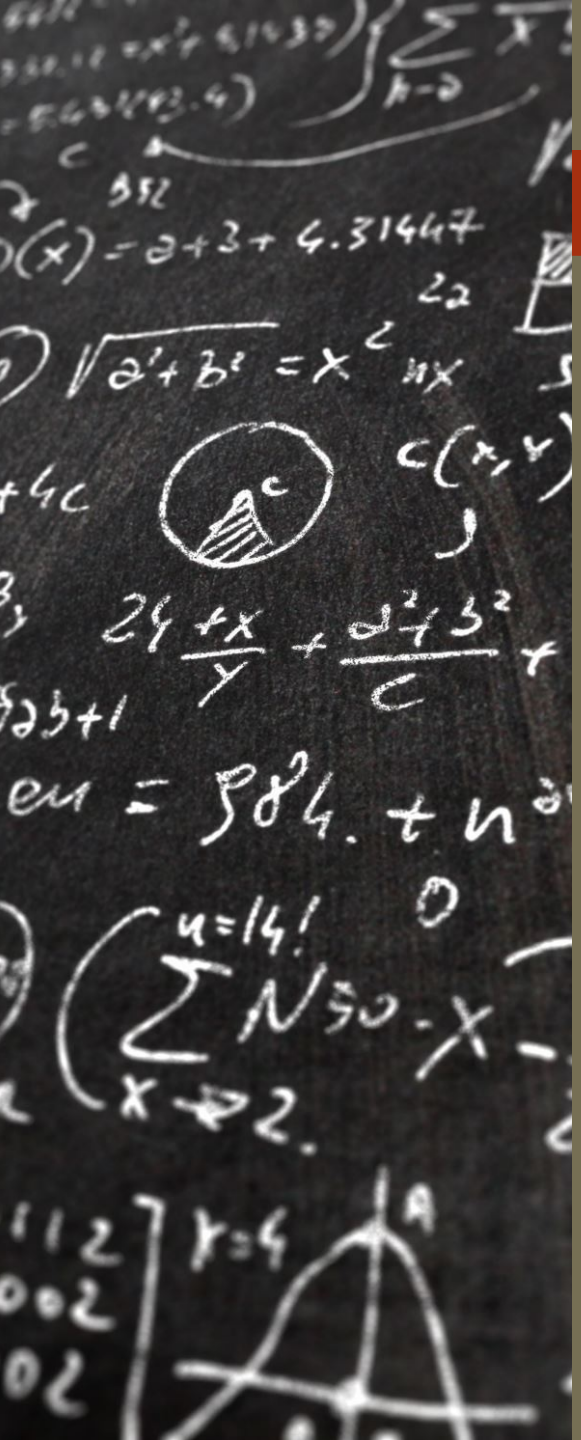


Formal Methods for Software Engineering

- Logic (Boolean)
- Regular Expressions
- Finite State Machine/Automaton
- Algorithms
- Petri Nets

Outline: Analysis

- Propositional Logic
- Specification in VDM-SL
- Algebraic Specifications
- Analyze well formlessness
  - Completeness
  - Consistency
  - Robustness
- Analyze correctness
  - Static analysis
  - Simulation
  - Model checking



Outline: Sets

- Sets for System Modelling
- Declaring and Defining Sets in VDM-SL
- Set Operations
- Implementing Sets in Programming Language
- Collection Classes

Outline: Sequences

Notation

Sequence Operators

Defining a Sequence by Comprehension

Using the Sequence Type in VDM-SL

Implementing Sequences

The VDMSequence Class

Outline: Composite Objects

- Defining Composite Object Types
- Composite Object operators
- Implementing Composite Objects
- Implementing the Process Management System

Outline: Maps

- Notation
- Map Operators
- Map Application
- Using the Map Type in VDM-SL
- Specifying a High-Security Building
- Implementing Maps
- The Hashtable Class
- The VDMMap Class
- Formal Methods in Block Handler

Formal Specifications

- Formal Specification Languages
- Algebraic Languages (Larch, OBJ, Lotos)
- Model Based Language (Z, VDM, B, CSP, Petri Nets)
- Formal Methods For Modeling Biological Regulatory Networks

Outline: Models

- VDM II
- Formal Methods for Software
- Specification and Analysis
- Abstract Model Specifications Alloy: A Lightweight Object Modeling Notation
- Object Constraint Language (OCL)
- Larch Shared Language (LSL)

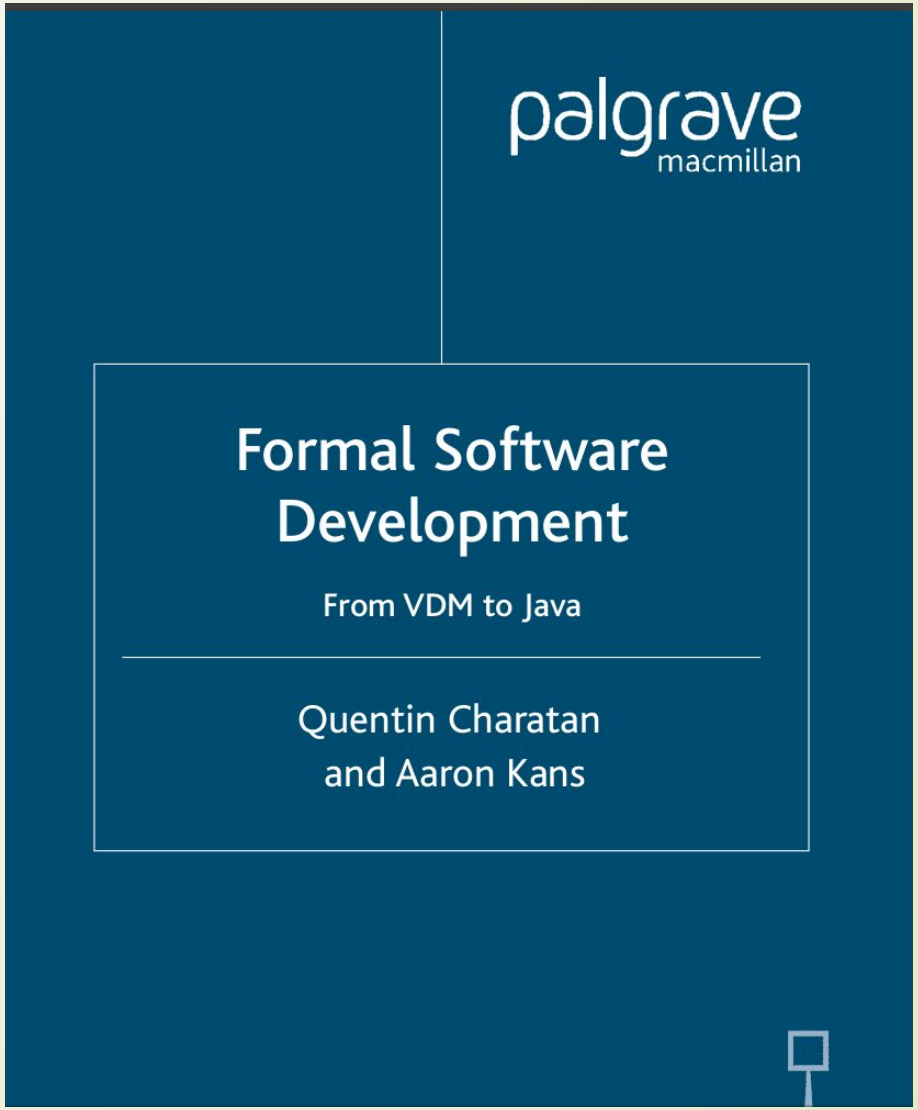
Outline: Z Notations

Z Notations

Relations in Z Specification

Books

- Formal Software Development From VDM to Java
- Quentin Charatan and Aaron Kans



Evaluations

Assessment Item	Number of Assessments	Weight (%)
Assignments	3	5
Quizzes	4	10
Midterm Exam	2	30 (15 each)
Final Exam	1	50