MUST

Wisdom & Virtue

MIRPUR UNIVERSITY OF SCIENCE AND TECHNOLOGY (MUST), MIRPUR
DEPARTMENT OF SOFTWARE ENGINEERING

Formal Methods in Software Engineering

Lecture [1] : Introduction to Software Engineering

Engr. Samiullah Khan

(Lecturer)

Topics discussed in Today’s Lectures

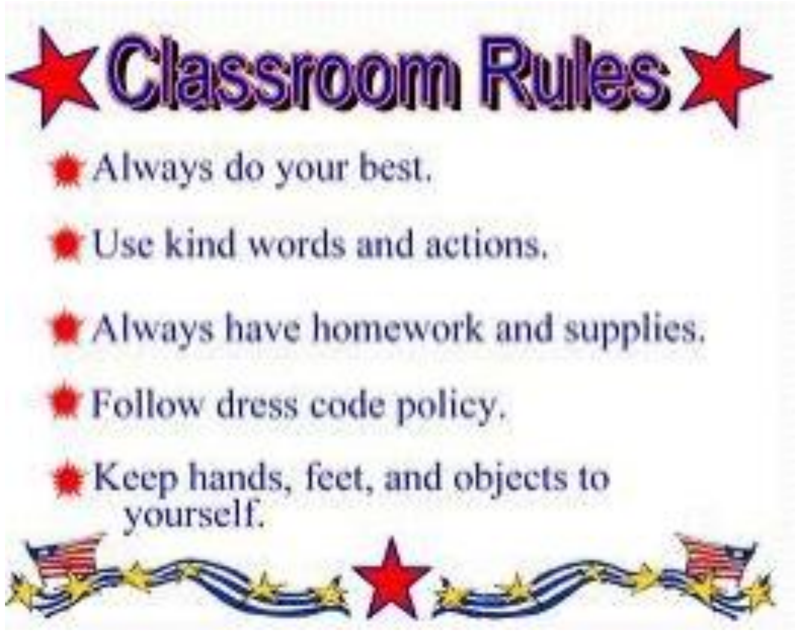
- Formal Methods Intro

Grading Policy

- Quizzes 10%
- Assignments 10%
- Mid Term 30%
- Final Exam 50%

Rules/Pattern of class

- Be punctual
- Switch off your mobile-phones
- Class participation is must
- Maintain discipline in class
- Dress well yourself
- Hair comb/ trim/ if required
- Revise your moral/ ethical values and follow them



Classroom Rules

- Always do your best.
- Use kind words and actions.
- Always have homework and supplies.
- Follow dress code policy.
- Keep hands, feet, and objects to yourself.

Course Learning Outcomes (CLOs)

Course Learning Outcomes	Domain
1) Recall foundational historical developments, principles, key concepts, cost and benefits, propositional calculus, and terminologies related to formal methods in software engineering.	C
2) Solve formal models of sequential hardware circuits, for concurrent software system verification, including various formal specification languages and their practical applications	C
3) Apply formal models and techniques to document and verify properties/attribute	C
4) Analyzes the formal correctness of simple procedural programs and the advantages and limitations of employing mathematical models and alternative techniques for software verification.	C

Formal Methods

- The **Encyclopedia** of Software Engineering defines formal methods in the following manner:
- Formal methods used in developing computer systems are:
  - Mathematically based techniques for describing system properties.
  - Such formal methods provide frameworks within which people can:
    - Specify
    - Develop, and
    - Verify systems in a systematic, rather than ad hoc manner.

Formal Method Definition

- A method is formal if it has a sound mathematical basis, typically given by a formal specification language

This basis provides a means of precisely defining notions like:

- Consistency,
- Completeness, and
- More relevantly specification,
- Implementation and
- Correctness

Formal Method Definition

- **Correctness:**
  - the property that an abstract model fulfills a set of well-defined requirements
- **Consistency:**
  - to be consistent, facts stated in one place in a specification should not be contradicted in another place
  - Used to specify programs, what the system is supposed to do
    - Used for creating programs
    - Used to verify the program

Formal Methods

- Formal methods are methods that use **formulas**
- A formula is a text or diagram constructed from predefined symbols combined according to explicit rules
- A good working definition of formula is *anything whose appearance or syntax can be checked by a computer*
- According to this definition, every computer program is a formula

Formal Methods

- Formal methods are methods that use **formulas**
- A formula is a text or diagram constructed from predefined symbols combined according to explicit rules
- A good working definition of formula is *anything whose appearance or syntax can be checked by a computer*
- According to this definition, every computer program is a formula

Formal vs Informal Problem Solving Framework

- Formal methods are practical
- and precise way of solving problems
- Figure 1-1 shows basic problem solving framework, which comprises formal and informal domains
- It is quite important to find suitable and comprehensive way to define and describe the underlying problem:
    - So that it becomes easier to find solution.

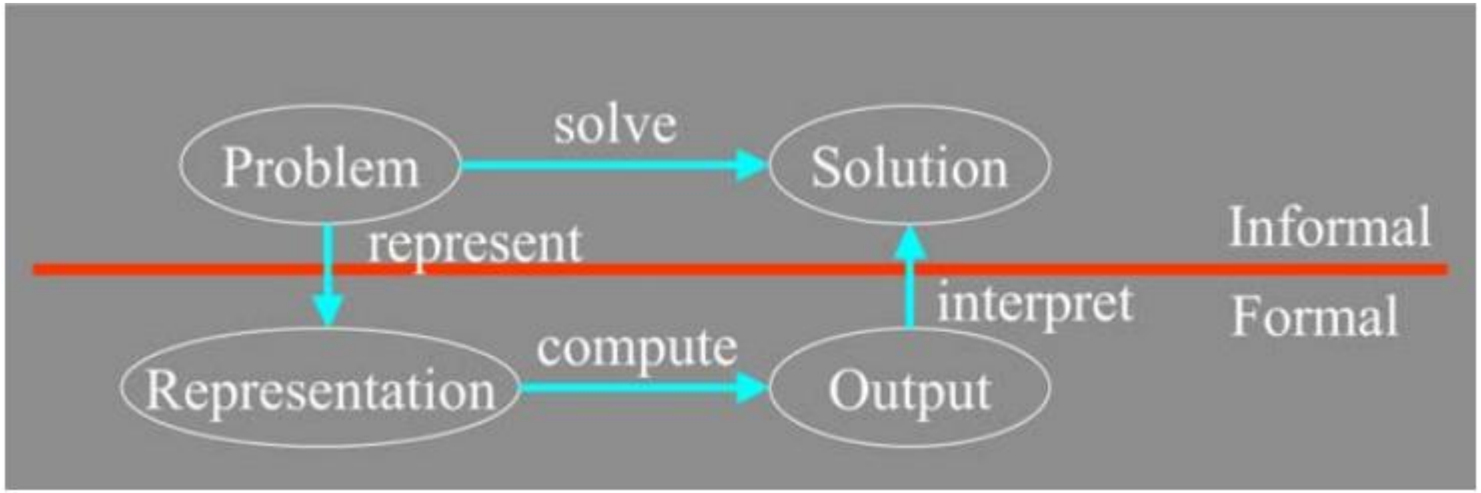


Figure 1-1. Problem Solving Framework

Graphical Languages in Formal Methods

- Formal methods can include graphical languages
- For example,

i. **Data Flow Diagrams** (DFDs) are the most well-known graphical technique for specifying the function of a system

   - DFDs can be considered a semi-formal method, and researchers have explored techniques for treating DFDs in a completely formal manner.

ii. **Petri nets** provide another well-known graphical technique, often used in distributed systems. Petri nets are a fully formal technique

iii. Another formal method is the **Finite state machines (FSM)**, which are commonly presented in tabular form

THANKS