Programming Theory

Advanced Level, 10 credits
Periods 1-2

Zafer Esen (zafer.esen@it.uu.se)
https://www.it.uu.se/katalog/zafes790

The course in a nutshell

- Course form: Lectures, tutorials, and labs. (Each part can be on-campus, online, or a combination thereof depending on the recommendations in effect at the time.)
- Mandatory Assignments: Home and lab assignments that all participants have to complete before hard deadlines.
- Quizzes: There will be quizzes at the beginning of some lectures where you will have the opportunity to earn bonus points for the final exam.
- Examination: Final written exam.
- Grade: To get the 10 credits of this course you must:
  - Pass the mandatory assignment, and
  - Get 50 out from 100 in the final exam: $50 \leq 3$, $70 \leq 4$, and $85 \leq 5$.

Prerequisites

- Background in Programming and Programming Languages.
- Basic understanding in Mathematical Logic.
- Course in Program Semantics is useful.

Goal of this course

In this course we study how to:

- Write rigorous descriptions of implementations and specifications of programs.
- Verify programs, i.e., prove that the implementation of a program meets its specification using formal methods.
- Write a provably correct program from a given specification.

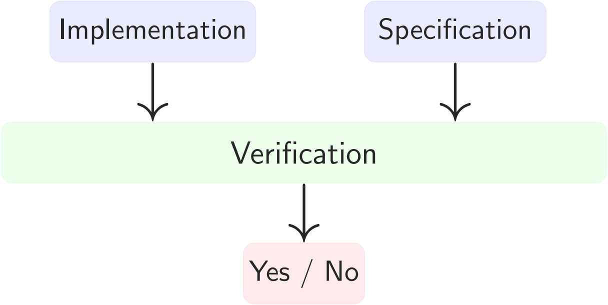
Checking Correctness - Testing

- Simulate/run the program for some input data.
- Check whether the output data is consistent with the specification.

Shortcomings

- Exhaustive testing is infeasible in practice.
- Testing can detect errors, but not prove their absence.

Checking Correctness - Formal Verification



Formal Verification

Given an implementation and a formal specification, the verification system answers yes/no:

- Yes: the program satisfies the specification (+ proof)
- No: the program is faulty (+ counterexample)

Software Bug: Space Disaster

- Ariane 5 Space mission
- $ 7, 000, 000, 000
- 10 Years in the making
- 40 seconds after take off the rocket exploded

Software Bug: Space Disaster

Attempt to cram a 64-floating point number to a 16-bit integer failed

Relevance

- Explore connections between mathematical logic and programming.
- Research area rich both in theory and practice.
- Industrial relevance: Widely used DO-178C and ISO26262 standards from the avionics and automative industries both recommend formal verification of safety critical systems to supplement testing. Formal methods used in Volvo, Ericsson, Bell Labs, Prover Technology, NASA, Microsoft, Airbus, . . .