Software Engineering

Formal approach for software quality

IDENTIFICATION

CODE :	IFA-4-S1-EC-AFQL
ECTS :	1.0

HOURS

Lectures :	10.0 h
Seminars :	8.0 h
Laboratory :	0.0 h
Project :	0.0 h
Teacher-student contact :	18.0 h
Personal work :	10.0 h
Total :	28.0 h

ASSESSMENT METHOD

DS

TEACHING AIDS

http://liris.cnrs.fr/pierre-edouard.portier/

TEACHING LANGUAGE

French

CONTACT

M. PROST Frederic
frederic.prost@insa-lyon.fr

AIMS

Targeted competence:
- enforce quality assurance and quality control through the derivation of programs correct by construction.

To do this, sub-competences are necessary:
- transform a natural language specification into a formal specification with the predicate calculus
- derive a correct program from its specification

This approach leads to a smart management of the complexity: checking the correction of a program is hard while deriving a program correct by construction splits the complexity in a sequence of simpler decisions.
After this module, one will be able to derive both sequential and concurrent programs correct by construction.

CONTENT

* Sequential Programs Correct by Construction
** Part 1, Theory
*** Predicate Calculus Reminder
*** Hoare Triples
*** Weakest Precondition
*** Guarded Command Language
** Part 2, Examples
*** Array subsequences (e.g., maximal AB subsequence, longest null subsequence, etc.)
*** Correct and efficient programs (e.g., integer division, fibonacci, etc.)
*** Sorting algorithms (Dutch National Flag, Quicksort, etc.)
* Concurrent Programs Correct by Construction
** Part 1, Theory
*** locally correct / globally correct
*** System invariant
*** Weakest liberal precondition
*** Atomicity
*** Progress
** Partie 2, Examples
*** Mutual Exclusion of Critical Sections
*** Safe Sluice
*** Peterson
*** Concurrent Linear Search
*** Election Algorithm
*** Alternating Bit Protocol

BIBLIOGRAPHY

* BACKHOUSE, 2002, Program Construction the Correct Way
* COHEN, 1990, Programming in the 1990s an Introduction to the Calculation of Programs
* DIJKSTRA, 1976, A Discipline of Programming
* GRIES, 1981, the Science of Programming
* KALDEWAIJ, 1990, Programming the Derivation of Algorithms
* KOURIE, WATSON, 2012, the Correctness by Construction Approach to Programming

PRE-REQUISITE

IFA-3-ALGO