Module II.3518

Formal Approaches

Pre-requisites: II.2408
Level: Advanced
Organization: 4 * 3h lecture/exercises, 3 * 3h lecture/lab
Assessment : Projects (40%), praticals (10%) and exam (50%)
ECTS : 2.5 credits

Overview

The conventional programming languages do not allow to claim that a program will be bug-free when it runs. Even the more sophisticated test techniques can let some defects pass through: a huge combinatory explosion happens when we mix the potential value of variables and the execution pathes, making it impossible to exhaustively consider them. Formal methods lead to a solution to this problem for a certain class of application. In particular, critical applications such as bank transactional systems, automatic piloting programs for rockets, airplanes of metro need for the use of methods able to mathematically prove that a program will run as expected.

Learning Objectives

Skills

Ensuring the safety and the reliability of applications intended to work inside critical systems. This unit initiates to the modelization of programs along upward of downward formal methods, with a degree of details adapted to the criticality of the system and its environment. The formal specification leads to a set of formal constraints, mechanically treated by tools strongly based on advanced mathematical and logical models. This process allows either to validate the program, or to point out the places where the code and the specifications differ.

Knowledge

Concepts

- Logical inference and proof-as-programs correspondence.
- Proof of program properties
- Typed programming languages, lambda-calcul
- Hoare logic
- Abstract interpretation
- Model-checking
- Logical, declarative, constraint programming languages
- Software testing
- Software certification

Know-how

- Specify and prove a program in a formal language
- Automatic program extraction from proofs
- PROLOG programming

Teaching method

The unit will be divided in 4 weeks of lecture and tutorials, used to introduce fundamental concepts. They will be followed by 3 weeks of lecture and practical lab sessions, that will give a concrete approach to the topic. One or two projects will be proposed during the unit.

Bibliography

- http://en.wikipedia.org/wiki/Model_checking
- http://www.liafa.jussieu.fr/~hf/verif/ens/cours/licence02/tout/node24.html
- http://caml.inria.fr/
- http://coq.inria.fr/ and http://coq.inria.fr/what-is-coq
- http://en.wikipedia.org/wiki/PROLOG