Program Logics

MAP-i – Proposal for the *Theory and Foundations* block, 2022-23

1 Context and Objectives

This document describes a proposal for a course on *Theory and Foundations* block to be offered in the 2022-23 MAP-i edition. The proposal is supported by a team from Aveiro University (Dep. of Mathematics) and Minho University (Dep. of Informatics).

The adoption of formal logics to modelling, design, implement and verify software is currently a well established practice. This course intends to make an overview on the topic, from the classic frameworks to imperative programs – Hoare and Dynamic Logics, to its current variants, prepared to aid the development of other less conventional computational domains as weighted, hybrid and quantum computations. The theoretical presentation of the topics will be enriched witha a tools support component.

The course builds on the team previous research on program semantics and logics in software development, the latter object of the following research projects that have been (or currently are) coordinated by the proponents:

- NASONI (`PTDC/EEI-CTP/2341/2012`) on *Heterogenous software coordination: Foundations, methods, tools.*
- DALÍ (`POCI-01-0145-FEDER-016692`) on *Dynamic Logics for cyber-physical systems.*
- KLEE (`POCI-01-0145-FEDER-030947`) on *Coalgebraic Modeling and Analysis for Computational Synthetic Biology.*
- AVIACC (`PTDC/EIA-CCO/117590/2010`) on *Logic-based Analysis and Verification of Critical Concurrent Programs.*

2 Learning outcomes

- Take contact with formal logic, with a special focus in modal and dynamic logic.
- Take contact with the foundations of software verification, including Floyd-Hoare deductive verification and the corresponding bridge with dynamic logic
- To learn the principles of the formal verification of software
- Take contact with some computational tools to aid the formal specification and verification of software, including SMT solvers and other platforms for deductive proofs

3 Pre-requisites

The course is almost self-contained, assuming only familiarity with elementary discrete mathematics at MSc level.

4 Format

Tutorial module.

5 Grading

Assessment is based on an individual report on a research topic, and a small programming exercise in `Why3`.

6 Course Contents

M1-Introdution to formal logic (Manuel A. Martins)

- Propositional Logic – Syntax and Semantics, Formal deducibility, Completeness.
- First-Order Logic – Syntax and Semantics, Logical Consequence, Formal deducibility, Completeness.
- Modal Logic – Syntax, Kripke Semantics, Decidability, Completeness.

M2-Principles of SMT solving (Maria J. Frade)

- Overview of SMT solving technologies
- SMT solvers: logics and theories, pragmatic features, and encoding problems

M3-Logics for verification of classic programs (Alexandre Madeira)

- Preliminaries – programs relational semantics and the Kleene Algebra of programs
- Propositional Dynamic Logic
- Equational Dynamic Logic
- Introduction to axiomatic verification of programs – Floyd-Hoare Logic and Dijkstra transformations

M4-Tools support (Jorge S. Pinto)

- Introduction to the logic and program verification levels of the Why3 tool:
  - The logic language and the WhyML programming language
  - The Why3 IDE; prover interfacing and proof transformations; inductive proofs
- Program development and specification based on contracts
- Verification of functional and imperative programs with Why3

M5-Advanced topics

- Quantum dynamic logics (Luis S. Barbosa)
- Logics for Hybrid Systems (Renato Neves)
- Principles of SMT solving (Maria J. Frade)

7 Bibliography

M1 - Introdution to formal logic [Bur98, Gol87]

M2 - Principles of SMT solving [BHvMW09, BM07]

M3 - Logics for the verification of standard programs: [HKT00, AFPdS11, Dij76]

M4 - Tools support: [AFPdS11, FP13]

8 Team

Alexandre Madeira (**coordinator**) is Assistant Professor at Department of Mathematics of Aveiro University and a researcher at CIDMA. He was a former MAP-i doctoral student. His PhD thesis on hybrid logic and software reconfiguration was later awarded the IBM Scientific Prize for 13. He coordinated an FCT project, and he has published more than thirty papers in several journals and conferences over the past 5 years.
Selected relevant publications: [MNBM16, MBHM18, HMW18].

Manuel António Martins is Associated Professor of Mathematics Department of University of Aveiro, , and a researcher at the Center for Research and Development in Mathematics and Applications (CIDMA). His research interests are related to Abstract Algebraic Logic, Modal Logic and Formal Methods. Namely, in what concerns the theoretical study of extensions of modal logics, over different paradigms such as fuzzy and paraconsistent ones, worth to reasoning about specific kinds of software systems. He participated in FCT-projects in themes related to the contents of this course. Currently, he is Co-PI of the Klee project, a project that aims to apply cyber-physical techniques to biological systems. He has published more than 25 papers in international journals and several in reviewed proceedings of relevant conferences in Computer Science. He has supervised 1 post-doc, 4 PhD and 10 MSc thesis.
Selected relevant publications: [CM17, BMMH19, MMH19, CFM20].

Maria João Frade is Assistant Professor of Informatics Department of University of Minho, and a member of the High Assurance Software Laboratory (HASLab) of INESC TEC. She received the PhD degree in computer science in 2004 from the University of Minho. In the past she worked on type theory, structural proof theory and type-systematic description of program analyses. In the last years her work focused on deductive program verification. She is one of the authors of a textbook in this area and published several papers in conferences and journals. *Selected relevant publications*: [LFP16a, FP11, AFPdS11].

Jorge Sousa Pinto is an Associate Professor at the Informatics Department of the University of Minho. He obtained his degree of Docteur de L'Ecole Polytechnique (Paris) in 2001 and his Habilitation from the University of Minho in 2015. In the past he has worked on linear logic and functional programming; more recently his work focused on deductive program verification. He is one of the authors of the textbook "Rigorous Software Development: an Introduction to Program Verification". He is currently the director of the MAP-i doctoral programme.
Selected relevant publications: [LFP16b, eSAB$^+$16, dMPPPP18].

Selected relevant publications: [GMB17, GMB19, GMJB19].

References

[AFPdS11] José Bacelar Almeida, Maria João Frade, Jorge Sousa Pinto, and Simão Melo de Sousa. *Rigorous Software Development - An Introduction to Program Verification*. Undergraduate Topics in Computer Science. Springer, 2011.

[BHvMW09] Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors. *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, 2009.

[BM07] Aaron R. Bradley and Zohar Manna. *The calculus of computation - decision procedures with applications to verification*. Springer, 2007.

[BMMH19] Patrick Blackburn, Manuel A. Martins, María Manzano, and Antonia Huertas. Rigid first-order hybrid logic. In Rosalie Iemhoff, Michael Moortgat, and Ruy J. G. B. de Queiroz, editors, *Logic, Language, Information, and Computation - 26th International Workshop, WoLLIC 2019, Utrecht, The Netherlands, July 2-5, 2019, Proceedings*, volume 11541 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2019.

[Bur98] Stanley N. Burris. *Logic for mathematics and computer science.* Upper Saddle River, NJ: Prentice Hall, 1998.

[CFM20] Madalena Chaves, Daniel Figueiredo, and Manuel A. Martins. Boolean dynamics revisited through feedback interconnections. *Nat. Comput.*, 19(1):29–49, 2020.

[CM17] Diana Costa and Manuel A. Martins. Paraconsistency in hybrid logic. *J. Log. Comput.*, 27(6):1825–1852, 2017.

[Dij76] Edsger W. Dijkstra. *A Discipline of Programming.* Prentice-Hall, 1976.

[dMPPPP18] André de Matos Pedro, Jorge Sousa Pinto, David Pereira, and Luís Miguel Pinho. Runtime verification of autopilot systems using a fragment of MTL-$\int$. *International Journal on Software Tools for Technology Transfer (STTT)*, 20(4):379–395, 2018.

[eSAB+16] Rovedy Aparecida Busquim e Silva, Nanci Naomi Arai, Luciana Akemi Burgareli, José Maria Parente de Oliveira, and Jorge Sousa Pinto. Formal verification with Frama-C: A case study in the space software domain. *IEEE Trans. Reliability*, 65(3):1163–1179, 2016.

[FP11] Maria João Frade and Jorge Sousa Pinto. Verification conditions for source-level imperative programs. *Computer Science Review*, 5(3):252–277, 2011.

[FP13] Jean-Christophe Filliâtre and Andrei Paskevich. Why3 - where programs meet provers. In *22nd European Symposium on Programming, ESOP 2013*, pages 125–128, 2013.

[GMB17] Leandro Gomes, Alexandre Madeira, and Luís Soares Barbosa. On Kleene algebras for weighted computation. In Simone André da Costa Cavalheiro and José Luiz Fiadeiro, editors, *Formal Methods: Foundations and Applications, Brazilian Symposium on Formal Methods SBMF 2017, Recife, Brazil, Proceedings*, volume 10623 of *Lecture Notes in Computer Science*, pages 271–286. Springer, Cham, 2017.

[GMB19] Leandro Gomes, Alexandre Madeira, and Luís Soares Barbosa. Generalising KAT to verify weighted computations. *Scientific Annals of Computer Science*, 29(2):141–184, 2019.

[GMJB19] Leandro Gomes, Alexandre Madeira, Manisha Jain, and Luís Soares Barbosa. On the generation of equational dynamic logics for weighted imperative programs. In Yamine Aït Ameur and Shengchao Qin, editors, *Formal Methods and Software Engineering - International Conference on Formal Engineering Methods, ICFEM 2019, Shenzhen, China, 2019, Proceedings*, volume 11852 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2019.

[Gol87] Robert Goldblatt. *Logics of time and computation.*, volume 7. CSLI Publications, Stanford, CA, 1987.

[HKT00] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[HMW18] Rolf Hennicker, Alexandre Madeira, and Martin Wirsing. Behavioural and abstractor specifications revisited. *Theor. Comput. Sci.*, 741:32–43, 2018.

[LFP16a] Cláudio Belo Lourenço, Maria João Frade, and Jorge Sousa Pinto. Formalizing single-assignment program verification: An adaptation-complete approach. In Peter Thiemann, editor, *Programming Languages and Systems - 25th European Symposium on Programming, ESOP 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*, volume 9632 of *Lecture Notes in Computer Science*, pages 41–67. Springer, 2016.

[LFP16b] Cláudio Belo Lourenço, Maria João Frade, and Jorge Sousa Pinto. Formalizing single-assignment program verification: an adaptation-complete approach. In Peter Thiemann, editor, *Proceedings of the 25th European Symposium on Programming (ESOP 2016)*, volume 9632 of *Lecture Notes in Computer Science*, pages 41–67, Berlin, Heidelberg, 2016. Springer-Verlag.

[MBHM18] Alexandre Madeira, Luís Soares Barbosa, Rolf Hennicker, and Manuel A. Martins. A logic for the stepwise development of reactive systems. *Theor. Comput. Sci.*, 744:78–96, 2018.

[MMH19] María Manzano, Manuel A. Martins, and Antonia Huertas. Completeness in equational hybrid propositional type theory. *Studia Logica*, 107(6):1159–1198, 2019.

[MNBM16] Alexandre Madeira, Renato Neves, Luís Soares Barbosa, and Manuel A. Martins. A method for rigorous design of reconfigurable systems. *Sci. Comput. Program.*, 132:50–76, 2016.

[MNM16] Alexandre Madeira, Renato Neves, and Manuel A. Martins. An exercise on the generation of many-valued dynamic logics. *Journal of Logical and Algebraic Methods in Programming*, 85(5):1011–1037, 2016.

[NW05] Hung T. Nguyen and Elbert A. Walker. *A first course in fuzzy logic (3. ed.)*. Chapman&Hall/CRC Press, 2005.

[Zad65] L.A. Zadeh. Fuzzy sets. *Information and Control*, 8(3):338 – 353, 1965.