Software Fondations

MAP-i – Proposal for the *Theory and Foundations* block, 2024-25

1 Context and Objectives

This document describes a proposal for a course on *Software Foundations* block to be offered in the 2023-24 MAP-i edition. The proposal is supported by a team from Aveiro University (Dep. of Mathematics) and Minho University (Dep. of Informatics).

The study and development of strong foundations for Software Engineering is a core aspect to support the development process of quality and safe complex systems.

On this view, computer science have been introduced a number of mathematical theories devoted to giving rigorous semantics to programs and their languages, as well as to calculus to express and verify their properties. This course makes an overview on three core pillars of such building, organized in the following modules:

M1 Foundations of Functional Programming

M2 Foundation of Imperative Programming

M3 Program Logics

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 λ-calculi
- Take contact with formal semantics of programs
- 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

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 within the course scope.

6 Course Contents

M1 - Foundations of Functional Programming (Sandra Alves and Mário Florido)

- Lambda calculus: syntax; reductions; normal forms.
- Extensions: let expressions; conditionals; integers.
- Simple Typed Lambda calculus: types; type inference.

M2 - Foundations of Imperative Programming (J.S. Pinto and M.J. Frade)

- Operational semantics: transition (small-step) and evaluation (big-step) semantics
- Other semantic frameworks: denotational and axiomatic
- Introduction to program verification: program annotations and verification condition generation; auto-active program verifiers

M3 - Program Logics (Alexandre Madeira and Manuel Martins)

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

7 Team

Sandra Alves is an Assistant Professor at the Faculty of Sciences of the Univerisity of Porto. Her main reserch activity is in the areas of quantitative type systems, substructural type systems and access control. *Selected relevant publications*: [AF22, AV22, AFFM10].

Mário Florido is an Associate Professor at the Faculty of Sciences of the Universty of Porto. His main research areas are substructural type systems (linear and ordered types), gradual typing and automated theorem proving. *Selected relevant publications*: [AF22, SVFJH12, FD04].

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].

Alexandre Madeira (**coordinator**) is Associate 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 2013. 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 Associate 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. He was Co-PI of the Klee project, a project that aims to apply cyber-physical techniques to biological systems. He has published more than 35 papers in international journals and several in reviewed proceedings of relevant conferences in Computer Science. He has supervised 1 post-doc, 4 PhD and several MSc thesis.
Selected relevant publications: [CM17, BMMH19, MMH19, CFM20, CSMF23, BMMH23, FM24].

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, SABOP16, PPPP18].

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.

[AFFM10] Sandra Alves, Maribel Fernández, Mário Florido, Ian Mackie. Gödel's system tau revisited. *TCS*, 2010.

[AF22] Sandra Alves, Mário Florido. Structural Rules and Algebraic Properties of Intersection Types. *ICTAC*, 2022.

[AV22] Sandra Alves, Daniel Ventura. Quantitative Weak Linearisation. *ICTAC*, 2022.

[B85] Hendrik Pieter Barendregt. The lambda calculus - its syntax and semantics. *Studies in logic and the foundations of mathematics*, 1985.

[BDS13] Hendrik Pieter Barendregt, Wil Dekkers, Richard Statman. Lambda Calculus with Types. *Perspectives in logic, Cambridge University Press*, 2013.

[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.

[BMMH23] Patrick Blackburn, Manuel A. Martins, María Manzano, Antonia Huertas. Exorcising the phantom zone. *Inf. Comput.*, 287: 104754, 2023

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

[CSMF23] Suene Campos, Regivan H. N. Santiago, Manuel A. Martins, Daniel Figueiredo. Aggregation-based operations for reversal fuzzy switch graphs. *Fuzzy Sets Syst.*, 466: 108273, 2023.

[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.

[FD04] Mário Florido, Luís Damas. Linearization of the lambda-calculus and its relation with intersection type systems. *Journal of Functional Programming*, 2004.

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

[FM24] Alfredo R. Freire and Manuel A. Martins. Modality Across Different Logics. *Logic Journal of the IGPL*, DOI: https://doi.org/10.1093/jigpal/jzae082

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

[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.

[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.

[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.

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

[NN07] Hanne Riis Nielson and Flemming Nielson. *Semantics with Applications: An Appetizer.* Undergraduate Topics in Computer Science. Springer, 2007.

[PPPP18] 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.

[Rey98] John C. Reynolds. *Theories of programming languages*. Cambridge University Press, 1998.

[SABOP16] 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.

[SVFJH12] Hugo R. Simões, Pedro B. Vasconcelos, Mário Florido, Steffen Jost, Kevin Hammond. Automatic amortised analysis of dynamic memory allocation for lazy functional programs. *ICFP*, 2012.