Quantum Computing

MAP-i – Proposal for the *Theory and Foundations* block, 2018-19

Summary

This document describes a proposal for a course on Theory and Foundations *to be offered in the 2018-19 MAP-i edition. The proposal is supported by a team from Aveiro University (Dep. of Mathematics) and Minho University (Dep. of Informatics).*

1 Context and Objectives

Arguably quantum computing is coming of age. With the race for quantum rising between major IT players (e.g. IBM, Intel, Google, Microsoft), and the announcement of prototype-machines up to 50 qubits until the end of the current year, it seems we are in the verge of a real shift. For the first time the viability of quantum computing may be demonstrated in a number of real problems extremely difficult to handle, if possible at all, classically, and its utility discussed across industries. In a sense, Feynman's dream of letting Nature, suitably engineered, compute for us through its own natural quantum behaviour, seems to be closer, even if the project of a universal quantum computer has still a long way to go. In the somehow emphatic language of the media, a 'second quantum revolution' is quickly approaching. It is characterised by the ability to harness the most weird quantum phenomena, namely *superposition* and *entanglement*, as computational resources, with practical advantage[1].

Putting Europe at the forefront of this move was the aim of the *Flagship Initiative on Quantum Technologies* launched by the European Commission with a 10 year timespan and an estimated budget over one billion euros. It followed the *Quantum Manifesto* [25] published in May 2016 and subsequently endorsed by over 3 000 leading scientists and decision makers.

In such a context, this course introduces, at a doctoral programme level, the foundations of quantum computing, as well as a number of specialised topics on the forefront of research on quantum program's design and verification.

The focus on the later has a clear motivation. The set of primitive techniques in quantum algorithmics increased over the past decade, exploring quantum effects in a number of unsuspected ways. But still quantum programming is hard, finding new and effective quantum algorithms is far from straightforward, some useful metaphors may still lack. Moreover, most current quantum algorithms assume an ideal quantum computer with many qubits that can hold information indefinitely. We are not yet there. In the short term, the challenge is to find real-world problems and applications that can benefit from the small, 'noisy' quantum computers that will soon be available. The spectrum of applications is vast, from cryptography and optimisation, to machine learning, computer graphics, or simulation of quantum-mechanical systems that are too complex to handle with classical computers.

Quantum computing is emerging within the Universities joined together in the MAP-i consortium as a new area of research and advanced training. Last June, 5th, 2018, the University of Minho and its partners at QuantaLab (`www.quantalab.org`), became part of the IBM Q network, with full access to a 20 to 50 qubit machine, to be used for developing use cases on testing the 'quantum advantage' on industrial applications.

[1] In the same language, the 'first revolution' focused on the microscopic level and brought up what are now familiar, but then highly disruptive, technologies, e.g. transistors, lasers, and GPS.

The course builds on the team previous research on algebraic and categorical methods in (classical) in software development, object of four research projects that have been (or currently are) coordinated by the proponents:

- QAIS (PTDC/EIA-CCO/122240/2010) on *Quantitative analysis of interacting systems: Foundations and algorithms.*
- 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: Towards contract based design.*

and the recently approved

- KLEE (FCT 2017 call - 030947) on *Coalgebraic Modeling and Analysis for Computational Synthetic Biology.*

Although none of them is directly addressing quantum computing, the techniques developed are being tuned to deal with the quantum case as well. In particular, a on-going PhD project on dynamic logic for verification of quantum systems is currently being developed in the context of the DALÍ project.

2 Learning outcomes

- Familiarity with the main topics, research questions and scientific challenges in the area of quantum computing:
- ability to apply them to build and reason about, abstract models for quantum programming languages and algorithms;
- ability to model and program simple quantum algorithms in QISKIT;
- ability to extract information from scientific papers and summarise them;
- enhanced technical writing and presentation skills.

3 Pre-requisites

The course is almost self-contained, assuming only familiarity with elementary linear algebra, logic, and algebraic structures at MSc level.

4 Format

Tutorial module.

5 Grading

Assessment is based on an individual report about a research paper and its presentation and discussion to the class, and a small programming exercise in a quantum programming language (typically QISKIT).

6 Course Contents

M1 - A Primer on Quantum Computing.

Aims This module aims at introducing quantum computing in an interdisciplinary way, blending physics and computer science from first principles. It provides an overview of basic quantum mechanics, including finite dimensional Hilbert spaces and their tensor products, quantum entanglement, its structure and physical consequences. The module introduces qubits, the interplay between state, transformation and observation.

The approach taken deviates from more conventional introductions, adopting the diagrammatic reasoning proposed by Coecke and Abramsky, also known as *quantum picturialism* [4], introducing string diagrams and quantum processes up to a detailed discussion of the teleportation protocol.

Syllabus Quantum mechanics as a computational theory. Notion of qubit. Overview of basic concepts: why do linear algebra and complex vector spaces matter? Processes, circuits and diagrams. Introduction to the graphical zx-calculus: Tensor product as parallel composition. String diagrams: states, effects, scalars, transposition and trace. Quantum processes. Example: the teleportation protocol.

Bibliography A light, well-structured introduction to Quantum mechanics: [9]; Introduction to quantum computing with accessible review of mathematical background: [26]; 'Quantum picturialism': [4].

M2 - Quantum Algorithms' Laboratory.

Aims Quantum algorithms are introduced as strategies for harnessing quantum effects to yield efficient computational systems.Those include *superposition* (objects placed in different states at the same time) and *entanglement* (objects deeply correlated without any direct physical interaction). Algorithms are also regarded as responses to computational problems classically too hard to solve. Shor's algorithm to factor large integers into primes, proposed in 1994, provides a first example. The module introduces other quantum algorithms systematically. Its laboratorial component, based on the IBM Q Experience platform and Qiskit, a scripting language and open source development kit, aims at providing a hands-on experience in programming by composition of quantum gates.

Syllabus The circuit model and quantum gates. Deutsh-Jozsa algorithm. Quantum Fourier transform. Shor and Grover algorithms; variants. Quantum simulation. Development in Qiskit.

Bibliography [26, 23, 27]. IBM Quantum Experience and Qiskit tutorials.

M3 - Quantum Logics.

Aims This advanced module addresses the construction, semantics and application of logics for quantum phenomena and computations. Two topics will be considered:

- **Logics for quantum mechanics.** Right after the mathematical formalization of quantum mechanics, some first attempts on the definition of formal logics to reason about quantum systems were proposed. Actually, the 'unconventional behaviour' of quantum measurements shows that Boolean algebra, which underlies semantic principles in classical logic, is not adequate to reason about quantum phenomena. The work [3] by Birkhoff and von Neumann adopts another lattice, the orthomodular lattice, for this end. This resulted into a suitable logic to reason about properties of quantum systems based on sentences (or propositions) which

refer to a closed linear subspace of the given Hilbert space. This work opened a line of research in non-classical logic that stills raising the interest of the computer science and logic communities.

- **Logics for the verification of quantum algorithms.** The advent of Quantum Computing motivated the study of program logics able to respond to new verification challenges within a completely new paradigm. One of such research avenues is due to Alexandru Baltag and Sonja Smets: Quantum Dynamic Logic [1] studies a number of variants of dynamic logics for quantum systems. This generalises the standard formalism for the verification of classic imperative programs, the (classic) Dynamic Logic [7], with new constructions and semantics for the verification of quantum algorithms.

Syllabus Ortholattices and frames; orthologic orthomodular. Quantum logic properties of Hilbert lattices. Quantum dynamic logic; quantum dynamic frames; logic of quantum programs. Case study: Quantum teleportation protocol in LQP.

Bibliography Quantum logics: [6, 3, 1]. General reference on dynamic logic: [7]

7 Team

Manuel António Martins is Associate Professor at the Department of Mathematics of Aveiro University, and a researcher at the Center for Research and Development in Mathematics and Applications. His research interests are related to Abstract Algebraic Logic and Modal Logic. 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 has published more than 20 papers in international journals. He has supervised 1 post-doc, 2 PhD and 8 MSc thesis (1 in the area of the current proposal) and is currently supervising 2 PhD projects. *Selected relevant publications*: [14, 20, 15, 16, 18, 17]

Alexandre Madeira is a post-doc researcher at HASLab INESC TEC, currently coordinating a FCT-funded research project on dynamic logic and contract-based programming. He was a former MAP-i doctoral student. His PhD thesis [10] on hybrid logic and software reconfiguration was later awarded the IBM Scientific Prize for 2013. He has published more than twenty papers in several journals and conferences over the past 5 years. *Selected relevant publications*: [11, 8, 13, 12, 5].

Luís Soares Barbosa is Associate Professor at the Department of Informatics of Minho University, senior researcher at the High Assurance Software Laboratory (HASLab) of INESC TEC. His research focuses on program semantics, logics and calculi applied to rigorous software analysis, design, and construction. He is particularly interested in the architectural dimension (interaction, composition, and reconfiguration) of different sorts of software components, namely non deterministic, probabilisitic, continuous, or hybrid). More recently he became interested in exploring connections between Physics and Computation at two levels: the discrete-continuous frontier and the classic-quantum interaction. In this context, he is currently serving as Director of the MSc Degree on Physics Engineering and Coordinator of the Q Hub at QuantaLab. On this topic he has published over the past 4 years more than 15 papers in several journals and conferences. He has supervised 7 PhD thesis and is currently supervising 5 PhD projects (one in quantum algorithmics and logic). He is a member of IFIP WG 1.3 (Foundations of System Specification). *Selected relevant publications*: [2, 22, 21, 24, 19].

References

[1] A. Baltag and S. Smets. Lqp: the dynamic logic of quantum information. *Mathematical Structures in Computer Science*, 16(3):491525, 2006.

[2] Luís Soares Barbosa and Alexandre Madeira. A research agenda on quantum algoritmics. *ERCIM News*, 2018(113), 2018.

[3] G Birkhoff and J Von Neumann. The logic of quantum mechanics. *Annals of mathematics*, 37(4):823, 1936.

[4] B. Coecke and A. Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.

[5] Razvan Diaconescu and Alexandre Madeira. Encoding hybridized institutions into first-order logic. *Mathematical Structures in Computer Science*, 26(5):745–788, 2016.

[6] Kurt Engesser, Dov M Gabbay, and Daniel Lehmann. *Handbook of Quantum Logic and Quantum Structures*. Quantum Logics. Elsevier, Agosto 2011.

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

[8] Rolf Hennicker, Alexandre Madeira, and Martin Wirsing. Behavioural and abstractor specifications revisited. *Theoretical Computer Science*, 2018.

[9] P. Kok. *A First Course in Quantum Mechanics*. (electronic edition only; available from AppleStore, 2014.

[10] A. Madeira. *Foundations and techniques for software reconfigurability*. PhD thesis, Universidades do Minho, Aveiro and Porto (Joint MAP-i Doctoral Programme), July 2013.

[11] Alexandre Madeira, Luis S. Barbosa, Rolf Hennicker, and Manuel A. Martins. A logic for the stepwise development of reactive systems. *Theoretical Computer Science (in print)*, 2018.

[12] 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.

[13] Alexandre Madeira, Renato Neves, and Manuel A. Martins. An exercise on the generation of many-valued dynamic logics. *J. Log. Algebr. Meth. Program.*, 85(5):1011–1037, 2016.

[14] M. A. Martins. Behavioral institutions and refinements in generalized hidden logics. *Journal of Universal Computer Science*, 12(8):1020–1049, 2006.

[15] M. A. Martins. Closure properties for the class of behavioral models. *Theor. Comput. Sci.*, 379(1-2):53–83, 2007.

[16] M. A. Martins. On the behavioral equivalence between k-data structures. *Comp. J.*, 50(3):181–191, 2008.

[17] M. A. Martins, A. Madeira, and L. S. Barbosa. Refinement by interpretation. In Dang Van Hung and Padmanabhan Krishnan, editors, *7th IEEE International Conference on Software Engineering and Formal Methods (SEFM'09)*, pages 250–259. IEEE Computer Society Press, 2009.

[18] M. A. Martins, A. Madeira, and L. S. Barbosa. Refinement by interpretation in a general setting. In J. Derrick E. Boiten and S. Reeves, editors, *Proc. Refinement Workshop 2009, Electr. Notes Theor. Comput. Sci. (256)*, pages 105–121. Elsevier, 2009.

[19] M. A. Martins, A. Madeira, and L. S. Barbosa. A coalgebraic perspective on logical interpretations. *Studia Logica*, 101(4):783–825, 2013.

[20] M. A. Martins and D. Pigozzi. Behavioural reasoning for conditional equations. *Math. Struct. Comput. Sci.*, 17(5):1075–1113, 2007.

[21] R. Neves and L. S Barbosa. Hybrid automata as coalgebras. In Augusto Sampaio and Farn Wang, editors, *Theoretical Aspects of Computing - ICTAC 2016 - 13th International Colloquium, Taiwan, Proceedings*, pages 385–402. Springer Lect. Notes Comp. Sci. (9965), 2016.

[22] R. Neves, L. S. Barbosa, D. Hofmann, and M. A. Martins. Continuity as a computational effect. *J. Log. Algebr. Meth. Program.*, 85(5):1057–1085, 2016.

[23] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary Edition)*. Cambridge University Press, 2010.

[24] N. Oliveira and L. S. Barbosa. Reasoning about software reconfigurations: The behavioural and structural perspectives. *Sci. Comput. Program.*, 110:78–103, 2015.

[25] QUROPE – Quantum Information Processing and Communication in Europe. *Quantum Manifesto: A new era of technology*. Available from `qurope.eu`, 2016.

[26] N. S. Yanofsky and M. A. Mannucc. *Quantum Computing for Computer Scientists*. Cambridge University Press, 2008.

[27] M. Ying. *Foundations of Quantum Programming*. Elsevier, 2016.