Quantum Computing

MAP-i – Proposal for the *Computing Paradigms* block, 2021-22

Summary

This document describes a proposal for a course on Computing Paradigms *to be offered in the 2021-22 MAP-i edition. The proposal is supported by a team from University of Aveiro (Dep. of Mathematics) and University of Minho (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, it seems that 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 of over one billion euros. It followed the *Quantum Manifesto* [24] 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 software engineering. The focus on the latter 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 there yet. 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. In 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.

The course builds on the team previous research on quantum computing, program semantics and logic in (classical) software development, the latter is object of three research projects that have been (or currently are) coordinated by the proponents:

[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.

- 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*
- KLEE (POCI-01-0145-FEDER-030947) on *Coalgebraic Modeling and Analysis for Computational Synthetic Biology.*

Although none of them directly addresses quantum computing, the techniques developed are being tuned to deal with the quantum case as well. In particular, an on-going PhD project on dynamic logic for verification of quantum systems is currently being developed in the context of the DALÍ project. A number of MSc dissertations exploring aspects of quantum computing are being prepared in the context of the KLEE project. A PhD project on programming languages for noisy quantum computers is also being explored in the context of the KLEE project.

2 Learning outcomes

- To master the principles and main techniques of quantum information and computation;
- To systematically design and analyse quantum algorithms, as well as implement and run them in the Qiskit open-source software development kit;
- To understand the essential elements of quantum programming languages, their current implementations, and associated dynamic logics.

3 Pre-requisites

The course is almost self-contained, assuming only familiarity with elementary linear algebra at the 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 a quantum programming language (typically QISKIT).

6 Course Contents

M1 - Introduction to Quantum Information and Computation.

- Quantum effects as computational resources: superposition, interference, entanglement.
- Mathematical background: (finite dimensional) Hilbert spaces.
- Notion of qubit. Structuring quantum data. Quantum information principles. Illustrations: the teleportation and superdense coding protocols.

M2 - Quantum Gates and Circuits.

- Unitary transformations and quantum gates.
- Measurement.

- The circuit model.

M3 - Quantum Algorithms.

- Design of quantum algorithms. Case study: the Deutcsh-Jozsa algorithm.
- Quantum search: Grover algorithm and variants.
- Quantum Fourier transform.
- Shor's algorithm.

M4 - Laboratory. Hands-on introduction to quantum programming based on the IBM Q Experience platform and Qiskit, a scripting language and open source development kit. This module aims at consolidating through laboratorial practice the concepts and methods introduced in modules M1 to M3.

M5 - Computability and Complexity.

- Classical, probabilistic and quantum Turing machines.
- Main complexity classes for classical, probabilistic and quantum computation.

M6 - Quantum λ-calculus.

- The classical λ-calculus.
- Variants of the quantum λ-calculus.

M7 - Error-correcting codes.

- Models of communication.
- Classical error correcting codes.
- Error correcting codes for quantum communication systems.
- Some examples of error correcting codes for quantum communications systems.

M8 - Logics for quantum programs.

- Programs, modalities, and properties – the ingredients of dynamic logic.
- Quantum dynamic logics.
- Reasoning about quantum programs in a quantum dynamic logic.

7 Bibliography

M1 - Quantum Information & Computation: [20, 26, 25]

M2 - The Circuit Model: [20, 26, 25]

M3 - Quantum Algorithms: [16, 27, 28]

M5 - Computability and Complexity: [2, 23, 27]

M6 - Quantum λ-calculus: [13, 14, 22]

M7 - Error-correcting codes: [12, 9, 1]

M8 - Logics for quantum programs: [28, 4, 5]

8 Team

Renato Neves (**coordinator**) is an Auxiliar Professor at the Department of Informatics, University of Minho and a researcher at INESC-TEC. His research topics incide on program semantics and program verification in the setting of cyber-physical and quantum computing. Among other things, he is currently supervising a PhD student on the topic of programming languages for noisy quantum computers and supervised a PhD student on observational equivalences for quantum systems.

He coauthored more than 20 scientific papers, and three successful scientific proposals (totalling around 550k euros in financial support) – the proposals aim at lifting programming theory to noise/imprecise computational systems (the quantum case being of course a prime example). He participated in several scientific program committees, and is supervising/supervised one postdoc, two PhD theses, and four MSc theses.

Selected relevant publications: [19, 18, 11, 10, 8].

Luís Soares Barbosa is a Full Professor at the Department of Informatics of Minho University, and senior researcher at HasLab INESC TEC. He coordinates the *Quantum Software Engineering* group at INL (International Iberian Nanotechnology Laboratory) and is responsible for the IBM Q Hub at QuantaLab, a research laboratory on Quantum Materials and Quantum Technologies. Luís holds a second academic affiliation to the United Nations University, currently serving as Deputy Director of its Operational Unit on digital governance. He has (co-)supervised 10 PhD thesis. Member of IFIP WG 1.3 (Foundations of System Specification) since 2014, Luís was appointed in January 2019 Chair of IFIP TC1 on *Foundations of Computer Science*.
Selected relevant publications: [6, 19, 18, 21, 15].

Raquel Pinto is an Assistant Professor at the Department of Mathematics at the University of Aveiro. Her research interests are in the field of coding theory with particular interest on convolutional coding and systems theory, namely the behavioral approach to systems theory. She has (co-)supervised 3 PhD thesis and she is currently supervising 2 PhD thesis. Member of the Management Committee of the ICT COST Action IC1104, 2012-16 (national manager)
Selected relevant publications: [7, 3, 17].

References

[1] *Quantum Error Correction*. Cambridge University Press, 2013.

[2] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[3] Diego Napp Avelli, Raquel Pinto, and Vladimir Sidorenko. Concatenation of convolutional codes and rank metric codes for multi-shot network coding. *Des. Codes Cryptography*, 86(2):303–318, 2018.

[4] A. Baltag and S. Smets. Quantum logic as a dynamic logic. *Synthese*, 179(2):285–306, 2011.

[5] A. Baltag and S. Smets. The dynamic turn in quantum logic. *Synthese*, 186(3):753–773, 2012.

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

[7] Joan-Josep Climent, Diego Napp, Carmen Perea, and Raquel Pinto. Maximum distance separable 2d convolutional codes. *IEEE Trans. Information Theory*, 62(2):669–680, 2016.

[8] Vıtor Fernandes, Renato Neves, and Luıs Barbosa. A type system for simple quantum processes. *EUTYPES-TYPES 2020-Abstracts*.

[9] Frank Gaitan. *Quantum Error Correction and Fault Tolerant Quantum Computing*. CRC Press, Inc., Boca Raton, FL, USA, 2007.

[10] Sergey Goncharov, Julian Jakob, and Renato Neves. A semantics for hybrid iteration. *arXiv preprint arXiv:1807.01053*, 2018.

[11] Sergey Goncharov and Renato Neves. An adequate while-language for hybrid computation. In *Proceedings of the 21st International Symposium on Principles and Practice of Programming Languages 2019*, pages 1–15, 2019.

[12] R. Hill. *A First Course in Coding Theory*. Oxford Applied Linguistics. Clarendon Press, 1986.

[13] J.R. Hindley and J.P. Seldin. *Lambda-calculus and Combinators: an Introduction*. Cambridge University Press, 2008.

[14] Ugo Dal Lago, Andrea Masini, and Margherita Zorzi. On a measurement-free quantum lambda calculus with classical control. *Mathematical Structures in Computer Science*, 19(2):297–335, 2009.

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

[16] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.

[17] Diego Napp, Raquel Pinto, and Marisa Toste. Column distances of convolutional codes over ${\mathbb Z}_{pˆr}$. *IEEE Trans. Information Theory*, 65(2):1063–1071, 2019.

[18] 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.

[19] 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.

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

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

[22] Michele Pagani, Peter Selinger, and Benoît Valiron. Applying quantitative semantics to higher-order quantum computing. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 647–658, 2014.

[23] C. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

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

[25] E. Rieffel and W. Polak. *Quantum Computing: A Gentle Introduction*. Scientific and Engineering Computation. MIT Press, 1992.

[26] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2017.

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

[28] Mingsheng Ying. *Foundations of Quantum Programming*. Morgan Kaufmann, Elsevier, 2016.