Quantum Computation 2022-23

Proposal for the *Computing Paradigms* block

Summary

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

1 Context and Objectives

Quantum computing is coming of age. With the race for 'quantum advantage' rising between major IT players (e.g. IBM, Intel, Google, Microsoft) and the announcement of prototype-machines up to 60 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 diverse 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*, *interference*, 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 computation, 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 surprising 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 computation is emerging within the Universities 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's previous research on quantum computation, program semantics and logic in (classical) software development. The latter is object of four 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*
- Ibex (PTDC/CCI-COM/4280/2021) *Quantitative methods for cyber-physical programming.*

Although none of them directly addresses quantum computation, the techniques developed there are being tuned to deal with the quantum case as well. For example, a PhD project on dynamic logic for verification of quantum systems was successfully accomplished in the context of the projects Dalí and Klee. A number of MSc dissertations that explored different aspects of quantum computation were written in the context of the Klee project. A PhD project on programming languages for noisy quantum computers is being explored in the context of the Ibex 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 to 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 a qubit. Structuring quantum data.

M2 - Quantum Gates and Circuits.

- Unitary transformations and quantum gates.

- Measurement.
- The circuit model.

M3 - Quantum Algorithms.

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

M4 - Laboratory. Hands-on introduction to quantum programming via the IBM Q platform and Qiskit, a scripting language and open source development kit. This module aims at consolidating through laboratorial practice the concepts and methods that were 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, 30, 25]

M2 - The Circuit Model: [20, 30, 25]

M3 - Quantum Algorithms: [16, 31, 32]

M5 - Computability and Complexity: [2, 23, 31]

M6 - Quantum λ-calculus: [13, 14, 22]

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

M8 - Logics for quantum programs: [32, 4, 5]

8 Team

Renato Neves (**coordinator**) is an Assistant 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 computation. 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 noisy/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, three PhD theses, and five 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. 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 theses. 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 Associate Professor at the Department of Mathematics, University of Aveiro. Her research interests are in the field of coding theory with particular interest on convolutional coding and systems theory, namely the behavioural approach to systems theory. She has (co-)supervised 5 PhD theses and she is currently supervising 2 PhD theses.
Selected relevant publications: [7, 3, 17].

José Carlos Espírito Santo is an Assistant Professor at the Department of Mathematics of Minho University since 2002. As a researcher, he is a member of the Centre of Mathematics of Minho University, and his research areas are λ-calculus, proof theory and type theory and their applications to computer science. He authored more than 35 research papers, supervised 1 post-doc student and 8 MSc theses. Currently he is supervising 3 PhD students and 3 MSc theses, and is a member of EuroProofNet, the european research network on digital proofs.
Selected relevant publications: [26, 27, 28, 29].

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 ${\mathbb Z}_{p^r}$. *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] José Espírito Santo and Gilda Ferreira. A refined interpretation of intuitionistic logic by means of atomic polymorphism. *Stud Logica*, 108(3):477–507, 2020.

[27] José Espírito Santo and Gilda Ferreira. The russell-prawitz embedding and the atomization of universal instantiation. *Log. J. IGPL*, 29(5):823–858, 2021.

[28] José Espírito Santo, Ralph Matthes, and Luís Pinto. A coinductive approach to proof search through typed lambda-calculi. *Ann. Pure Appl. Log.*, 172(10):103026, 2021.

[29] José Espírito Santo, Luís Pinto, and Tarmo Uustalu. Plotkin's call-by-value λ-calculus as a modal calculus. *J. Log. Algebraic Methods Program.*, 127:100775, 2022.

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

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

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