PhD Position Offer

Specification and Verification of Quantum Programs

Supervisor: A. Giorgetti[1]
Co-Supervisors: Frédéric Holweck[2] and Pierre-Alain Masson[1]
Université Bourgogne Franche-Comté

[1] Université de Franche-Comté
Institut FEMTO-ST (UMR CNRS 6174)
Département d'Informatique des Systèmes Complexes (DISC), équipe VESONTIO
25030 Besançon cedex
firstname.lastname@femto-st.fr

[2] Université de Technologie de Belfort-Montbéliard (UTBM)
Laboratoire Interdisciplinaire Carnot de Bourgogne (ICB UMR 6303)
90000 Belfort
frederic.holweck@utbm.fr

Laboratory	FEMTO-ST Institute, DISC (Département d'Informatique des Systèmes Complexes)
Institution	UBFC, Université de Bourgogne Franche-Comté
Time span	3 years starting from October 2018
Funding	36 months doctoral contract at UBFC
Contact	`alain.giorgetti@femto-st.fr`

Abstract

Although actual quantum computers are currently limited to using a few numbers of quantum bits, quantum program theory foundations have been growing from the past 20 years. The FEMTO-ST/DISC department has expertise in formal specification, deductive verification and model-based testing of classical programs. The goal of the PhD is to extend this expertise to quantum programs.

Keywords: Quantum Algorithms, Formal Annotations, Static Analysis, Dynamic Analysis, Formal Semantics, Model-Based Testing, Program Proof

1 Scientific Context

The theory of quantum programming is increasingly studied since the beginning of the 21st century. Several quantum programming languages have been proposed (see [2, 8] for a survey until 2006). Various aspects of quantum computing have been modelized in Haskell [7], Coq [1] or Isabelle [4, 9].

This work is in relation with I-QUINS, an I-SITE-BFC project (contract ANR-15-IDEX-03), which brings together theoretical and practical researchers in the field of quantum computing, working together on the building and miniaturization of physical quantum systems.

2 PhD Objectives

The general intention of this PhD is to enrich the theory of quantum programming by studying the formal aspects of the existing quantum programming languages, and extend both their operational and axiomatic formalized semantics.

The PhD is expected to achieve the following objectives.

- Development of skills in quantum programming on the available quantum computers[1] or quantum simulators[2]. Such expertise will be necessary for the PhD core but also useful to develop interdisciplinary cooperations within the I-QUINS project.
- An extended state of the art about quantum programming languages and the formalizations of their semantics will be provided. The aim is to identify, with respect to classical programming [3, 5, 6] and Hoare logic for quantum programs [1, 4, 9], which aspects are already mechanized and which are not;
- The PhD will explore the possibility of applying existing software engineering methods (such as modelling, annotation, refinement, abstraction, testing, formal proof, etc.) to the quantum world. In particular, quantum annotations for specifying such properties as, e.g. entanglement, will be proposed.
- In [3], a mechanized semantics (in Coq) is proposed to prove the semantic equivalence of various formalized semantics for classical programs. A transposition of this approach to quantum programming shall be proposed, in Coq or Isabelle, ideally as simple as possible.
- Proofs of existing but yet unproved quantum algorithms will be realized, by means of existing quantum proof tools, or their adaptation for the purpose of the PhD. Algorithms related to the I-QUINS project will receive a particular focus.

3 Work Environment and Framework

The research will take place at the premises of the DISC department at the FEMTO-ST institute, located in Besançon, France. The supervision will be in collaboration with UTBM. The PhD student will settle in the VESONTIO research team, whose research domains are the formal specification and verification of programs by test or by proof, based on program models. The work will partly be realized in relation with the I-SITE-BFC project I-QUINS, dedicated to quantum information.

4 Candidates Profile and Application

The candidates should have a master degree in computer science, with proved skills in the general area of formal methods, formal specification, verification and validation. Skills in Coq or Isabelle proof environments will be appreciated. Proficiency in English is important, and the candidates shall master writing and presenting scientific work.

The application consists of one PDF file comprising:

- a CV,
- a letter of motivation justifying the interest for this particular PhD subject,
- a recommendation letter from the supervisor of the master's thesis, with contact details,
- a short summary of the master's thesis,
- the transcript of records of the license and master degree (or equivalent), with rank and size of the promotion.

The application should be sent by e-mail to `alain.giorgetti@femto-st.fr`, `pierre-alain.masson@femto-st.fr` and `frederic.holweck@utbm.fr`. The closing date for applying is 31 May 2018.

[1] The IBM quantum experience: `https://quantumexperience.ng.bluemix.net/qx/experience`.

[2] Like the Quantum Learning Machine developed by ATOS: `https://atos.net/en/insights-and-innovation/quantum-computing/atos-quantum`.

References

[1] J. Boender, F. Kammüller, and R. Nagarajan. Formalization of quantum protocols using coq. In *Proceedings 12th International Workshop on Quantum Physics and Logic, QPL 2015, Oxford, UK, July 15-17, 2015.*, pages 71–83, 2015.

[2] S. J. Gay. Quantum programming languages: Survey and bibliography. *Mathematical. Structures in Comp. Sci.*, 16(4):581–600, Aug. 2006.

[3] X. Leroy. Mechanized semantics. École d'été VSTA (*Verification Technology, Systems & Applications*), `http://gallium.inria.fr/~xleroy/courses/VTSA-2013/notes.pdf`, 2013.

[4] T. Liu, Y. Li, M. Ying, and N. Zhan. A theorem prover for quantum hoare logic and its applications. 2016.

[5] T. Nipkow and G. Klein. *Concrete Semantics - With Isabelle/HOL*. Springer, 2014.

[6] B. C. Pierce, A. Azevedo de Amorim, C. Casinghino, M. Gaboardi, M. Greenberg, C. Hriţcu, V. Sjöberg, A. Tolmach, and B. Yorgey. *Software foundations*, volume 2: Programming Language Foundations. 2017. `https://softwarefoundations.cis.upenn.edu/`.

[7] A. Sabry. Modeling quantum computing in haskell. In *Proceedings of the 2003 ACM SIGPLAN Workshop on Haskell*, Haskell '03, pages 39–49, New York, NY, USA, 2003. ACM.

[8] D. Unruh. Quantum programming languages. *Informatik - Forschung und Entwicklung*, 21(1):55–63, Oct 2006.

[9] D. Unruh. Quantum Relational Hoare Logic. *ArXiv e-prints*, Feb. 2018.