# A Tool for the Formal Verification of Quantum Optical Computing Systems

Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud and Sofiène Tahar

Electrical and Computer Engineering Dept., Concordia University, Montréal, Québec, Canada
{beillahi,mo_solim,tahar}@ece.concordia.ca

**Abstract:** Quantum optics systems provide a promising platform for universal quantum computing, since they link quantum computation and quantum communication in the same framework. Thanks to their high capability, quantum computers are considered good candidates to replace classical cryptography and supercomputing systems which require a robust and accurate verification process. In this paper, we introduce a tool for the formal verification of quantum computing systems based on the soundness and accuracy of high-order-logic theorem proving augmented by a set of decision procedures to automate the proof process.

## 1 Introduction

Quantum computers promise to increase greatly the efficiency of solving problems such as factoring large integers, combinatorial optimization and quantum physics simulation. Compared to traditional computers, quantum computers allow performing optimization calculations exponentially faster. It has been proved that it is indeed possible to create universal quantum computers with linear optics (e.g., beam splitters, phase shifters), single photons, and photon detection, resulting of what is called Linear Optical Quantum Computing (LOQC) systems [3]. Despite major progresses in the area, several challenges remain unresolved. For example, the verification of quantum devices and algorithms did not yet receive enough attention, particularly when quantum devices and algorithms are used in some high computing domains (i.e., aerospace, cybersecurity, biomedical...). In order to verify quantum computers which exploit the laws of quantum physics we have to express these laws in mathematical forms. Generally, quantum devices and protocols are verified using traditional techniques (e.g., numerical methods, lab simulations...) which are uncertain, and costly. In lab simulation, in order to measure the effect of different initial conditions or parametric variation over the quantum circuit operation, it is necessary to perform exhaustive tests. However, even by doing this, there is no guarantee of the full correctness of the results, because it will be necessary to test the system for an infinite number of operating conditions. We believe that there is a dire need of an accurate framework to build high assurance quantum systems. In the last decades, formal methods based techniques have proven to be an effective approach to analyze physical systems, thanks to their solid mathematical foundation. We believe that nowadays formal tools, in particular theorem proving systems, have reached to the maturity, where complex physical models can be expressed with less efforts than ever before, and formal methods can assist in the verification of futuristic quantum computers. In this paper, we propose to build a formal verification tool to study quantum systems in particular LOQC systems by applying higher-order-logic theorem proving. The first step towards our goal is to formally analyze quantum universal gates (i.e., controlled-not, controlled-phase and Fredkin) which are the counterparts of classical gates (i.e., OR, AND, XOR) in quantum physics. The next step is to build a verification tool, based on the same underlying theory, to reason about larger circuits composed of the above universal gates. Recently, a work on the formalization of linear quantum optics was proposed in [7] using process calculus. However, process calculus is mostly used for the verification of concurrent systems such as quantum cryptography. Moreover, the models expressed using this technique are quite complex to understand and proof steps are lengthy and not readable, especially for large circuits. Another work was proposed in [8] to model and analyse quantum systems using the CWB-NC model checker. Though, the CWB-NC can only be used for verifying and modeling finite-state concurrent systems. In [4], a comprehensive linear algebra library was formalized in the HOL Light theorem prover [1], using this library, coherent states, beam splitters, phase shifters, and flip gates were formalized in higher-order-logic [5]. In our work, we will build on top of this formalization, for the sake of developing a tool for formalizing quantum systems in a more sound and expressive fashion.

## 2 Quantum Linear Optics

Linear-optical networks, i.e., passive networks constructed from beam splitters, phase shifters and mirrors, can be used to build universal quantum computing system. In LOQC systems, the qubit is usually taken as a single photon that can be in two different modes, $|0\rangle_L = |1\rangle \bigotimes |0\rangle \equiv |1,0\rangle$ and $|1\rangle_L = |0\rangle \bigotimes |1\rangle \equiv |0,1\rangle$ which is called dual_rail. When the two modes represent the internal polarization degree of freedom of the photon ($|0\rangle_L = |H\rangle$ and $|1\rangle_L = |V\rangle$), we call it a polarization qubit. Knill, Laflamme, and Milburn [2] showed that linear optics combined with adaptive measurements is considered a viable proposal for building a universal quantum computer . Although logical gates can only be implemented probabilistically, it has been proved that they can be rendered deterministic (near-deterministic) by making use of ancillary resources, mea-

surements, cluster-state techniques, and feed-forward [3]. The controlled-phase or CZ gate can be constructed in linear optics using two nonlinear sign (NS) gates [3] and the Fredkin gate can be constructed using quantum linear swap gate and beam splitters. On the other hand, the NS and swap gates can be built using linear optics elements.

## 3 Proposed Tool Structure

The proposed structure, given in Figure 3, outlines the main idea to graphically model quantum optical systems and to formally prove that they satisfy certain system specications. The whole framework can be decomposed into two major parts. First, the graphical interface and the connection with HOL, where the quantum circuit will be drawn by connecting the chosen components from available quantum blocks to obtain the final circuit. Also the quantum circuit specification should be represented or given as parameters of the circuit. Consequently, for the connection between HOL and the interface, we will use Java Script Object Notation (JSON). JSON has been proposed as parser in [6] to implement a graphical interface connected to HOL, to analyze web services. The parser will then express the system model and specifications as HOL predicates. Next, the interface can execute HOL scripts to conduct the formal proof of the given theorem, by applying developed rules and tactics in HOL to provide effective automation. These tactics are automated in order to reduce the painful manual interaction often required with interactive (higher-order-logic) theorem proving. Once the formal verification completed, the parser will take the proof result to be visualised in the interface.

The second part is composed of a library for quantum optics, which mainly contains quantum universal gates and most common applications of these gates. Note that, our formalization will be based on the formalization of linear space, and basic quantum components (e.g., phase shifter, beam splitter and interferometer) [3]. Using this we are going to formalize the notions of linear quantum optics. Next, we will conduct the formal verification of frequently used quantum universal gates such as the Fredkin and CZ gates. Finally, using these gates we can investigate some widely used quantum applications (i.e., Shor's and Grover's algorithms, and Benes network). By then, we will have a complete HOL library of quantum optics and some common applications in the field.

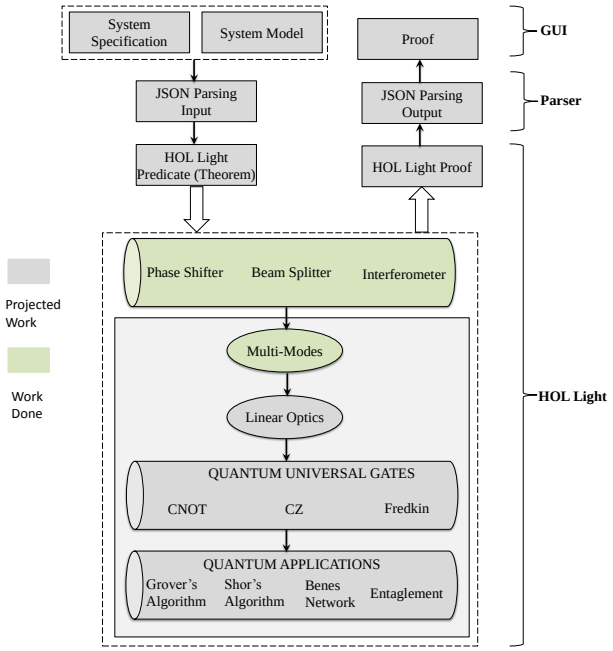


Figure 1: Proposed Formal Tool Structure

## 4 Conclusion

We introduced a new alternative for the verication of quantum optical systems. An overview of our proposed tool and quantum linear optics were presented. We are currently working on the formalization of quantum universal gates and the implementation of the first components of the tool to conduct the formal verification of quantum systems.

## References


[1] J. Harrison. HOL Light: A Tutorial Introduction. In *Formal Methods in Computer-Aided Design*, volume 1166 of *LNCS*, pages 265–269. Springer, 1996.

[2] E. Knill, R. Laflamme, and G. J. Milburn. A Scheme for Efficient Quantum Computation with Linear Optics. *Nature*, 409:46–52, 2001.

[3] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear Optical Quantum Computing with Photonic Qubits. *Rev. Mod. Phys.*, 79:135–174, 2007.

[4] M. Y. Mahmoud, V. Aravantinos and S. Tahar. Formalization of Infinite Dimension Linear Spaces with Application to Quantum Theory. In *NASA Formal Methods*, volume 7871 of *LNCS*, pages 413–427. Springer, 2013.

[5] M. Y. Mahmoud, V. Aravantinos and S. Tahar. Formal Verification of Optical Quantum Flip Gate. In *Interactive Theorem Proving*, volume 8558 of *LNCS*, pages 358–373. Springer, 2014.

[6] P. Papapanagiotou, and J. Fleuriot, and S. Wilson. Diagrammatically-Driven Formal Verification of Web-Services Composition. In *Diagrammatic Representation and Inference*, volume 7352 of *LNCS*, pages 241–255. Springer, 2012.

[7] S. F. Arnold, S. J. Gay and I. V. Puthoor. Quantum Process Calculus for Linear Optical Computing. In *Reversible Computation*, volume 7948 of *LNCS*, pages 234–246. Springer, 2013.

[8] S. J. Gay, N. Papanikolaou, and R. Nagarajan. QMC: A Model Checker for Quantum. In *Computer Aided Verification*, LNCS, pages 543–547. Springer, 2008.