Towards the Formal Verification of Quantum Optical Systems

M. Yousri V. Aravantinos S. Tahar

Electrical and Computer Engineering Dept.
Concordia University
Montreal, Canada

mosolim@ece.concordia.ca vincent@ece.concordia.ca tahar@ece.concordia.ca

Nowadays, optics has several applications in many industries. Quantum optics in particular plays an important role, e.g., in information technology. The systems developed using quantum optics have several applications which can be critical (with respect to either safety or financial aspects). Their verification is thus an extremely important problem. This is done usually with paper-and-pencil analysis, simulation or computer algebra systems. However these techniques have some flaws that we propose to address using formal verification, and, more specifically, theorem proving. In this position paper, we sketch a formalization of quantum optics using a theorem prover and describe potential applications of these techniques. We focus in particular on the implementation of quantum bits (i.e., the first step towards a quantum computer) using coherent laser light.

1 Introduction

Classical physics (electromagnetic theory and Maxwell equations) studies light as an electromagnetic wave. On the contrary, quantum optics studies light as a stream of particles, called *photons* [4]. Based on this concept, quantum optics investigates new properties and phenomena about the light, especially with low number of photons [12]. This investigation allows a better use of existing optical devices, e.g., beam splitters [9], and the invention of totally new quantum devices, e.g., single photon devices [11]. These devices help in different fields; sometimes they enhance the performance, e.g., detection of gravitational waves, and in other cases they define totaly new solutions, e.g., quantum communications [15]. In addition, quantum optics is one of the most practical implementations of quantum computers [13].

System verification represents a critical issue in every design process. For quantum mechanics and especially quantum optics, the available verification methods are simulation, paper-and-pencil, numerical methods, and computer algebra systems ("CAS"). In the first case, the systems are simulated on computer and in optical laboratories. For large systems, laboratories are more efficient and effective than computer simulation since it was proved in 1982 by Feyman that quantum systems cannot be simulated on ordinary computers [3]. Although laboratories can be sufficient, they raise cost and safety issues. In the paper-and-pencil approach, all the verification process is done by modeling the system and proving, using existing physic knowledge, that the system satisfies its specifications. However all this process is done by a human and is thus much error-prone, particularly when the system is very large. Thus, computer methods can be used to help the human – and thus decrease the risk if errors – which yields the two last methods: numerical methods (typically Matlab [14]) and CAS (typically Mathematica [2]). Both kinds of tools are used to help the simplification and generation of intermediate mathematical steps. However, these tools are not sufficient: they cannot be substituted fully to the paper-and-pencil approach since they cannot mathematically express the whole model of the system.

Formal verification is an alternative to the techniques mentioned above. This approach involves the development of a formal (i.e., mathematical) proof that the system satisfies its specifications. This can be

Submitted to:
FTSCS 2012

done in particular using a *theorem prover*, i.e., a software allowing to express the specification and model of the system in a mathematical way. We can then prove properties about the system *inside* the theorem prover (typically, we prove that the model of the system satisfies its specifications). The whole interest of the method is that the theorem prover is able to ensure that the provided proof is mathematically flawless. The language allowing to express the mathematical properties in the theorem prover is usually *first-order logic (FOL)* or *higher-order logic (HOL)*. Several theorem provers exist such as HOL4, HOL Light, PVS, Isabelle or Coq (see, e.g., [**?**]).

In this work, we investigate the use of theorem proving for the verification of quantum optical systems. We target the formalization of the quantum optics theory in HOL Light and the use of this formalization in quantum system verification. In addition, we sketch the verification of a quantum computer implementation as a coherent laser light [13] using this formalization.

2 Quantum Optics Formalization

In this section, we sketch some essential aspects of quantum mechanics that are useful to quantum optics, which we have formalized. In addition, we give the basic definition and some important results of quantum optics.

Any system considered in physics has a so-called *state* which sums up the information that we know about the system at a given time. A state in classical physics can be evaluated deterministically, but a quantum state is known only probabilistically. Thus a quantum state can be considered as a probability distribution function. Since such a function is square-integrable, it can be represented mathematically as an element of the Hilbert space L_2 (usually written with the notation $|\varphi\rangle$). Then system observables (e.g., position and velocity of a moving particle) are represented as linear hermitian transformations over L_2. A real value is obtained from such an observable $\mathscr{O}$ by computing $\langle\varphi|\mathscr{O}\varphi\rangle$, i.e., the L_2 inner product of the state $|\varphi\rangle$ with $|\mathscr{O}\varphi\rangle$.

The above notions have been formalized in HOL Light. More precisely, we defined the notion of Hilbert space, of hermitian transformations, and we proved related properties. From these, we could define quantum states as elements of the space L_2, and observables as linear hermitian transformations over L_2. This allowed us to prove important results such as the uncertainty principle which states that some observables cannot be measured simultaneously with high accuracy [4].

In quantum mechanics, we make a distinction between *originally quantum systems* and *originally classical systems*. Originally classical systems have to be transformed into quantum systems by a so-called *quantization* process. In 1930, Paul Dirac defined such a transformation called the *canonical quantization*. This process was used in the quantization of many systems. A well known quantization example is the quantization of electromagnetic field which results in quantum optics theory. The quantization of an electromagnetic field, especially a single-mode field[1], forms the basis of quantum optics. Important results were discovered in the quantized single-mode field. For example, the fact that the total energy in the field is a discrete value, the fact that the field consists of particles called photons, and the relation between the total energy in the field and the number of photons in it.

Using our quantum mechanics HOL library, we have implemented the canonical quantization process and used it successfully to quantize the single mode field. Currently, we have a library for the single mode in which we have proved several theorems. For example, we proved that the total energy in the field is discrete. In addition, the definition of photons was added and the relation between photons number and

[1] i.e., an electromagnetic field with single resonance frequency.

the total energy in the field was proved. We are currently working on the implementation of the coherent light definitions and related theorems.

The above libraries show that our objective, i.e., quantum optics formalization, is reasonable. We now plan to formalize more advanced topics in order to be able to target tangible applications as we will see in the next section.

3 Formal Verification of a Quantum Bit Implementation

One of the most promising applications of quantum optics is quantum computers. In this section, we propose to apply our framework to this field and, more specifically, to the implementation of quantum bits. We hope that using formal verification in this field will help the development of the quantum bit in the industry, since it is a cheap ,but accurate, verification tool compared to the optical laboratories simulation.

The first model of quantum computer was proposed in 1985 by Deutsch [1]. The essential advantage of quantum computers is that they can run exponentially faster than ordinary computers [5]. In a way similar to ordinary computers which are based on bits, quantum computers are based on quantum bits, called *Qubits*. Then, similarly, operations between qubits are achieved by so-called *quantum gates*. There are different implementations of quantum computers, e.g., [7], [10], [6] and [16]. The main difference among these implementations is how qubits are implemented: it can be either photons, electrons or ions. Among these implementations, the ones based on photons and quantum optics seem to be the most promising for a practical use [13].

In quantum mechanics, any system has a collection of quantum states[2] $|\varphi_i\rangle$ called *pure states*. At any time, the system state $|\varphi\rangle$ is formally defined as: $|\varphi\rangle = \sum_i c_i|\varphi_i\rangle$, where $c_i \in \mathbf{C}$ and $\sum_i |c_i|^2 = 1$. For a qubit, the system has only two pure states: one for $|0\rangle$ and one for $|1\rangle$. Thus, the qubit state is defined as follows: $|Qu_{state}\rangle = \delta|0\rangle + \beta|1\rangle$, where δ and $\beta \in \mathbf{C}$. Now, we sketch how qubits are implemented as coherent light.

The light is called *coherent* when the number of photons, at any time, is randomly distributed with Poisson probability distribution function (p.d.f). A coherent light at a quantum state $|\alpha\rangle$ means that the Poisson p.d.f parameter is $|\alpha|^2$. In [13] a qubit is implemented as a prepared coherent light with two pure states: $|\alpha\rangle$ and $|-\alpha\rangle$ which represent $|0\rangle$ and $|1\rangle$ respectively. In addition, the implementation of basic quantum gates is introduced. For example, the quantum flip gate, which converts $\delta|0\rangle + \beta|1\rangle$ into $\beta|0\rangle + \delta|1\rangle$, is implemented as an optical phase shifter. We plan, after finishing the formalization of coherent light, to formally verify two properties:

1. $\forall\alpha.\ |\alpha\rangle$ and $|-\alpha\rangle$ are orthonormal[3].

2. $\forall\delta\ \beta.$ an optical phase shifter converts $\delta|\alpha\rangle + \beta|-\alpha\rangle$ into $\beta|\alpha\rangle + \delta|-\alpha\rangle$.

One can notice that the first property cannot be verified by simulation at all. And verifying requires to simulate all possible values of δ and β, which is impossible. On the other hand, our proposed framework can handle such problems, which gives it advantage over the the simulation methodology. In addition, its ability to express all the system specification mathematically gives it advantage over CSA .

[2] We usually denote a quantum state (i.e., the vector of L_2) as $|\varphi\rangle$.

[3] By the definition, the qubit pure states sould be orthonormal.

4 Conclusion

We introduced a new alternative for the verification of quantum optics systems which covers the flaws of simulation and CSA. HOL Light libraries for quantum mechanics and single-mode field quantization were implemented. We are currently working on the formalization of coherent light to formally verify the implementation of qubits as coherent light. In the long run, we plan to develop a full, generic, library that could be easily applied to the verification of more complex optical systems.

References

[1] D. Deutsch (1985): *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*. *Proceedings of the Royal Society* 400(1818), pp. 97–117, doi: 10.1098/rspa.1985.0070.

[2] J.M. Feagin (2002): *Quantum Methods with Mathematica*. Springer, doi:http://www.google.com.eg/books?id=tXIukmOFqscC.

[3] Richard Feynman (1982): *Simulating physics with computers*. *International Journal of Theoretical Physics* 21, pp. 467–488, doi:http://dx.doi.org/10.1007/BF02650179. 10.1007/BF02650179.

[4] M. Fox (2006): *Quantum Optics: An Introduction*. Oxford Master Series in Physics, Oxford University Press, doi:http://books.google.com.eg/books?id=Q-4dIthPuL4C.

[5] M. Hirvensalo (2004): *Quantum Computing*. Natural Computing Series, Springer, doi:http://books.google.com.eg/books?id=oCd5fWPqf7UC.

[6] H. Hffner, C.F. Roos & R. Blatt (2008): *Quantum computing with trapped ions*. *Physics Reports* 469(4), pp. 155 – 203, doi:10.1016/j.physrep.2008.09.003.

[7] Thomas Jennewein, Marco Barbieri & Andrew G. White (2011): *Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis*. *Journal of Modern Optics* 58(3-4), pp. 276–287, doi:10.1080/09500340.2010.546894.

[8] Christoph Kern & Mark R. Greenstreet (1999): *Formal verification in hardware design: a survey*. *ACM Trans. Des. Autom. Electron. Syst.* 4(2), pp. 123–193, doi:10.1145/307988.307989.

[9] Ulf Leonhardt (2003): *Quantum physics of simple optical instruments*. *Reports on Progress in Physics* 66(7), p. 1207, doi:http://stacks.iop.org/0034-4885/66/i=7/a=203.

[10] Ying Li, Daniel E. Browne, Leong Chuan Kwek, Robert Raussendorf & Tzu-Chieh Wei (2011): *Thermal States as Universal Resources for Quantum Computation with Always-On Interactions*. *Phys. Rev. Lett.* 107, p. 060501, doi:10.1103/PhysRevLett.107.060501.

[11] Brahim Lounis & Michel Orrit (2005): *Single-photon sources*. *Reports on Progress in Physics* 68(5), p. 1129, doi:http://stacks.iop.org/0034-4885/68/i=5/a=R04.

[12] L. Mandel & E. Wolf (1995): *Optical Coherence and Quantum Optics*. Cambridge University Press, doi:http://books.google.com.eg/books?id=FeBix14iM70C.

[13] T.C. Ralph, G.J. Milburn & W.J. Munro (2002): *Quantum computation with optical coherent states*. In: *Quantum Electronics and Laser Science Conference, 2002. QELS '02. Technical Digest. Summaries of Papers Presented at the*, pp. 264 – 265, doi:10.1109/QELS.2002.1031403.

[14] Sze M Tan (1999): *A computational toolbox for quantum and atomic optics*. *Journal of Optics B: Quantum and Semiclassical Optics* 1(4), p. 424, doi:http://stacks.iop.org/1464-4266/1/i=4/a=312.

[15] Henning Vahlbruch, Moritz Mehmet, Simon Chelkowski, Boris Hage, Alexander Franzen, Nico Lastzka, Stefan Goßler, Karsten Danzmann & Roman Schnabel (2008): *Observation of Squeezed Light with 10-dB Quantum-Noise Reduction*. *Phys. Rev. Lett.* 100, p. 033602, doi:10.1103/PhysRevLett.100.033602.

[16] J. H. Wesenberg, A. Ardavan, G. A. D. Briggs, J. J. L. Morton, R. J. Schoelkopf, D. I. Schuster & K. Mølmer (2009): *Quantum Computing with an Electron Spin Ensemble*. *Phys. Rev. Lett.* 103, p. 070502, doi:10.1103/PhysRevLett.103.070502.