Quantum Model Checking Isn't Evil

It Is Mandatory For Quantum Robots

Zhiyang Ong

Department of Electrical and Computer Engineering
Dwight Look College of Engineering,
Texas A&M University
College Station, TX

July 5, 2015

Table of Contents

Acknowledgments

Dott. Francesco Stefanni, University of Verona

Soon-to-be Dr. Prateek Tandon, who initiated the formation of this reading group on quantum robotics.

Reference: Ying, M., Li, Y., Yu, N., and Feng, Y. Model-checking linear-time properties of quantum systems. ACM Transactions on Computational Logic 15, 3 (July 2014), 22:1–22:31.

Table of Contents

Background Information

- Designs of quantum systems (e.g., quantum robots) must be verified, tested, and validated
- Formally verify these designs via quantum model checking
- Carry out quantum model checking on invariants of quantum automata.
- Extend this to verify safety properties for reversible automata
- Extend this to verify ω-properties for reversible Büchi automata
- Meet requirements for correctness, safety, & reliability

Problem Statement

- Verify functional correctness of quantum systems.
- Input: Description of system behavior
  - i.e., specifications based on quantum automata
- Input: Functional linear-time properties
  - Linear-time invariants of quantum automata-based model
- Output: Boolean flag indicating correct/incorrect system behavior/functionality
- Examine only a finite number of representative elements of the state space of a quantum system
  - Or at most countably infinitely many representative elements

Shortcomings of Traditional Model Checking

- Cannot formalize behavior/functionality of quantum systems
  - Discrete state spaces of classical systems are finite or countably finite
  - Continuous state spaces of quantum systems cannot be addressed by discrete state spaces
  - State spaces of quantum systems are continuous, even for finite-dimensional quantum systems
  - Need to examine a finite number of representative elements (in an orthonormal basis) of the state space of a quantum system
  - Or, at most, examine countably infinitely many representative elements of this state space
  - Always preserve the linear algebraic structure of the representative elements [& linear-time properties]
- Cannot formally describe temporal properties of quantum systems

Prior Work

- Almost all previous work use model checking to verify quantum communication protocols
- Use quantum process algebra to verify quantum communication systems, including quantum error correction codes
- Use simulation tools for quantum systems to verify their behavior/functionality, especially their correctness and safety properties

Design Decisions

- Quantum model checking framework for the formal verification of generic quantum engineering systems
  - Not just quantum communication systems
- Use a formal method based on modeling quantum systems with quantum automaton
  - Exploit similar work in quantum Markov chains, quantum dot automata, & quantum cellular automata
- Only consider linear-time properties of generic quantum systems
  - Describe these linear-time properties as infinite sequences of sets of atomic propositions, just like LTL model checking
- Extend this to verify safety properties for reversible automata
- Extend this to verify ω-properties for reversible Büchi automata
- Meet requirements for correctness, safety, & reliability

Key Contributions of (Ying 2014)

- Almost all previous work use model checking to verify quantum communication protocols
- Use quantum process algebra to verify quantum communication systems, including quantum error correction codes
- Use simulation tools for quantum systems to verify their behavior/functionality, especially their correctness and safety properties
- Extend this to verify safety properties for reversible automata
- Extend this to verify ω-properties for reversible Büchi automata
- Meet requirements for correctness, safety, & reliability

Table of Contents

Additional Formal Verification Techniques for Quantum Robots (1)

- Reachability analysis:
  -
  - Possible solution: Quantum partially-observable Markov decision processes (QMDPs)
  - Reference: Shenggang Ying and Mingsheng Ying, "Reachability Analysis of Quantum Markov Decision Processes," *arXiv*, Cornell University, Ithaca, NY, July 9, 2014. Available online from *arXiv* as Version 2 at: `http://arxiv.org/abs/1406.6146v2`; May 30, 2015 was the last accessed date.
- Quantum Equivalence Checking:
  - Given 2 models of a quantum robot, determine if they are functionally equivalent.
  - Use quantum information decision diagrams (QuIDD), global-phase equivalence, and relative-phase equivalence (Viamontes et al., 2009).
  - Ditto for tensor calculus, dynamic tensor products, partial

Additional Formal Verification Techniques for Quantum Robots (2)

- SMT-based quantum formal verification:
  - Use SMT solver (decision procedure for satisfiability modulo theories) as reasoning engine for formal verification
  - Use reasoning/computational engine for hybrid model checking and theorem proving or model checking and equivalence checking
  - Use fragments of 1st-order logic, such as differential dynamic logics, for hybrid systems verification; see work by Prof. André Platzer at `http://symbolaris.com/`.
  - Get the quantum logic equivalent of these.
  - References:

1. Platzer, A. Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics. Springer- Verlag Berlin Heidelberg, Heidelberg, Germany, 2010.

Additional Formal Verification Techniques for Quantum Robots (3)

- Exploit equivalence of maximum satisfiability (Max-SAT), pseudo-boolean optimization (PBO) , and wighted PBO:
  1. Use meta-algorithms via algorithmic portfolio optimization to select the "best" or set of good solutions (Max-SAT, Max-SMT, PBO, or Weighted PBO).
  2. Engineer quantum logic variant/equivalent.
  3. Turn numerical models in the time domain to algebraic models in the frequency domain, via transform methods (e.g., Fourier transform, Laplace transform, and z-transform) and approximations via parameterization and (quasi-) linearization
  4. The meta-algorithms enable us to plug-and-play (or plug-and-pray) components for quantum formal verification.

Additional Formal Verification Techniques for Quantum Robots (4)

- Use Quantum Model Order Reduction for Approximation:
  1. Quantum Model Order Reduction approximates components of quantum robots as continuous-time dynamical systems.
  2. Reference: [1] Viamontes, G. F., Markov, I. L., and Hayes, J. P. Quantum Circuit Simulation. Springer Science+Business Media, B.V., Dordrecht, The Netherlands, 2009.