Taint Analysis of Microarchitecture Synthesis Software and Designs

Not Using It to Secure Microarchitectures is Foolish

Zhiyang Ong

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

September 26, 2016

Table of Contents

Acknowledgments

Dott. Francesco Stefanni, University of Verona

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

Dr. Shenggang Ying for responding to my queries about their *arXiv* research paper.

Reference: Shenggang Ying and Mingsheng Ying, "Reachability Analysis of Quantum Markov Decision Processes," in *arXiv*, Cornell University, Ithaca, NY, July 9, 2014. Available online from *arXiv* as Version 2 at: `http://arxiv.org/abs/1406.6146` and `http://arxiv.org/abs/1406.6146v2`; May 30, 2015 was the last accessed date.

Warnings!!!

- Research publications on formal verification or formal methods have lots of definitions.
- Exact/Approximate algorithms and heuristics for formal verification or formal methods are based on these definitions.
- Hence, exact definitions of terms in formal verification or formal methods are required for proving these algorithms and heuristics and theorems.
- This set of presentation slides does not cover the paper in the same order.
- Some rearrangements are made to present the material as a hybrid of a brief research presentation and tutorial.
- $\underline{\varrho}_{\kappa}$
- $\overline{\varrho}_{\kappa}$
- ρ

Table of Contents

Classical Reachability Analysis

If there exists a path from vertex s in a graph G to vertex t in G, t is reachable from s. All vertices in G are "reachable from themselves" (Yuan, 2006, §5.2, pp. 85).

- Reachability Analysis is :
  - Definition of reachable state in a Petri Net or FSM.
  - Define reachability analysis, based on the definition of the reachability of a state in a Petri Net or FSM.
  - E.g., A small bounded Petri Net can have many states, which are represented in the state/reachability graph. Use symmetry or stubborn set reductions, followed by creating and checking CTL formulae and predicates. Determine if a target state/marking is reachable from the initial state/marking, not necessarily via the minimal path. Check CTL properties/predicates for testing liveness properties.
  - Give more examples of reachability analysis
- Explain the importance of reachability analysis

Classical Reachability Analysis

Reachability analysis is defined as follows:

1. "A fixed-point analysis" technique to determine if a "set of states [is] reachable from a designated set of initial states" (Yuan, 2006, §1.8.2., pp. 16).
2.

- :
    - Definition of reachable state in a Petri Net or FSM.
    - Define reachability analysis, based on the definition of the reachability of a state in a Petri Net or FSM.
    - E.g., A small bounded Petri Net can have many states, which are represented in the state/reachability graph. Use symmetry or stubborn set reductions, followed by creating and checking CTL formulae and predicates. Determine if a target state/marking is reachable from the initial state/marking, not necessarily via the minimal path. Check CTL properties/predicates for testing liveness properties.
    - Give more examples of reachability analysis

References for Classical Reachability Analysis

(Yuan, 2006) Yuan, J., Pixley, C., and Aziz, A. Constrained-Based Verification. Springer Science+Business Media, Inc., New York, NY, 2006.

Table of Contents

Problem Statement

- Models of concurrent and nondeterministic quantum systems need to be verified.
- Quantum Markov decision processes (qMDPs) can model such quantum systems.
- Question: How can we carry out reachability analysis on concurrent and nondeterministic quantum systems, modeled as qMDPs?
- Input: qMDP $\mathcal{M}$
- Input: state space $\mathcal{H}$, which is a Hilbert space
- Input: state space $B \in \mathcal{H}$
- Output: Scheduler $\mathfrak{S}$
- Output: Non-negative integer, n.

Shortcomings of Classical Reachability Analysis

- Classic Markov chains cannot capture concurrency.
- A Markov chain only allows one “choice” of action per state, which implies that all “rewards” of the Markov chain are the same.
- 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]

Table of Contents

Prior and Related 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
- Quantum partially observable Markov decision processes (QOMDPs), which are introduced by (Barry, Barry, and Aaronson, 2014), only care about the reachability of a single state (i.e., goal state).:
    - The paper does not specifically address the reachability of invariant subspaces.
    - Goal-state reachability is undecidable for QOMDPs.

Invariant subspace: sounds like T: V–¿V something that transforms you into the same space

Table of Contents

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

Table of Contents

Key Contributions of (Ying 2014)

-

Table of Contents

Analysis on Decidability of Quantum Reachability Analysis In the Finite-Horizon

-

Analysis on Decidability of Quantum Reachability Analysis In the Infinite-Horizon

-

Table of Contents

Analysis on Complexity of Quantum Reachability Analysis In the Finite-Horizon

-

Analysis on Complexity of Quantum Reachability Analysis In the Infinite-Horizon

-

Table of Contents

Questions That I Have

- I assume that uncomputable problems are the same as undecidable problems (Barry, Barry, and Aaronson, 2014).
- From (Barry, Barry, and Aaronson, 2014), can QOMDPs be reduced to qMDPs?
- The authors mentioned that quantum systems can be modeled as qMDPs? Do such quantum systems include robots, which can be modeled as quantum dynamical systems? Or, is it restricted to quantum computer programs?
- What is the ortho-complement of a subspace?
- What does it mean for a measurement to be projective? What does it mean mathematically?
- Is "W" on page 2, right column, in the last paragraph ($w \in W$), a set of words "w"?
- $\otimes$, right column, in paragraph 1/2 on page 2

do Markov chains inherently model nondeterminism?

Are there extensions of Markov chains to capture/model concurrency?

Table of Contents

Discussions

- (What do I think about this work?)
-

Table of Contents

Future Work

- Extensions of