Model Checking Quantum Systems

Mingsheng Ying and Yuan Feng
Centre for Quantum Software and Information, University of Technology Sydney, Australia
State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China
Department of Computer Science and Technology, Tsinghua University, China
Email: Mingsheng.Ying@uts.edu.au; Yuan.Feng@uts.edu.au

***Abstract*—This article discusses the essential difficulties in developing model-checking techniques for quantum systems that are never present in model checking classical systems. It further reviews some early researches on checking quantum communication protocols as well as a new line of researches pursued by the authors and their collaborators on checking general quantum systems, applicable to both physical systems and quantum programs.**

***Index Terms*—quantum computing; model checking**

I. Introduction

We are currently in the midst of a second quantum revolution: *transition from quantum theory to quantum engineering* (e.g. quantum computing, communication, sensing). The main purpose of quantum theory is to find fundamental rules governing the existing physical systems. In contrast, quantum engineering aims at designing and implementing new systems (machines, devices, etc) to achieve some desirable tasks, based on quantum theory.

From experience in today's engineering, it is not always easy for a human designer to completely understand the behaviours of the system she/he is designing, and an error in her/his design may cause serious problems and even disasters. Consequently, theories and methodologies for verification of correctness, safety and reliability of complex engineering systems have been systematically studied in various engineering fields. In particular, computer scientists have developed techniques to verify the correctness of both hardware and software as well as the security of communication protocols.

A. Second Quantum Revolution Requires New Verification Techniques

Human intuition is poorly adapted to the quantum world than the classical world, which implies that human engineers will make many more mistakes in designing and implementing complex quantum systems such as quantum computer hardware and software and communication protocols. Even worse, because of the essential differences between the classical and quantum worlds, verification techniques for classical systems cannot be directly used to quantum systems. Novel verification techniques will be indispensable for the coming era of quantum engineering and technology.

B. Model Checking Techniques for Classical Systems

Model-checking is an effective technique to check whether a system satisfies a desired property. The properties that are checked are usually specified in a temporal logic; typical properties are deadlock freedom, invariants, safety, request-response properties. The systems under checking are mathematically modelled as e.g. (finite-state) automata, transition systems, Markov chains and Markov decision processes [1].

In the last three decades, model-checking has become one of the dominant techniques for verification of computer hardware and software, and has proved mature as witnessed by a large number of successful industrial applications. Techniques of model checking were even applied in systems biology recently.

With quantum engineering and quantum technology being emerging, a question then naturally arises: *is it possible and how to apply model-checking techniques in verifying the correctness and safety of quantum engineering systems*?

C. Difficulty in Model Checking Quantum Systems

Unfortunately, due to some essential differences between the classical and quantum systems, it seems unlikely that the classical model-checking techniques can be directly applied to quantum systems. Basically, to make model-checking techniques effective for quantum systems, the following three problems must be systematically addressed:

- ***System modelling and property specification***: Behaviours of quantum systems cannot be described using classical modelling methods, and consequently, properties of quantum systems to be checked cannot be formalised by classical specification languages. As a result, novel conceptual frameworks must be proposed to properly model and reason about quantum systems, including *formal models* and *formal description of temporal properties* of quantum systems.
- ***Quantum measurements***: Model-checking is usually applied to check long-term behaviours of the systems. But to check whether a quantum system satisfies a certain property at a time point, one has to perform a quantum measurement on the system, which can change the state of the system. This makes studies of the long-term behaviours of quantum systems much harder than that of classical systems.
- ***Algorithms***: Classical model-checking algorithms normally assume the state spaces to be finite or countably infinite. However, state spaces of quantum systems are inherently continuous. To develop algorithms for model-checking quantum systems, deep mathematical properties of the systems have to be exploited, so that a finite (or

countably infinite) number of representative elements in the state spaces will suffice. Note that the state space of any quantum system has a natural linear algebraic structure. A well developed algorithm for verifying quantum systems should make clever use of this structure.

II. Early Research on Model Checking of Quantum Systems

Despite the difficulties discussed above, a few model-checking techniques for quantum systems have been developed in the last 10 years. The earliest work mainly targeted checking quantum communication protocols:

- Taking the probabilism arising from quantum measurements into account, the probabilistic model-checker PRISM is used in [11] to verify the correctness of quantum protocols, including superdense coding, quantum teleportation and quantum error correction.
- A branching-time temporal extension of exogenous quantum propositional logic was introduced and then the model-checking problem for this logic was studied in [2], with verification of the correctness of quantum key distribution BB84 as an application.
- A linear temporal extension of exogenous quantum propositional logic was then defined and the corresponding model-checking problem was investigated in [16].
- Model-checking techniques were developed in [4] for quantum communication protocols modelled in process algebra CQP (Communicating Quantum Processes) [10].
- A model-checker for quantum communication protocols was also developed in [12], where only the protocols that can be modelled as quantum circuits expressible in the stabiliser formalism were considered. This technique was further extended beyond stabiliser states and used to check equivalence of quantum protocols.

III. Model Checking Quantum Automata

A research line pursued by the authors and their collaborators is to develop model-checking techniques that can be used not only for quantum communication protocols but also for general quantum systems, including physical systems and quantum programs.

Quantum automata were adopted in [19], [15] as the model of the systems:

Definition 3.1 (Quantum automata [14]): A quantum automaton is a 4-tuple $\mathcal{A} = (\mathcal{H}, Act, \{U_\alpha : \alpha \in Act\}, \mathcal{H}_0)$, where:

1) $\mathcal{H}$ is a finite-dimensional Hilbert space, called the state space;
2) Act is a finite set of action names;
3) for each action name $\alpha \in Act$, U_α is a unitary operator on $\mathcal{H}$;
4) $\mathcal{H}_0 \subseteq \mathcal{H}$ is the subspace of initial states.

A quantum automaton behaves as follows: it starts from some initial state in $\mathcal{H}_0$, and at each step it performs a unitary transformation U_α for some $\alpha \in Act$. An algorithm for checking certain linear-time properties (e.g. invariants and safety properties) was proposed in [19], where following Birkhoff-von Neumann quantum logic, closed subspaces of the state Hilbert space are used as the atomic propositions about the state of system, and the checked linear-time properties are defined as infinite sequences of sets of atomic propositions. Furthermore, decidability or undecidability of several reachability problems for quantum automata were established in [15].

IV. Model Checking Quantum Markov Chains

The model-checking problem for a larger class of quantum systems than quantum automata, namely quantum Markov chains was studied in [20].

Note that continuous-time quantum Markov processes have been studied intensively in mathematical physics. Discrete-time quantum Markov chains were recently introduced as a semantic model for quantum programs.

Definition 4.1 (Quantum Markov chains [20]): A quantum Markov chain is a triple $(\mathcal{H}, \mathcal{E}, \mathcal{H}_0)$, where $\mathcal{H}$ and $\mathcal{H}_0$ are the same as in Definition 3.1, and $\mathcal{E}$ is a super-operator on $\mathcal{H}$.

A quantum Markov chain starts in an initial state in $\mathcal{H}_0$, and at each step it performs (the same) quantum operation modelled by the super-operator $\mathcal{E}$. Note that the (discrete-time) dynamics of closed quantum systems are usually depicted by unitary operators, and the behaviours of open quantum systems are described by super-operators. Obviously, the notion of quantum automata can be generalised by replacing unitary operators U_α in Definition 3.1 by super-operators $\mathcal{E}_\alpha$. Furthermore, quantum Markov decision processes [3] can be defined by introducing decision strategies into such generalised quantum automata.

Several algorithms for checking reachability of quantum Markov chains and quantum Markov decision processes were developed. As in checking classical Markov chains and Markov decision processes, graph reachability is a key to these algorithms. However, classical graph theory is not suited to our purpose; instead a new theory of quantum graphs (i.e. graphs in a Hilbert space with adjacency relation induced by a super-operator) was developed, and in particular, an algorithm for the BSCC (bottom strongly connected components) decomposition of the state Hilbert spaces was found in [20]. Another decomposition technique, namely periodic decomposition, for quantum Markov chains was recently proposed.

V. Model Checking Super-Operator-Valued Markov chains

The notion of super-operator-valued Markov chain is introduced in [6] as a higher-level model of quantum programs and quantum cryptographic protocols.

Definition 5.1 (Super-operator-valued Markov chains [6]): A labelled super-operator-valued Markov chain over a set AP of predefined atomic propositions is a 5-tuple $(S, s_0, \mathcal{H}, Q, L)$, where:

1) S is a finite set of *classical states* with $s_0 \in S$ being the initial state;

2) $\mathcal{H}$ is a finite-dimensional Hilbert space, called the quantum state space;
3) $Q : S \times S \to \mathcal{SO}_{\mathcal{H}}$ is a transition super-operator function, where $\mathcal{SO}_{\mathcal{H}}$ denotes the set of trace-nonincreasing super-operators on $\mathcal{H}$, and for each $s \in S$, $\sum_{t \in S} Q(s,t)$ is trace-preserving; and
4) $L : S \to 2^{AP}$ is a labelling function.

A super-operator-valued Markov chain has two state spaces, a classical one and a quantum one, which are connected through the transition super-operator function. It behaves in a similar manner as classical Markov chains. It starts from the classical initial state s_0 but with the quantum initial state unspecified (it can be taken arbitrarily). Then at each step, given the current classical state s and quantum state ρ, it proceeds to classical state t with probability $\mathrm{tr}[Q(s,t)(\rho)]$, and the accompanied quantum state evolves into $Q(s,t)(\rho)/\mathrm{tr}[Q(s,t)(\rho)]$ provided that $\mathrm{tr}[Q(s,t)(\rho)] \neq 0$. The normalisation requirement that $\sum_{t \in S} Q(s,t)$ is trace-preserving guarantees that the probabilities of going from s to some classical state sum up to 1.

As the atomic propositions are taken to be classical (they apply only to classical states), this Markov chain model is suitable for verification of quantum systems against classical properties, such as running time, termination, reachability, etc. One distinct feature of this model, however, is that it allows us to check properties of the system *once-for-all*; that is, the verified results apply to all initial quantum states. For example, the model checking algorithm for the reachability problem essentially calculates a positive operator Π, accounting for all (classical) paths satisfying the concerned property. Then the reachability *probability* when the Markov chain starts in the initial quantum state ρ is simply $\mathrm{tr}(\Pi\rho)$.

A corresponding computation tree logic (CTL) for super-operator-valued Markov chains was defined, and algorithms for checking such properties were developed in [6]. A tool implementation of these algorithms has been provided [7] based on a probabilistic model checker. Algorithms for model checking ω-regular properties, a general class of properties subsuming LTL formulas, against super-operator-valued Markov chains were proposed [8], thus allowing analysis of a wide range of properties such as repeated reachability, reachability in a restricted order, and nested Until properties. Furthermore, the reachability problem of a recursive extension of super-operator-valued Markov chains was studied in [9], with the application of analysing quantum programs with procedure calls.

VI. Conclusion

As reviewed in previous sections, several theoretical frameworks and algorithms of quantum model-checking have been developed. But certainly, quantum model-checking is still at a very early stage of its development; in particular, its applications are only at the level of toy examples. We envisage that in the future, quantum model-checking techniques can be applied to the following areas:

1) *Checking physical systems*: Physicists already considered the algorithmic checking problem of certain properties of quantum systems, for example, quantum measurement occurrence [5] and reachability of quantum states [17]. Quantum model-checking can offer a systematic view of this line of research.
2) *Verification of quantum circuits*: Verification of circuits has been one of the major application areas of classical model-checking. But model-checking applied to verification of quantum circuits is an area to be systematically exploited.
3) *Analysis and verification of quantum programs*: Another important application area of classical model-checking is analysis and verification of programs. Several techniques for analysis and verification of quantum programs have been reported in the last few years [13], [18]. However, model-checking techniques specifically designed for quantum programs are still missing.
4) *Verification of security of quantum communication protocols*: Applications of model-checking mentioned in Section II focus on verification of correctness of quantum communication protocols. But verification of the security of quantum protocols is much more difficult, and model-checking applied to it is an interesting topic for future research.

References

[1] C. Baier and J. -P. Katoen, 2008. *Principles of Model Checking*. MIT Press, Cambridge, Massachusetts.

[2] P. Baltazar, R. Chadha, and P. Mateus. Quantum computation tree logic - model checking and complete calculus. *International Journal of Quantum Information 6*, 2008, 219–236.

[3] J. Barry, d. T. Barry and S. Aaronson, Quantum partially observable Markov decision processes, *Physical Review A* 90(2014), art. no. 032311.

[4] T. Davidson, S. J. Gay, H. Mlnarik, R. Nagarajan, and N. Papanikolaou. Model checking for Communicating Quantum Processes. *International Journal of Unconventional Computing 8*, 2012, 73–98.

[5] J. Eisert, M. P. Müller and C. Gogolin, Quantum measurement occurrence is undecidable, *Physical Review Letters*, 108(2012)260501.

[6] Y. Feng, N. K. Yu and M. S. Ying, Model checking quantum Markov chains, *Journal of Computer and System Sciences*, 79(2013) 1181-1198.

[7] Y. Feng, E. M. Hahn, A. Turrini, and L. Zhang. QPMC: A model checker for quantum programs and protocols. In *FM'15*, volume 9109 of *Lecture Notes in Computer Science*, pages 265–272. Springer, 2015.

[8] Y. Feng, E. M. Hahn, A. Turrini, and S. Ying. Model Checking Omega-regular Properties for Quantum Markov Chains. In: *Proceedings of the Concur*, 2017, pp. 35:1–35:16.

[9] Y. Feng, N. K. Yu and M. S. Ying, Reachability analysis of recursive quantum Markov chains, *Proceedings of MFCS*, 2013, pp. 385-396.

[10] S. J. Gay and R. Nagarajan, Communicating Quantum Processes, in: *Proceedings of the 32nd ACM Symposium on Principles of Programming Languages (POPL)*, 2005, pp. 145-157.

[11] S. J. Gay, R. Nagarajan, and N. Papanikolaou. Probabilistic model-checking of quantum protocols *arXiv:quant-ph/0504007*, 2005.

[12] S. J. Gay, R. Nagarajan, and N. Papanikolaou. QMC: a model checker for quantum systems. In: *Proceedings of the 20th International Conference on Automated Verification (CAV'08)*, 2008, Lecture Notes in Computer Science 5123, Springer, 543–547.

[13] A. JavadiAbhari, S. Patil, D. Kudrow, J. Heckey, A. Lvov, F. T. Chong and M. Martonosi, ScaffCC: Scalable compilation and analysis of quantum programs, *Parallel Computing*, 45 (2015), 2-17.

[14] A. Kondacs and J. Watrous. On the power of quantum finite state automata. In: *Proc. 38th Symposium on Foundation of Computer Science (FOCS'97)*, 1997, 66–75.

[15] Y. J. Li and M. S. Ying, (Un)decidable problems about reachability of quantum systems, In: *Proceedings of the Concur*, 2014, Springer, pp. 482-496.

[16] P. Mateus, J. Ramos, A. Sernadas and C. Sernadas, Temporal logics for reasoning about quantum systems. In: I. Mackie and S. Gay (eds.), *Semantic Techniques in Quantum Computation*, Cambridge University Press, 389–413.

[17] S. G. Schirmer, A. I. Solomon and J. V. Leahy, Criteria for reachability of quantum states, *Journal of Physics A: Mathematical and General*, 35 (2002) 8551-8562.

[18] M. S. Ying, *Foundations of Quantum Programming*, Morgan Kaufmann, 2016.

[19] M. S. Ying, Y. J. Li, N. K. Yu and Y. Feng, Model-checking linear-time properties of quantum systems, *ACM Transactions on Computational Logic*, 15 (2014), art. no. 22.

[20] S. G. Ying, Y. Feng, N. K. Yu and M. S. Ying, Reachability probabilities of quantum Markov chains, *Proceedings of Concur'13*, 2013, Springer, pp. 334-348.