Information and Computation 244 (2015) 229–244

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Quantum Markov chains: Description of hybrid systems, decidability of equivalence, and model checking linear-time properties

Lvzhou Li [a,b,d,*], Yuan Feng [b,c]

[a] Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China
[b] Center for Quantum Computation and Intelligent Systems, FEIT, University of Technology Sydney, Sydney 2007, Australia
[c] AMSS-UTS Joint Research Laboratory for Quantum Computation, Chinese Academy of Sciences, Beijing, China
[d] The Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, 510006, China

A R T I C L E I N F O

Article history:
Received 26 March 2013
Received in revised form 15 April 2015
Available online 15 July 2015

Keywords:
Quantum Markov chains
Hybrid systems
Quantum automata
Equivalence
Model checking
Linear-time property

A B S T R A C T

In this paper, we study a model of quantum Markov chains that is a quantum analogue of Markov chains and is obtained by replacing probabilities in transition matrices with quantum operations. We show that this model is very suited to describe hybrid systems that consist of a quantum component and a classical one. Indeed, hybrid systems are often encountered in quantum information processing. Thus, we further propose a model called hybrid quantum automata (HQA) that can be used to describe the hybrid systems receiving inputs (actions) from the outer world. We show the language equivalence problem of HQA is decidable in polynomial time. Furthermore, we apply this result to the trace equivalence problem of quantum Markov chains, and thus it is also decidable in polynomial time. Finally, we discuss model checking linear-time properties of quantum Markov chains, and show the quantitative analysis of regular safety properties can be addressed successfully.

1. Introduction

As we know, Markov chains as a mathematical model for stochastic systems play a fundamental role in computer science and even in the whole field of information science. A Markov chain is usually represented by a pair (P, π_0) where π_0 is a vector standing for the initial state of a stochastic system, and P is a stochastic matrix[1] characterizing the evolution of the system. Over the past two decades, quantum computing and quantum information have attracted considerable attention from the academic community. Then it is natural to study the quantum analogue of Markov chains. Actually, the terminology "quantum Markov chains" has appeared many times in the literature [1,2,9,8,17,28], although it does not mean exactly the same thing in different references. A usual approach to defining quantum Markov chains is to view a quantum Markov chain as a pair $(\mathcal{E}, \rho_0)$ where ρ_0, a density operator, denotes an initial state of a quantum system, and $\mathcal{E}$ is a trace-preserving quantum operation that characterizes the dynamics of the quantum system. This resembles very closely a classical Markov chain represented by a pair (P, π_0). Indeed, in the textbook [19], when quantum operations were intro-

* Corresponding author at: Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China.
E-mail addresses: lilvzh@mail.sysu.edu.cn (L. Li), Yuan.Feng@uts.edu.au (Y. Feng).

[1] In this paper, a matrix is said to be a stochastic matrix if each column of it is a probabilistic distribution.

http://dx.doi.org/10.1016/j.ic.2015.07.001
0890-5401/

duced, they were viewed as a quantum analogue of Markov processes. In [17,28], a quantum Markov chain means the same thing as mentioned here, while it mainly means a quantum walk in [1].

In this paper, we focus on the quantum Markov model reported in [9,8] which is greatly different from the one mentioned above but will be shown to be very suited to describe hybrid systems that consist of a quantum component and a classical one. Such a quantum Markov chain can be roughly represented by a pair (M, μ_0) where M is a transition matrix resembling P in a classical Markov chain but replacing each transition probability with a quantum operation and satisfying the condition that the sum of each column of M is a trace-preserving quantum operation. μ_0, standing for the initial state of the model, is a vector with each entry being a density operator up to a factor. This model looks very strange at first glance, but it has the same expressive power as the conventional one given by $(\mathcal{E}, \rho_0)$. Specially, we will show that this model is very suited to describe hybrid systems that consist of a quantum component and a classical one. Indeed, hybrid systems are often encountered in quantum computing and quantum information, varying from quantum Turing machines [26] and quantum finite automata [14,22] to quantum programs [24] and quantum protocols such as BB84. Quantum engineering systems developed in the future will most probably have a classical human-interactive interface and a quantum processor, and thus they will be hybrid models. Therefore, it is worth developing a theory for describing and verifying hybrid systems.

In order to describe hybrid systems that receive inputs or actions from the outer world, we propose the notion of hybrid quantum automata (HQA) that generalize semi-quantum finite automata or other models studied by Ambainis and Watrous, and Qiu etc. (see e.g. [3,5,21,30,31,29]). In fact, these automata in the mentioned references as hybrid systems have been described in a uniform way by the authors [14]. When viewing HQA as language acceptors, we show their language equivalence problem is decidable in polynomial time by transforming this problem to the equivalence problem of probabilistic automata. Furthermore, we apply this result to the trace equivalence problem of quantum Markov chains, showing the trace equivalence problem is also decidable in polynomial time.

Finally, we consider model checking linear-time properties of hybrid systems that are modeled by quantum Markov chains. We show that the quantitative analysis of regular safety properties can be addressed as done for stochastic systems, by transforming it to the reachability problem that can be addressed by determining a least solution of a system of linear equations. For general ω-regular properties, the similar technical treatments used for stochastic systems no longer take effect for our purpose, and some new techniques need to be explored in the further study.

2. Preliminaries

A Hilbert space is usually denoted by the symbol $\mathcal{H}$. $dim(\mathcal{H})$ stands for the dimension of $\mathcal{H}$. Let $\mathcal{L}(\mathcal{H})$ be the set of all linear operators from $\mathcal{H}$ to itself. A^*, $A^\dagger$ and $A^\top$ denote respectively the conjugate, the conjugate-transpose, and the transpose of operator A. The trace of A is denoted by $\mathrm{Tr}(A)$. $A \in \mathcal{L}(\mathcal{H})$ is said to be positive, denoted by $A \geq 0$, if $\langle\psi|A|\psi\rangle \geq 0$ for any $|\psi\rangle \in \mathcal{H}$. $A \geq B$ if $A - B$ is positive. Let

$$\mathcal{P}(\mathcal{H}) = \{A \in \mathcal{L}(\mathcal{H}) : A \geq 0\}.$$

Given a nonempty and countable set S, let

$$Dist_{\mathcal{H}}(S) = \{\mu : S \to \mathcal{P}(\mathcal{H}) : \sum_{s \in S} \mathrm{Tr}(\mu(s)) = 1\}.$$

Elements in $Dist_{\mathcal{H}}(S)$ are called *positive-operator valued distributions.*

The detailed background on quantum information can be referred to the textbook [19] and lecture notes [27]. Here we just introduce briefly some necessary notions. States of a quantum system are described by density operators that are positive operators having unit trace. Let

$$\mathcal{D}(\mathcal{H}) = \{A \in \mathcal{P}(\mathcal{H}) : \mathrm{Tr}(A) = 1\},$$

which denotes the set of all density operators on Hilbert space $\mathcal{H}$. An element in $\mathcal{D}(\mathcal{H})$ is generally indicated by the symbol ρ. A positive operator with trace less than 1 is called a *partial quantum state*.

A mapping $\mathcal{E}$: $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is called a *super-operator* on $\mathcal{H}$. $\mathcal{E}$ is said to be *trace-preserving* if $\mathrm{Tr}(\mathcal{E}(A)) = \mathrm{Tr}(A)$ for all $A \in \mathcal{L}(\mathcal{H})$. Let $\mathcal{I}_{\mathcal{H}}$ and $\mathbf{0}_{\mathcal{H}}$ denote the identity and zero super-operators, respectively, and if $\mathcal{H}$ is clear from the context the subscript $\mathcal{H}$ is omitted. For two super-operators $\mathcal{E}$ and $\mathcal{F}$, their summation, subtraction and multiplication, denoted by $\mathcal{E} + \mathcal{F}$, $\mathcal{E} - \mathcal{F}$ and $\mathcal{E} \circ \mathcal{F}$, respectively, are defined by

$$(\mathcal{E} + \mathcal{F})(A) = \mathcal{E}(A) + \mathcal{F}(A),$$
$$(\mathcal{E} - \mathcal{F})(A) = \mathcal{E}(A) - \mathcal{F}(A),$$
$$\mathcal{E} \circ \mathcal{F}(A) = \mathcal{E}(\mathcal{F}(A))$$

for all $A \in \mathcal{L}(\mathcal{H})$. We always omit the symbol $\circ$ and write $\mathcal{E}\mathcal{F}$ simply for $\mathcal{E} \circ \mathcal{F}$. The relation $\eqsim$ between super-operators on $\mathcal{H}$ is defined by: $\mathcal{E} \eqsim \mathcal{F}$ if $\mathrm{Tr}(\mathcal{E}(\rho)) = \mathrm{Tr}(\mathcal{F}(\rho))$ for all $\rho \in \mathcal{D}(\mathcal{H})$.