Model checking quantum Markov chains

Yuan Feng, Nengkun Yu, and Mingsheng Ying

University of Technology Sydney, Australia,
Tsinghua University, China

Model checking quantum Markov chains. *Journal of Computer and System Sciences* 79, 1181-1198, (2013)

Reachability of recursive quantum Markov chains. *Proceedings of the 38th Int. Symp. on Mathematical Foundations of Computer Science (MFCS'13)* 385-396.

UTS:QCIS
QUANTUM COMPUTATION & INTELLIGENT SYSTEMS

Outline

Outline

Motivation

- Quantum mechanics is highly counterintuitive; flaws and errors creep in during the design of quantum programs and quantum protocols.
- So, it is indispensable to develop techniques of verifying and debugging quantum systems.

Model checking

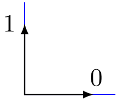
- Model-checking is one of the dominant techniques for verification of classical hardware as well as software systems.
- It has proved mature as witnessed by a large number of successful industrial applications.
- Quantum model checking???

Outline

Probability Theory v.s. Quantum Information Theory

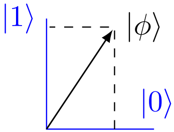
Binary Random Varable X:

$X = 0$ or $X = 1$



Quantum bit:

Unit vector in a 2D Hilbert space
$|\phi\rangle = a_0|0\rangle + a_1|1\rangle$,
$a_i \in \mathcal{C}$, $|a_0|^2 + |a_1|^2 = 1$

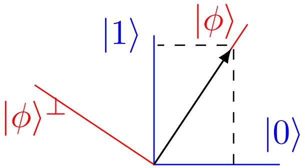


Probability Theory v.s. Quantum Information Theory

Evolution: Stochastic Matrices	Evolution: Unitary Matrices
Preserve l_1-norm $p' = S \cdot p$	Preserve l_2-norm $\lvert\phi'\rangle = U \cdot \lvert\phi\rangle$
$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(a_0 + a_1) \\ \frac{1}{\sqrt{2}}(a_0 - a_1) \end{pmatrix}$

Probability Theory v.s. Quantum Information Theory

Observation: $\Pr(X = b) = p_b$, $p_b \in [0, 1]$	**Measurement:** A measurement of $\vert\phi\rangle$ according to a Hermitian operator $M = \sum_i \lambda_i \vert b_i\rangle\langle b_i\vert$ is a projection onto the orthonormal vectors $\vert b_i\rangle$, and $\Pr[\text{outcome is } \lambda_i] = \vert\langle\phi\vert b_i\rangle\vert^2$.



Density operators

- Mixed state: Classical distribution over (pure) quantum states.

  $$\rho = \begin{cases} |\phi_1\rangle, & \texttt{with probability } p_1 \\ \vdots & \vdots \\ |\phi_k\rangle, & \texttt{with probability } p_k \end{cases}$$

  Ensemble: $\{p_i : |\phi_i\rangle\}$.
- Density operator: $\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|$ (hermitian, trace 1, positive)
  - Contains all information about the state.
  - Different ensembles can have the same density operator.

Density operators

- Different ensembles can have the same density operator.

$$\left\{ \begin{array}{lll} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \texttt{w.p.} & \frac{1}{2} \\ |0\rangle, & \texttt{w.p.} & \frac{1}{2} \end{array} \right. =$$

$$\left\{ \begin{array}{lll} \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle, & \texttt{w.p.} & \frac{1}{\sqrt{3}} \\ |0\rangle, & \texttt{w.p.} & \frac{3}{4}(1 - \frac{1}{\sqrt{3}}) \\ |1\rangle, & \texttt{w.p.} & \frac{1}{4}(1 - \frac{1}{\sqrt{3}}) \end{array} \right. = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

Super-operators and Kraus theorem

- Super-operators: (special) mapping from density operators to density operators.
- Kraus representation theorem: A map $\mathcal{E}$ is a super-operator if and only if

$$\mathcal{E}(\rho) = \sum_{i=1}^{d} E_i \rho E_i^\dagger$$

for some set of matrices $\{E_i, i = 1, \ldots, d\}$ with $\sum_i E_i^\dagger E_i \leq I$.

- Special case:
  - Unitary transformation: $\rho \to U\rho U^\dagger$
  - Measurement with outcome i: $\rho \to |b_i\rangle\langle b_i|\rho|b_i\rangle\langle b_i|$
  - Measurement with reading outcome: $\rho \to \sum_i |b_i\rangle\langle b_i|\rho|b_i\rangle\langle b_i|$

Matrix representation of super-operators

Let $\mathcal{E} = \{E_i : i \in I\}$ be a super-operator. The matrix representation of $\mathcal{E}$ is defined as

$$M_{\mathcal{E}} = \sum_{i \in I} E_i \otimes E_i^*.$$

Here the complex conjugate is taken according to the orthonormal basis $\{|k\rangle : k \in K\}$. It is easy to check that $M_{\mathcal{E}}$ is independent of the choice of orthonormal basis and the Kraus operators E_i.

Outline

Markov chains

A Markov chain (MC) is a tuple (S, P) where

- S is a countable set of states;
- $P : S \times S \to [0, 1]$ such that for each $s \in S$,

$$\sum_{t \in S} P(s, t) = 1,$$

or equivalently, $P(s, \cdot)$ is a probabilistic distribution over S.

Quantum Markov chains

(S, P)	$\Rightarrow$	$(\mathcal{H}, \mathcal{E})$
Set S	$\Rightarrow$	Hilbert space $\mathcal{H}$
Prob. distributions	$\Rightarrow$	Density operators
$P : Dist(S) \rightarrow Dist(S)$	$\Rightarrow$	$\mathcal{E} : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H})$

Obstacles for model checking quantum system

- The set of all possible *quantum* states, $\mathcal{H}$, is a continuum, even when it is finite dimensional.
- The techniques of classical model checking, which normally work for finite state spaces, cannot be applied directly.

In this talk, we propose...

- A super-operator weighted Markov chain model which aims at providing finite models for general quantum programs and quantum communication protocols.
- A quantum extension QCTL of the logic PCTL to descibe properties we are interested in for QMCs.
- An algorithm to model check logic formulas in QCTL against a QMC model.

Some more notations

Let $\mathcal{SO}(\mathcal{H})$ be the set of super-operators on $\mathcal{H}$, ranged over by $\mathcal{E}, \mathcal{F}, \cdots$.

Definition

Let $\mathcal{E}, \mathcal{F} \in \mathcal{SO}(\mathcal{H})$.

1. $\mathcal{E} \sqsubseteq \mathcal{F}$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\mathcal{F}(\rho) - \mathcal{E}(\rho)$ is positive semi-definite;
2. $\mathcal{E} \lesssim \mathcal{F}$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\mathrm{tr}(\mathcal{E}(\rho)) \leq \mathrm{tr}(\mathcal{F}(\rho))$.

Let $\eqsim$ be $\lesssim \cap \gtrsim$; it is obviously an equivalence relation.

Some notations

Let

$$\mathcal{SI}(\mathcal{H}) = \{\mathcal{E} \in \mathcal{SO}(\mathcal{H}) : \mathcal{E} \lesssim \mathcal{I}_{\mathcal{H}}\}$$

be the 'quantum' correspondence of the unit interval $[0, 1]$ for real numbers.

Quantum Markov chains

A super-operator weighted Markov chain, or quantum Markov chain (QMC), over $\mathcal{H}$ is a tuple $(S, \mathbf{Q}, AP, L)$, where

- S is a countable set of states;
- $\mathbf{Q} : S \times S \to \mathcal{SI}(\mathcal{H})$ such that for each $s \in S$, $\sum_{t \in S} \mathbf{Q}(s,t) \eqsim \mathcal{I}_{\mathcal{H}}$,
- AP is a finite set of atomic propositions;
- L is a mapping from S to 2^{AP}.

A classical Markov chain may be viewed as a degenerate quantum Markov chain in which all super-operators appear in the transition matrix have the form $p\mathcal{I}_{\mathcal{H}}$ for some $0 \leq p \leq 1$.

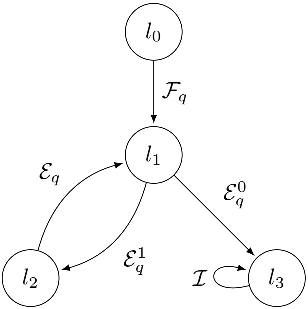
Example: quantum loop

A simple quantum loop program goes as follows:

$$\begin{array}{lcl} l_0 & : & q := \mathcal{F}(q) \\ l_1 & : & \textbf{while } M[q] \textbf{ do} \\ l_2 & : & \qquad q := \mathcal{E}(q) \\ l_3 & : & \textbf{od} \end{array}$$

where $M = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$.

Example: quantum loop



Here $\mathcal{E}_q^0 = \{|0\rangle_q\langle 0|\}$ and $\mathcal{E}_q^1 = \{|1\rangle_q\langle 1|\}$.

Outline

QCTL

The syntax of quantum computation tree logic (QCTL) is as follows:

$$
\begin{aligned}
\Phi &::= a \mid \neg\Phi \mid \Phi \wedge \Psi \mid \mathbb{Q}_{\sim\mathcal{E}}[\psi] \\
\psi &::= \mathbf{X}\Phi \mid \Phi\mathbf{U}\Psi
\end{aligned}
$$

where a is an atomic proposition, $\sim \in \{\lesssim, \gtrsim\}$, and $\mathcal{E} \in \mathcal{SI}(\mathcal{H})$. We call Φ a *state formula* and ψ a *path formula*.

QCTL

Let $\mathcal{M} = (S, \mathbf{Q}, AP, L)$. The satisfaction relation $\models$ is defined inductively: for any state $s \in S$,

$$\begin{aligned} s &\models a && \text{iff} && a \in L(s) \\ s &\models \neg\Phi && \text{iff} && s \not\models \Phi \\ s &\models \Phi \wedge \Psi && \text{iff} && s \models \Phi \text{ and } s \models \Psi \end{aligned}$$

and for any path $\pi \in Path^{\mathcal{M}}(s)$,

$$\begin{aligned} \pi &\models \mathbf{X}\Phi && \text{iff} && \pi(1) \models \Phi \\ \pi &\models \Phi\mathbf{U}\Psi && \text{iff} && \exists i \in \mathbb{N}.(\pi(i) \models \Psi \wedge \forall j < i.(\pi(j) \models \Phi)). \end{aligned}$$

QCTL

Finally,

$$s \models \mathbb{Q}_{\sim\mathcal{E}}[\psi] \text{ iff } Q^{\mathcal{M}}(s,\psi) \sim \mathcal{E}$$

where

$$Q^{\mathcal{M}}(s,\psi) = Q_s(\{\pi \in Path^{\mathcal{M}}(s) \mid \pi \models \psi\}).$$

`But how to define` Q_s?

Super-operator valued measures

Let (Ω, Σ) be a measurable space; that is, Ω is a non-empty set and Σ a σ-algebra over Ω. A function $\Delta : \Sigma \to \mathcal{SI}(\mathcal{H})$ is said to be a super-operator valued measure (SVM for short) if Δ satisfies the following properties:

1. $\Delta(\Omega) \eqsim \mathcal{I}_{\mathcal{H}}$;
2. $\Delta(\biguplus_i A_i) \eqsim \sum_i \Delta(A_i)$ for all pairwise disjoint and countable sequence A_1, A_2, ... in Ω.

We call the triple (Ω, Σ, Δ) a (super-operator valued) measure space.

Properties of super-operator valued measures

Let (Ω, Σ, Δ) be a measure space. Then

1. $\Delta(\emptyset) = 0_{\mathcal{H}}$;
2. $\Delta(A^c) + \Delta(A) \eqsim \mathcal{I}_{\mathcal{H}}$;
3. for any $A, A' \in \Sigma$, if $A \subseteq A'$ then $\Delta(A) \lesssim \Delta(A')$;
4. for any sequence $A_1, A_2, \ldots$ in Σ,
   - if $A_1 \subseteq A_2 \subseteq \ldots$, then there exists a sequence $\mathcal{E}_1 \sqsubseteq \mathcal{E}_2 \sqsubseteq \ldots$ in $\mathcal{SI}(\mathcal{H})$ such that for any i, $\Delta(A_i) \eqsim \mathcal{E}_i$, and $\Delta(\bigcup_{i\geq 1} A_i) = \lim_{i\to\infty} \mathcal{E}_i$.
   - if $A_1 \supseteq A_2 \supseteq \ldots$, then there exists a sequence $\mathcal{E}_1 \sqsupseteq \mathcal{E}_2 \sqsupseteq \ldots$ in $\mathcal{SI}(\mathcal{H})$ such that for any i, $\Delta(A_i) \eqsim \mathcal{E}_i$, and $\Delta(\bigcap_{i\geq 1} A_i) = \lim_{i\to\infty} \mathcal{E}_i$.

SVM for a QMC

Fix a state $s \in S$.

- Sample space $\Omega = Path^{\mathcal{M}}(s)$.
- Let the cylinder set $Cyl(\widehat{\pi}) \subseteq Path^{\mathcal{M}}(s)$ be defined as

$$Cyl(\widehat{\pi}) = \{\pi \in Path^{\mathcal{M}}(s) : \widehat{\pi} \text{ is a prefix of } \pi\};$$

  that is, the set of all infinite paths with prefix $\widehat{\pi}$.
- σ-algebra over Ω:

$$\Sigma^s = \sigma(\{Cyl(\widehat{\pi}) : \widehat{\pi} \in Path_{fin}^{\mathcal{M}}(s)\}$$

SVM for QMCs

- For any finite path $\widehat{\pi} = s_0 \dots s_n \in Path_{fin}^{\mathcal{M}}(s)$, we define the super-operator

$$\mathbf{Q}(\widehat{\pi}) = \begin{cases} \mathcal{I}_{\mathcal{H}}, & \text{if } n = 0; \\ \mathbf{Q}(s_{n-1}, s_n) \cdots \mathbf{Q}(s_0, s_1), & \text{otherwise.} \end{cases}$$

- Let a mapping Q_s be defined by letting $Q_s(\emptyset) = 0_{\mathcal{H}}$ and

$$Q_s(Cyl(\widehat{\pi})) = \mathbf{Q}(\widehat{\pi}). \tag{1}$$

Extend Q_s to a SVM

Theorem

The mapping Q_s can be extended to a SVM on the σ-algebra Σ^s. Furthermore, this extension is unique up to the equivalence relation $\eqsim$.

Remark: The main tool we use to prove this theorem is the Kluvanek's generalisation of the Carathéodory-Hahn extension theorem from vector measure theory.

QCTL

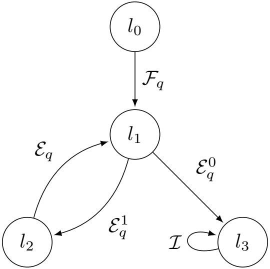
Theorem

For each path formula ψ and each state s in a QMC $\mathcal{M}$, the set

$$\{\pi \in Path^{\mathcal{M}}(s) \mid \pi \models \psi\}$$

is measurable.

Back to the example



Let $\Diamond\Psi \equiv \mathtt{tt}\mathbf{U}\Psi$. The QCTL formula $\mathbb{Q}_{\gtrsim\mathcal{E}}[\Diamond\ l_3]$ asserts that the probability that the loop program terminates is lower bounded by $\mathcal{E}$. That is, for any initial quantum state ρ, the termination probability is not less than $\mathrm{tr}(\mathcal{E}(\rho))$.

In particular, the property that it terminates everywhere can be described as $\mathbb{Q}_{\gtrsim\mathcal{I}_{\mathcal{H}}}[\Diamond\ l_3]$.

Outline

Model checking

Given a state s in a qMC $\mathcal{M} = (S, \mathbf{Q}, AP, L)$ and a state formula Φ expressed in QCTL, model checking if $s \models \Phi$ is essentially to determine whether s belongs to the satisfaction set $Sat(\Phi) = \{s \in S : s \models \Phi\}$ which is defined inductively as follows:

$$\begin{aligned}
Sat(a) &= \{s \in S : a \in L(s)\} \\
Sat(\neg\Psi) &= S \backslash Sat(\Psi) \\
Sat(\Psi \wedge \Phi) &= Sat(\Psi) \cap Sat(\Phi) \\
Sat(\mathbb{Q}_{\sim\mathcal{E}}[\psi]) &= \{s \in S : Q^{\mathcal{M}}(s, \psi) \sim \mathcal{E}\}.
\end{aligned}$$

`Recall:` $Q^{\mathcal{M}}(s, \psi) = Q_s(\{\pi \in Path^{\mathcal{M}}(s) \mid \pi \models \psi\})$

Case 1: $\psi = \mathbf{X}\Phi$

By definition, $\{\pi \in Path^{\mathcal{M}}(s) : \pi \models \mathbf{X}\Phi\} = \biguplus_{t \in Sat(\Phi)} Cyl(st)$.
Thus

$$\begin{aligned} Q^{\mathcal{M}}(s, \mathbf{X}\Phi) &= Q_s\left(\biguplus_{t \in Sat(\Phi)} Cyl(st)\right) \approx \sum_{t \in Sat(\Phi)} Q_s(Cyl(st)) \\ &= \sum_{t \in Sat(\Phi)} \mathbf{Q}(s, t). \end{aligned}$$

This can be calculated easily since by the recursive nature of the definition, we can assume that $Sat(\Phi)$ is already known.

Case 2: $\psi = \Phi \mathbf{U} \Psi$

In this case, after some calculation, we get the equation system

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \approx \begin{cases} \mathcal{I}_{\mathcal{H}}, & \text{if } s \in Sat(\Psi); \\ 0_{\mathcal{H}}, & \text{if } s \notin Sat(\Phi) \cup Sat(\Psi); \\ \sum_{t \in S} Q^{\mathcal{M}}(t, \Phi \mathbf{U} \Psi)\mathbf{Q}(s,t), & \text{if } s \in Sat(\Phi) \backslash Sat(\Psi). \end{cases}$$

Then for each $s \in Sat(\Phi) \backslash Sat(\Psi)$,

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \approx \sum_{t \in Sat(\Phi) \backslash Sat(\Psi)} Q^{\mathcal{M}}(t, \Phi \mathbf{U} \Psi)\mathbf{Q}(s,t) + \sum_{t \in Sat(\Psi)} \mathbf{Q}(s,t).$$

Let $S' = Sat(\Phi)\backslash Sat(\Psi)$. For any $s \in S'$,

$$Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi) \approx \sum_{t \in S'} Q^{\mathcal{M}}(t, \Phi \mathbf{U} \Psi)\mathbf{Q}(s, t) + \sum_{t \in Sat(\Psi)} \mathbf{Q}(s, t).$$

Let

$$\mathcal{T} = [\mathbf{Q}(t, s)]_{s, t \in S'}$$

and

$$\mathcal{G} = \left[\sum_{t \in Sat(\Psi)} \mathbf{Q}(s, t) \right]_{s \in S'}.$$

Then the required row vector $(Q^{\mathcal{M}}(s, \Phi \mathbf{U} \Psi))_{s \in S'}$ is equivalent to the fixed point of the function

$$f(X) = X\mathcal{T} + \mathcal{G}.$$

A theorem

Theorem

Let

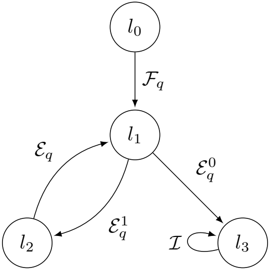
$$f(X) = X\mathcal{T} + \mathcal{G}$$

be defined above. Then

1. $f(X)$ *has the least fixed point, denoted by* $\mathcal{E}^0$, *in* $\mathcal{SI}(\mathcal{H})^{|S'|}$ *under the order* $\sqsubseteq$;
2. *Given any* $\mathcal{E} \in \mathcal{SI}(\mathcal{H})$ *and* $1 \leq i \leq |S'|$, *it can be decided whether* $\mathcal{E} \sim \mathcal{E}_i^0$, $\sim \in \{\lesssim, \gtrsim\}$, *in time* $O(n^2 d^4)$ *where* $d = dim(\mathcal{H})$ *is the dimension of* $\mathcal{H}$ *and* $n = |S'|$.

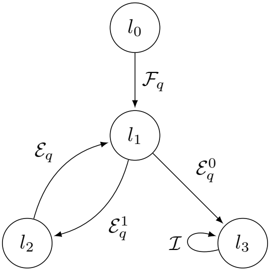
Back to the example again

We check the property $\mathbb{Q}_{\gtrsim\mathcal{E}}[\Diamond\ l_3] = \mathbb{Q}_{\gtrsim\mathcal{E}}[\mathtt{tt}\mathbf{U}l_3]$ when $\mathcal{F} = \{|+\rangle\langle i| : i = 0, 1\}$, $\mathcal{E}^i = \{|i\rangle\langle i|\}$, $i = 0, 1$, and $\mathcal{E} = \mathcal{X}$.



We first calculate that $Sat(l_3) = \{l_3\}$ and $Sat(\mathtt{tt}) = \{l_0, l_1, l_2, l_3\}$.

Back to the example again



$$
\begin{aligned}
Q^{\mathcal{M}}(l_0, \Diamond\ l_3) &= Q^{\mathcal{M}}(l_1, \Diamond\ l_3)\mathcal{F} \\
Q^{\mathcal{M}}(l_1, \Diamond\ l_3) &= Q^{\mathcal{M}}(l_2, \Diamond\ l_3)\mathcal{E}^1 + \mathcal{E}^0 \\
Q^{\mathcal{M}}(l_2, \Diamond\ l_3) &= Q^{\mathcal{M}}(l_1, \Diamond\ l_3)\mathcal{E}
\end{aligned}
$$

Example

We calculate that for $i = 0, 1, 2$,

$$Q^{\mathcal{M}}(l_i, \Diamond\ l_3) = Set^0$$

where $Set^0 = \{|0\rangle\langle 0|, |0\rangle\langle 1|\} \approx \mathcal{I}$, and so

$$l_i \models \mathbb{Q}_{\gtrsim \mathcal{E}}[\Diamond\ l_3]$$

for any $\mathcal{E} \lesssim \mathcal{I}$.

Outline

Summary

- A super-operator weighted Markov chain model which aims at providing finite models for general quantum programs and quantum communication protocols.
- A quantum extension QCTL of the logic PCTL to descibe properties we are interested in for QMCs.
- An algorithm to model check logic formulas in QCTL against a QMC model.

Topics for further studies

- Tools to implement the model checking algorithm.
- Model checking quantum properties.
- Check security of physically implemented quantum cryptographic systems.

Thank you!

Questions or Comments?