Foundations of Quantum Programming

Lecture 6: Model-Checking Quantum Systems

Mingsheng Ying

University of Technology Sydney, Australia

Outline

Quantum Graph Theory
- Basic Definitions
- Bottom Strongly Connected Components
- Decomposition of the State Hilbert Space

Reachability Analysis of Quantum Markov Chains

Outline

Quantum Graph Theory
- Basic Definitions
- Bottom Strongly Connected Components
- Decomposition of the State Hilbert Space

Reachability Analysis of Quantum Markov Chains

Quantum Markov Chains

- A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, where:

Quantum Markov Chains

- A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, where:
  1. $\mathcal{H}$ is a finite-dimensional Hilbert space;

Quantum Markov Chains

- A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, where:
  1. $\mathcal{H}$ is a finite-dimensional Hilbert space;
  2. $\mathcal{E}$ is a quantum operation (or super-operator) in $\mathcal{H}$.

Quantum Markov Chains

- A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, where:
  1. $\mathcal{H}$ is a finite-dimensional Hilbert space;
  2. $\mathcal{E}$ is a quantum operation (or super-operator) in $\mathcal{H}$.
- Behaviour of a quantum Markov chain: if currently the process is in a mixed state ρ, then it will be in state $\mathcal{E}(\rho)$ in the next step.

Quantum Markov Chains

- A quantum Markov chain is a pair $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$, where:
  1. $\mathcal{H}$ is a finite-dimensional Hilbert space;
  2. $\mathcal{E}$ is a quantum operation (or super-operator) in $\mathcal{H}$.
- Behaviour of a quantum Markov chain: if currently the process is in a mixed state ρ, then it will be in state $\mathcal{E}(\rho)$ in the next step.
- A quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$ is a discrete-time quantum system of which the state space is $\mathcal{H}$ and the dynamics is described by quantum operation $\mathcal{E}$.

Notations

- $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{H}$; that is, positive operators ρ with trace $tr(\rho) \leq 1$.

Notations

- $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{H}$; that is, positive operators ρ with trace $tr(\rho) \leq 1$.
- For any subset X of $\mathcal{H}$, $spanX$ is the subspace of $\mathcal{H}$ spanned by X; that is, it consists of all finite linear combinations of vectors in X.

Notations

- $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{H}$; that is, positive operators ρ with trace $tr(\rho) \leq 1$.
- For any subset X of $\mathcal{H}$, $spanX$ is the subspace of $\mathcal{H}$ spanned by X; that is, it consists of all finite linear combinations of vectors in X.
- The support $supp(\rho)$ of $\rho \in \mathcal{D}(\mathcal{H})$ is the subspace of $\mathcal{H}$ spanned by the eigenvectors of ρ with non-zero eigenvalues.

Notations

- $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{H}$; that is, positive operators ρ with trace $tr(\rho) \leq 1$.
- For any subset X of $\mathcal{H}$, $spanX$ is the subspace of $\mathcal{H}$ spanned by X; that is, it consists of all finite linear combinations of vectors in X.
- The support $supp(\rho)$ of $\rho \in \mathcal{D}(\mathcal{H})$ is the subspace of $\mathcal{H}$ spanned by the eigenvectors of ρ with non-zero eigenvalues.
- Let $\{X_k\}$ be a family of subspaces of $\mathcal{H}$. Then the join of $\{X_k\}$ is

$$\bigvee_k X_k = span\left(\bigcup_k X_k\right).$$

Notations

- $\mathcal{D}(\mathcal{H})$ is the set of partial density operators in $\mathcal{H}$; that is, positive operators ρ with trace $tr(\rho) \leq 1$.
- For any subset X of $\mathcal{H}$, $spanX$ is the subspace of $\mathcal{H}$ spanned by X; that is, it consists of all finite linear combinations of vectors in X.
- The support $supp(\rho)$ of $\rho \in \mathcal{D}(\mathcal{H})$ is the subspace of $\mathcal{H}$ spanned by the eigenvectors of ρ with non-zero eigenvalues.
- Let $\{X_k\}$ be a family of subspaces of $\mathcal{H}$. Then the join of $\{X_k\}$ is

$$\bigvee_k X_k = span\left(\bigcup_k X_k\right).$$

- The image of a subspace X of $\mathcal{H}$ under a quantum operation $\mathcal{E}$ is

$$\mathcal{E}(X) = \bigvee_{|\psi\rangle \in X} supp(\mathcal{E}(|\psi\rangle\langle\psi|)).$$

Proposition

1. If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;

Proposition

1. If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;
2. $supp(\rho + \sigma) = supp(\rho) \vee supp(\sigma)$;

Proposition

1. If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;
2. $supp(\rho + \sigma) = supp(\rho) \vee supp(\sigma)$;
3. If $\mathcal{E}$ has the Kraus operator-sum representation $\mathcal{E} = \sum_{i \in I} E_i \circ E_i^\dagger$, then
$$\mathcal{E}(X) = span\{E_i|\psi\rangle : i \in I \text{ and } |\psi\rangle \in X\};$$

Proposition

1. If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;
2. $supp(\rho + \sigma) = supp(\rho) \vee supp(\sigma)$;
3. If $\mathcal{E}$ has the Kraus operator-sum representation $\mathcal{E} = \sum_{i\in I} E_i \circ E_i^\dagger$, then
$$\mathcal{E}(X) = span\{E_i|\psi\rangle : i \in I \text{ and } |\psi\rangle \in X\};$$
4. $\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$. Thus, $X \subseteq Y \Rightarrow \mathcal{E}(X) \subseteq \mathcal{E}(Y)$;

Proposition

1. If $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ where all $\lambda_k > 0$ (but $|\psi_k\rangle$'s are not required to be pairwise orthogonal), then $supp(\rho) = span\{|\psi_k\rangle\}$;
2. $supp(\rho + \sigma) = supp(\rho) \vee supp(\sigma)$;
3. If $\mathcal{E}$ has the Kraus operator-sum representation $\mathcal{E} = \sum_{i \in I} E_i \circ E_i^\dagger$, then
$$\mathcal{E}(X) = span\{E_i|\psi\rangle : i \in I \text{ and } |\psi\rangle \in X\};$$
4. $\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$. Thus, $X \subseteq Y \Rightarrow \mathcal{E}(X) \subseteq \mathcal{E}(Y)$;
5. $\mathcal{E}(supp(\rho)) = supp(\mathcal{E}(\rho))$.

Adjacency Relation

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ be pure states and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ be mixed states in $\mathcal{H}$. Then

1. $|\varphi\rangle$ is adjacent to $|\psi\rangle$ in $\mathcal{C}$, written $|\psi\rangle \rightarrow |\varphi\rangle$, if $|\varphi\rangle \in supp(\mathcal{E}(|\psi\rangle\langle\psi|))$.

Adjacency Relation

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ be pure states and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ be mixed states in $\mathcal{H}$. Then

1. $|\varphi\rangle$ is adjacent to $|\psi\rangle$ in $\mathcal{C}$, written $|\psi\rangle \to |\varphi\rangle$, if $|\varphi\rangle \in supp(\mathcal{E}(|\psi\rangle\langle\psi|))$.
2. $|\varphi\rangle$ is adjacent to ρ, written $\rho \to |\varphi\rangle$, if $|\varphi\rangle \in \mathcal{E}(supp(\rho))$.

Adjacency Relation

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ be pure states and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ be mixed states in $\mathcal{H}$. Then

1. $|\varphi\rangle$ is adjacent to $|\psi\rangle$ in $\mathcal{C}$, written $|\psi\rangle \rightarrow |\varphi\rangle$, if $|\varphi\rangle \in supp(\mathcal{E}(|\psi\rangle\langle\psi|))$.
2. $|\varphi\rangle$ is adjacent to ρ, written $\rho \rightarrow |\varphi\rangle$, if $|\varphi\rangle \in \mathcal{E}(supp(\rho))$.
3. σ is adjacent to ρ, written $\rho \rightarrow \sigma$, if $supp(\sigma) \subseteq \mathcal{E}(supp(\rho))$.

Reachability

1. A path from ρ to σ in a quantum Markov chain $\mathcal{C}$ is a sequence

$$\pi = \rho_0 \to \rho_1 \to \cdots \to \rho_n \ (n \geq 0)$$

of adjacent density operators in $\mathcal{C}$ such that $supp(\rho_0) \subseteq supp(\rho)$ and $\rho_n = \sigma$.

Reachability

1. A path from ρ to σ in a quantum Markov chain $\mathcal{C}$ is a sequence

$$\pi = \rho_0 \rightarrow \rho_1 \rightarrow \cdots \rightarrow \rho_n \ (n \geq 0)$$

   of adjacent density operators in $\mathcal{C}$ such that $supp(\rho_0) \subseteq supp(\rho)$ and $\rho_n = \sigma$.
2. For any density operators ρ and σ, if there is a path from ρ to σ then σ is reachable from ρ in $\mathcal{C}$.

Reachable Space

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. For any $\rho \in \mathcal{D}(\mathcal{H})$, its reachable space in $\mathcal{C}$ is:

$$\mathcal{R}_{\mathcal{C}}(\rho) = span\{|\psi\rangle \in \mathcal{H} : |\psi\rangle \text{ is reachable from } \rho \text{ in } \mathcal{C}\}.$$

Transitivity of Reachability

For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, if $supp(\rho) \subseteq \mathcal{R}_\mathcal{C}(\sigma)$, then $\mathcal{R}_\mathcal{C}(\rho) \subseteq \mathcal{R}_\mathcal{C}(\sigma)$.

Theorem

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. If $d = \dim \mathcal{H}$, then for any $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$\mathcal{R}_\mathcal{C}(\rho) = \bigvee_{i=0}^{d-1} supp\left(\mathcal{E}^i(\rho)\right)$$

where $\mathcal{E}^i$ is the ith power of $\mathcal{E}$; that is, $\mathcal{E}^0 = \mathcal{I}$ and $\mathcal{E}^{i+1} = \mathcal{E} \circ \mathcal{E}^i$ for $i \geq 0$.

Strong Connectivity

- Let X be a subspace of $\mathcal{H}$ and $\mathcal{E}$ a quantum operation in $\mathcal{H}$. Then the restriction of $\mathcal{E}$ on X is defined by

$$\mathcal{E}_X(\rho) = P_X \mathcal{E}(\rho) P_X$$

  for all $\rho \in \mathcal{D}(X)$.

Strong Connectivity

- Let X be a subspace of $\mathcal{H}$ and $\mathcal{E}$ a quantum operation in $\mathcal{H}$. Then the restriction of $\mathcal{E}$ on X is defined by

$$\mathcal{E}_X(\rho) = P_X \mathcal{E}(\rho) P_X$$

for all $\rho \in \mathcal{D}(X)$.

- Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. A subspace X of $\mathcal{H}$ is strongly connected in $\mathcal{C}$ if for any $|\varphi\rangle, |\psi\rangle \in X$:

$$|\varphi\rangle \in \mathcal{R}_{\mathcal{C}_X}(\psi) \textit{ and } |\psi\rangle \in \mathcal{R}_{\mathcal{C}_X}(\varphi)$$

where $\varphi = |\varphi\rangle\langle\varphi|$ and $\psi = |\psi\rangle\langle\psi|$, quantum Markov chain $\mathcal{C}_X = \langle X, \mathcal{E}_X \rangle$ is the restriction of $\mathcal{C}$ on X.

Inductive Partial Order

- Let $(L, \sqsubseteq)$ be a partial order. If any two elements $x, y \in L$ are comparable; that is, either $x \sqsubseteq y$ or $y \sqsubseteq x$, then L is linearly ordered by $\sqsubseteq$.

Inductive Partial Order

- Let $(L, \sqsubseteq)$ be a partial order. If any two elements $x, y \in L$ are comparable; that is, either $x \sqsubseteq y$ or $y \sqsubseteq x$, then L is linearly ordered by $\sqsubseteq$.
- A partial order $(L, \sqsubseteq)$ is inductive if for any subset K of L that is linearly ordered by $\sqsubseteq$, the least upper bound $\bigsqcup K$ exists in L.

Lemm

Write $SC(\mathcal{C})$ for the set of all strongly connected subspaces of $\mathcal{H}$ in $\mathcal{C}$. Then partial order $(SC(\mathcal{C}), \subseteq)$ is inductive.

Zorn Lemma

Every inductive partial order has (at least one) maximal elements.

Zorn Lemma

Every inductive partial order has (at least one) maximal elements.

Strongly Connected Components

A maximal element of $(SC(\mathcal{C}), \subseteq)$ is a strongly connected component (SCC) of $\mathcal{C}$.

Zorn Lemma

Every inductive partial order has (at least one) maximal elements.

Strongly Connected Components

A maximal element of $(SC(\mathcal{C}), \subseteq)$ is a strongly connected component (SCC) of $\mathcal{C}$.

Invariants

A subspace X of $\mathcal{H}$ is invariant under a quantum operation $\mathcal{E}$ if $\mathcal{E}(X) \subseteq X$.

Zorn Lemma

Every inductive partial order has (at least one) maximal elements.

Strongly Connected Components

A maximal element of $(SC(\mathcal{C}), \subseteq)$ is a strongly connected component (SCC) of $\mathcal{C}$.

Invariants

A subspace X of $\mathcal{H}$ is invariant under a quantum operation $\mathcal{E}$ if $\mathcal{E}(X) \subseteq X$.

Theorem

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. If subspace X of $\mathcal{H}$ is invariant under $\mathcal{E}$, then:

$$tr(P_X \mathcal{E}(\rho)) \geq tr(P_X \rho)$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Bottom Strongly Connected Components

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then a subspace X of $\mathcal{H}$ is a bottom strongly connected component (BSCC) of $\mathcal{C}$ if it is an SCC of $\mathcal{C}$ and it is invariant under $\mathcal{E}$.

Bottom Strongly Connected Components

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then a subspace X of $\mathcal{H}$ is a bottom strongly connected component (BSCC) of $\mathcal{C}$ if it is an SCC of $\mathcal{C}$ and it is invariant under $\mathcal{E}$.

Characterisations of BSCCs, I

A subspace X is a BSCC of quantum Markov chain $\mathcal{C}$ if and only if $\mathcal{R}_{\mathcal{C}}(|\varphi\rangle\langle\varphi|) = X$ for any $|\varphi\rangle \in X$.

Characterisations of BSCCs, II

- A density operator ρ in $\mathcal{H}$ is a fixed point state of quantum operation $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.

Characterisations of BSCCs, II

- A density operator ρ in $\mathcal{H}$ is a fixed point state of quantum operation $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.
- A fixed point state ρ of quantum operation $\mathcal{E}$ is minimal if for any fixed point state σ of $\mathcal{E}$, $supp(\sigma) \subseteq supp(\rho)$ implies $\sigma = \rho$.

Characterisations of BSCCs, II

- A density operator ρ in $\mathcal{H}$ is a fixed point state of quantum operation $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.
- A fixed point state ρ of quantum operation $\mathcal{E}$ is minimal if for any fixed point state σ of $\mathcal{E}$, $supp(\sigma) \subseteq supp(\rho)$ implies $\sigma = \rho$.
- If ρ is a fixed point state of $\mathcal{E}$, then $supp(\rho)$ is invariant under $\mathcal{E}$. Conversely, if X is invariant under $\mathcal{E}$, then there exists a fixed point state ρ_X of $\mathcal{E}$ such that $supp(\rho_X) \subseteq X$.

Characterisations of BSCCs, II

- A density operator ρ in $\mathcal{H}$ is a fixed point state of quantum operation $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$.
- A fixed point state ρ of quantum operation $\mathcal{E}$ is minimal if for any fixed point state σ of $\mathcal{E}$, $supp(\sigma) \subseteq supp(\rho)$ implies $\sigma = \rho$.
- If ρ is a fixed point state of $\mathcal{E}$, then $supp(\rho)$ is invariant under $\mathcal{E}$. Conversely, if X is invariant under $\mathcal{E}$, then there exists a fixed point state ρ_X of $\mathcal{E}$ such that $supp(\rho_X) \subseteq X$.
- A subspace X is a BSCC of quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ if and only if there exists a minimal fixed point state ρ of $\mathcal{E}$ such that $supp(\rho) = X$.

Lemma

1. For any two different BSCCs X and Y of quantum Markov chain $\mathcal{C}$: $X \cap Y = \{0\}$ (0-dimensional Hilbert space).

Lemma

1. For any two different BSCCs X and Y of quantum Markov chain $\mathcal{C}$: $X \cap Y = \{0\}$ (0-dimensional Hilbert space).
2. If X and Y are two BSCCs of $\mathcal{C}$ with $\dim X \neq \dim Y$, then they are orthogonal: $X \perp Y$.

Transient Subspaces

A subspace $X \subseteq \mathcal{H}$ is transient in a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ if

$$\lim_{k \to \infty} tr\left(P_X \mathcal{E}^k(\rho)\right) = 0$$

for any $\rho \in \mathcal{D}(\mathcal{H})$.

Transient Subspaces

A subspace $X \subseteq \mathcal{H}$ is transient in a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ if

$$\lim_{k \to \infty} tr\left(P_X \mathcal{E}^k(\rho)\right) = 0$$

for any $\rho \in \mathcal{D}(\mathcal{H})$.

Asymptotic Average

Let $\mathcal{E}$ be a quantum operation in $\mathcal{H}$. Then its asymptotic average is

$$\mathcal{E}_\infty = \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}^n.$$

Lemma

1. For any density operator ρ, $\mathcal{E}_\infty(\rho)$ is a fixed point state of $\mathcal{E}$;

Lemma

1. For any density operator ρ, $\mathcal{E}_\infty(\rho)$ is a fixed point state of $\mathcal{E}$;
2. For any fixed point state σ: $supp(\sigma) \subseteq \mathcal{E}_\infty(\mathcal{H})$.

Theorem - Largest Transient Subspace

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then

$$T_\mathcal{E} = \mathcal{E}_\infty(\mathcal{H})^\perp$$

is the largest transient subspace in $\mathcal{C}$, where $^\perp$ stands for orthocomplement.

Lemma

Let ρ and σ be two fixed point state of $\mathcal{E}$, $supp(\sigma) \subsetneq supp(\rho)$. Then there exists another fixed point state η such that

1. $supp(\eta) \bot supp(\sigma)$; and

Lemma

Let ρ and σ be two fixed point state of $\mathcal{E}$, $supp(\sigma) \subsetneq supp(\rho)$. Then there exists another fixed point state η such that

1. $supp(\eta) \perp supp(\sigma)$; and
2. $supp(\rho) = supp(\eta) \oplus supp(\sigma)$.

Theorem - BSCC Decomposition

Lemma

Let ρ and σ be two fixed point state of $\mathcal{E}$, $supp(\sigma) \subsetneq supp(\rho)$. Then there exists another fixed point state η such that

1. $supp(\eta) \bot supp(\sigma)$; and
2. $supp(\rho) = supp(\eta) \oplus supp(\sigma)$.

Theorem - BSCC Decomposition

- Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then $\mathcal{E}_\infty(\mathcal{H})$ can be decomposed into the direct sum of orthogonal BSCCs of $\mathcal{C}$.

Lemma

Let ρ and σ be two fixed point state of $\mathcal{E}$, $supp(\sigma) \subsetneq supp(\rho)$. Then there exists another fixed point state η such that

1. $supp(\eta) \perp supp(\sigma)$; and
2. $supp(\rho) = supp(\eta) \oplus supp(\sigma)$.

Theorem - BSCC Decomposition

- Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain. Then $\mathcal{E}_\infty(\mathcal{H})$ can be decomposed into the direct sum of orthogonal BSCCs of $\mathcal{C}$.
- The Hilbert space of a quantum Markov chain $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ can be decomposed into:

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}}$$

where B_i's are orthogonal BSCCs of $\mathcal{C}$, $T_{\mathcal{E}}$ is the largest transient subspace.

Theorem - (Weak) Uniqueness of BSCC Decomposition

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain,

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} = D_1 \oplus \cdots \oplus D_v \oplus T_{\mathcal{E}}$$

be two BSCC decompositions, B_is and D_is are arranged, respectively, according to the increasing order of the dimensions. Then

1. $u = v$; and

Theorem - (Weak) Uniqueness of BSCC Decomposition

Let $\mathcal{C} = \langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain,

$$\mathcal{H} = B_1 \oplus \cdots \oplus B_u \oplus T_{\mathcal{E}} = D_1 \oplus \cdots \oplus D_v \oplus T_{\mathcal{E}}$$

be two BSCC decompositions, B_is and D_is are arranged, respectively, according to the increasing order of the dimensions. Then

1. $u = v$; and
2. $\dim B_i = \dim D_i$ for each $1 \leq i \leq u$.

Theorem - Decomposition Algorithm

Given a quantum Markov chain $\langle \mathcal{H}, \mathcal{E} \rangle$, Algorithm QDECOM decomposes the Hilbert space $\mathcal{H}$ into the direct sum of a family of orthogonal BSCCs and a transient subspace of $\mathcal{C}$ in time $O(d^8)$, where $d = \dim \mathcal{H}$.

Outline

Quantum Graph Theory
Basic Definitions
Bottom Strongly Connected Components
Decomposition of the State Hilbert Space

Reachability Analysis of Quantum Markov Chains

Reachability Probability

Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$ an initial state, and $X \subseteq \mathcal{H}$ a subspace. Then the probability of reaching X, starting from ρ, is

$$\Pr(\rho \vDash \Diamond X) = \lim_{i \to \infty} tr\left(P_X \widetilde{\mathcal{E}}^i(\rho)\right)$$

where $\widetilde{\mathcal{E}}^i$ is the composition of i copies of $\widetilde{\mathcal{E}}$, and $\widetilde{\mathcal{E}}$ is the quantum operation defined by

$$\widetilde{\mathcal{E}}(\sigma) = P_X \sigma P_X + \mathcal{E}\left(P_{X^\perp} \sigma P_{X^\perp}\right)$$

for all density operator σ.

Lemma

Let $\{B_i\}$ be a BSCC decomposition of $\mathcal{E}_\infty(\mathcal{H})$, P_{B_i} the projection onto B_i. Then for each i, we have

$$\lim_{k\to\infty} tr\left(P_{B_i}\mathcal{E}^k(\rho)\right) = tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right)$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Lemma

Let $\{B_i\}$ be a BSCC decomposition of $\mathcal{E}_\infty(\mathcal{H})$, P_{B_i} the projection onto B_i. Then for each i, we have

$$\lim_{k\to\infty} tr\left(P_{B_i}\mathcal{E}^k(\rho)\right) = tr\left(P_{B_i}\mathcal{E}_\infty(\rho)\right)$$

for all $\rho \in \mathcal{D}(\mathcal{H})$.

Theorem - Computing Reachability Probability

Let $\langle \mathcal{H}, \mathcal{E} \rangle$ be a quantum Markov chain, $\rho \in \mathcal{D}(\mathcal{H})$, $X \subseteq \mathcal{H}$ a subspace. Then

$$\Pr(\rho \models \Diamond X) = tr\left(P_X \widetilde{\mathcal{E}}_\infty(\rho)\right),$$

and this probability can be computed in time $O(d^8)$ where $d = \dim(\mathcal{H})$.