量子马尔可夫链安全性模型检测

林运国[1,2],雷红轩[3],李永明[1]
(1.陕西师范大学计算机科学学院,陕西西安 710119;2.福建农林大学计算机与信息学院,福建福州 350002;
3.内江师范学院数学与信息科学学院,四川内江 641112)

摘 要: 本文定义了量子线性时间属性,包括量子安全性,量子不变性,讨论了它们的关系和性质.结合测量一次、测量多次的单向量子有穷自动机,构建了两类乘积量子马尔可夫链,提出了基于自动机技术的量子正则安全性检测方法.通过验证乘积量子马尔可夫链的可达终状态来判断量子正则安全性的可满足性,并给出了可满足性的概率计算公式.作为应用,分析了广义量子 loop 程序,将程序终止归结为验证量子正则安全性的可满足性.

关键词: 量子马尔可夫链; 模型检测; 安全性; 量子有穷自动机; 广义量子 loop 程序
中图分类号: TP301.6 **文献标识码:** A **文章编号:** 0372-2112 (2014)11-2191-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.11.010

Model Checking of Safety Property over Quantum Markov Chain

LIN Yun-guo[1,2], LEI Hong-xuan[3], LI Yong-ming[1]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*;
2. *College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou, Fujian* 350002, *China*;
3. *School of Mathematics and Information Science, Neijiang Normal University, Neijiang, Sichuan* 641112, *China*)

Abstract: Quantum linear time property is defined, including quantum safety property, quantum invariant which their relationships and properties are studied. Together with measure-one and measure many one way quantum finite automata, two kinds of the product quantum markov chains are constructed, the checking method of quantum regular propertyis provided based on automaton technique. This method shows the satisfaction of quantum regular safety is decided by the reachable termination verification of the product quantum markov chain, and thecomputation formula of satisfaction probability is given. As an application example, the generalized quantum loop program is analyzed. It shows the termination of program is turned into the satisfaction for the verification of quantum regular safety property.

Key words: quantum Markov chain; model checking; safety property; quantum finite automata; generalized quantum loop program

1 引言

量子计算起源于量子力学和计算机科学,是一门发展 20 多年的新兴交叉学科.一旦量子计算机研制成功,量子软件的开发将成为实现量子计算机功能的核心,而量子程序设计的理论和实现则是其中一项重要的课题.程序验证是保证程序正确性的关键技术,模型检测则是验证的理论方法[1].对于量子通信协议、量子程序等量子系统,研究它们的属性检测技术是有意义的[2~7].文献[2~5]研究了量子通信协议的模型检测器,给出了量子计算树逻辑的检测算法.文献[5]介绍了在 Exogenous 环境下,构造量子计算树逻辑并提出了检测算法.文献[6]利用量子自动机对量子系统进行建模,用 Hilbert 的闭子空间表示原子命题,建立了量子线性时间属性,提出了基于自动机的属性检测算法.

量子马尔可夫链用来描述量子系统的动态演化[8,9],其中量子游走是一类特殊的量子马尔可夫链,已经成功应用于设计和分析量子算法[10].文献[11]定义了量子马尔可夫链,它适合于量子密钥协议等,其中量子效应被编码为超算子用来标签状态转移,状态采用经典逻辑来刻画,最后提出了检测算法.该量子马尔可夫链的模型检测是概率计算树逻辑的量子推广.文献

收稿日期:2014-01-06;修回日期:2014-05-08;责任编辑:马兰英
基金项目:国家自然科学基金(No.11271237,No.61228305);高等学校博士学科点专项科研基金(No.20130202110001,No.20130202120002);中央高校基本科研业务费专项资金(No.GK201302054)

[12]利用 Bottom 强连通分支(BSCC)和算子渐近平均值提出了计算量子马尔可夫链的可达性、重复可达性、一致可达性概率的方法.目前量子马尔可夫链线性时间属性还未得到充分研究,特别是量子安全性和量子不变性的检测,开展这方面工作是有意义的.借助于量子自动机技术,本文研究了量子正则安全性的检测.

2 基本概念

设一个由有穷量子比特所构成的量子命题变元集 $qB=\{qb_1,qb_2,\cdots,qb_n\}$,给定一个由赋值集 2^{qB} 张成的 Hilbert 空间 $H_{qB}:=span\{|v\rangle|v\in 2^{qB}\}$. qB 上的任意一个子集 A 都有惟一基向量与之一一对应,当 $qb\in A$ 时,赋值为真;当 $qb\notin A$ 时,赋值为假.对于任意一个 $v\in 2^{qB}$,引入一个量子命题公式短语 φ_v,该短语是由量子命题和否定量子命题的合取来表示.每个短语 φ_v 与 2^{qB} 中的元素一一对应.进一步任意 $X\subseteq 2^{qB}$,给定一个量子析取范式 Φ_X,它由短语析取构成量子命题公式 $\vee\varphi_v$,其中 $v\in X$.令 $AP=\{\varphi_v|v\in 2^{qB}\}$,$2^{AP}=\{\Phi_X|X\subseteq 2^{qB}\}$.

相关量子计算和模型检测的概念和符号规定详见文献[1,13].

3 量子马尔可夫链及线性时间属性

设 $\rho\in D(H_{qB})$表示 Hilbert 空间上的所有密度算子的集合.

定义 1 一个量子马尔可夫链(简写为 QMC)是一个五元组 $M=<H_{qB},\varepsilon,l_{init},AP,L>$,其中:(1)$\varepsilon$ 是量子运算;(2)$l_{init}\subseteq H_{qB}$是量子初态的子空间;(3)$L:D(H_{qB})\to 2^{AP}$称为标签函数.

设任意 $\rho\in D(H_{qB})$,$L(\rho)\in 2^{AP}$使得 $supp(\rho)=span\{L(\rho)\}$,其中 $supp(\rho)$表示密度算子 ρ 的非零特征值对应的特征向量生成的本征空间.

设任意 $\rho,\rho'\in D(H_{qB})$,若 $supp(\rho')\subseteq supp(\varepsilon(\rho))$,则称 ρ 可达 ρ',记为 $\rho\to\rho'$. $\pi=\rho_0\to\rho_1\to\cdots$表示为从量子初态 ρ_0 出发的一条无穷路径,$\hat{\pi}=\rho_0\to\rho_1\to\cdots\to\rho_n$ 表示为从量子初态 ρ_0 出发的一条有穷路径. $Paths(\rho_0)$($\widehat{Paths}(\rho_0)$)是所有从 ρ_0 出发的无穷(有穷)路径集合.任意 $\pi\in Paths(\rho_0)$,迹 $trace(\pi)=L(\rho_0)L(\rho_1)\cdots$,类似有 $trace(\hat{\pi})$;从 ρ_0 出发所有无穷、有穷迹记为:$Traces(\rho_0)=\bigcup_{\pi\in Paths(\rho_0)}\{trace(\pi)\}$,$Traces_{fin}(\rho_0)=\bigcup_{\hat{\pi}\in Paths(\rho_0)}\{trace(\hat{\pi})\}$.$(2^{AP})^*$、$(2^{AP})^\omega$ 表示所有的有穷迹、无穷迹的集合.

定义 2 若 P 是$(2^{AP})^\omega$ 的一个子集,则称 P 是一个量子线性时间属性.

若任意 $\sigma=X_1X_2\cdots\in P$,则称 $\hat{\sigma}=X_1X_2\cdots X_n$ 为 σ 的一个前缀. σ 所有前缀记为 $Pref(\sigma)$, P 所有前缀集 $Pref(P)=\bigcup_{\sigma\in P}Pref(\sigma)$.任意 $\hat{\sigma}=X_1X_2\cdots X_n\in Pref(\sigma)$,$\hat{\sigma}$ 的闭集为 $closure(\hat{\sigma})=\{X_1'X_2'\cdots X_n'|X_i'\subseteq X_i,\forall i\in\{1,2,\cdots,n\}\}$;$Pref(\sigma)$的闭集为 $closure(Pref(\sigma))=\bigcup_{\hat{\sigma}\in Pref(\sigma)}closure(\hat{\sigma})$;$Pref(P)$的闭集为 $closure(Pref(P))=\bigcup_{\sigma\in P}closure(Pref(\sigma))$;$\sigma$ 的闭集为 $closure(\sigma)=\{\sigma'\in(2^{AP})^\omega|Pref(\sigma')\subseteq closure(Pref(\sigma))\}$; P 的闭集为 $closure(P)=\bigcup_{\sigma\in P}closure(\sigma)$.

设任意一个量子初态 $\rho\in D(H_{qB})$和一个量子线性时间属性 P,若 $Traces(\rho)\subseteq P$,则称 ρ 逻辑可满足 P,记为 $\rho|=P$.

定义 3 若存在一个子空间 $X\subseteq H_{qB}$使得 $P_{inv}=\{X_0X_1\cdots\in(2^{AP})^\omega|\forall i\geq 0,X_i\subseteq X\}$,则称量子线性时间属性 P_{inv}是一个量子不变性,X 称为量子线性时间属性 P_{inv}的不变性条件.

定义 4 设 $P_{safe}\subseteq(2^{AP})^\omega$,对于任意的 $\sigma\in(2^{AP})^\omega\setminus P_{safe}$,若存在一个 σ 的前缀$\hat{\sigma}$ 使得$P_{safe}\cap\{\sigma'\in(2^{AP})^\omega|\hat{\sigma}\in closure(\hat{\sigma}')\}=\varnothing$,则称量子线性时间属性 P_{safe}是一个量子安全性,$\hat{\sigma}$ 为 P_{safe}一个坏前缀.

所有坏前缀集记为 $BadPref(P_{safe})$,所有长度最短坏前缀集记为 $MBadPref(P_{safe})$.若 $\hat{\sigma}$ 为P_{safe}的坏前缀,则 $closure(\hat{\sigma})\subseteq BadPref(P_{safe})$.

引理 1 设 P_{safe}是一个量子线性时间属性,那么 P_{safe}是一个量子安全性当且仅当 $closure(P_{safe})=P_{safe}$.

证明 充分性.由于 $closure(P_{safe})=P_{safe}$,对任意 $\sigma\in(2^{AP})^\omega\setminus P_{safe}$,有 $\sigma\notin P_{safe}$,故 $\sigma\notin closure(P_{safe})$.任意 $\sigma'\in P_{safe}$,不存在一个 $\hat{\sigma}\in Pref(\sigma)$使得 $\hat{\sigma}'\in closure(\hat{\sigma})$,所以 P_{safe}是一个量子安全性.

必要性 P_{safe}是量子安全性及 $P_{safe}\subseteq closure(P_{safe})$,可知当 $closure(P_{safe})=P_{safe}$成立,则有 $closure(P_{safe})\subseteq P_{safe}$.采用反证法.假设存在 $\sigma\in closure(P_{safe})\setminus P_{safe}$,因 P_{safe}是一个量子安全性,所以存在 $\hat{\sigma}\in Pref(\sigma)$使得 $\hat{\sigma}\in BadPref(P_{safe})$和 $closure(\hat{\sigma})\in BadPref(P_{safe})$.因为 $\sigma\in closure(P_{safe})$,有 $Pref(\sigma)\in closure(Pref(P_{safe}))$成立,所以 $closure(Pref(\sigma))\in closure(Pref(P_{safe}))$,即 $closure(\hat{\sigma})\in closure(Pref(P_{safe}))$,故 $BadPref(P_{safe})\cap Pref(P_{safe})\neq\varnothing$和 $BadPref(P_{safe})\cap closure(Pref(P_{safe}))\neq\varnothing$.产生矛盾.上式 $closure(P_{safe})\subseteq P_{safe}$成立.故结论成立.

定理 1 $\rho|=P_{safe}$当且仅当 $Traces_{fin}(\rho)\cap MBadPref(P_{safe})=\varnothing$.

证明 充分性.采用反证法.如果 $Traces_{fin}(\rho)\cap MBadPref(P_{safe})=\varnothing$成立,而 $\rho|\neq P_{safe}$,也就是 $Traces(\rho)\not\subseteq P_{safe}$,则存在 $\sigma\in Traces(\rho)$且 $\sigma\notin P_{safe}$,因而 $\hat{\sigma}\in MBadPref(P_{safe})$和 $\hat{\sigma}\in Traces_{fin}(\rho)$,故 $Traces_{fin}(\rho)\cap MBadPref(P_{safe})\neq\varnothing$.因而产生矛盾,则 $Traces(\rho)\subseteq$

P_{safe},即 $\rho_{\mid} = P_{safe}$.

必要性　反证法.如果 $\rho_{\mid} = P_{safe}$ 成立,而 $Traces_{fin}(\rho) \cap MBadPref(P_{safe}) \neq \varnothing$,那么存在 $\hat{\sigma} \in MBadPref(P_{safe})$ 且 $\hat{\sigma} \in Traces_{fin}(\rho)$;进一步存在一个 σ 使得 $\sigma \in Traces(\rho)$ 和 $\sigma \notin closure(P_{safe})$,$\rho_{\mid} \neq closure(P_{safe})$.根据引理 1 得 $closure(P_{safe}) = P_{safe}$,所以 $\rho_{\mid} \neq P_{safe}$.这与假设相矛盾,则 $Traces_{fin}(\rho) \cap MBadPref(P_{safe}) = \varnothing$ 成立.

定理 2　设 P_{inv} 是一个量子不变性,那么 P_{inv} 是一个量子安全性.

4　量子正则安全性及其模型检测

4.1　量子有穷自动机与量子正则安全性

经典马尔可夫链的安全性检测是基于自动机技术,可将这一思想运用到量子马尔可夫链的安全性检测.首先给出量子有穷自动机[14-16],将所有坏前缀能被量子有穷自动机接受的量子安全性称为量子正则安全性;其次构造出乘积量子马尔可夫链;最后研究了量子正则安全性的可满足性与乘积量子马尔可夫链可达空间的关系.

4.1.1　测量多次的单向量子有穷自动机

定义 5[15,16]　测量多次的单向量子有穷自动机是一个五元组 MM-1QFA

$$A = < Q, \Sigma, \Delta, \mid q_0\rangle; Q_{acc}, Q_{rej}, \#, \$ >,$$

其中(1)Q 为有穷状态集;(2)Σ 为有穷输入字母表,#、$ 不属于 Σ 分别是开始标记符和结束标记符,记 $\Gamma = \Sigma \cup \{\#, \$\}$;(3)$Q_{acc}, Q_{rej} \subseteq Q(Q_{acc} \cap Q_{rej} = \varphi)$ 分别是接受状态集和拒绝状态集,统称为终止状态集;(4)$\Delta: \Gamma \to U$ 是状态转移函数;(5)$\mid q_0\rangle (q_0 \in Q)$ 是量子初态.

$\mid Q \mid = n$ 表示自动机 A 有 n 个状态.在任意时刻自动机所处的状态均以叠加态形式出现.称 $Q_{non} = Q \setminus (Q_{acc} \cup Q_{rej})$ 为非终止状态集.状态转移函数 $\Delta: \Gamma \to U$,它对任意 $\omega \in \Gamma$ 指定一个酉矩阵 $\Delta(\omega)$,即 $\forall \omega \in \Gamma$,$\Delta(\omega) \in U$ 是一个酉矩阵 U_ω.设 H_A 是一个 Hilbert 空间,令 $H_A = E^A_{acc} \oplus E^A_{rej} \oplus E^A_{non}$,其中接受本征空间 $E^A_{acc} = span\{\mid q\rangle \mid q \in Q_{acc}\}$,拒绝本征空间 $E^A_{rej} = span\{\mid q\rangle \mid q \in Q_{rej}\}$,非终止本征空间 $E^A_{non} = \overline{E^A_{acc} \oplus E^A_{rej}}$ 是 $E^A_{acc} \oplus E^A_{rej}$ 的正交补.设 $x \in \{E^A_{acc}, E^A_{rej}, E^A_{non}\}$,$P^A_x$ 表示到特征值为 acc,rej,non 的接受本征空间 E^A_x 的投影算子.$O = \{P_{E^A_{acc}}, P_{E^A_{rej}}, P_{E^A_{non}}\}$ 表示可观测量.

设一个状态转移函数 Δ 和一个线性算子 $\delta: Q \times \Gamma \times Q \to C_{[0,1]}$,任意 $x \in \Gamma$,$\Delta(x) \mid q\rangle = \sum_{q' \in Q} \delta(q, x, q') \mid q'\rangle = \sum_{\mid q'\rangle \in E^A_{acc}} \delta(q, x, q') \mid q'\rangle + \sum_{\mid q'\rangle \in E^A_{rej}} \delta(q, x, q') \mid q'\rangle + \sum_{\mid q'\rangle \in E^A_{non}} \delta(q, x, q') \mid q'\rangle$,$\delta(q, x, q')$ 是 $\mid q'\rangle$ 的概率振幅.

给定一个初态 q_0 和输入字符串 $\# \omega_1\omega_2\cdots\omega_n \$ \in \Sigma^*$.MM-1QFA 从量子初态 $\mid q_0\rangle$(或 $\rho_0 = \mid q_0\rangle\langle q_0 \mid$)出发,将 $\Delta_\#$ 作用在量子态 ρ_0,得到变换后量子态 $\rho_1 = U_\# \rho_0 U^\dagger_\#$,接着 O 作用在 ρ_1 上,以概率 $tr(P_{E^A_i}\rho_1)$ 得到测量结果 $i \in \{acc, rej, non\}$ 且量子态演化为 $\rho_1' = P_{E^A_i}\rho_1 (P_{E^A_i})^\dagger / tr(P_{E^A_i}\rho_1)$.假如 $i = acc$,那么字符 # 被自动机接受;假如 $i = rej$,那么字符 # 被自动机拒绝;假如 $j = non$,那么经过正规化后的量子态 ρ_1' 进一步使用酉变换 Δ_{ω_1},得到量子态为 $\rho_2 = U_{\omega_1} U_\# \rho_1' (U_{\omega_1} U_\#)^\dagger$,再进行 O 的测量计算,得到量子态 $\rho_2' = P_{E^A_i}\rho_1 (P_{E^A_i})^\dagger / tr(P_{E^A_i}\rho_1)$.重复该计算过程,每次酉变换后都进行一次测量.可知当且仅当量子态属于 E^A_{non} 时,继续下一步计算.整个非终止计算过程可表示为:$\hat{U}_\$ \hat{U}_{\omega_n} \cdots \hat{U}_{\omega_1} \hat{U}_\# \mid q_0\rangle$,其中 $\hat{U}_{\omega_i} = P_{x_i} U_{\omega_i}$,$x_i \in \{E^A_{acc}, E^A_{rej}, E^A_{non}\}$,$i \in \{1, 2, \cdots, n\}$.

定义 6　测量多次的单向量子有穷自动机所接受语言称为 MM-1 量子正则语言,称坏前缀被 MM-1 量子自动机接受的量子安全性 P_{safe} 为 MM-1 量子正则安全性.

4.1.2　测量一次的单向量子有穷自动机

定义 7[15,16]　测量一次的单向量子有穷自动机是一个五元组 MO-1QFA

$$A = < Q, \Sigma, \Delta, q_0, Q_{acc} >,$$

其中(1)Q 为有穷状态集,$\mid Q \mid = n$ 表示 n 个状态;(2)Σ 为有穷输入字母表;(3)$\Delta: \Sigma \to U$ 是任意 $\omega \in \Sigma$ 指定一个酉矩阵 $\Delta(\omega)$;(4)$\mid q_0\rangle (q_0 \in Q)$ 是量子初态;(5)$Q_{acc} \subseteq Q$ 是接受状态集.

称 $Q_{rej} = Q \setminus Q_{acc}$ 为拒绝状态集;$E^A_{acc} = span\{\mid q_i\rangle \mid q_i \in Q_{acc}\}$,$E^A_{rej} = span\{\mid q_i\rangle \mid q_i \in Q_{rej}\}$ 分别表示接受本征空间和拒绝本征空间.设 H_A 是一个 Hilbert 空间,$H_A = E^A_{acc} \oplus E^A_{rej}$,$\{\mid q_i\rangle \mid q_i \in Q\}$ 是 H_A 的一组标准正交基.根据量子力学假设,量子有穷自动机在任意 t 时刻所处的状态以叠加态形式出现:$\mid \psi\rangle_t = \sum_i a_i \mid q_i\rangle$,对应密度算子表示为 $\rho_t = \sum_i \mid a_i \mid^2 \mid q_i\rangle\langle q_i \mid$,其中 $\sum_i \mid a_i \mid^2 = 1$.

设一个测量一次的单向量子有穷自动机,给定输入字符串 $\omega = \omega_1\omega_2\cdots\omega_n \in \Sigma^*$,自动机从量子初态 $\mid q_0\rangle$($\rho_0 = \mid q_0\rangle\langle q_0 \mid$)出发.在第 i 步计算过程中,自动机读入字符 ω_i,通过酉变换 $U_{\omega_i} = \Delta(\omega_i)$,密度算子 ρ_{i-1} 发生演化.记 U_ω 表示自动机读入字符串 ω 后使量子态发生演化的酉变换,即 $U_\omega = U_{\omega_n} U_{\omega_{n-1}} \cdots U_{\omega_1}$.自动机读完该字符串后,得到量子终态 $\rho_n = U_\omega \mid q_0\rangle\langle q_0 \mid U^\dagger_\omega$.将 $U_\omega \mid q_0\rangle\langle q_0 \mid U^\dagger_\omega$ 记号为 $\eta_\omega(\rho_0)$.该字符串被接受的概率为 $tr(P_{E^A_{acc}} U_\omega \rho_0 U^\dagger_\omega)$,其中 $P_{E^A_{acc}}$ 是本征空间 E^A_{acc} 上的投影算子.

定义 8　测量一次的单向量子有穷自动机所接受的

语言称为 MO-1 量子正则语言,称坏前缀被 MO-1 量子自动机接受的量子安全性 P_{safe}是 MO-1 量子正则安全性.

4.2 量子正则安全性模型检测

给定一个量子马尔可夫链 $M=<H_{qB},\varepsilon,l_{init},AP,L>$和 MM-1(或 MO-1)量子正则安全性 P_{safe},下面给出从量子初态出发 MM-1(MO-1)量子正则安全性 P_{safe}可满足性的检测方法.

4.2.1 MM-1 量子正则安全性模型检测

定义 9 设 $M=<H_{qB},\varepsilon,l_{init},qB,L>$是一个量子马尔可夫链,$A=<Q,\Sigma,\Delta,|q_0\rangle;\ Q_{acc},Q_{rej},\#,\$>$是一个测量多次的单向量子有穷自动机,MM-1 乘积量子马尔可夫链定义为:

$$M\otimes A=<H'_{qB},\varepsilon',l'_{init},\{accept\},L'>.$$

其中:(1)$H'_{qB}=H_{qB}\otimes H_A$.

(2) $l'_{init}=l_{init}\otimes\bigvee\limits_{\rho_0^M\in l_{init}}supp(U_{L(\varepsilon(\rho_0^M))}|q_0\rangle\langle q_0|(U_{L(\varepsilon(\rho_0^M))})^{\dagger})$.

(3) $\forall\rho^M\in D(H_{qB})$, $\rho^A\in D(H_A)$, $succ(\rho^A,L(\varepsilon(\rho^M)))$是 ρ^A 的后继,

$$\varepsilon'(\rho^M\otimes\rho^A)=\begin{cases}\varepsilon(\rho^M)\otimes\eta'(\rho^A), & succ(\rho^A,L(\varepsilon(\rho^M)))\neq\varnothing\\ 0, & \text{其他}\end{cases},$$

$\eta'(\rho^A)=\eta_{L(\varepsilon(\rho^M))}(\rho^A)=(P_x^AU_\omega)\rho^A(P_x^AU_\omega)^{\dagger}$, $\omega=L(\varepsilon(\rho^M))$, $x\in\{E^A_{acc},E^A_{rej},E^A_{non}\}$.

(4) *accept* 表示本征空间 $E^{M\otimes A}_{accept}$对应的特征值,其中 $E^{M\otimes A}_{accept}=supp(\{\rho^M\otimes\rho^A|L'(\rho^M\otimes\rho^A)=\{accept\},\rho^A\in E^A_{acc}\})$.

(5)若 $\rho^A\in E^A_{acc}$, $L'(\rho^M\otimes\rho^A)=\{accept\}$;否则 $L'(\rho^M\otimes\rho^A)=\varnothing$.

$\varepsilon'=\varepsilon\otimes\eta'$是一个量子运算,$E^{M\otimes A}_{accept}$为两个本征空间的张量积 $E^{M\otimes A}_{accept}=I^M\otimes E^A_{acc}$, $P_{E^{M\otimes A}_{accept}}=I^M\otimes P_{E^A_{acc}}$表示到特征值为 *accept* 的本征空间 $E^{M\otimes A}_{accept}$的投影算子.

定义 10 设一个乘积马尔可夫链 $M\otimes A=<H_{qB}\otimes Q,\varepsilon',l'_{init},\{accept\},L'>$,定义量子转移算子 $\tilde{\varepsilon}'$如下:

$$\tilde{\varepsilon}'=(I^M\otimes I^A)\circ(I^M\otimes P_{E^A_{acc}})+(\varepsilon\otimes\eta')\circ(I^M\otimes P_{E^A_{rej}})+(\varepsilon\otimes\eta')\circ(I^M\otimes P_{E^A_{non}})$$

$\tilde{\varepsilon}'$解释如下:通过可观测量 O 的测量,量子自动机所处的量子态 ρ^A_{i-1}将以一定的概率进入其中一个的本征空间 E^A_{acc}, E^A_{rej}, E^A_{non},量子态演化为$(\rho^A_{i-1})'$.如果$(\rho^A_{i-1})'\in E^A_{acc}$,读入字符将被量子自动机所接受并且用 I^A 表示量子自动机进入下一步计算,同时对应在量子马尔可夫链中用 I^M 表示量子态演化为吸收态;如果$(\rho^A_{i-1})'\in E^A_{rej}$,读入字符将被拒绝,计算过程将中止,用算子 O 表示量子自动机计算中止;如果$(\rho^A_{i-1})'\in E^A_{non}$,量子自动机将继续计算,同时量子马尔可夫链中的量子态也将进一步演化.

当$(\rho^A_{i-1})'\in E^A_{acc}$,量子转移算子 $\tilde{\varepsilon}'$简化为:

$$(I^M\otimes I^A)\circ(I^M\otimes P_{E^M_{acc}})+(\varepsilon\otimes\eta')\circ(I^M\otimes P_{E^A_{non}})$$

设 $M\otimes A=<H_{qB}\otimes Q,\varepsilon',l'_{init},\{accept\},L'>$, $\rho_0^M\otimes\rho_1^A\in l'_{init}$,其中 $\rho_1^A=(P_{E^A_{non}}U_{L(\varepsilon(\rho_0^M))})|q_0\rangle\langle q_0|(P_{E^A_{non}}U_{L(\varepsilon(\rho_0^M))})^{\dagger}$,从 $\rho_0^M\otimes\rho_1^A$ 出发到达可达空间 $E^{M\otimes A}_{accept}$的概率按下式计算:

$$\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A|=\diamondsuit E^{M\otimes A}_{accept})=tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'_\infty(\rho_0^M\otimes\rho_1^A))$$

其中:(1)$\tilde{\varepsilon}'=(I^M\otimes I^A)\circ(I^M\otimes P_{E^A_{acc}})+(\varepsilon\otimes\eta')\circ(I^M\otimes P_{E^A_{non}})$;(2)$\tilde{\varepsilon}'^i=\tilde{\varepsilon}'^{i-1}\tilde{\varepsilon}'$,量子转移算子的渐近平均值 $\tilde{\varepsilon}'_\infty=\lim\limits_{N\to\infty}\frac{1}{N}\sum\limits_{n=1}^{N}\tilde{\varepsilon}'^n$;(3)可达空间 $E^{M\otimes A}_{accept}$具有不变性,$tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'^i(\rho_0^M\otimes\rho_1^A))$单调增加;(4)$\lim\limits_{i\to\infty}tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'^i(\rho_0^M\otimes\rho_1^A))=tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'_\infty(\rho_0^M\otimes\rho_1^A))$[12].

定理 3 $\Pr^M(\rho_0^M\vdash P_{safe})=\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\not\models\diamondsuit E^{M\otimes A}_{accept})=1-\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\vdash\diamondsuit E^{M\otimes A}_{accept})$,其中 $\rho_1^A=(P_{E^A_{non}}U_{L(\varepsilon(\rho_0^M))})|q_0\rangle\langle q_0|(P_{E^A_{non}}U_{L(\varepsilon(\rho_0^M))})^{\dagger}$.

证明 由于 $\rho_0^M\vdash P_{safe}$当且仅当 $Traces_{fin}(\rho_0^M)\cap MBadPref(P_{safe})=\varnothing$,故 $\forall\hat{\pi}=\rho_0^M\to\rho_1^M\to\cdots\to\rho_{n-1}^M$使得 $supp(\rho^M)\subseteq l_{init}$,且 $\hat{\sigma}=L(\hat{\pi})=L(\rho_0^M)L(\rho_1^M)\cdots L(\rho_{n-1}^M)\notin MBadPref(P_{safe})=L(A)$. $L(A)$是被 MM-1QFA 所接受的.

对于乘积量子马尔可夫链 $M\otimes A$,存在一个状态序列 $\rho_0^A,\rho_1^A,\cdots,\rho_n^A\in H_A$ 使得 $\rho_0^A\xrightarrow[\#]{P_{E^A_{non}}U_{L(\rho_0^M)}}\rho_1^A\xrightarrow[\omega_1]{P_{x_1}U_{L(\rho_1^M)}}\rho_2^A\cdots\xrightarrow[\omega_{n-1}]{P_{x_{n-1}}U_{L(\rho_{n-1}^M)}}\rho_n^A$,其中 $\omega_i=L(\rho_i)$, $x_i\in\{E^A_{acc},E^A_{rej},E^A_{non}\}$, $i\in\{0,1,\cdots,n-1\}$.由于 $\rho_n^A\notin E^A_{acc}$,则 $\#\omega_1\cdots\omega_{n-1}$是不被自动机所接受的.对于 $\rho_0^M\otimes\rho_1^A\to\rho_1^M\otimes\rho_2^A\to\rho_2^M\otimes\rho_3^A\cdots\to\rho_{n-1}^M\otimes\rho_n^A$, $L'(\rho_{n-1}^M\otimes\rho_n^A)\neq\{accept\}$, $\rho_{n-1}^M\otimes\rho_n^A\notin E^{M\otimes A}_{accept}$,即 $\rho_0^M\otimes\rho_1^A|\neq\diamondsuit E^{M\otimes A}_{accept}$.故$\Pr^M(\rho_0^M\vdash P_{safe})=\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\not\models\diamondsuit E^{M\otimes A}_{accept})=1-\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\vdash\diamondsuit E^{M\otimes A}_{accept})$.结论成立.

该定理表明计算从量子初态出发的量子正则安全性的可满足概率可以等价归结为求乘积量子马尔可夫链的可达空间的概率.再根据量子态的 Bottom 强连通分支分解和渐近平均值 $\varepsilon'_\infty=\lim\limits_{N\to\infty}\frac{1}{N}\sum\limits_{n=1}^{N}\varepsilon'^n$[12],量子马尔可夫链的量子正则安全性可满足概率为:$1-tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'_\infty(\rho_0^M\otimes\rho_1^A))$.

4.2.2 MO-1 量子正则安全性模型检测

定义 11 设 $M=<H_{qB},\varepsilon,l_{init},AP,L>$是一个量子

马尔可夫链,$A=<Q,\Sigma,\Delta,|q_0\rangle,Q_{acc}>$是一个测量一次的单向量子有穷自动机,MO-1 乘积量子马尔可夫链定义为:$M\otimes A=<H'_{qB},\varepsilon',l'_{init},\{accept\},L'>$,其中:

(1)$H'_{qB}=H_{qB}\otimes H_A$.

(2)$l'_{init}=l_{init}\otimes\bigvee_{\rho_0^M\in l_{init}}supp(U_{L(\varepsilon(\rho_0^M))}|q_0\rangle\langle q_0|(U_{L(\varepsilon(\rho_0^M))})^\dagger)$.

(3)$\forall\rho^M\in D(H_{qB}),\rho^A\in D(H_A),succ(\rho^A,L(\varepsilon(\rho^M)))$是$\rho^A$的后继,

$$\varepsilon'(\rho^M\otimes\rho^A)=\begin{cases}\varepsilon(\rho^M)\otimes\eta'(\rho^A), & succ(\rho^A,L(\varepsilon(\rho^M)))\neq\varnothing\\ 0, & \text{其他}\end{cases}$$

此处$\eta'(\rho^A)=\eta_{L(\varepsilon(\rho^M))}(\rho^A)=U_\omega\rho^AU_\omega^\dagger,\omega=L(\varepsilon(\rho^M))$.

(4)$\{accept\}$表示本征空间$E^{M\otimes A}_{accept}$对应的特征值,其中$E^{M\otimes A}_{accept}=supp(\{\rho^M\otimes\rho^A|L'(\rho^M\otimes\rho^A)=\{accept\},\rho^A\in E^A_{acc}\})$.

(5)若$\rho^A\in E^A_{acc},L'(\rho^M\otimes\rho^A)=\{accept\}$;否则$L'(\rho^M\otimes\rho^A)=\varnothing$.

其中$E^{M\otimes A}_{accept}$为两个本征空间的张量积$E^{M\otimes A}_{accept}=I^M\otimes E^A_{acc}$,$P_{E^{M\otimes A}_{accept}}=I^M\otimes P_{E^A_{acc}}$表示到 *accept* 的本征空间$E^{M\otimes A}_{accept}$的投影算子.

定义 12　设一个乘积马尔可夫链$M\otimes A=<H_{qB}\otimes Q,\varepsilon',l'_{init},\{accept\},L'>$,　定义量子转移算子$\tilde{\varepsilon}'$如下:$\tilde{\varepsilon}'=(I^M\otimes I^A)\circ(I^M\otimes P_{E^A_{acc}})+(\varepsilon\otimes\eta')\circ(I^M\otimes P_{E^A_{rej}})$.

设$M\otimes A=<H_{qB}\otimes Q,\varepsilon',l'_{init},\{accept\},L'>,\rho_0^M\otimes\rho_1^A\in l'_{init},\rho_1^A=U_{L(\varepsilon(\rho_0^M))}|q_0\rangle\langle q_0|U^\dagger_{L(\varepsilon(\rho_0^M))}$,

从$\rho_0^M\otimes\rho_1^A$出发的可达空间$E^{M\otimes A}_{accept}$概率为:$\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\models\Diamond E^{M\otimes A}_{accept})=\lim_{i\to\infty}tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'^i(\rho_0^M\otimes\rho_1^A))=tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'_\infty(\rho_0^M\otimes\rho_1^A))$.

定义 11 和定义 12 相关规定和解释相似于 MM-1 乘积量子马尔可夫链.

定理 4　$\Pr^M(\rho_0^M\models P_{safe})=\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\models\Diamond E^{M\otimes A}_{accept})=1-\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\models\Diamond E^{M\otimes A}_{accept})$,其中$\rho_1^A=U_{L(\varepsilon(\rho_0^M))}|q_0\rangle\langle q_0|U^\dagger_{L(\varepsilon(\rho_0^M))}$.

证明　因为$\rho_0^M\models P_{safe}$当且仅当$Traces_{fin}(\rho_0^M)\cap MBadPref(P_{safe})=\varnothing$,故$\forall\hat{\pi}=\rho_0^M\to\rho_1^M\to\cdots\to\rho_{n-1}^M$使得$supp(\rho_0^M)\subseteq l_{init}$,且$\hat{\sigma}=L(\hat{\pi})=L(\rho_0^M)L(\rho_1^M)\cdots L(\rho_{n-1}^M)\notin MBadPref(P_{safe})=L(A)$. $L(A)$是被 MO-1QFA 所接受.

对于乘积量子马尔可夫链$M\otimes A$,存在状态序列$\rho_0^A,\rho_1^A,\cdots,\rho_n^A\in H_A$使得$\rho_0^A\xrightarrow[\omega_0]{U_{L(\rho_0^M)}}\rho_1^A\xrightarrow[\omega_1]{U_{L(\rho_1^M)}}\rho_2^A\xrightarrow{U_{L(\rho_{n-1}^M)}}\rho_n^A$,其中$\omega_i=L(\rho_i^M),i\in\{0,1,2,\cdots,n-1\}$.

由于$\rho_n^A\notin E^A_{acc}$,字符串$\omega_0\omega_1\cdots\omega_{n-1}$是不被自动机所接受的.对于$\rho_0^M\otimes\rho_1^A\to\rho_1^M\otimes\rho_2^A\to\rho_1^M\otimes\rho_2^A\to\rho_2^M\otimes\rho_3^A\cdots\to\rho_{n-1}^M\otimes\rho_n^A$,有$L'(\rho_{n-1}^M\otimes\rho_n^A)\neq\{accept\},\rho_{n-1}^M\otimes\rho_n^A\notin E^{M\otimes A}_{accept}$,即$\rho_0^M\otimes\rho_1^A\not\models\Diamond E^{M\otimes A}_{accept}$,故$\Pr^M(\rho_0^M\models P_{safe})=\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\not\models\Diamond E^{M\otimes A}_{accept})=1-\Pr^{M\otimes A}(\rho_0^M\otimes\rho_1^A\models\Diamond E^{M\otimes A}_{accept})$,因而$\Pr^M(\rho_0^M\models P_{safe})=1-tr(P_{E^{M\otimes A}_{accept}}\tilde{\varepsilon}'_\infty(\rho_0^M\otimes\rho_1^A))$.结论成立.

5　广义量子 loop 程序的终止问题

按照 Selinger[17]的观点,一个量子程序由超算子描述.文献[18]中给出了主体是酉运算的量子 loop 程序以及程序终止、几乎终止的定义,并给出了程序终止、几乎终止的充要条件.文献[19]中给出了在单量子比特空间上分别对广义量子 loop 程序(简记为 GQLoop)主体由比特翻转、去极化、幅值阻尼、相位阻尼等信道描述时,GQLoop 终止(或几乎终止)问题进行研究.

5.1　GQLoop 的量子马尔可夫链表示

假设有一个包含有 n 个量子系统$q_1,q_2,\cdots q_n$的量子寄存器,并且对于每个 $i\leqslant n$,q_i 的状态空间是H_i,ε是 Hilbert 空间H_{qB}上的一个量子运算,$\tilde{M}=\sum_m mP_m$是H_{qB}上可观测量.对于任意的$X\subseteq spec(\tilde{M})$,广义量子 loop 程序由$\varepsilon,\tilde{M}$和$X$定义为

$$while(\tilde{M}[\bar{q}]\in X)\{\bar{q}:=\varepsilon(\bar{q})\}\qquad(1)$$

其中$\bar{q}$表示$q_1,q_2,\cdots q_n$.设$P_X=\sum_{m\in X}P_m,P_{\bar{X}}=I_{H_{qB}}-P_X=\sum_{m\in spec(\tilde{M})-X}P_m$,$I_{H_{qB}}$是$H_{qB}$上的单位算子,测量算子$P_X$和$P_{\bar{X}}$可分别称为"yes-no"测量.式子(1)的控制部分"$\tilde{M}\in X$"表示投影测量P_X和$P_{\bar{X}}$在$\bar{q}$上的作用.GQLoop 的工作方式和计算过程见图 1 和图 2,其中$\rho_{in}^{(n)}$为输入态,$\rho_{mid}^{(n)},p_{NT}^{(n)}(\rho)$分别表示不终止的量子态和概率,$\rho_{out}^{(n)},p_T^{(n)}(\rho)$分别表示终止的量子态和概率.

广义量子 loop 程序是一个量子马尔可夫链,分析表明程序终止问题恰好对应了量子马尔可夫链的安全性问题,因而可以将终止的验证归结为检测量子安全性的可满足性.

设一个广义量子 loop 程序,输入态是$\rho_0\in D(H_{qB})$,算子$\tilde{M}=\sum_m mP_m(m=0,1)$是$H_{qB}$上的可观测量,测量算子$P_0=|0\rangle\langle0|,P_1=|1\rangle\langle1|$对应程序中"yes-no",$\varepsilon_0$为量子运算.该广义量子 loop 程序对应量子马尔可夫链表示为$M=<H_{qB},\varepsilon,l_{init},AP,L>$,其中$qB=\{qb\}$,$H_{qB}=span\{|0\rangle,|1\rangle\}$;量子运算$\varepsilon$如图 3;$l_{init}=supp(\rho_0)$;标签函数$L(l_{01})=\{\varphi_0,\varphi_1\},L(l_0)=\{\varphi_0\},L(l_1)$

$=\{\varphi_1\}$.字符 φ_0,φ_1 分别对应"yes-no"测量结果.结合图1和图3,GQLoop 在输入态 ρ_0 上不终止的情形相当于量子马尔可夫链从初态 l_{init} 出发进入到状态 l_{01} 后无穷多次访问状态 l_0.因而计算广义量子 loop 程序在输入态 ρ_0 上不终止的概率可以归结为计算量子马尔可夫链从初态 l_{init} 出发无穷多次访问状态 l_0 的概率,它等价于量子安全性$(\{\varphi_0\})^\omega$ 在量子马尔可夫链中可满足的概率.

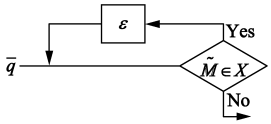

图1 GQLoop的工作方式

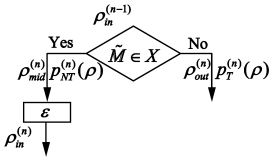

图2 GQLoop的计算过程

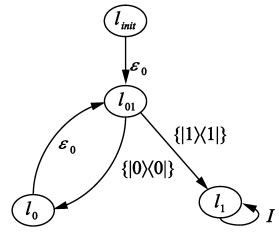

图3 GQLoop的量子马尔可夫链表示

5.2 GQLoop 的终止验证

设 $P_{safe}=(\{\varphi_0\})^\omega$ 是量子正则安全性,其坏前缀$(\{\varphi_0\})^*\{\varphi_1\}$被测量一次的单向量子有穷自动机 $A=<Q,\Sigma,\Delta,|q_0\rangle,Q_{acc}>$所接受,其中 $Q=\{0,1\}$;有穷输入字母表 $\Sigma=\{\varphi_0,\varphi_1,\varphi_0\vee\varphi_1\}$;$\Delta:\Sigma\to U$;$|q_0\rangle=|0\rangle$,$|q_1\rangle=|1\rangle$;$Q_{acc}=\{1\}$,$E_{acc}^A=span\{|1\rangle\}$.字符串 $\omega=(\{\varphi_0\})^*\{\varphi_1\}$以概率 $tr(P_{E_{acc}^A}U_\omega|q_0\rangle\langle q_0|U_\omega^\dagger)$被量子有穷自动机所接受.

由于广义量子 loop 程序在输入态 ρ_0 上不终止的概率归结为求量子正则安全性的可满足概率 $\Pr^M(\rho_0|=P_{safe})$,根据定理3,它等价于计算 $1-tr(P_{E_{accept}^{M\otimes A}}\tilde{\varepsilon}'_\infty(\tilde{\varepsilon}'(\rho_0^M\otimes\rho_1^A)))$.具体求解过程如下:

(1)首先构造乘积量子马尔可夫链:$M\otimes A=<H_{qB}\otimes Q,\varepsilon',l'_{init},\{accept\},L'>$,其中 $\varepsilon'=\varepsilon\otimes U_\omega=\varepsilon_0\circ P_0\otimes U_\omega,\varepsilon_0\circ P_0=\varepsilon_0(P_0\rho^M P_0/tr(P_0\rho^M P_0))$;$U_\omega(\rho^A)=\sum_{i=1}^{2}E_{iA}\rho^A E_{iA}^\dagger,\omega=L(\varepsilon_0\circ P_0(\rho_0^M))$;令 $E_{1A}=\sqrt{p}I$,$E_{2A}=\sqrt{(1-p)}X$,其中 $p=tr(P_0(\varepsilon_0\circ P_0(\rho^M))P_0^\dagger)$;$l'_{init}=supp(\rho_0\otimes\rho_1^A)$,$\rho_0=|0\rangle\langle 0|$.$\rho_0^A=|0\rangle\langle 0|$,$L(\rho_0^M)=\varphi_1$,$\rho_1^A=U_{\varphi_1}|0\rangle\langle 0|U_{\varphi_1}^\dagger=|0\rangle\langle 0|$,所以 $\rho_0^M\otimes\rho_1^A=|0\rangle\langle 0|\otimes|0\rangle\langle 0|$.

(2)计算 $\tilde{\varepsilon}'_\infty(|0\rangle\langle 0|\otimes|0\rangle\langle 0|)=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\tilde{\varepsilon}'^n(|0\rangle\langle 0|\otimes|0\rangle\langle 0|)$,其中 $\tilde{\varepsilon}'=(I^M\otimes I^A)\circ(I^M\otimes P_{E_{acc}^A})+(\varepsilon_0\circ P_0\otimes U_{L(\varepsilon_0\circ P_0(\rho^M))})\circ(I^M\otimes P_{E_{rej}^A})$.利用迭代计算出 $\tilde{\varepsilon}'^n(|0\rangle\langle 0|\otimes|0\rangle\langle 0|)=\frac{1}{2}I\otimes\sum_{k=1}^{n-1}\frac{1}{2^k}|1\rangle\langle 1|+\frac{1}{2}I\otimes\frac{1}{2^N}I$.

(3)计算 $tr(P_{E_{accept}^{M\otimes A}}\tilde{\varepsilon}'_\infty(\tilde{\varepsilon}'(\rho_0\otimes\rho_1^A)))=tr((|01\rangle\langle 01|+|11\rangle\langle 11|)(\frac{1}{2}I\otimes|1\rangle\langle 1|))=1$,因而 $\Pr^M(\rho_0\vdash P_{safe})=1-tr(P_{E_{accept}^{M\otimes A}}\tilde{\varepsilon}'_\infty(\tilde{\varepsilon}'(\rho_0\otimes\rho_1^A)))=0$.

根据上式计算从量子初态 ρ_0 出发量子正则安全性可满足的概率为0,即广义量子 loop 程序在输入态 ρ_0 上是几乎终止的.

6 结论

本文研究了量子马尔可夫链的安全性检测.引入了量子马尔可夫链,定义了量子线性时间属性等相关概念,重点研究了量子马尔可夫链的安全性,给出了相关性质.基于测量一次、测量多次的单向量子有穷自动机,构造了量子有穷自动机和量子马尔可夫链的乘积系统,建立了量子正则安全性检测方法,给出了可满足性的概率计算公式.表明了若乘积系统终状态是可达的,则量子正则安全性是不可满足的,反之量子正则安全性则可满足.作为应用,研究了广义量子 loop 程序终止问题.由于广义量子 loop 程序是量子马尔可夫链,将终止问题看作是量子马尔可夫链的线性时间属性,把程序是否终止归结为量子正则安全性的可满足性,最后给出了终止的判定过程.在此基础上,今后将给出量子安全性检测的实际应用,特别深入研究各种复杂的广义量子 loop 程序的终止判定.

参考文献

[1] C Baier, J P Katoen. Principles of Model Checking[M]. Cambridge, Massachusetts: MIT Press, 2008.

[2] Papanikolaou, Nikolaos K. Model checking quantum protocols [D]. Coventry, England: the War wick University, 2009.

[3] E Ardeshir Larijani, S J Gay, R Nagarajan. Equivalence checking of quantum protocols[A]. Proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems[C]. Heidelberg: Springer, 2013, 7795: 466 – 480.

[4] T Davidson, S J Gay, H Mlnarik, R Nagarajan, N. Papanikolaou. Model checking forcommunicating quantum processes[J]. International Journal of Unconventional Computing, 2012, 8(1): 73 – 98.

[5] P Baltazar, R Chadha, P Mateus. Quantum computation tree logic

model checking andcomplete calculus[J]. International Journal of Quantum Information,2008,6(2):281 – 302.

[6] M S Ying,Y J Li,N K Yu,Y Feng. Model checking linear time properties of quan tum systems[DB/O L]. http://arXiv. org/abs/Quant-ph/arXiv:1101.0303,2010.

[7] 雷红轩,席政军,李永明.量子最弱自由前置条件的交换性及其性质[J].软件学报,2013,24(5):933 – 941.
H X Lei,Z J Xi,Y M Li. Commutativity of quantum weakest liberal precondition and its properties[J]. Journal of Software,2013,24(5):933 – 941.(in Chinese)

[8] Jaroslav Novotny,Gernot Alber,Igor Jex. Asymptotic properties of quantum mark ovchains[DB/OL]. http://arXiv. org/math-ph/arXiv:1208.0764,2012.

[9] Stan Gudder. Quantum markov chains. Journal of Mathematical Physics[J].2008,49(7):072105.

[10] Andris Ambainis. Quantum walks and their algorithmic applications [DB/OL]. http://arXiv. org/quant-ph/arXiv:0403120v3,2006.

[11] Y Feng,N K Yu,M S Ying. Model checking quantum markov chains[DB/OL]. http://arXiv. org/abs /Quant-ph/arXiv:1205.2187,2012.

[12] S G Ying,Y Feng,N K Yu,M S Ying. Reachability probabilities of quantum markovchains[DB /OL]. http://arXiv. org/abs/Quant-ph/arXiv:1304.0060,2013.

[13] M A Nielsen,Chuang I L. Quantum computation and quantum Information[M]. Cambridge:Canbridge University Press,2000.

[14] 李永明.基于量子逻辑的有穷自动机与单体二阶量子逻辑[J].中国科学 F 辑:信息科学,2009,39(11):1135 – 1145.
Y M Li. Finite automata based on quantum logic and monadic second-order quantum logic[J]. Science China Information Sciences,2009,39(11):1135 – 1145.(in Chinese)

[15] Ambainis,M Beaudry,M Golovkins,et al. Algebraic results on quantum automata [J]. Theory of Computing Systems,2006,39(1):165 – 188.

[16] 李绿周.量子计算模型的等价性判定及量子通信中的若干基本问题[D].广州:中山大学,2009.
L Z Li. Determination of equivalence between quantum computing models and some basic problems in quantum communication [D]. Guang Zhou:Sun Yat-Sen University,2009.(in Chinese)

[17] P Selinger. Towards a quantum programming language[J]. Mathematical Structures in Computer Science,2004,14(4):527 – 586.

[18] M S Ying,Y Feng. Quantum loop programs[J]. Acta Informatica,2010,47(4):221 – 250.

[19] 雷红轩,席政军,李永明.广义量子 loop 程序的若干性质[J].电子学报,2013,41(4):727 – 732.
H X Lei,Z J Xi,Y M Li. Some properties of generalized quantum loop program[J]. Acta Electronica Sinica,2013,41(4):727 – 732.(in Chinese)

作者简介

林运国　男,1979 年出生于福建福清,博士研究生,讲师,主要研究领域为量子程序验证和量子模型检测.
E-mail:fjaulyg@126.com

雷红轩　男,1967 年出生于陕西洋县,博士,教授,主要研究领域为量子程序验证和量子模型检测.

李永明　男,1966 年出生于陕西大荔,博士,教授,博士生导师,研究方向为计算智能、量子逻辑、量子计算、模型检测.