软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(12):2994−3002 [doi: 10.13328/j.cnki.jos.004916]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

Exogenous 量子马尔可夫链及其可达性分析*

林运国[1,2], 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)

通讯作者: 李永明, E-mail: liyongm@snnu.edu.cn

摘 要: 为了刻画开放量子系统的量子属性,扩展现有的量子马尔可夫链是有必要的.通过构建 Exogenous 量子算子逻辑,定义了 Exogenous 量子马尔可夫链.作为新型量子马尔可夫链,重点研究了 4 种可达性公式,给出可达性公式可满足性问题的求解,并分析了它们的可判定性问题.作为应用,实例说明广义量子 Loop 程序的终止问题可以归结为 Exogenous 量子马尔可夫链的最终可达性,进而通过检测量子公式可满足性来判定程序的终止问题.

关键词: 量子马尔可夫链;量子逻辑;可达性;可满足性问题;可判定性问题

中图法分类号: TP301

中文引用格式: 林运国,李永明.Exogenous 量子马尔可夫链及其可达性分析.软件学报,2016,27(12):2994−3002. http://www.jos.org.cn/1000-9825/4916.htm

英文引用格式: Lin YG, Li YM. Exogenous quantum Markov chains and reachability analysis. Ruan Jian Xue Bao/Journal of Software, 2016,27(12):2994−3002 (in Chinese). http://www.jos.org.cn/1000-9825/4916.htm

Exogenous Quantum Markov Chains and Reachability Analysis

LIN Yun-Guo[1,2], LI Yong-Ming[1]

[1](College of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

[2](College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China)

Abstract: In order to describe quantum properties of open quantum system, it is necessary to extend the existing quantum Markov chains. In this paper, Exogenous quantum Markov chains is introduced through building Exogenous quantum operator logic. For this new type of quantum Markov chain, the paper focuses on four reachability formulas, gives the solution of their satisfiability problems, and analyzes their decidability problems. As an application, an example is provided to show that the termination of the generalized quantum loop program corresponds to the future reachability of Exogenous quantum Markov chains, and therefore can be decided by checking satisfaction of quantum formulas.

Key words: quantum Markov chains; quantum logic; reachability; satisfiability problem; decidability problem

由于在通信协议、密码安全、信息处理、分布式计算上的应用,量子系统的推理、验证已经受到广泛的关注[1],特别量子系统的模型检测[2−4].量子系统的模型检测至少需要包含 3 个元素:模型、属性和检测算法;而刻画量子系统属性的逻辑工具主要有经典命题逻辑、量子逻辑、量子计算逻辑[1].

近年来,学者们针对不同量子系统提出了不同模型检测方法.应明生提出了利用量子自动机刻画封闭量子

* 基金项目: 国家自然科学基金(11271237, 61228305); 福建省自然科学基金资助项目(2016J01283); 福建省教育厅中青年教师教育科研项目(JA13115)

Foundation item: National Natural Science Foundation of China (11271237, 61228305); Natural Science Foundation of Fujian Province of China (2016J01283); The Young and Middle-Aged Education and Scientific Research Foundation of Fujian Educational Committee(JA13115)

收稿时间: 2014-12-08; 采用时间: 2015-09-10; jos 在线出版时间: 2015-11-12

CNKI 网络优先出版: 2015-11-11 17:04:05, http://www.cnki.net/kcms/detail/11.2560.TP.20151111.1704.007.html

系统,用闭子空间表示原子命题,利用毕克霍夫-冯·诺依曼量子逻辑刻画量子状态的属性,描述了量子系统的安全性、不变性、公平性等线性时间属性,基于自动机技术给出了量子线性时间属性的检测算法[2].关于这种量子系统的线性时序逻辑和计算树逻辑的检测仍然是公开性问题.冯元提出了利用量子马尔可夫链描述开放量子系统,用经典的计算树逻辑描述量子状态属性,给出了量子马尔可夫链的计算树检测算法,并且将方法应用于检测量子 BB84 协议,其中状态属性是经典的[3].Mateus 等人提出了 Exogenous 量子命题逻辑,并证明该逻辑公理系统的可靠性和完备性;构造了量子线性时序逻辑 QLTL 和量子计算树逻辑 QCTL,通过量子 Kripke 结构对封闭量子系统进行建模;用 QLTL 和 QCTL 刻画量子状态属性,说明了 QLTL、QCTL 的公式和经典的 LTL,CTL 公式之间的关系,利用经典算法给出 QLTL,QCTL 的检测方法.这方面的工作还未涉及到用密度算子描述的开放量子系统[5,6].

在经典迁移系统和概率系统,可达性检测是一个关键性问题.比如:基于自动机技术的迁移系统安全性检测,它等价于乘积系统的终状态是否可达;强公平性检测,它等价于状态是否是无限经常可达;而弱公平性检测,它等价于状态是否是最终永远可达[7,8].在量子系统中,同样存在着这方面的研究.文献[9]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.文献[10]研究了量子系统的可达性的可判定性问题.文献[11]研究了递归式量子马尔可夫链的可达性分析.

本文首先回顾几种量子马尔可夫链模型;其次构建 Exogenous 量子算子逻辑,该逻辑是可靠完备的;接着给出检测量子算子公式可满足性的复杂度;然后,在 Exogenous 量子算子逻辑基础上定义 Exogenous 量子马尔可夫链,提出几种常用的可达性,分析可达性公式的可满足性问题和可判定性问题;最后,通过实例说明 Exogenous 量子马尔可夫链及其可达性与广义量子 Loop 程序终止问题的关系.

1 符号规定

设 n 个单量子比特构成的集合 $qB=\{qb_1,qb_2,\ldots,qb_n\}$,$H_{qB}$ 表示赋值集 2^{qB} 张成的 Hilbert 空间,即:

$$H_{qB}=span\{|v\rangle|v\in 2^{qB}\}.$$

将 qB 看作是量子命题变元集,任意子集 $A\subseteq qB$ 都有唯一基向量与其一一对应,当 $qb\in A$ 时,赋值为真;当 $qb\notin A$ 时,赋值为假.设 $B(H_{qB})$为 H_{qB} 上有界线性算子,$P(H_{qB})=\{P\in B(H_{qB})|P=P^*=P^2\}$为 H_{qB} 上的投影算子,$D(H_{qB})=\{\rho\in B(H_{qB})|t(\rho)r=1\}$为 H_{qB} 上的量子密度算子.

2 Exogenous 量子马尔可夫链

量子马尔可夫链已经被学者们所研究,它主要用来刻画量子系统的动态演化[12−14].量子行走是一类特殊的量子马尔可夫链,得到广泛关注,已经成功应用于设计和分析量子算法[15,16].文献[17]将量子马尔可夫链定义为二元组$\langle G,\varepsilon\rangle$,$G$ 是有向图,$\varepsilon=[\varepsilon_{ij}]$是迁移算子矩阵(TOM).矩阵 TOM 的每一个元素ε_{ij}标签为点 i 到点 j 的边,它满足完全正性,且每列的和为一个量子运算.该量子马尔可夫链给出量子系统状态转移的特性,每一个节点代表一个状态,但状态是经典的且状态数是有限的,而量子系统的状态是用量子态描述且 Hilbert 空间是连续的.文献[9]将经典马尔可夫链$\langle S,P\rangle$推广到量子情形,定义了量子马尔可夫链$\langle H,\varepsilon\rangle$,用 Hilbert 空间 H 替代状态空间 S,用超算子ε替代概率转移矩阵 P,量子状态空间是连续的.文献[3]定义了量子马尔可夫链$\langle S,H,Q\rangle$,其中,S 是经典状态集,H 是量子状态空间,Q 表示状态转移算子矩阵,该模型采用经典命题逻辑来刻画量子系统的状态属性,但不是用量子逻辑刻画量子态.

如何用量子逻辑刻画量子马尔可夫链的量子态,合适的量子逻辑是关键.关于量子逻辑,一般是指毕克霍夫-冯·诺依曼等学者提出的一类正交模格数学代数结构.然而,文献[5]提出了基于 Exogenous 的量子命题逻辑,刻画了量子态$|\psi\rangle$的属性,同时还保持经典命题逻辑特性.不过,Exogenous 量子命题逻辑系统只适合刻画量子态$|\psi\rangle$,而不适合刻画用密度算子描述的开放量子系统.针对该问题,本文提出一种 Exogenous 量子算子逻辑,记号为 L_E,并通过该逻辑描述量子马尔可夫链.

2.1 L_E的语法

Exogenous 量子算子逻辑的语法由 3 部分组成:经典命题公式、算子项和量子算子公式.

(1) 经典命题公式α:=$\bot_C|qb|\alpha\to_C\alpha$.

由 qB 中的 n 个量子比特$\{qb_1,qb_2,\ldots,qb_n\}$作为命题变元,$\neg_C,\vee_C,\wedge_C,\to_C,\leftrightarrow_C$ 作为联结词.所有经典命题公式记为Γ_C.经典命题公式用来刻画经典属性.

(2) 算子项 $t::=O\,|\,I\,|\,x\,|\int\alpha\,|\,T_A^G\,|\,t+t\,|\,t\otimes t$.

算子项的论域是有界线性算子 $B(H_{qB})$,其中:O,I 分别表示零算子、恒等算子;$x\in X$ 为项变元,$X=\{x_k|k\in N\}\subseteq B(H_{qB})$; $\int\alpha$ 为概率算子项;$A\subseteq G\subseteq qB$; T_A^G 为投影算子项;$t+t$ 算子和项;$t\otimes t$ 张量积算子项.所有量子算子项记为 $Term$.算子项用来描述投影测量、量子运算等.

(3) 量子算子公式γ:=$t\leqslant t|\bot_Q|\gamma\to_Q\gamma$.

$t\leqslant t$ 称为量子算子原子公式,称 $qAtom$:=$\{t\leqslant t\}$为量子算子原子命题集.$\bot_Q$ 为量子算子矛盾式,量子算子公式是由 $qAtom$ 经联结词$\bot_Q,\to_Q$ 联结递归形成的公式.所有量子算子公式记为Γ_Q.称没有项变元的量子算子公式为量子算子闭式.量子算子公式用来描述测量结果的比较.

在 L_E 定义中有两组联结词:一组是针对经典命题公式,一组是针对量子算子公式.在不引起歧义的条件下,去掉下标 C,Q.

关于$\int\alpha$ 和 T_A^G 的含义解释是:概率算子项$\int\alpha$ 表示使公式α为真的概率;投影算子 T_A^G 定义为 $P_{(\wedge A)G}\otimes I_{qB/G}$,其中,$A\subseteq G\subseteq qB$, $(\wedge A)_G:=\underset{qb_k\in A}{\wedge}qb_k\wedge\underset{qb_k\notin G\setminus A}{\wedge}\neg qb_k$,$P_{(\wedge A)G}$ 表示使公式$(\wedge A)_G$ 为真的赋值作为一组基向量所张成的 H_G 子空间上的投影算子,$H_g\subseteq H_{qB}$ 表示由 2^G 张成的 Hilbert 空间.

量子算子公式γ否定定义为$\neg_Q$:=$\gamma\to_Q\bot_Q$,类似于经典命题公式定义下列联结词$\vee_Q,\wedge_Q,\to_Q,\leftrightarrow_Q$.定义 $t_1=t_2$:=$(t_1\leqslant t_2)\wedge_Q(t_2\leqslant t_1)$,$t_1<t_2$:=$(t_1\leqslant t_2)\wedge_Q\neg_Q(t_1=t_2)$,$t_1>t_2$:=$t_2<t_1$.统称$\{t_1\leqslant t_2,t_1=t_2,t_1<t_2,t_1>t_2\}$为量子算子比较公式.设任意的$\gamma,\gamma_1,\gamma_2\in\Gamma_Q$,量子算子公式$\gamma$长度或复杂度记号为$|\gamma|$,长度$|\gamma|$递归定义为:(1) $|\gamma|=0$;(2) $|\neg_Q\gamma|=|\gamma|+1$;(3) $|\gamma_1\to_Q\gamma_2|=\max(\gamma_1,\gamma_2)+1$.

2.2 L_E的语义

Exogenous 量子算子逻辑的语义包括对经典命题公式、项和量子算子公式的解释.对于经典命题公式α,给出 qB 上的赋值 $v\in 2^{qB}$,记 v 可满足α为 $v\models\alpha$,同时记$|\alpha|=\{v\in 2^{qB}|v\models\alpha\}$表示使$\alpha$为真的赋值集.关于项变元 x 的解释,定义指派函数$\sigma:X\to B(H_{qB})$,其中,X 为所有项变元之集.给定一个量子密度算子$\rho\in D(H_{qB})$,项和量子算子公式语义递归定义如下:

算子项的语义:

- $[\![x]\!]=tr(x(\rho))$;
- $[\![O]\!]=tr(O(\rho))=0$;
- $[\![I]\!]=tr(I(\rho))=1$;
- $[\![\int\alpha]\!]=\sum_{v\in|\alpha|}tr(P_v(\rho))$;
- $[\![T_A^G]\!]=tr(T_A^G(\rho))$,其中,$A\subseteq G\subseteq qB$;
- $[\![t_1+t_2]\!]=[\![t_1]\!]+[\![t_2]\!]=tr(t_1(\rho))+tr(t_2(\rho))$;
- $[\![t_1\otimes t_2]\!]=tr((t_1\otimes t_2)\rho)=tr(t_1(\rho_1))\cdot tr(t_2(\rho_2))$,其中,$\rho=\rho_1\otimes\rho_2$.

量子算子公式的语义:

- $\rho\models t_1\leqslant t_2$ 当且仅当$[\![t_1\leqslant t_2]\!]=[\![t_1]\!]\leqslant[\![t_2]\!]$,即 $tr(t_1(\rho))\leqslant tr(t_2(\rho))$;
- $\rho\not\models\bot_Q,\rho\models\gamma_1\to_Q\gamma_2$ 当且仅当$\rho\not\models\gamma_1$ 或者$\rho\models\gamma_2$.

若$\rho\models\gamma$,则称ρ可满足γ.Exogenous 量子算子逻辑 L_E 能够刻画用密度算子描述的开放量子系统.例如:任意给

定量子密度算子$\rho\in D(H_{qB})$,设量子算子公式$\gamma:=T_A^{qB}\leqslant\frac{1}{2}I$,若有$\rho\vDash\gamma$,则语义解释为$tr(T_A^{qB}(\rho))\leqslant\frac{1}{2}$,它表示投影测量结果 m(m 是使得命题公式$(\wedge A)_{qB}$为真的赋值)的概率小于等于$\frac{1}{2}$.在第 2.3 节,将用该逻辑描述开放的量子马尔可夫链.

Exogenous 量子算子逻辑 L_E 的推理规则包括两条:(1) $\alpha_1,\alpha_1\to_C\alpha_2\vdash\alpha_2$;(2) $\gamma_1,\gamma_1\to_Q\gamma_2\vdash\gamma_2$.

作为公理化系统,Exogenous 量子算子逻辑 L_E 具有可靠性和完备性.由于篇幅原因,另文给予证明.

定理 1. Exogenous 量子算子逻辑 L_E 是可靠且完备的.

给定量子密度算子$\rho\in D(H_{qB})$,对于量子算子公式(闭式)γ的可满足检测算法的复杂度分析如下:

设$|qB|=n$,密度算子用 $2^n\times2^n$ 矩阵表示,矩阵的相加减的复杂度是 $O(2^n\times2^n)$,矩阵的乘法复杂度是 $O(2^{3n})$,量子算子公式的长度为$|\gamma|$.解释量子算子公式γ中的项$[\![\int\alpha]\!]=\sum_{v\in|\alpha|}tr(P_v(\rho))$的复杂度为 $O(2^{3n})$,解释项$[\![t_1\otimes t_2]\!]=tr((t_1\otimes t_2)\rho)$的复杂度为 $O(2^{4n})$,解释项$[\![T_A^G]\!]=tr(T_A^G(\rho))$的复杂度为 $O(2^{4n})$,解释项$[\![t_1+t_2]\!]$的复杂度为 $O(2^{2n})$.

综上所述,检测量子算子公式γ的可满足性需要的复杂度为 $O(2^{4n}|\gamma|)$.

定理 2. 给定量子密度算子$\rho\in D(H_{qB})$、量子算子公式γ,检测ρ可满足γ($\rho\vDash\gamma$)的时间复杂度为$O(2^{4n}|\gamma|)$.

2.3 基于L_E的量子马尔可夫链

为了应用 L_E 描述开放量子系统,首先,先建立一类量子马尔可夫链:

$$\langle S,H_{qB},\varepsilon\rangle.$$

与文献[3]相比,这里 $S\subseteq D(H_{qB})$,$|S|=m$ 为有限状态集,量子算子$\varepsilon:D(H_{qB})\to D(H_{qB})$.

在实际应用中,利用该量子马尔可夫链模型能够描述一类开放量子系统,比如开放量子行走[16].考虑二点图上的开放量子行走,$S=\{\rho_1,\rho_2\}$,量子态之间转移如图 1,其中,$B_1B_1^\dagger+B_2B_2^\dagger=I$,$C_1C_1^\dagger+C_2C_2^\dagger=I$.

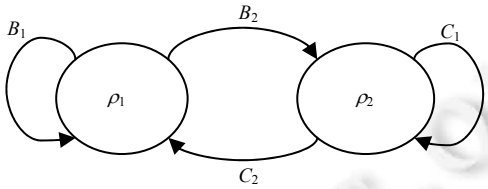

Fig.1 Open quantum walk over a graph with two vertices

图 1 二点图上的开放量子行走

Baltazar 等人基于 Exogenous 量子命题逻辑建立了量子计算树逻辑,构造有限量子 Kripke 结构刻画了逻辑语义,但它只适合于描述封闭量子系统[18].为了刻画开放量子系统的量子态属性,下面定义基于 Exogenous 量子算子逻辑的量子马尔可夫链.

定义 1. Exogenous 量子马尔可夫链是五元组 $M=\langle S,H_{qB},\varepsilon,l_{init},2^{AP},L\rangle$,其中,

(1) ε是 H_{qB} 上的量子运算;

(2) $l_{init}\subseteq H_{qB}$ 是量子初态的 Hilbert 子空间;

(3) $L:S\to2^{AP}$ 称为标签函数,其中,$AP\subseteq qAtom$,$|AP|=n$,$S\subseteq D(H_{qB})$,$|S|=m$.

任意$\rho\in S$,$supp(\rho)$表示为ρ的非零特征值对应的特征向量生成的本征空间.设$\rho,\rho'\in S$,若 $supp(\rho')\subseteq supp(\varepsilon(\rho))$,则称$\rho$可达$\rho'$,记号为$\rho\to\rho'$.定义从量子初态$\rho_0\in l_{init}$ 出发的一条无穷路径为$\pi=\rho_0\to\rho_1\to\ldots$,所有从$\rho_0$ 出发的无穷路径记为 $Paths(\rho_0)$.$\pi[i]=\rho_i$ 表示路径π的第 i 个量子态;$\pi[i..]=\rho_i\rho_{i+1}\ldots$表示从$\rho_i$ 出发的一条无穷路径;$\pi[..i]=\rho_0\rho_1\ldots\rho_i$表示从$\rho_0$出发到$\rho_i$的一条有穷路径.

文献[9]定义的量子马尔可夫链是$\langle H_{qB},\varepsilon,l_{init},2^{AP},L\rangle$,其中,$AP=\{qb_1,qb_2,\ldots,qb_n\}$.该模型与

Exogenous 量子马尔可夫链$\langle S,H_{qB},\varepsilon,l_{init},2^{AP},L\rangle$相比,模型形式是相近的,但是前一个模型中 AP 是经典原子命题集,刻画的是量子态经典属性;后一个模型AP是量子算子原子命题集,它利用Exogenous量子算子逻辑刻画量子态的量子属性.与文献[17]构造的量子 Kripke 结构 $T=\langle S,R\rangle$相比,两个都是用来描述有限量子态的量子属性,但一个是针对封闭量子系统,另一个是针对开放量子系统.

3 可达性分析

3.1 常用可达性

在经典模型检测中,属性的检测一般归结为验证状态可达性;对于量子模型检测,验证量子状态是否可达对量子属性的检测也是有意义的.常见可达性公式有下一步可达(next)、最终可达(future)、一致可达(global)、无限经常可达(infinitely often)、最终永远可达(ultimately forever).关于 Exogenous 量子马尔可夫链,重点提出下列 4 种常用可达性:

(1) 最终可达:$\pi\models F\gamma$当且仅当$\exists i\geqslant 0,\pi[i]\models\gamma$;

(2) 一致可达:$\pi\models G\gamma$当且仅当$\forall i\geqslant 0,\pi[i]\models\gamma$;

(3) 最终永远可达:$\pi\models U\gamma$当且仅当$\exists i\geqslant 0,\forall j\geqslant i,\pi[j]\models\gamma$;

(4) 无限经常可达:$\pi\models I\gamma$当且仅当$\forall i\geqslant 0,\exists j\geqslant i,\pi[j]\models\gamma$.

定义 2. 给定一个 Exogenous 量子马尔可夫链 $M,\rho_0\in l_{init},\Delta=\{F,G,U,I\},\gamma$是一个 Exogenous 量子算子公式,定义 $M,\rho_0\models\Delta\gamma$当且仅当对于任意的$\pi\in Paths(\rho_0)$,有$\pi\models\Delta\gamma$.

例 1:给定一个 Exogenous 量子马尔可夫链:$M=\langle S,H_{qB},\varepsilon,l_{init},2^{AP},L\rangle$,其中,

- 量子运算 $\varepsilon=\sum_{i=1}^{5}E_i\cdot E_i^{\dagger}$,运算元 $E_i(i=1,2,\ldots,5)$分别为

$$E_1=\frac{1}{\sqrt{2}}(|1\rangle\langle 0+1|+|3\rangle\langle 2+3|),$$

$$E_2=\frac{1}{\sqrt{2}}(|1\rangle\langle 0-1|+|3\rangle\langle 2-3|),$$

$$E_3=\frac{1}{\sqrt{2}}(|0\rangle\langle 0+1|+|2\rangle\langle 2+3|),$$

$$E_4=\frac{1}{\sqrt{2}}(|0\rangle\langle 0-1|+|2\rangle\langle 2-3|),$$

$$E_5=\frac{1}{10}(|0\rangle\langle 4|+|1\rangle\langle 4|+|2\rangle\langle 4|+4|3\rangle\langle 4|+9|4\rangle\langle 4|),$$

其中,式子$|0\pm 1\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle),|2\pm 3\rangle=\frac{1}{\sqrt{2}}(|2\rangle\pm|3\rangle)$.

- $S=\{\varepsilon^n(|\varphi\rangle\langle\varphi|)|n\in N,|\varphi\rangle\langle\varphi|\in l_{init}\}$;
- $AP=\{t\leqslant t\}$为量子算子原子命题集,t 的论域是有界线性算子 $B(H_{qB})$;
- $L:S\to 2^{AP}$;
- $l_{init}=span\{|0\rangle,|1\rangle\}\cup span\{|2\rangle,|3\rangle\}$.

下面讨论几种量子属性的可达性.

(1) 给定量子算子公式 $\gamma_1:=T_{\{0,1\}}^{\{0,1,2,3,4\}}=I$,语义解释为:投影测量结果属于{0,1}的概率等于 1.取$\rho_0=|0\rangle\langle 0|\in l_{init},G\gamma_1$ 表示对于从初始状态ρ_0 出发的每条路径的每一个可达量子态,量子算子公式γ_1 都是可满足的,即,投影测量结果属于{0,1}.注意到:对于任意 $n\in N$,均有 $\varepsilon^n(|0\rangle\langle 0|)=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)$,因而有 $M,\rho_0\models G\gamma_1$ 成立.

(2) 给定量子算子公式 $\gamma_2:=aI\leqslant T_{\{1,2,3,4\}}^{\{0,1,2,3,4\}}$,其中,$a$ 为任意小的非零正数,语义解释为:投影测量结果属于

{1,2,3,4}的概率大于等于 a.设一组投影算子 $P_0=\{|0\rangle\langle 0|\}$,$P_1=I-P_0$.取$\rho_0=|0\rangle\langle 0|\in l_{init}$,$F\neg_Q\gamma_2$ 表示对于从初始状态ρ_0出发的每条路径存在着一个可达量子状态,量子算子公式γ_2 是不可满足的.由于 $\lim_{k\to+\infty}(P_1\cdot\varepsilon)^k(\rho_0)=0$,所以一定存在一个可达量子状态$\rho_1$ 使得$\rho_1\models\neg_Q\gamma_2$,所以有 $M,\rho_0\models\neg_Q\gamma_2$ 成立.该结论也说明了量子态$|0\rangle\langle 0|$为吸收态[9].

(3) 给定量子算子公式 $\gamma_3:=T_{\{3\}}^{\{0,1,2,3,4\}}=\frac{1}{2}I$,语义解释为:投影测量结果为 3 的概率等于 $\frac{1}{2}$.

取 $\rho_0=\frac{1}{2}(|3\rangle\langle 3|+|4\rangle\langle 4|)\in l_{init}$,$I\gamma_3$ 表示对于从初始状态ρ_0 出发的每条路径的每一个可达量子态,量子算子公式γ_3 是无限经常可达(可满足).由于对于任意$\rho\in span\{|3\rangle,|4\rangle\}$,$\forall n\in N$ 均有 $\varepsilon^n(\rho)=\frac{1}{2}(|3\rangle\langle 3|+|4\rangle\langle 4|)$,所以投影测量结果 3 是以一定概率无限经常可达的,因而有 $M,\rho_0\models I\gamma_3$.

(4) (续(3)),对于任意$\rho_0\in l_{init}$,可推导出 $M,\rho_0\models\neg_Q U\gamma_3$.

在定义 2 中,称ρ为$\Delta\gamma$的一个可满足解,所有可满足解记为 $Sat_M(\Delta\gamma)$.对于 4 种可达性公式的可满足解算法分析如下.

3.2 可满足性

4 种可达性公式的可满足集记为 $Sat_M(\Delta\gamma)=\{\rho\in S|M,\rho_0\models\Delta\gamma\}$,具体分析如下:

(1) $Sat_M(F\gamma)=\{\rho\in S|\exists n\in N,supp(\varepsilon^n(\rho))\cap S\cap Sat_M(\gamma)\neq 0\}$;

(2) $Sat_M(G\gamma)=S\backslash Sat_M(F\neg\gamma)$;

(3) $Sat_M(U\gamma)=Fixpoint\{\lambda x.\{supp(\varepsilon^{-1}(X))\cap S\}\cup X,Sat_M(\gamma)\}$,其中,$\varepsilon^{-1}(X)=\{\rho\in S|\varepsilon(\rho)\subseteq X\}$;

(4) $Sat_M(I\gamma)=S\backslash Sat_M(U\neg\gamma)$.

可达性检测算法的复杂度计算分为两个过程:首先是 Exogenous 量子马尔可夫链的检测算法,如果将量子原子命题替换为经典原子命题,利用经典检测算法[7,18],求出算法的复杂度为 $O(|\gamma||S|^2)$;其次是 Exogenous 量子算子公式的检测算法,根据定理 2 可知算法的复杂度为 $O(2^{4n}|\gamma|)$,所以计算出可达性公式$\Delta\gamma$的可满足性检测算法复杂度如下:

定理 3. 给定一个 Exogenous 量子马尔可夫链 $M,\rho\in l_{init},,\Delta\gamma$的可满足性检测算法复杂度为 $O(|\gamma|^2|S|^2 2^{4n})$.

3.3 可判定性

文献[19,20]表明了给定一个马尔可夫链,判定是否存在一个正整数 n 使得经过 n 步从起始状态达到目标状态的概率为有理数 r 是一个 Skolem 问题.所谓 Skolem 问题是指给定一个方阵 M,是否存在一个正整数 n 使得 $(M^n)_{ij}=0$.Skolem 问题属于数论可判定性问题,是一个公开未解决的问题.Exogenous 量子马尔可夫链作为马尔可夫链的量子意义下的推广,也存在可判定性问题.

给定一个 Exogenous 量子马尔可夫链 $M,\rho_0\in l_{init},$,一个量子算子公式γ,$M,\rho_0\models\Delta\gamma$是否是可判定的,下面对此进行分析.

命题 1. 设 $V=Sat_M(\gamma)=\{\rho\in S|\rho\models\gamma\}$,$Z=\{n\in N|\varepsilon^n(\rho)\in V\}$,给定 4 种可达性公式$\Delta\gamma$,$\Delta=\{F,G,U,I\}$,有:

(1) 若最终可达 $F\gamma$是可判定的当且仅当判定 Z 是非空的;

(2) 若一致可达 $G\gamma$是可判定的当且仅当判定 Z 是自然数集;

(3) 若最终永远可达 $U\gamma$是可判定的当且仅当判定 Z 是无穷多;

(4) 若无限经常可达 $I\gamma$是可判定的当且仅当判定 Z 是去除有限多个自然数外的无穷多个.

命题 1 表明,对可达性公式$\Delta\gamma$的判定可以转化为一类正整数集合 Z 的属性判定.

定义 3[21,22]. 给定一个 m 阶方阵 A,一个向量 $x\in Q^m$ 和一个子空间 $V\subseteq Q^m$,判定是否存在一个非负整数 n 使得 $A^n x\in V$,称这类问题为高阶轨道问题.

命题 2. 关于 $Z=\{n\in N|\varepsilon^n(\rho)\in V\}$的判定是一个高阶轨道问题.

记 $Z=\{n\in N|\varepsilon^n(\rho)\in V\}$的判定问题为 DProblem.若$\varepsilon^n(\rho)\in V$,则有 $P_{V^\perp}\varepsilon^n(\rho)=O$,因而有 $tr(P_{V^\perp}\varepsilon^n(\rho))=0$.这样,

对 DProblem 判定等价于对集合 $Z=\{n\in N\mid tr(P_{V^\perp}\varepsilon^n(\rho))=0\}$ 的属性判定.由于ε是开放量子系统的一个量子运算,U 是作用在复合量子系统$\rho\otimes|0\rangle\langle 0|$(不妨设环境处于量子态$|0\rangle$)的酉运算,则 $\varepsilon^n(\rho)=Tr_{env}(U^n(\rho\otimes|0\rangle\langle 0|)(U^\dagger)^n)$,因而,对DProblem的判定又可以转化为对集合 $Z=\{n\in N\mid tr(P_{V^\perp}Tr_{env}(U^n(\rho\otimes|0\rangle\langle 0|)(U^\dagger)^n))=0\}$ 的属性判定.若给定一个系综$\{p_i,\rho_i\}$,密度算子ρ表示为 $\sum_i p_i\rho_i$,其中,$\rho_i=|\varphi_i\rangle\langle\varphi_i|$,则 DProblem 的判定又可转化为对 $Z=\{n\in N\mid U^n|\varphi_i\rangle|0\rangle\in V\otimes|0\rangle,\forall i\}$的属性判定.根据命题 2,DProblem 为一类高阶轨道问题.

高阶轨道问题由 Kannan 和 Lipton 提出,该问题与 Skolem 问题紧密相关[23],关于它的判定是一个公开性问题.相关工作已经证明:当 V 是一维的,高阶轨道问题有多项式时间算法;当 V 是二维和三维的,高阶轨道问题属于 NP^{RP}[19].

4 广义量子 Loop 程序终止问题

假设有一个含有 n 个量子系统 $qb_1,qb_2,\ldots,qb_n$ 的量子寄存器,并且对于每个 $i\leqslant n$,qb_i 的状态空间是 H_{qb_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 $X\subseteq spec(\tilde{M})$ (谱分解),广义量子 Loop 程序(记为 GQLoop)由ε, $\tilde{M}$ 和 X 定义为

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

其中, $\bar{q}$ 表示 $qb_1,qb_2,\ldots,qb_n$.设 $M_1=M_X=\sum_{m\in X}M_m$ 并且 $M_0=M_{\bar{X}}=I-M_X=\sum_{m\in spec(M)-X}M_m$,其中,$I$ 是恒等算子,控制部分 $\tilde{M}[\bar{q}]\in X$ 或 $M\in X$ 表示为投影测量算子 $M_X, M_{\bar{X}}$ 在 $\bar{q}$ 上的作用.广义量子 Loop 程序的工作方式和计算过程如图 2 和图 3 所示,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.

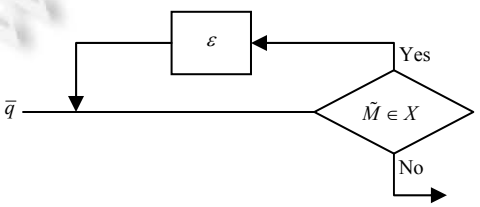

Fig.2 The working style of GQLoop

图 2 GQLoop 的工作方式

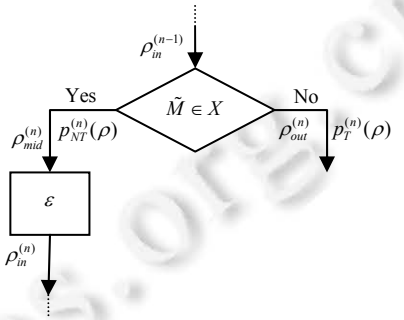

Fig.3 The computational process of GQLoop

图 3 GQLoop 的计算过程

给定输入态 $\rho_{in}^{(0)}$ 和广义量子 Loop 程序,如果对于某一个正整数 n,有 $p_{NT}^{(n)}(\rho_{in}^{(0)})=0$, 则称广义量子 Loop 程序在输入态 $\rho_{in}^{(0)}$ 上是终止的.

广义量子 Loop 程序是一个量子马尔可夫链$\langle H_{qB},\varepsilon,l_{init},2^{AP},L\rangle$.若取 $AP=\{t\leqslant t\},t$ 的论域是有界线性算子$B(H_{qB})$,同时,量子状态集为有限,则广义量子 Loop 程序也是一个 Exogenous 量子马尔可夫链.控制部分 $M\in X$ 用量子算子公式表示为 $\gamma\equiv(O\leqslant T_X^{qB})\wedge_Q(T_X^{qB}\leqslant I)$,其中, T_X^{qB} 为一个投影算子项.量子算子公式γ的语义解释如下:

对于任意给定一个输入态 $\rho_{in}^{(n)}$, $\rho_{in}^{(n)}\models\gamma$,当且仅当 $\rho_{in}^{(n)}\models(O\leqslant T_X^{qB})$ 且 $\rho_{in}^{(n)}\models(T_X^{qB}\leqslant I)$,也就是:

$$0\leqslant tr(T_X^{qB}(\rho_{in}^{(n)}))\leqslant 1.$$

从语义角度分析, T_X^{qB} 是广义量子 Loop 程序中的投影算子 M_1,意味着 $p_{NT}^{(n)}(\rho_{in}^{(0)})=tr(T_X^{qB}(\rho_{in}^{(n)}))$.

终止问题是(广义)量子 Loop 程序的一个重要研究对象[24],对于广义量子 Loop 程序的终止问题,它可以用可达性公式来表示.

命题 3. 任意给定输入态 $\rho_{in}^{(0)}$,若存在正整数 n,使得 $p_{NT}^{n}(\rho_{in}^{(0)})=0$,即广义量子 Loop 程序经过 n 步计算后在输入态 $\rho_{in}^{(0)}$ 上是终止的,当且仅当存在一个 Exogenous 量子马尔可夫链 M,使得 $M,\rho_{in}^{(0)}\models F\gamma$,其中,

$$\gamma := T_X^{qB} = O.$$

在命题中,$M,\rho_{in}^{(0)}\models F\gamma$ 意味着:对于任意 $\pi\in Paths(\rho_{in}^{(0)})$,有 $\pi\models F\gamma$,则存在一个正整数 n,使得 $\pi[n]=\rho_{in}^{(n)}\models\gamma$,其语义解释为 $tr(T_X^{qB}(\rho_{in}^{(n)}))=0$,所以 $p_{NT}^{n}(\rho_{in}^{(0)})=0$,即,在输入态 $\rho_{in}^{(0)}$ 上是终止的.因而,广义量子 Loop 程序终止对应了 Exogenous 量子马尔可夫链中量子算子公式 $T_X^{qB}=O$ 是最终可达的.

命题 3 表明了广义量子 Loop 程序终止问题可以归结为 Exogenous 量子马尔可夫链的最终可达性 $F\gamma$,因而,验证广义量子 Loop 程序的终止问题等价于检测 $F\gamma$ 的可满足性.

5 结束语

量子马尔可夫链作为量子世界有噪声环境下的数学模型,有着广泛的理论和实际的应用价值,对量子马尔可夫链的研究是有意义的.在量子信息论中,量子通信信道是一类量子马尔可夫链;在量子程序语言中,量子 Loop 程序是以量子马尔可夫链为数学模型.文中构造了 Exogenous 量子算子逻辑,它用来刻画开放量子系统.与毕克霍夫-冯·诺依曼量子逻辑相比,数学结构更为简单.在建立 Exogenous 量子马尔可夫链基础上,利用量子算子逻辑刻画量子马尔可夫链的量子态属性.与已有工作相比,该模型能够描述量子态的量子属性,可以应用于量子属性的模型检测.可达性是模型检测的关键性问题,文中定义了 4 种常用可达性,给出了它们的可满足检测算法和计算复杂度,并且分析了它们的判定性问题.作为应用,分析了广义量子 Loop 程序是一个 Exogenous 量子马尔可夫链,将程序终止问题与可达性问题联系在一起.

致谢 在此,我们向对本文的工作给予支持和建议的同行、同学和老师表示感谢.

References:

[1] Engesser K, Gabbay DM, Lehmann D. Handbook of Quantum Logic and Quantum Structures: Quantum Logic. Amsteldam: Elsevier Science Ltd., 2009. 1−22.

[2] Ying MS, Li YJ, Yu NK, Feng Y. Model checking linear time properties of quantum systems. ACM Trans. on Computational Logic, 2014,15(3):Article 22. [doi: 10.1145/2629680]

[3] Feng Y, Yu NK, Ying MS. Model checking quantum Markov chains. Journal of Computer and System Sciences, 2013,79: 1181−1198. [doi: 10.1016/j.jcss.2013.04.002]

[4] Ardeshir-Larijani E, Gay SJ, Nagarajan R. Equivalence checking of quantum protocols. In: Proc. of the Tools and Algorithms for the Construction and Analysis of Systems. Berlin, Heidelberg: Springer-Verlag, 2013. 478−492. [doi: 10.1007/978-3-642-36742-7_33]

[5] Mateus P, Sernadas A. Weakly complete axiomatization of exogenous quantum propositional logic. Information and Computation, 2006,204(5):771−794. [doi: 10.1016/j.ic.2006.02.001]

[6] Chadha R, Mateus P, Sernadas A, Sernadas C. Extending classical logic for reasoning about quantum systems. In: Handbook of Quantum Logic and Quantum Structures: Quantum Logic. Amsteldam: Elsevier Science Ltd., 2009. 325−372.

[7] Baier C, Katoen JP. Principles of Model Checking, Cambridge: MIT Press, 2008. 89−142.

[8] Clarke EM, Emerson EA. Design and synthesis of synronization skeletons using branching time temporal logic. In: Proc. of the 25 Years of Model Checking. Berlin, Heidelberg: Springer-Verlag, 2008. 196−215. [doi: 10.1007/978-3-540-69850-0_12]

[9] Ying SG, Feng Y, Yu NK, Ying MS. Reachability probabilities of quantum Markov chains. 2013. http://arXiv.org/abs/Quantph/arXiv:\quad1304.0060

[10] Li YJ, Ying MS. (Un) decidable problems about reachability of quantum systems. 2014. http://arxiv.org/abs/1401.6249

[11] Feng Y, Yu NK, Ying MS. Reachability analysis of recursive quantum Markov chains. In: Proc. of the Mathematical Foundations of Computer Science. 2013. 385−396. [doi: 10.1007/978-3-642-40313-2_35]

[12] Accardi L. Nonrelativistic quantum mechanics as a noncommutative markov process. Advances in Mathematics, 1976,20:329−366. [doi: 10.1016/0001-8708(76)90201-2]

[13] Accardi L. Topics in quantum probability. Physics Reports, 1981,77(3):169−192. [doi: 10.1016/0370-1573(81)90070-3]

[14] Ohno H. Extendability of generalized quantum Markov chains on gauge invariant C*-algebras. Infinite Dimensional Analysis, Quantum Probability and Related Topics, 2005,8:141−152. [doi: 10.1142/S0219025705001901]

[15] Ambainis A. Quantum walks and their algorithmic applications. Int'l Journal of Quantum Information, 2003,1(4):507−518. [doi: 10.1142/S0219749903000383]

[16] Attal S, Petruccione F, Sabot C, Sinayskiy I. Open quantum random walks. 2014. http://arxiv.org/abs/1402.3253

[17] Gudder S. Quantum Markov chains. Journal of Mathematical Physics, 2008,49(7):072105. [doi: 10.1063/1.2953952]

[18] Baltazar P, Chadha R, Mateus P. Quantum computation tree logic-model checking and complete calculus. Int'l Journal of Quantum Information, 2008,6(2):219−236. [doi: 10.1142/S0219749908003530]

[19] Akshay S, Antonopoulos T, Ouaknine J, Worrell J. Reachability problems for Markov chains. Information Processing Letters, 2015,115:155−158. [doi: 10.1016/j.ipl.2014.08.013]

[20] Beauquier D, Rabinovich A, Slissenko A. A logic of probability with decidable model checking. In: Proc. of the Computer Science Logic. Berlin, Heidelberg: Springer-Verlag, 2002. 306−321. [doi: 10.1007/3-540-45793-3_21]

[21] Chonev V, Ouaknine J, Worrell J. The orbit problem in higher dimensions. In: Proc. of the 45th Annual ACM Symp. on Theory of Computing. 2013. 941−950. [doi: 10.1145/2488608.2488728]

[22] Chonev V, Ouaknine J, Worrell J. On the complexity of the orbit problem. 2014. http://arxiv.org/abs/1303.2981

[23] Kannan R, Lipton RJ. Polynomial-Time algorithm for the orbit problem. Journal of the ACM, 1986,33(4):808−821. [doi: 10.1145/6490.6496]

[24] Ying MS, Feng Y. Quantum loop programs. Acta Informatica, 2010,47(4):221−250. [doi: 10.1145/6490.6496]

林运国(1979－),男,福建福清人,博士,讲师,主要研究领域为量子计算,模型检测.

李永明(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算智能,量子逻辑,量子计算,模型检测.