论 文

基于安全性检测的广义量子 Loop 程序终止验证

林运国^{①②}, 李永明^{①*}^① 陕西师范大学计算机科学学院, 西安 710119^② 福建农林大学计算机与信息学院, 福州 350002

* 通信作者. E-mail: liyongm@snnu.edu.cn

收稿日期: 2015-07-07; 接受日期: 2015-08-26; 网络出版日期: 2015-10-27

国家自然科学基金 (批准号: 11271237, 61228305) 和高等学校博士学科点专项科研基金 (批准号: 20130202110001) 资助项目

摘要 针对广义量子 Loop 程序的终止问题, 首先介绍终止和几乎终止的两种定义, 说明它们在刻画程序终止问题上的能力不足. 为了弥补这种缺陷, 引入另外两种定义: 以一定概率在第 n 步终止和可终止, 并且对这四种终止定义进行比较. 其次, 量子 (正则) 安全性是量子 Markov 链中重要的一类线性时间属性, 证明出量子正则安全性的可满足概率等于乘积量子 Markov 链终状态不可达的概率, 从而给出量子正则安全性检测技术. 运用该检测技术, 将广义量子 Loop 程序的终止问题归结为量子正则安全性的可满足性问题, 并给出算法来计算第 n 步终止、可终止的概率和量子终态. 针对多 (单) 量子比特系统、复合系统、嵌套系统, 推导出第 n 步终止、可终止的终态和概率, 并提供计算的显式表达式. 最后证明广义量子 Loop 程序有限步内终止和可终止的充要条件.

关键词 量子 Loop 程序 量子 Markov 链 量子自动机 程序终止 安全性

1 引言

量子计算是一门发展了 20 多年的新兴交叉学科, 起源于量子力学和计算机科学. 随着硬件技术的进步, 量子计算机的物理实现取得很大进展^[1]. 一旦量子计算机研制成功, 软件的开发将成为实现量子计算机功能的核心. 目前量子软件的研究仍然极富有挑战性, 量子程序设计的理论和实现就是其中一项重要研究的课题^[2]. 程序验证是保证程序正确性的关键技术, 如基于逻辑推理的验证, 最著名的是霍尔逻辑^[3,4].

循环是程序语言的关键, 巧妙地运用循环技术可以为程序设计带来很大的方便. 然而, 对于循环程序的分析却是非常困难, 比如终止条件^[5]. 在量子计算的情形下, Selinger 在其函数式量子程序语言 QFC 中研究了循环和递归等高阶控制特征^[2]; Ying 等作者详细研究了量子程序的 Floyd-Hoare 逻辑^[6]、量子 Loop 程序和量子程序的验证问题^[4,7], 特别是在文献[7]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, 给出了程序终止、几乎终止的充要条件和量子态的计算函数, 解决了几乎终止对噪声的敏感性等问题. 事实上一般量子循环的终止是不可判定的. 为了简化讨论, Ying 等考虑程序状态空间是“固定的和有限维的”这一特定情形, 首先对任意输入态给出了量子循环程序终止的充要条件. 在此基础上找到了量子循环处处终止的简单判定方法. 在循环体是酉变换

引用格式: 林运国, 李永明. 基于安全性检测的广义量子 Loop 程序终止验证. 中国科学: 信息科学, 2015, 45: 1615–1631, doi: 10.1360/N112015-00072

的特殊情形下, 他们还给出了其在有限步内终止的充要条件和循环的终态的函数显式表达式. Feng 等在文献 [8] 中给出量子 Markov 链的模型检测方法, 说明了量子 Loop 程序能够用量子 Markov 链来刻画, 同时针对一类属性提出检测算法, 并开发量子程序和协议的模型检测器 [9]. Li 等 [10] 定义了非确定型量子程序一种独立于语言的模型, 建立了非确定程序终止的充分必要条件, 并且基于这些条件提出检测非确定型量子程序的终止情况的算法. 李小鹏 [11] 在上述文献的基础上提出了量子 Loop 程序的主体是超算子 (量子信道) 的量子 Loop 程序, 即广义量子 Loop 程序, 讨论了它的终止、几乎终止等问题. 雷红轩研究了广义量子 Loop 程序的主体由比特翻转、去极化、幅值阻尼、相位阻尼等量子信道描述时, 广义量子 Loop 程序终止 (几乎终止) 等问题 [12,13]. 在前期研究工作中, 我们针对广义量子 Loop 程序, 将程序的终止情况归结为验证量子正则安全性的可满足性 [14]. 然而上述工作并没有研究广义量子 Loop 程序的一般量子信道终止问题, 没有给出一般情况下的终止概率、终态的显式表达式和程序终止的充分必要条件. 同时注意到终止、几乎终止只能刻画以概率为 1 终止的广义量子 Loop 程序, 而不能很好描述以一定概率 $0 < p < 1$ 终止的情形. 另外对于多 (单) 量子比特系统、复合系统、嵌套系统的广义量子 Loop 程序的一般终止问题还未得研究. 这些正是本文要研究的工作.

本文的组织结构如下: 第 2 节引入广义量子 Loop 程序, 给出几种终止定义; 第 3 节给出广义量子 Loop 程序的量子 Markov 链表示, 基于量子自动机技术给出终止判定的验证方法; 随后的第 4 节到第 6 节, 分别给出多 (单) 量子比特系统、复合系统、嵌套系统的广义量子 Loop 程序终止验证; 第 7 节给出广义量子 Loop 程序的终止充分必要条件; 最后总结全文.

2 广义量子 Loop 程序

2.1 基本概念

假设有一个含有 n 个量子系统的 $qb_1, qb_2, \dots, qb_n$ 的量子寄存器, 并且对于每个 $i \leq n$, qb_i 的状态空间为 H_i . 设复合空间 $H_{qB} = \otimes_{i=1}^n H_i$ 上的一个超算子 $K: D(H_{qB}) \rightarrow D(H_{qB})$, 即 $K(\rho) = \sum_{i=1}^d E_i \rho E_i^\dagger$, 其中 $\{E_i\}$ 是一组运算元, 满足 $\sum_{i=1}^d E_i^\dagger E_i = I$, $\rho \in D(H_{qB})$ (所有密度算子之集), $d = \dim(H_{qB})$. 设算子 $M = \sum_m m M_m$ 是 H_{qB} 上的可观测量, 记 $\text{spec}(M) = \{m\}$ 为 M 的谱. 对于任意的 $X \subseteq \text{spec}(M)$, 广义量子 Loop 程序 (generalized quantum loop program, 简记为 GQLoop) 由 K, M 和 X 定义为 [11,13]

$$\text{while}(M[\bar{q}] \in X) \{ \bar{q} := K(\bar{q}) \}, \quad (1)$$

其中 $\bar{q}$ 表示量子寄存器 $qb_1, qb_2, \dots, qb_n$. 设 $M_1 = M_X = \sum_{m \in X} M_m$ 并且 $M_0 = M_{\bar{X}} = I_{H_{qB}} - M_X = \sum_{m \in \text{spec}(M) - X} M_m$, 其中 $I_{H_{qB}}$ 是 H_{qB} 上的单位算子, 那么式 (1) 的控制部分 “ $M \in X$ ” 表示投影测量算子 $M_X, M_{\bar{X}}$ 在 $\bar{q}$ 上的作用. GQLoop 的工作方式如图 1, 计算过程如图 2.

对于任意的输入态 $\rho_{\text{in}}^{(0)} = \rho_0 \in D(H_{qB})$, 如果 GQLoop 在前 $n-1$ 步是不终止的, 那么在第 n 步中, 程序以 $p_T(\rho_{\text{in}}^{(n-1)}) = \text{tr}(M_{\bar{X}} \rho_{\text{in}}^{(n-1)})$ 的概率终止于量子态 $\rho_{\text{out}}^{(n)} = \frac{M_{\bar{X}} \rho_{\text{in}}^{(n-1)} M_{\bar{X}}^\dagger}{p_T(\rho_{\text{in}}^{(n-1)})}$; 以 $p_{NT}(\rho_{\text{in}}^{(n-1)}) = 1 - p_T(\rho_{\text{in}}^{(n-1)}) = \text{tr}(M_X \rho_{\text{in}}^{(n-1)})$ 的概率继续进行 GQLoop, 不终止的量子态为 $\rho_{\text{mid}}^{(n)} = \frac{M_X \rho_{\text{in}}^{(n-1)} M_X^\dagger}{p_{NT}(\rho_{\text{in}}^{(n-1)})}$ 且下一步输入态为 $\rho_{\text{in}}^{(n)} = K(\rho_{\text{mid}}^{(n)})$. 为了方便, 第 n 步终止的概率和不终止的概率也分别记为 $p_T^{(n)}(\rho)$, $p_{NT}^{(n)}(\rho)$.

2.2 几种终止定义

关于 (广义) 量子 Loop 程序的终止问题, 文献 [12] 给出在输入态 ρ 上终止、几乎终止以及终止量

图 1 GQLoop 的工作方式

Figure 1 The working style of GQLoop

图 2 GQLoop 的计算过程

Figure 2 The computational process of GQLoop

子态 (终态) 的计算函数.

定义 1 给定一个输入态 $\rho \in D(H_{qB})$ 和一个广义量子 Loop 程序, (1) 如果对于某个正整数 n , 有 $p_{NT}^{(n)}(\rho) = 0$, 则称 GQLoop 在输入态 ρ 上 (有限步内) 终止; (2) 输入态 ρ 上 GQLoop 不终止概率定义为 $p_{NT}(\rho) = \lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho)$, 其中 $p_{NT}^{(n+)}(\rho) = \prod_{i=1}^n p_{NT}^{(i)}(\rho)$ 表示在第 n 步后 GQLoop 不终止的概率, 特别记 $p_{NT}^{(0+)}(\rho) = 1$; (3) 如果 $p_{NT}(\rho) = 0$, 则称 GQLoop 在输入态 ρ 上几乎终止; (4) 如果 $p_{NT}(\rho) > 0$, 则称 GQLoop 在输入态 ρ 上不终止.

定义 2 如果一个广义量子 Loop 程序在所有的输入态 ρ 上都终止 (几乎终止), 则称它是终止的 (几乎终止).

在定义 (1) 中, 对于 GQLoop 在输入态 ρ 上终止, n 取多少才会使得 $p_{NT}^{(n)}(\rho) = 0$, 这是不易求解的. 同时注意到对于任意的 $n \in \mathbb{N}$, GQLoop 在第 n 步都会以一定概率 $\text{tr}(M_{\bar{X}} \rho_{\text{in}}^{(n-1)} M_{\bar{X}})$ 终止程序, 与之相比 $p_{NT}^{(n)}(\rho) = 0$ 是它的一种特殊情形. 对于几乎终止定义, 当 $\forall n \in \mathbb{N}, \lim_{n \rightarrow \infty} p_{NT}^{(n)}(\rho) < 1$ 时, $\lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho) = 0$, GQLoop 是几乎终止的, 这表明了如果第 n 步不终止的概率极限小于 1 时, GQLoop 都是几乎终止的, 该定义条件太强. 另外在后续例子中表明存在以一定概率终止但不是几乎终止. 下面给出广义量子 Loop 程序的两种更一般终止定义: 第 n 步终止和可终止.

定义 3 给定一个输入态 $\rho \in D(H_{qB})$ 和一个广义量子 Loop 程序, (1) 称 GQLoop 在输入态 ρ 上以概率 $p_{NT}^{(n+)}(\rho)$ 在第 n 步不终止, 以概率 $p_T^{(n+)}(\rho) = 1 - p_{NT}^{(n+)}(\rho)$ 在第 n 步终止; (2) 称 GQLoop 在输入态 ρ 上以概率 $p_{NT}^\infty(\rho) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho)$ 不可终止, 以概率 $p_T^\infty(\rho) = 1 - p_{NT}^\infty(\rho)$ 可终止, 特别地当 $p_T^\infty(\rho) = 1$ 时称 GQLoop 在输入态 ρ 上是可终止.

如果在所有的输入态 ρ 上都是可终止的, 则称 GQLoop 是可终止的, 否则称为不可终止.

在定义 1 中, 对于几乎终止, 只计算了经过第 n 步计算后的 GQLoop 不终止的概率收敛值, 但是程序在每一步均有可能以一定概率终止, 该收敛值并没有反映每一步都有可能 (不) 终止的情况. 而与定义 1 有所不同的是在定义 3 中对于不可终止, 采用了前 n 步经过每一步计算后 GQLoop 不终止的概率的算术平均值的收敛值来刻画程序 (不) 终止情况.

定理 1 广义量子 Loop 程序在输入态 ρ 上几乎终止当且仅当可终止.

证明 设广义量子 Loop 程序在输入态 ρ 上几乎终止, 意味着 $p_{NT}(\rho) = 0$, 即 $\lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho) = 0$, 而对于 $p_{NT}^\infty(\rho) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho)$, 该式本质上为数列 $\{p_{NT}^{(n+)}(\rho)\}$ 的 cesàro 算术平均值 $\frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho)$ 的极限值. 可知若 $\lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho) = 0$, 则 $\lim_{n \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho) = 0$, 即 $p_{NT}^\infty(\rho) = 0$, 所以若 GQLoop 在输入态 ρ 上几乎终止则也是可终止的.

设广义量子 Loop 程序在输入态 ρ 上可终止, 则 $\lim_{n \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho) = 0$. 因为 $\sum_{n=1}^N p_{NT}^{(n+)}(\rho) \geq$

$Np_{NT}^{(n+)}(\rho)$, 有 $\lim_{n \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho) \geq \lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho)$, 所以当 $\lim_{n \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N p_{NT}^{(n+)}(\rho) = 0$, 有 $\lim_{n \rightarrow \infty} p_{NT}^{(n+)}(\rho) = 0$, 因而若 GQLoop 在输入态 $\rho_{in}^{(0)}$ 上是可终止的则也是几乎终止的.

定义 1 和 3 给出了四种终止定义, 它们之间有区别和联系. 首先, 根据定理 1, 几乎终止也是可终止的, 反之亦然; 其次, 广义量子 Loop 程序在输入态 ρ 上终止则也是几乎终止的或可终止的, 同时也是以概率为 1 在第 n 步终止; 最后广义量子 Loop 程序以一定概率可终止但不一定意味着几乎终止.

例 1 设 $\rho = 0.1|0\rangle\langle 0| + 0.9|1\rangle\langle 1| \in D(H_{qB})$, 一个广义量子 Loop 程序由 K, M, X 定义, 其中 $K(|1\rangle\langle 1|) = 0.1|0\rangle\langle 0| + 0.9|1\rangle\langle 1|$, $M = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, $X = \{1\}$, 可知就每一次循环来说程序终止概率非常小, 但是 $p_{NT}(\rho) = 0$, 说明了程序是几乎终止的, 同时它也是可终止的. 若 $K(|1\rangle\langle 1|) = |1\rangle\langle 1|$, 程序是不终止的, 但它是概率 $p_{NT}^\infty(\rho) = 0.1$ 可终止的.

定义 4 广义量子 Loop 程序对输入态 $\rho \in D(H_{qB})$ 的作用看成一个函数 $F: D(H_{qB}) \rightarrow D(H_{qB})^-$: $F(\rho) = \rho_{out} = \sum_{n=1}^\infty p_{NT}^{(n-1)+}(\rho) p_T^{(n)}(\rho) \rho_{out}^{(n)}$, 称 F 为 GQLoop 的终态计算函数.

该计算函数给出 GQLoop 的终止量子态, 它是从密度算子 $D(H_{qB})$ 到部分密度算子 $D(H_{qB})^-$, 是非保迹的量子运算. 与定义 3 中可终止定义相对应的也有相应的终态计算函数.

定义 5 GQLoop 对输入态 $\rho \in D(H_{qB})$ 的作用看成一个函数 $\varepsilon_\infty: D(H_{qB}) \rightarrow D(H_{qB})$, $\varepsilon_\infty(\rho) = \rho_{out}^\infty = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \rho_{out}^{(n)}$, 也称 ε_∞ 为 GQLoop 的终态计算函数.

ε_∞ 是一个保迹的量子运算 (超算子)¹⁾.

3 广义量子 Loop 程序的数学模型

广义量子 Loop 程序的数学模型是量子 Markov 链^[7], 其终止情况可表示为量子 Markov 链一类属性, 因而对广义量子 Loop 程序的终止判定可转化为验证一类量子 Markov 链属性.

3.1 量子 Markov 链与量子安全性

定义 6 一个量子 Markov 链^[8,15] 是一个五元组 $MC = \langle H_{qB}, \varepsilon, l_{init}, 2^{AP}, \rangle$, 其中: (1) ε 是 H_{qB} 上一个超算子; (2) $l_{init} \subseteq H_{qB}$ 是量子初态的 Hilbert 子空间; (3) $AP = 2^{qB}$, $qB = \{qb_1, qb_2, \dots, qb_n\}$; (4) $L: D(H_{qB}) \rightarrow 2^{AP}$ 称为标签函数.

任给 $\rho \in D(H_{qB})$, $\text{supp}(\rho)$ 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 $\rho, \rho' \in D(H_{qB})$, 若 $\text{supp}(\rho') \subseteq \text{supp}(\varepsilon(\rho))$, 则记 $\rho \rightarrow \rho'$. 定义从量子初态 ρ_0 出发一条有穷 (无穷) 路径为 $\hat{\pi} = \rho_0 \rightarrow \rho_1 \rightarrow \dots \rho_n (\pi = \rho_0 \rightarrow \rho_1 \rightarrow \dots)$, 有穷 (无穷) 迹定义为 $\text{trace}(\hat{\pi}) = L(\rho_0)L(\rho_1) \cdots L(\rho_n) (\text{trace}(\pi) = L(\rho_0)L(\rho_1) \cdots)$. $(2^{AP})^*$ 、 $(2^{AP})^\omega$ 表示所有有穷、无穷迹序列的集合.

定义 7 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.

给定一个量子线性时间属性 P , 一个有穷迹序列 $\hat{\sigma} \in (2^{AP})^*$, 若对于任意的 $\sigma \in (2^{AP})^\omega$ 有 $\hat{\sigma}\sigma \notin P$, 则称 $\hat{\sigma}$ 为量子线性时间属性 P 的坏前缀. P 的所有坏前缀记为 $\text{Bpref}(P)$. 设 $\hat{\sigma} \in (2^{AP})^*$ 且 $\sigma \in (2^{AP})^\omega$, 对于每个 $\sigma' \in (2^{AP})^\omega$, 若 $\sigma = \hat{\sigma}\sigma'$, 则称 $\hat{\sigma}$ 为 σ 的一个前缀.

定义 8 若对于任意的 $\sigma \notin P$, 存在一个坏前缀 $\hat{\sigma} \in \text{Bpref}(P)$, 则称 P 为量子安全性.

定义 9 若存在一个子空间 $X \subseteq AP$ 使得 $P_{inv} = \{X_0 X_1 \cdots \in (2^{AP})^\omega | \forall i \geq 0, X_i \subseteq X\}$, 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.

量子不变性也是一种量子安全性.

1) Wolf M M. Quantum Channels and Operators: Guided Tour. 2012

图 3 GQLoop 的量子 Markov 链表示

Figure 3 The representation of quantum Markov chain for GQLoop

3.2 模型建立

广义量子 Loop 程序 (式 (1)) 是一个量子 Markov 链^[7], 数学模型为 $MC = \langle H_{qB}, \{F, K \circ M_1, M_0, I\}, l_{init}, 2^{AP}, L \rangle$, 其中超算子 $K(\cdot) = \sum_{i=1}^d E_i \cdot E_i^\dagger$; 算子 $M = \sum_m m M_m$ 是 H_{qB} 上的可观测量; 超算子 $K \circ M_1(\rho) = K(M_1 \rho M_1^\dagger / \text{tr}(M_1 \rho M_1^\dagger))$ 表示 l_1 自身状态的转移 (如图 3); 设量子初态为 ρ_0^M , $l_{init} = \text{supp}(\rho_0^M)$, $L(l_{init}) = \text{spec}(M)$, $L(l_0) = \text{spec}(M) - X$, $L(l_1) = X$, 为了方便记 $L(l_1)$ 、 $L(l_0)$ 为 A_1 、 A_0 ; 称 $F(\rho_0^M)$ 为量子初始输入态, 记为 $\rho_{in}^{(0)}$.

设 $\rho \in D(H_{qB})$, 算子 $M = \sum_m m M_m$ 是 H_{qB} 上的可观测量, M_X (或 M_1) 与 $M_{\bar{X}}$ (或 M_0) 对应程序中的 “yes-no”, $L(l_1)$, $L(l_0)$ 分别对应 “yes-no” 测量结果. 结合图 1 和 3, 对 GQLoop 的工作方式和量子 Markov 链表示分析如下. 量子初始输入态 $\rho_{in}^{(0)}$ 输入到 GQLoop 中, 进入控制部分 $M \in X$, 将 M_1, M_0 作用在 $\rho_{in}^{(0)}$ 上, GQLoop 或以一定的概率不终止且进入超算子 K 运算, 并再次进入控制部分 $M \in X$ 中进行下一步循环运算, 或以一定的概率终止运算. 这一过程在量子 Markov 链中表现为: 初始量子态 ρ_0^M 进行 F 运算 (初始化过程), 得到量子初始输入态 $\rho_{in}^{(0)}$, 转移到状态 l_1 , 接下来或以一定的概率进行自身状态转移, 或以一定的概率转移到状态 l_0 , 之后状态将进入无限自循环. 同理若 GQLoop 进入不终止计算, 相当于量子 Markov 链不间断访问状态 l_1 , 否则若是终止计算则进入状态 l_0 . 对状态 l_0, l_1 分别标签为 A_0, A_1 , 则 GQLoop 不终止对应于一个无穷迹序列 $(\{A_1\})^\omega$. 注意到该序列是一个量子不变性, 也是量子安全性.

通过上述分析, 可以用量子安全性来表示广义量子 Loop 的终止, 将终止的判定归结为量子安全性的可满足性验证.

3.3 终止判定的自动机验证法

经典迁移系统的正则安全性检测, 是基于有穷自动机, 将所要检测的属性的补转化为有穷自动机, 并且构造出迁移系统与有穷自动机的乘积系统, 通过交集是否为空集来判断系统是否满足特定的属性^[16]. Ying 等^[17] 将这一思想推广到量子情形. 针对量子 Markov 链的安全性检测, 本文通过构造量子 Markov 链和量子有穷自动机的乘积系统, 将量子 Markov 链的安全性的可满足问题归结为量子乘积系统的终状态的可达性问题. 结合 3.2 小节, 广义量子 Loop 程序的终止验证等价于检测量子乘积系统的终状态的可达性.

定义 10 量子有穷自动机^[18,19] 是一个五元组:

$$A = \langle Q, \Sigma, \Delta, q_0, Q_{acc} \rangle,$$

其中 (1) Q 为有穷状态集, 状态数 $|Q| = n$; (2) Σ 为有穷输入字母表; (3) 映射 $\Delta: \Sigma \rightarrow U$ 表示对任意一个 $\omega \in \Sigma$ 指定一个酉矩阵 $\Delta(\omega)$; (4) $|q_0\rangle$ ($q_0 \in Q$) 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; 称 $E_{acc}^A = \text{span}\{|q_i\rangle | q_i \in Q_{acc}\}$ 、 $E_{rej}^A = \text{span}\{|q_i\rangle | q_i \in Q_{rej}\}$ 为接受本征空间和拒绝本征空间, 记 $H_A = E_{acc}^A \oplus E_{rej}^A$.

定义 10 的量子有穷自动机是 Moore 和 Crutchfield 所提出的测量一次单向量子有穷自动机 (MO-1QFA), 它的特点是读完整个输入字符串后做一次量子测量 [19]. 区别于 MO-1QFA, Kondacs 和 Watrous 提出了测量多次单向量子有穷自动 (MM-1QFA), 它的特点是每读完一个输入字符做一次量子测量 [20]. 文献 [21] 表明了测量一次单向量子有穷自动机所接受的语言是正则的; 文献 [22,23] 表明了 MO-1QFA 接受的语言为群自动机所接受的语言, 是正则语言的真子集. 虽然 MM-1QFA 能够接受比 MO-1QFA 更多的语言 [24], 但是两个量子自动机接受的语言都为正则语言的真子集 [25]. Bianchi 和 Qiu 等提出的带有经典状态的单向量子有穷自动机, 能够识别所有正则语言 [26,27]. 在本文中, 为了体现检测的基本思想, 本文只采用了测量一次单向量子有穷自动机 (MO-1QFA).

定义 11 [24] 量子有穷自动机 (MO-1QFA) 所接受的语言称为量子正则语言.

量子安全性 $(\{A_1\})^\omega$, 它的坏前缀 $(\{A_1\})^* \{A_0\}$ 是能够被量子有穷自动机 $A = \langle Q, \Sigma, \Delta, q_0, Q_{\text{acc}} \rangle$ 接受, 其中 $Q = \{0, 1\}$, $\Sigma = \{\emptyset, \{A_0\}, \{A_1\}, \{A_0, A_1\}\}$, $q_0 = 1$, $Q_{\text{acc}} = \{|0\rangle\}$, $\Delta: \Sigma \rightarrow U$. 对 Δ 规定如下: 对于任意的 $\rho \in D(H_A)$, 当读入字符 A_1 时, 酉矩阵 $\Delta(A_1)$ 将恒等作用在前一个状态上; 当读入字符 A_0 时, 酉矩阵 $\Delta(A_0)$ 将作用在前一个状态上, 使到新的状态为 $\Delta(A_0)(\rho) = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$, 读完后做测量, 可知量子有穷自动机以一定概率接受 $(\{A_1\})^* \{A_0\}$, 它是一个量子正则语言. 称 $(\{A_1\})^\omega$ 为量子正则安全性.

定义 12 设 $MC = \langle H_{qB}, \varepsilon, l_{\text{init}}, 2^{AP}, L \rangle$ 是一个量子 Markov 链, $A = \langle Q, \Sigma, \Delta, q_0, Q_{\text{acc}} \rangle$ 是一个量子有穷自动机, 乘积量子 Markov 链定义为

$$MC \otimes A = \langle H', \varepsilon', l'_{\text{init}}, \{\text{accept}\}, L' \rangle.$$

在定义中, (1) $H' = H_{qB} \otimes H_A$; (2) $l'_{\text{init}} = l_{\text{init}} \otimes \bigvee_{\rho_0^M \in l_{\text{init}}} \text{supp}(U_{\omega_0} | q_0 \rangle \langle q_0 | (U_{\omega_0})^\dagger)$, $\omega_0 = L(\varepsilon(\rho_0^M))$; (3) $\forall \rho^M \in D(H_{qB})$, $\rho^A \in D(H_A)$, $\text{succ}(\rho^A, L(\varepsilon(\rho^M)))$ 是 ρ^A 的后续,

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

其中 $\eta'(\rho^A) = \eta_\omega(\rho^A) = U_\omega \rho^A U_\omega^\dagger$, $\omega = L(\varepsilon(\rho^M))$; (4) 对于任意的 $\rho^M \in D(H_{qB})$, 若 $\rho^A \in E_{\text{acc}}^A$, 则称 $\rho^M \otimes \rho^A$ 为乘积量子 Markov 链的终状态, 状态标签为 $L'(\rho^M \otimes \rho^A) = \{\text{accept}\}$, 否则 $L'(\rho^M \otimes \rho^A) = \emptyset$; (5) $E_{\text{accept}}^{M \otimes A} = I \otimes E_{\text{acc}}^A$ 表示为乘积 Markov 链的特征值为 accept 本征空间, 也表示乘积量子 Markov 链终状态可达空间, $P_{E_{\text{accept}}^{M \otimes A}} = I \otimes P_{E_{\text{acc}}^A}$ 表示到特征值为 accept 的本征空间 $E_{\text{accept}}^{M \otimes A}$ 的投影算子.

定义 13 设一个乘积量子 Markov 链 $MC \otimes A = \langle H', \varepsilon', l'_{\text{init}}, \{\text{accept}\}, L' \rangle$, 转移超算子 $\tilde{\varepsilon}$ 定义为

$$\tilde{\varepsilon} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + (\varepsilon \otimes \eta') \circ (I \otimes P_{E_{\text{rej}}^A}). \quad (2)$$

该超算子 $\tilde{\varepsilon}$ 表示当测量结果为 accept 时, 坏前缀被量子有穷自动机接受, 乘积量子 Markov 链状态不再演化, 程序终止; 否则乘积量子 Markov 链进入下一步状态转移, 程序进入下一次循环.

设 $MC \otimes A = \langle H', \varepsilon', l'_{\text{init}}, \{\text{accept}\}, L' \rangle$ 是一个乘积量子 Markov 链, 用 $\Diamond E_{\text{accept}}^{M \otimes A}$ 表示最终可达的状态空间, 其中 $\Diamond$ 是个模态词表示最终可达, 称从 $\rho_0^M \otimes \rho_1^A$ 出发达到可达状态空间 $E_{\text{accept}}^{M \otimes A}$ 为 $\rho_0^M \otimes \rho_1^A$ 可满足 $\Diamond E_{\text{accept}}^{M \otimes A}$, 记号为 $\rho_0^M \otimes \rho_1^A \models \Diamond E_{\text{accept}}^{M \otimes A}$, 其概率计算公式为

$$\text{Pr}^{M \otimes A}(\rho_0^M \otimes \rho_1^A \models \Diamond E_{\text{accept}}^{M \otimes A}) = \lim_{i \rightarrow \infty} \text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}^i(\rho_0^M \otimes \rho_1^A)) = \text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}_\infty(\rho_0^M \otimes \rho_1^A)), \quad (3)$$

其中 $\tilde{\varepsilon}_\infty$ 为终态计算函数, $\tilde{\varepsilon}_\infty(\rho_0^M \otimes \rho_1^A) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\varepsilon}^n(\rho_0^M \otimes \rho_1^A)$.

表 1 两种安全性检测的对比

Table 1 The contrast between two kinds of the safety checking

Type	Quantum	Property	Automaton
$\mathbb{A} \models P_{\text{safe}}$	Closed	Non-probabilistic	Co-deterministic automaton
$\rho_0^M \models P_{\text{safe}}$	Open	Probabilistic	Quantum finite automaton

定理2 $\Pr^M(\rho_0^M \models P_{\text{safe}}) = \Pr^{M \otimes A}(\rho_0^M \otimes \rho_1^A \models \Diamond E_{\text{accept}}^{M \otimes A}) = 1 - \Pr^{M \otimes A}(\rho_0^M \otimes \rho_1^A \models \Diamond E_{\text{accept}}^{M \otimes A})$, 其中 $\rho_1^A = U_\omega |q_0\rangle\langle q_0| U_\omega^\dagger$, $\omega = L(\varepsilon(\rho_0^M))$.

定理 2 指出了量子正则安全性 P_{safe} 可满足概率, 等于乘积量子 Markov 链的终状态不可达的概率. 该定理给出了量子正则安全性的检测方法, 同经典 (概率) 系统的安全性以及文献 [17] 所提出的量子系统的安全性检测思想方法一样, 都是基于自动机技术, 将检测系统的安全性转化为检测乘积系统的不变性. 值得注意的是, 该定理针对开放量子系统利用量子有穷自动机对安全性进行检测 ($\rho_0^M \models P_{\text{safe}}$), 同时也给出可满足的概率计算公式 ($\Pr^M(\rho_0^M \models P_{\text{safe}})$), 它改进了文献 [17] 的定理 5.1 关于封闭量子系统的安全性检测 ($\mathbb{A} \models P_{\text{safe}}$) 的结果. 两种安全性检测的对比可见表 1.

通过定理 2, 可以验证广义量子 Loop 程序是否终止以及终止的概率. 结合 3.2 小节, 广义量子 Loop 程序在输入态 ρ_0^M 上第 n 步终止的概率和可终止的概率分别为 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}^n(\rho_0^M \otimes \rho_1^A))$ 和 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}_\infty(\rho_0^M \otimes \rho_1^A))$. 关于这两种概率以及终态的计算步骤如下:

- (1) 建立广义量子 Loop 程序的量子 Markov 链表示;
- (2) 构造量子 Markov 链和量子自动机的乘积系统 $MC \otimes A$;
- (3) 定义乘积系统的转移超算子 $\tilde{\varepsilon}$;
- (4) 利用迭代计算 $\tilde{\varepsilon}^n(\rho_0^M \otimes \rho_1^A)$ 以及 $\tilde{\varepsilon}_\infty(\rho_0^M \otimes \rho_1^A)$, 得到第 n 步终止的概率 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}^n(\rho_0^M \otimes \rho_1^A))$ 和可终止的概率 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}_\infty(\rho_0^M \otimes \rho_1^A))$;
- (5) 利用偏迹, 计算出第 n 步终止的量子态和可终止的量子态.

4 多 (单) 量子比特系统的 GQLoop 终止验证

设由 K, M 和 X 定义的多 (单) 量子比特系统的广义量子 Loop 程序, 记为 $\text{GQLoop}(1)$, 对应的量子 Markov 链 $MC = \langle H_{qB}, \{F, K \circ M_1, M_0, I\}, l_{\text{init}}, 2^{AP}, L \rangle$, 其中 $qB = \{qb_1, qb_2, \dots, qb_n\}$ (当 $n = 1$ 时对应单量子比特系统), $X \subseteq \text{spec}(M)$, $M_1 = M_X = \sum_{m \in X} M_m$, $M_0 = M_{\bar{X}} = I_{H_{qB}} - M_X = \sum_{m \in \text{spec}(M) - X} M_m$. 设量子初态记为 ρ_0^M , 量子初始输入态记为 $\rho_{\text{in}}^{(0)} = F(\rho_0^M)$ (F 为初始化超算子). 构造一个量子有穷自动机, $A = \langle Q, \Sigma, \Delta, q_0, Q_{\text{acc}} \rangle$, 其中 $Q = \{0, 1\}$, $\Sigma = \{\emptyset, \{A_0\}, \{A_1\}, \{A_0, A_1\}\}$, $q_0 = 1$, $\Delta: \Sigma \rightarrow U$, $q_0 = 1$, $Q_{\text{acc}} = \{0\}$. 对 Δ 规定如下: 对于任意 $\rho^M \in D(H_{qB})$, $\rho^A \in D(H_A)$, 取 $\omega = L(K \circ M_1(\rho^M))$, $\Delta(\omega)(\rho^A) = p|1\rangle\langle 1| + (1-p)|0\rangle\langle 0|$, 其中 $p = \text{tr}(M_1(K \circ M_1)(\rho^M)M_1^\dagger)$. 构造乘积量子 Markov 链系统 $MC \otimes A = \langle H_{qB} \otimes H_A, \varepsilon', l'_{\text{init}}, \{\text{accept}\}, L' \rangle$, 乘积量子 Markov 链的量子初始输入态为 $\rho_{\text{in}}^{(0)} \otimes \rho_2^A = \rho_{\text{in}}^{(0)} \otimes [p_{\text{NT}}(\rho_{\text{in}}^{(0)})|1\rangle\langle 1| + p_{\text{T}}(\rho_{\text{in}}^{(0)})|0\rangle\langle 0|]$, 其中 $p_{\text{NT}}(\rho_{\text{in}}^{(0)}) = \text{tr}(M_1 \rho_{\text{in}}^{(0)} M_1^\dagger)$, $p_{\text{T}}(\rho_{\text{in}}^{(0)}) = \text{tr}(M_0 \rho_{\text{in}}^{(0)} M_0^\dagger)$.

针对 $\text{GQLoop}(1)$ 的乘积量子 Markov 链, 转移超算子 $\tilde{\varepsilon}$ 定义为

$$\tilde{\varepsilon} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + [(K \circ M_1) \otimes \Delta(\omega)] \circ (I \otimes P_{E_{\text{rej}}^A}). \quad (4)$$

为了计算第 n 步终止概率和可终止概率, 首先计算 $\tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)$ 和 $\tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)$, 然后再计算 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A))$ 和 $\text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A))$, 具体计算过程如下.

利用迭代计算出

$$\begin{aligned}\tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) &= \rho_{\text{in}}^{(0)} \otimes p_{\text{T}}(\rho_{\text{in}}^{(0)})|0\rangle\langle 0| + \sum_{k=1}^{n-1} \rho_{\text{in}}^{(k)} \otimes \prod_{l=0}^{k-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)})p_{\text{T}}(\rho_{\text{in}}^{(k)})|0\rangle\langle 0| \\ &\quad + \rho_{\text{in}}^{(n)} \otimes \prod_{l=0}^{n-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)})[p_{\text{T}}(\rho_{\text{in}}^{(n)})|0\rangle\langle 0| + p_{\text{NT}}(\rho_{\text{in}}^{(n)})|1\rangle\langle 1|].\end{aligned}$$

进一步得到

$$\begin{aligned}\tilde{\varepsilon}_{\infty}(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) &= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) \\ &= \lim_{N \rightarrow \infty} \frac{1}{N} [\rho_{\text{in}}^{(0)} \otimes p_{\text{T}}(\rho_{\text{in}}^{(0)})|0\rangle\langle 0| + \sum_{k=1}^{n-1} \rho_{\text{in}}^{(k)} \otimes \prod_{l=0}^{k-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)})p_{\text{T}}(\rho_{\text{in}}^{(k)})|0\rangle\langle 0| \\ &\quad + \rho_{\text{in}}^{(n)} \otimes \prod_{l=0}^{n-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)})[p_{\text{T}}(\rho_{\text{in}}^{(n)})|0\rangle\langle 0| + p_{\text{NT}}(\rho_{\text{in}}^{(n)})|1\rangle\langle 1|]].\end{aligned}$$

引理1 $\prod_{l=0}^n p_{\text{NT}}(\rho_{\text{in}}^{(l)}) = p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))$, 其中记 $K_{M_1}^{(1)}(\rho_{\text{in}}^{(0)}) = K(M_1 \rho_{\text{in}}^{(0)} M_1^{\dagger})$, $K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) = K(M_1 (K_{M_1}^{(n-1)}(\rho_{\text{in}}^{(0)})) M_1^{\dagger})$.

证明 当 $l = 0$ 时, $p_{\text{NT}}(\rho_{\text{in}}^{(0)}) = \text{tr}(M_1 \rho_{\text{in}}^{(0)} M_1^{\dagger})$;

当 $l = 1$ 时, $p_{\text{NT}}(\rho_{\text{in}}^{(1)}) = \text{tr}(M_1 \rho_{\text{in}}^{(1)} M_1^{\dagger}) = \text{tr}(M_1 (K_1 \circ M_1(\rho_{\text{in}}^{(0)})) M_1^{\dagger}) = \text{tr}(M_1 K[M_1 \rho_{\text{in}}^{(0)} M_1^{\dagger} / \text{tr}(M_1 \rho_{\text{in}}^{(0)} M_1^{\dagger})])$, 则 $p_{\text{NT}}(\rho_{\text{in}}^{(1)}) = \text{tr}(M_1 K_{M_1}^{(1)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger}) / \text{tr}(M_1 \rho_{\text{in}}^{(0)} M_1^{\dagger})$;

当 $l = 2$ 时, $p_{\text{NT}}(\rho_{\text{in}}^{(2)}) = \text{tr}(M_1 (K_1 \circ M_1)^2(\rho_{\text{in}}^{(0)}) M_1^{\dagger}) = \text{tr}(M_1 K_{M_1}^{(2)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger}) / \text{tr}(M_1 K_{M_1}^{(1)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger})$;

同理可以推出: $p_{\text{NT}}(\rho_{\text{in}}^{(n)}) = \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger}) / \text{tr}(M_1 K_{M_1}^{(n-1)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger})$;

所以 $\prod_{l=0}^n p_{\text{NT}}(\rho_{\text{in}}^{(l)}) = p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))$.

根据引理 1,

$$\begin{aligned}\prod_{l=0}^{k-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)}) p_{\text{T}}(\rho_{\text{in}}^{(k)}) &= \prod_{l=0}^{k-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)}) [1 - p_{\text{NT}}(\rho_{\text{in}}^{(k)})] \\ &= \prod_{l=0}^{k-1} p_{\text{NT}}(\rho_{\text{in}}^{(l)}) - \prod_{l=0}^k p_{\text{NT}}(\rho_{\text{in}}^{(l)}) = p_{\text{NT}}(K_{M_1}^{(k-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(k)}(\rho_{\text{in}}^{(0)})).\end{aligned}$$

综上所述, $\tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \rho_{\text{in}}^{(0)} \otimes p_{\text{T}}(\rho_{\text{in}}^{(0)})|0\rangle\langle 0| + \sum_{k=1}^{n-1} \rho_{\text{in}}^{(k)} \otimes [p_{\text{NT}}(K_{M_1}^{(k-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(k)}(\rho_{\text{in}}^{(0)}))]|0\rangle\langle 0| + \rho_{\text{in}}^{(n)} \otimes \{[p_{\text{NT}}(K_{M_1}^{(n-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))]|0\rangle\langle 0| + p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))|1\rangle\langle 1|\}$.

因而 GQLoop(1) 第 n 步终止的概率为

$$p_{\text{out}}^{(n)}(\rho_{\text{in}}^{(0)}) = \text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)) = 1 - \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger}).$$

进一步 $\tilde{\varepsilon}_{\infty}(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \lim_{N \rightarrow \infty} \{ \rho_{\text{in}}^{(0)} \otimes p_{\text{T}}(\rho_{\text{in}}^{(0)})|0\rangle\langle 0| + \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^{n-1} \rho_{\text{in}}^{(k)} \otimes [p_{\text{NT}}(K_{M_1}^{(k-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(k)}(\rho_{\text{in}}^{(0)}))]|0\rangle\langle 0| + \sum_{n=1}^N \rho_{\text{in}}^{(n)} \otimes \{[p_{\text{NT}}(K_{M_1}^{(n-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))]|0\rangle\langle 0| + p_{\text{NT}}(K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}))|1\rangle\langle 1|\} \}$.

所以 GQLoop(1) 可终止的概率为

$$p_{\text{out}}^{\infty}(\rho_{\text{in}}^{(0)}) = \text{tr}(P_{E_{\text{accept}}^{M \otimes A}} \tilde{\varepsilon}_{\infty}(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^{\dagger}).$$

图 4 (网络版彩图) 单量子比特系统第 n 步终止示意图Figure 4 (Color online) The n th termination figure of single qubit quantum system

定理3 对于多(单)量子比特系统, 针对 GQLoop(1), 有

- (1) 第 n 步终止的概率为 $p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger)$;
 - (2) 第 n 步终止的量子态为 $\rho_{\text{out}}^{(n)} = \sum_{k=0}^n [p_{\text{NT}}^{(k-1)}(\rho_{\text{in}}^{(0)}) - p_{\text{NT}}^{(k)}(\rho_{\text{in}}^{(0)})] \rho_{\text{in}}^{(k)} / p_T^{(n)}(\rho_{\text{in}}^{(0)})$, 其中 $p_{\text{NT}}(K_{M_1}^{(-1)}(\rho_{\text{in}}^{(0)})) = 1$, $\rho_{\text{in}}^{(k)} = K_{M_1}^{(k)}(\rho_{\text{in}}^{(0)})$;
 - (3) 可终止的概率为 $p_T^\infty(\rho_{\text{in}}^{(0)}) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger)$;
 - (4) 可终止的终态为 $\rho_{\text{out}}^\infty = \tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \rho_{\text{out}}^{(n)}$.
- 该定理也适用于单量子比特系统的广义量子 Loop 程序终止验证.

例2 设一个广义量子 Loop 程序 (GQLoop(2)), 其输入态为 $\rho_{\text{in}}^{(0)} = \alpha^2|0\rangle\langle 0| + \alpha\sqrt{1-\alpha^2}|0\rangle\langle 1| + \alpha\sqrt{1-\alpha^2}|1\rangle\langle 0| + (1-\alpha^2)|1\rangle\langle 1|$, 其中 α 为实数; 投影算子是 $M_1 = |1\rangle\langle 1|$, $M_0 = |0\rangle\langle 0|$, K 表示比特翻转信道. 其运算元 $E_0 = \sqrt{p}I$, $E_1 = \sqrt{1-p}X$, X 为 pauli 算子.

根据定理 3, 计算出 $p_{\text{NT}}^n(\rho_{\text{in}}^{(0)}) = \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger)$, $K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) = (1-\alpha^2)p^{n-1}(1-p)|0\rangle\langle 0| + (1-\alpha^2)p^n|1\rangle\langle 1|$, 得到 $p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - (1-\alpha^2)p^n$. GQLoop(2) 终止情况如下:

- (1) 在第 n 步终止概率为 $p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - (1-\alpha^2)p^n$ (终止情况如图 4).
- (2) 当 $0 < p < 1$ 时, GQLoop(2) 可终止概率为 $p_T^\infty(\rho_{\text{in}}^{(0)}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N (1-\alpha^2)p^n = 1$, GQLoop(2) 是可终止的; 当 $p = 0$ 时, GQLoop(2) 是终止的; 当 $p = 1$ 且 $\alpha^2 = 1$, GQLoop(2) 是终止的.

图 4 是使用不同的 α 和不同的 p 获得的终止示意图, 由图 4 可知单量子比特系统第 n 步终止情况与初始输入态、超算子 (量子信道)、测量算子有关.

5 复合系统的 GQLoop 终止验证

设在复合系统上执行广义量子 Loop 程序, 记为 GQLoop(3). 这里的复合系统是指主系统与环境系统耦合 (张量积) 形成的一个封闭的量子系统. 设主系统和环境在超算子 K 下执行 Loop 程序, 有三种测量算子 $M_1 \otimes I$, $I \otimes M_1$, $M_1 \otimes M_1$.

针对 GQLoop(3) 的乘积量子 Markov 链, 转移超算子 $\tilde{\varepsilon}$ 定义为

$$\tilde{\varepsilon} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + \{K \circ \tilde{M} \otimes \Delta(\omega)\} \circ (I \otimes P_{E_{\text{rej}}^A}), \quad (5)$$

其中 $\tilde{M}$ 指的是 $M_1 \otimes I$, $I \otimes M_1$, $M_1 \otimes M_1$ 其中之一, 其余符号规定如式 (4).

定理4 对于复合系统, GQLoop(3) 的量子初始输入态为 $\rho_{\text{in}}^{(0)}$, 环境从状态 $|e_0\rangle$ 出发, 则有

- (1) 第 n 步终止的概率为 $p_{\text{T}}^{(n)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|) = 1 - \text{tr}(\tilde{M}K_{\tilde{M}}^{(n)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)\tilde{M}^\dagger)$;
- (2) 第 n 步终态为 $\rho_{\text{out}}^{(n)} = \text{Tr}_e(\sum_{k=0}^n p_{\text{NT}}(K_{\tilde{M}}^{(k-1)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)) - p_{\text{NT}}(K_{\tilde{M}}^{(k)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)))(\rho_{\text{in}}^{(k)} \otimes |e_0\rangle\langle e_0|) / p_{\text{T}}^{(n)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)$;
- (3) 可终止的概率为 $p_{\text{T}}^\infty(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(\tilde{M}K_{\tilde{M}}^{(n)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)\tilde{M}^\dagger)$;
- (4) 可终止的终态为 $\rho_{\text{out}}^\infty = \tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \rho_{\text{out}}^{(n)}$.

例3 设一个主系统是单量子比特系统, 它通过控制非门变换 $K = M_0 \otimes I + M_1 \otimes X$, X 为 Pauli 算子, 测量算子 $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. 假定环境从状态 $|e_0\rangle = |0\rangle$ 出发, 主系统处于初始输入态 $\rho_{\text{in}}^{(0)}$, 则 $E_0 = \langle 0|K|0\rangle = |0\rangle\langle 0|$, $E_1 = \langle 1|K|0\rangle = |1\rangle\langle 1|$, 于是 $K(\rho_{\text{in}}^{(0)} \otimes |0\rangle\langle 0|)K^\dagger = \sum_{ij} E_i \rho_{\text{in}}^{(0)} E_j^\dagger \otimes |i\rangle\langle j|$, $i, j = 0, 1$. 关于第 n 步终止概率和可终止的概率计算如下:

(1) 第 n 步终止概率为 $1 - \text{tr}((M_1 \otimes I)K_{M_1 \otimes I}^{(n)}(\tilde{\rho})(M_1 \otimes I)^\dagger)$, 其中 $\tilde{\rho} = K(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|) = U(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|)$.

进一步计算 $(M_1 \otimes I)\tilde{\rho}(M_1 \otimes I)^\dagger = M_1 \rho_{\text{in}}^{(0)} M_1^\dagger \otimes |1\rangle\langle 1|$, $K(M_1 \rho_{\text{in}}^{(0)} M_1^\dagger \otimes |1\rangle\langle 1|) = E_1 \rho_{\text{in}}^{(0)} E_1^\dagger \otimes |0\rangle\langle 0|$.

利用迭代计算出: 当 n 为奇数, $K_{M_1 \otimes I}^{(n)}(\tilde{\rho}) = E_1 \rho_{\text{in}}^{(0)} E_1^\dagger \otimes |0\rangle\langle 0|$; 当 n 为偶数, $K_{M_1 \otimes I}^{(n)}(\tilde{\rho}) = E_1 \rho_{\text{in}}^{(0)} E_1^\dagger \otimes |1\rangle\langle 1|$, 则

$$\text{tr}((M_1 \otimes I)K_{M_1 \otimes I}^{(n)}(\tilde{\rho})(M_1 \otimes I)^\dagger) = \text{tr}(M_1 \rho_{\text{in}}^{(0)} M_1^\dagger) = \text{tr}(M_1 \rho_{\text{in}}^{(0)}).$$

故 GQLoop(3) 在测量算子为 $M_1 \otimes I$ 下, 第 n 步终止概率为

$$p_{\text{out}}^{(n)}(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|) = 1 - \text{tr}(M_1 \rho_{\text{in}}^{(0)}).$$

(2) 可终止概率为

$$\begin{aligned} p_{\text{out}}^\infty(\rho_{\text{in}}^{(0)} \otimes |e_0\rangle\langle e_0|) &= 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1 \otimes I}^{(n)}(\tilde{\rho}) M_1^\dagger) \\ &= 1 - \lim_{2N' \rightarrow \infty} \frac{1}{2N'} \sum_{n=1}^{2N'} \text{tr}(M_1 K_{M_1 \otimes I}^{(n)}(\tilde{\rho}) M_1^\dagger) = 1 - \text{tr}(M_1 \rho_{\text{in}}^{(0)}). \end{aligned}$$

根据上述计算, 在测量算子为 $M_1 \otimes I$ 作用下, 第 n 步终止和可终止的概率都为 $1 - \text{tr}(M_1 \rho_{\text{in}}^{(0)})$. 同理计算, 若测量算子是 $I \otimes M_1$ 和 $M_1 \otimes M_1$, 则第 n 步终止和可终止的概率为 1. 该结果表明在复合系统上执行酉变换量子 Loop 程序时, 在不同测量算子下会得到不同的结果.

另外, 若不考虑环境情况, 需要对 $\tilde{\rho}$ 求偏迹, 得到主系统 $K(\rho_{\text{in}}^{(0)}) = E_0 \rho_{\text{in}}^{(0)} E_0 + E_1 \rho_{\text{in}}^{(0)} E_1$, 计算出第 n 步终止和可终止的概率为 $1 - \text{tr}(M_1 \rho_{\text{in}}^{(0)})$, 但不等于 1. 该结果表明在子系统上是否执行 Loop 程序与复合系统上的测量有直接关系.

量子行走 (quantum walk) 由 Aharonov 等 [28] 给出, 是作为经典随机游走 (classical random walk) 的量子扩展, 在算法设计上具有广泛应用. 同时, 量子行走是一类典型的量子马氏链 (quantum Markov chains), 是作为分析量子马氏链性质的重要例子. 其中, 击中时 (hitting time) 是衡量量子行走到达某一 (类) 顶点速度的标准, 分为单次击中时和并行击中时 [29,30]. 对于量子行走的定义依赖于一个无向图 $G = \langle V, E \rangle$, V 为顶点集, E 为边集. 取 $v \in V$ 为目标顶点, 称投影测量 $\{M_1, M_0 = I - M_1\}$, 其中 $M_1 = |v\rangle\langle v|$ 为吸收壁 (absorbing boundary) [31]. 在系统每一步演化中, 该投影测量作用于系统演化运算 (超算子) K 之后. 若结果为 v , 则系统停止运算, 否则进入下一步循环运算. 因而借助于吸收壁, 系统运算可以看作是一个量子 Loop 程序. 此处, 目标顶点的状态可以看作是量子 Loop 程序的终状态, 目标顶点状态被吸收概率可以看作是终止概率.

图 5 双体态的开放量子行走 $G = \langle V, E \rangle$ 示意图Figure 5 The figure of open quantum walk with two qubits $G = \langle V, E \rangle$

下面针对开放量子行走 (open quantum walk)²⁾, 给出计算目标顶点状态被吸收的概率计算公式.

例4 考虑一个双体态的开放量子行走 $G = \langle V, E \rangle$, 如图 5 所示.

该系统由两个行走者 (walker) 组成, 演化先上下行走, 再左右行走, 其中 $B_z = \frac{1}{2}(I - H_1 H_2)$, $C_z = \frac{1}{2}(I + H_1 H_2)$, $B_x = \frac{1}{2}(I - X_1 X_2)$, $C_x = \frac{1}{2}(I + X_1 X_2)$, X_i 和 H_i 分别表示为作用在 qubit($i = 1, 2$) 上的 Pauli 矩阵和 Hadamard 门. 系统的量子初态为 $\rho_{\text{in}}^{(0)} = \rho_0 \otimes |U, L\rangle\langle U, L|$, 其中

$$\rho_0 = \begin{bmatrix} \frac{1}{3} & \frac{1}{\sqrt{18}} & \frac{i}{3} & \frac{i}{\sqrt{18}} \\ \frac{1}{\sqrt{18}} & \frac{1}{6} & \frac{i}{\sqrt{18}} & \frac{i}{6} \\ \frac{-i}{3} & \frac{-i}{\sqrt{18}} & \frac{1}{3} & \frac{1}{\sqrt{18}} \\ \frac{-i}{\sqrt{18}} & \frac{-i}{6} & \frac{1}{\sqrt{18}} & \frac{1}{6} \end{bmatrix}.$$

超算子 K 定义为

$$K(\rho_{\text{in}}^{(0)}) = (B_z B_x) \rho_0 (B_z B_x)^\dagger \otimes |U, L\rangle\langle U, L| + (C_z B_x) \rho_0 (C_z B_x)^\dagger \otimes |U, R\rangle\langle U, R| \\ + (B_z C_x) \rho_0 (B_z C_x)^\dagger \otimes |D, L\rangle\langle D, L| + (C_z C_x) \rho_0 (C_z C_x)^\dagger \otimes |D, R\rangle\langle D, R|.$$

进一步 $K^n(\rho_{\text{in}}^{(0)}) = K^{n-1}(K(\rho_{\text{in}}^{(0)}))$.

设目标顶点为 $\{(D, R)\}$, 吸收壁为 $\{I \otimes M_1, I \otimes (I - M_1)\}$, 其中 $M_1 = |D, R\rangle\langle D, R|$. 现考虑如下两种目标顶点状态被吸收的概率计算:

(1) 第 n 步终止概率

$$p_{\text{out}}^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - \text{tr}((I \otimes M_1) K_{I \otimes M_1}^{(n)}(\rho_{\text{in}}^{(0)})(I \otimes M_1)^\dagger) = 0.75,$$

(2) 可终止的概率

$$p_{\text{out}}^\infty(\rho_{\text{in}}^{(0)}) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}((I \otimes M_1) K_{I \otimes M_1}^{(n)}(\rho_{\text{in}}^{(0)})(I \otimes M_1)^\dagger) = 0.75.$$

上述结论表明在吸收壁为 $\{I \otimes M_1, I \otimes (I - M_1)\}$, 两种终止概率计算结果是相等的.

2) Attal S, Petruccione F, Sinayskiy I. Open quantum walks on graphs. 2014, arXiv:quant-ph/1401.3305v1

6 嵌套系统的 GQLoop 终止验证

设在嵌套系统上执行广义量子 Loop 程序, 记为 GQLoop(4). 嵌套系统是指当一个 GQLoop(内层) 嵌套到另一个 GQLoop(外层) 中, 内层的终态将作为外层的一个输入态. 嵌套系统的终止情况是相当复杂的, 当被嵌套程序终止时, 若它的终态为 0, 就不能作为外层的输入态. 本文考虑当内层是可终止的且其终态作为外层输入态时, 嵌套广义量子 Loop 程序的终止情况.

设 ρ_0^M 为量子初态, $\rho_{\text{in}}^{(0)} = F(\rho_0^M) = \alpha^2|0\rangle\langle 0| + \alpha\sqrt{1-\alpha^2}|0\rangle\langle 1| + \alpha\sqrt{1-\alpha^2}|1\rangle\langle 0| + (1-\alpha^2)|1\rangle\langle 1|$ 为量子初始输入态. 内层 GQLoop 由 $K_1, T = \{T_0, T_1\}, T_0 = |0\rangle\langle 0|, T_1 = |1\rangle\langle 1|$ 和 $X_1 = \{1\}$ 来定义, 外层 GQLoop 由 $K_2, S = \{S_0, S_1\}, S_0 = |0\rangle\langle 0|, S_1 = |1\rangle\langle 1|$ 和 $X_2 = \{1\}$ 来定义. 其中设内层 GQLoop 是可终止的, 且终止的量子态作为外层 GQLoop 的输入态.

设 ρ_0^A 为量子有穷自动机的量子初态, $\rho_{\text{in}}^{(0)} \otimes \rho_2^A$ 为乘积量子 Markov 链的量子初始输入态, 其中 $\rho_2^A = \alpha^2|0\rangle\langle 0| + (1-\alpha^2)|1\rangle\langle 1|$, 嵌套系统的转移超算子定义为

$$\tilde{\varepsilon} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + [K_2 \circ \tilde{\eta}_\infty \circ S_1 \otimes \Delta_2(\omega)] \circ [I \otimes P_{E_{\text{rej}}^A}], \quad (6)$$

其中对于任意的 $\rho \in D(H_{qB})$, $\tilde{\eta}_\infty(\rho) = \text{Tr}_A(\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\eta}^n(\rho \otimes |1\rangle\langle 1|))$, $\tilde{\eta} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + [K_1 \circ T_1 \otimes \Delta_1(\omega)] \circ (I \otimes P_{E_{\text{rej}}^A})$, 其余符号规定如式 (4).

定理5 对于嵌套系统广义量子 Loop 程序, 有

- (1) 第 n 步终止的概率为 $p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger)$;
- (2) 第 n 步终止的量子态为 $\rho_{\text{out}}^{(n)} = \sum_{k=0}^n [p_{\text{NT}}(K_{M_1}^{(k-1)}(\rho_{\text{in}}^{(0)})) - p_{\text{NT}}(K_{M_1}^{(k)}(\rho_{\text{in}}^{(0)}))] \rho_{\text{in}}^{(k)} / p_{\text{out}}^{(n)}(\rho_{\text{in}}^{(0)})$, 其中令 $p_{\text{NT}}(K_{M_1}^{(-1)}(\rho_{\text{in}}^{(0)})) = 1$;
- (3) 可终止的概率为 $p_T^\infty(\rho_{\text{in}}^{(0)}) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger)$;
- (4) 可终止的终态 $\rho_{\text{out}}^\infty = \tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \rho_{\text{out}}^{(n)}$, 其中 $K_{M_1}(\rho_{\text{in}}^{(0)}) = K_2 \circ \tilde{\eta}_\infty[M_1 \rho_{\text{in}}^{(0)} M_1^\dagger]$, $K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) = K_{M_1}^{(n-1)}(K_{M_1}(\rho_{\text{in}}^{(0)}))$.

可将定理 5 推广到 m 重嵌套情形. 设在嵌套系统上执行广义量子 Loop 程序, 最内层到最外层 GQLoop 由 $K_i, T_i = \{T_0^i, T_1^i\}, T_0^i = |0\rangle\langle 0|, T_1^i = |1\rangle\langle 1|$ 和 $X_i = 1$ 来定义, 其中 $i = 1, 2, \dots, m$, 则转移超算子定义为

$$\tilde{\varepsilon} = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + [K_m \circ \tilde{\eta}_\infty^{m-1} \circ \tilde{\eta}_\infty^{m-2} \circ \dots \circ \tilde{\eta}_\infty^1 \circ T_1^m \otimes \Delta_m(\omega)] \circ [I \otimes P_{E_{\text{rej}}^A}], \quad (7)$$

其中对于任意的 $\rho \in D(H_{qB})$, $\tilde{\eta}_\infty^i(\rho) = \text{Tr}_A(\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N (\tilde{\eta}^i)^n(\rho \otimes |1\rangle\langle 1|))$, $\tilde{\eta}^i = (I \otimes I) \circ (I \otimes P_{E_{\text{acc}}^A}) + [K_i \circ T_1^i \otimes \Delta_i(\omega)] \circ (I \otimes P_{E_{\text{rej}}^A})$. 经计算有

$$p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger), \quad (8)$$

$$p_T^\infty(\rho_{\text{in}}^{(0)}) = 1 - \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger), \quad (9)$$

其中 $K_{M_1}(\rho_{\text{in}}^{(0)}) = K_m \circ \tilde{\eta}_\infty^{m-1} \circ \tilde{\eta}_\infty^{m-2} \circ \dots \circ \tilde{\eta}_\infty^1 (M_1 \rho_{\text{in}}^{(0)} M_1^\dagger)$, $K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) = K_{M_1}^{(n)}(K_{M_1}(\rho_{\text{in}}^{(0)}))$.

例5 设一个嵌套系统的广义量子 Loop 程序, 其中内层 GQLoop 的主体由比特翻转信道 K_1 (运算元 $\sqrt{p}I, \sqrt{1-p}X$) 描述, 并由其终态作为外层 GQLoop 的输入态, 外层 GQLoop 由幅值阻尼信道 K_2 (运算元 $\sqrt{1-r}|1\rangle\langle 1| + |0\rangle\langle 0|, \sqrt{r}|0\rangle\langle 1|$) 描述 (见图 6). 该嵌套系统的广义量子 Loop 程序的终止情况如下.

图 6 嵌套系统的 GQLoop

Figure 6 The GQLoop for the nested quantum system

图 7 (网络版彩图) 嵌套系统第 n 步终止示意图Figure 7 (Color online) The n th termination figure of the nested system

(1) $\tilde{\varepsilon}(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \rho_{\text{in}}^{(0)} \otimes \alpha^2 |0\rangle\langle 0| + [K_2 \circ \tilde{\eta}_\infty \circ S_1 \otimes \Delta_1(\omega)](\rho_{\text{in}}^{(0)} \otimes (1 - \alpha^2) |1\rangle\langle 1|) = \rho_{\text{in}}^{(0)} \otimes \alpha^2 |0\rangle\langle 0| + K_2 \circ \tilde{\eta}_\infty(|1\rangle\langle 1| \otimes \eta_\infty((1 - \alpha^2) |1\rangle\langle 1|))$.

(2) $\tilde{\eta}_\infty(|1\rangle\langle 1|) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\eta}^n(|1\rangle\langle 1| \otimes |1\rangle\langle 1|)$, 其中

$$\begin{aligned} \tilde{\eta}(|1\rangle\langle 1| \otimes |1\rangle\langle 1|) &= [(K_1 \circ T_1) \otimes \Delta_2(\omega)] \circ [I \otimes P_{E_{\text{acc}}^A}] (|1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\ &= [(1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|] \otimes [1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|]. \end{aligned}$$

设 $B = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$, 则

$$\begin{aligned} \sum_{n=1}^N \tilde{\eta}^n(|1\rangle\langle 1| \otimes |1\rangle\langle 1|) &= \sum_{n=1}^N \left[\sum_{k=0}^{n-1} B \otimes (1-p)p^k |0\rangle\langle 0| + B \otimes p^{n-1} B \right] \\ &= B \otimes \left[1 - \frac{1-p^{N-1}}{N(1-p)} \right] |0\rangle\langle 0| + B \otimes \frac{1-p^{N-1}}{(1-p)^N} B, \end{aligned}$$

所以

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\eta}^n(|1\rangle\langle 1| \otimes |1\rangle\langle 1|) = B \otimes |0\rangle\langle 0|,$$

因而 $\tilde{\eta}_\infty(\rho) = \text{Tr}_A(B \otimes |0\rangle\langle 0|) = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$.

(3) $K_2 \circ \tilde{\eta}_\infty(|1\rangle\langle 1|) = K_2(B) = (1-p+rp)|0\rangle\langle 0| + (1-r)p|1\rangle\langle 1|$.

另外, $\Delta_1(\omega)(1-\alpha^2)|1\rangle\langle 1| = (1-\alpha^2)[(1-p+rp)|0\rangle\langle 0| + (1-r)p|1\rangle\langle 1|]$.

令 $C = (1-p+rp)|0\rangle\langle 0| + (1-r)p|1\rangle\langle 1|$.

(4) $\tilde{\varepsilon}(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \rho_{\text{in}}^{(0)} \otimes \alpha^2 |0\rangle\langle 0| + C \otimes (1-\alpha^2) |1\rangle\langle 1|$.

利用迭代计算出

$$\tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \rho_{\text{in}}^{(0)} \otimes \alpha^2 |0\rangle\langle 0| + C \otimes (1-\alpha^2)[1 - ((1-r)p)^{N-1}] |0\rangle\langle 0| + C \otimes [p(1-r)]^{n-1} (1-\alpha^2) |1\rangle\langle 1|,$$

$$\tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \rho_{\text{in}}^{(0)} \otimes \alpha^2 |0\rangle\langle 0| + C \otimes (1-\alpha^2) |0\rangle\langle 0|,$$

得到 GQLoop 第 n 步终止的概率为

$$p_T^{(n)}(\rho_{\text{in}}^{(0)}) = 1 - p_{\text{NT}}(\tilde{\varepsilon}^n(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)) = 1 - (1-\alpha^2)(p(1-r))^n \text{ (终止情况示意图如图 7);}$$

当 $|1 - p + rp| < 1$ 时, 可终止的概率为

$$p_T^\infty(\rho_{\text{in}}^{(0)}) = 1 - p_{NT}(\tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)) = 1,$$

即 GQLoop 可终止.

图 7 是使用不同的 α 、不同的 p 、不同的 r 获得的终止示意图, 由图可知嵌套系统第 n 步终止情况与初始输入态、内外层超算子 (量子信道)、测量算子有关.

7 GQLoop 终止的充要条件

7.1 有限步内终止的充要条件

下面给出广义量子 Loop 程序在任意输入态 $\rho_{\text{in}}^{(0)}$ 上有限步内终止的充要条件.

引理2 设 $\rho_{\text{in}}^{(0)} = \sum_{i=1}^n p_i \rho_i^{(0)}$, 其中对于每一个 i , 有 $p_i > 0$, $\rho_i^{(0)} \in D(H_{qB})$ 且 $\sum_i p_i = 1$, 那么广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止当且仅当它对每一个 i , GQLoop 都是在 $\rho_i^{(0)}$ 上终止.

证明 若广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止, 则有 $\text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger) = 0$. 该式成立当且仅当 $\sum_i p_i \text{tr}(M_1 K_{M_1}^{(n)}(\rho_i^{(0)}) M_1^\dagger) = 0$, $\text{tr}(M_1 K_{M_1}^{(n)}(\rho_i^{(0)}) M_1^\dagger) = 0$, 即对每一个 i 都是在 $\rho_i^{(0)}$ 上终止.

推论1 广义量子 Loop 程序终止当且仅当在所有输入纯态上终止.

定义14 设 ε 和 ε^* 是两个超算子, 如果对于任意的 Hermite 算子 M 和 $\rho \in D(H_{qB})$, 有 $\text{tr}(M\varepsilon(\rho)) = \text{tr}(\varepsilon^*(M)\rho)$, 则称 ε 和 ε^* 是 (Schrödinger-Heisenberg) 对偶的 [4].

定理6 设 ε 有算子和表示 $\varepsilon(\rho) = \sum_i E_i \rho E_i^\dagger$, 任意的 Hermite 算子 M 和对于任意的 $\rho \in D(H_{qB})$, 有 $\varepsilon^*(M) = \sum_i E_i^\dagger M E_i$ [12].

设广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止, 则存在 $n \in \mathbb{N}$, $\text{tr}(M_1 K_{M_1}^{(n)}(\rho_{\text{in}}^{(0)}) M_1^\dagger) = 0$, 或 $\text{tr}((K_{M_1}^{(n)})^* (M_1) \rho_{\text{in}}^{(0)}) = 0$, 故有 $(K_{M_1}^{(n)})^* (M_1) \rho_{\text{in}}^{(0)} = 0$.

引理3 广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止当且仅当存在 $n \in \mathbb{N}$ 有 $(K_{M_1}^{(n)})^* (M_1) \rho_{\text{in}}^{(0)} = 0$.

定理7 广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止的充要条件是存在 $n \in \mathbb{N}$, $j = \{1, 2, \dots, n\}$, $i_j = \{1, 2, \dots, d\}$, 有 $E_{i_1 i_2 \dots i_n}^\dagger M_1 E_{i_1 i_2 \dots i_n} \rho_{\text{in}}^{(0)} = 0$, 其中 $E_{i_1 i_2 \dots i_n} = E_{i_1} E_{i_2} \dots E_{i_n}$.

证明 根据引理 3, 广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上终止, 当且仅当存在某一个正整数 n 有 $(K_{M_1}^{(n)})^* (M_1) \rho_{\text{in}}^{(0)} = 0$, 故当且仅当 $\sum_i F_i^\dagger M_1 F_i \rho_{\text{in}}^{(0)} = 0$, 其中 $F_i = E_{i_1} E_{i_2} \dots E_{i_n}$. $F_i^\dagger M_1 F_i \rho_{\text{in}}^{(0)}$ 是半正定, 所以对于任意的 i , $F_i^\dagger M_1 F_i \rho_{\text{in}}^{(0)} = 0$.

引理 3 和定理 7 表明判定 GQLoop 在输入态 $\rho_{\text{in}}^{(0)}$ 上有限步内是否终止可以归结为矩阵的乘积计算.

7.2 可终止的充要条件

下面给出广义量子 Loop 程序在任意输入态 $\rho_{\text{in}}^{(0)}$ 上可终止的充要条件.

引理4 设 $\rho_{\text{in}}^{(0)} = \sum_{i=1}^n p_i \rho_i^{(0)}$, 其中对于每一个 i , 有 $p_i > 0$, $\rho_i^{(0)} \in D(H_{qB})$ 且 $\sum_i p_i = 1$, 那么广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上可终止当且仅当它对每一个 i , GQLoop 都是在 $\rho_i^{(0)}$ 上可终止.

证明 由于 $\rho_{\text{in}}^{(0)} = \sum_{i=1}^n p_i \rho_i^{(0)}$, $\tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A) = \tilde{\varepsilon}_\infty(\sum_{i=1}^n p_i \rho_i^{(0)} \otimes \rho_2^A) = \sum_{i=1}^n p_i \tilde{\varepsilon}_\infty(\rho_i^{(0)} \otimes \rho_2^A)$, 所以 $\text{tr}(P_{\text{accept}}^{M \otimes A} \tilde{\varepsilon}_\infty(\rho_{\text{in}}^{(0)} \otimes \rho_2^A)) = 0$, 当且仅当 $\text{tr}(P_{\text{accept}}^{M \otimes A} \tilde{\varepsilon}_\infty(\rho_i^{(0)} \otimes \rho_2^A)) = 0$.

推论2 广义量子 Loop 程序是可终止的当且仅当在所有输入纯态上是可终止的.

引理5 广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上可终止当且仅当 $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N (K_{M_1}^{(n)})^* (M_1) \rho_{\text{in}}^{(0)} = 0$.

定理8 广义量子 Loop 程序在输入态 $\rho_{\text{in}}^{(0)}$ 上可终止的充要条件是对于任意的 $j = \{1, 2, \dots, n\}$, $i_j = \{1, 2, \dots, d\}$, 有 $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N E_{i_1 i_2 \dots i_n}^\dagger M_1 E_{i_1 i_2 \dots i_n} \rho_{\text{in}}^{(0)} = 0$, 其中 $E_{i_1 i_2 \dots i_n} = E_{i_1} E_{i_2} \dots E_{i_n}$.

引理 5 和定理 8 表明, 判定 GQLoop 在输入态上是否可终止可以归结为求无穷序列 $\{E_{i_1 i_2 \dots i_n}^\dagger M_1 E_{i_1 i_2 \dots i_n} \rho_{\text{in}}^{(0)}\}$ 的 cesàro 算术平均值的极限值.

8 结论

有限步内终止和几乎终止的两种定义只能刻画以概率为 1 终止的广义量子 Loop 程序, 而不能很好描述以任意概率终止的情形. 为了解决该问题, 本文引入了以一定概率在第 n 步终止和可终止, 并对该四种终止定义进行了比较, 说明了后两者是前两者的推广. 广义量子 Loop 程序是一种量子 Markov 链, 相应程序终止问题可以归结为量子 Markov 链的量子正则安全性的可满足性问题, 运用模型检测技术推导出广义量子 Loop 程序在第 n 步终止和可终止的概率和量子终态的函数显式表达式. 针对单量子比特系统、多量子比特系统、复合系统、嵌套系统的广义量子 Loop 程序, 利用算法, 给出终止概率、终态的计算公式, 并通过几种常用量子信道, 验证了广义量子 Loop 程序的终止情况. 最后, 针对广义量子 Loop 程序在有限步内终止和可终止的两种情况, 研究了程序终止的充要条件. 从而, 本文基于量子安全性检测很好地解决了广义量子 Loop 程序一般性终止验证的问题.

参考文献

- Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 1–12
- Selinger P. Towards a quantum programming language. Math Struct Comput Sci, 2004, 14: 527–586
- Apt K R, De Boer F S, Olderog E R. Verification of Sequential and Concurrent Programs. 3rd ed. New York: Springer, 2009. 55–79
- Ying M S, Yu N K, Feng Y, et al. Verification of quantum programs. Sci Comput Program, 2013, 78: 1679–1700
- Dijkstra E W. A Discipline of Programming. Englewood Cliffs: Prentice Hall Inc, 1976. 41–44
- Ying M S. Floyd-hoare logic for quantum programs. ACM Trans Program Lang Syst, 2011, 33: 1–49
- Ying M S, Feng Y. Quantum loop programs. Acta Inform, 2010, 47: 221–250
- Feng Y, Yu N K, Ying M S. Model checking quantum Markov chains. J Comput Syst Sci, 2013, 79: 1181–1198
- Feng Y, Hahn E M, Turrini A, et al. QPMC: a model checker for quantum programs and protocols. In: Proceedings of the 20th International Symposium on Formal Methods. Switzerland: Springer International Publishing, 2015. 265–272
- Li Y J, Yu N K, Ying M S. Termination of nondeterministic quantum programs. Acta Inform, 2014, 51: 1–24
- Li X P. Generalized quantum loop program. Dissertation for M.A. Degree. Xi'an: Shaanxi Normal University, 2011 [李小鹏. 广义量子 Loop 程序. 硕士学位论文. 西安: 陕西师范大学, 2011]
- Lei H X. Study on some problems about verification of quantum program. Dissertation for PH.D. Degree. Xi'an: Shaanxi Normal University, 2013 [雷红轩. 量子程序验证中若干问题研究. 博士学位论文. 西安: 陕西师范大学, 2013]
- Lei H X, Xi Z J, Li Y M. Some properties of generalized quantum loop program. Acta Electron Sin, 2013, 41: 727–732 [雷红轩, 席政军, 李永明. 广义量子 Loop 程序的若干性质. 电子学报, 2013, 41: 727–732]
- Lin Y G, Lei H X, Li Y M. Model checking of safety property over quantum Markov chain. Acta Electron Sin, 2014, 42: 2191–2197 [林运国, 雷红轩, 李永明. 量子马尔可夫链安全性模型检测. 电子学报, 2014, 42: 2191–2197]

- 15 Ying S G, Feng Y, Yu N K, et al. Reachability probabilities of quantum Markov chains. In: Proceedings of the 24th International Conference on Concurrency Theory. Berlin: Springer, 2013. 334–348
- 16 Baier C, Katoen J P. Principles of Model Checking. Cambridge: MIT Press, 2008
- 17 Ying M S, Li Y J, Yu N K, et al. Model-checking linear-time properties of quantum systems. ACM Trans Comput Logic, 2014, 15: 1–31
- 18 Li L Z. Determination of equivalence between quantum computing models and some basic problems in quantum communication. Dissertation for PH.D. Degree. Guang zhou: Sun Yat-Sen University, 2009 [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. 博士学位论文. 广州: 中山大学, 2009]
- 19 Moore C, Crutchfield J P. Quantum automata and quantum grammars. Theor Comput Sci, 2000, 237: 275–306
- 20 Kondacs A, Watrous J. On the power of quantum finite state automata. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science. Miami Beach: IEEE Computer Society Press, 1997. 66–75
- 21 Ambainis A, Kikusts A, Valdat M. On the class of languages recognizable by 1-way quantum finite automata. In: Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science. Berlin: Springer, 2001. 75–86
- 22 Bertoni A, Carpentieri M. Regular languages accepted by quantum automata. Inform Comput, 2001, 165: 174–182
- 23 Brodsky A, Pippenger N. Characterizations of 1-way quantum finite automata. SIAM J Comput, 2002, 31: 1456–1478
- 24 Ambainis A, Freivalds R. One-way quantum finite automata: strengths, weaknesses and generalizations. In: Proceedings of the 39th Annual Symposium on Foundations of Computer Science. Palo Alto: IEEE Computer Society Press, 1998. 332–341
- 25 Mischczak J A. High-Level Structures for Quantum Computing. California: Morgan & Claypool Publishers, 2012. 19–32
- 26 Bianchi M P, Mereghetti C, Palano B. On the power of one-way automata with quantum and classical states. In: Proceedings of the 20th International Conference on Implementation and Application of Automata. Berlin: Springer, 2014. 84–97
- 27 Zheng S G, Qiu D W, Li L Z, et al. One-way finite automata with quantum and classical states. In: Bordihn H, Kutrib M, Truthe B, eds. Languages Alive. Berlin: Springer, 2012. 273–290
- 28 Aharonov Y, Davidovich L, Zagury N. Quantum random walks. Phys Rev A, 1993, 48: 1687–1690
- 29 Krovi H, Brun T A. Hitting time for quantum walks on the hypercube. Phys Rev A, 2006, 73: 032341
- 30 Kempe J. Discrete quantum walks hit exponentially faster. Probab Theory Related Fields, 2005, 133: 215–235
- 31 Ambainis A, Bach E, Nayak A, et al. One-dimensional quantum walks. In: Proceedings of the 33th ACM Symposium on Theory of Computation. New York: ACM Press, 2001. 60–69

Verification of termination of generalized quantum Loop program based on safety checking

LIN YunGuo^{1,2} & LI YongMing^{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

*E-mail: liyongm@snnu.edu.cn

Abstract To address the termination problem of the generalized quantum Loop program, in this paper, we first introduce two definitions of termination and almost termination. We show that their expressive power regarding the termination of a program is not sufficient. To compensate for this, we define two other definitions: the n th termination with a specified probability and terminability, and we obtain some conclusions by comparing these four definitions. Secondly, we introduce the definition of the quantum (regular) safety property, which is an

important kind of linear-time property of quantum Markov chains. We show that the satisfiability probability of the quantum (regular) safety property is equivalent to the unreachability probability of the termination state in the product of the quantum Markov chains. Then, we discuss a checking technique for the quantum regular safety property. By applying this technique, we reduce the termination problem of the generalized quantum Loop program into the satisfiability problem of the quantum regular safety property, and we propose an algorithm to calculate the probability and the termination state of the n th termination and the terminability. To determine the termination state and the probability of a multi-qubit (single-qubit) quantum system, compound quantum system, and nested quantum system, we derive the probability and the termination state of their n th termination and their terminability, and we present expressions for calculating them. Finally, we prove the necessary and sufficient conditions for the finite-step termination and terminability of the generalized quantum Loop program.

Keywords quantum Loop program, quantum Markov chains, quantum automata, program termination, safety property

LIN YunGuo was born in 1979. Currently, he is a Ph.D. student in the College of Computer Science at the Shaanxi Normal University, Xi'an, China. His research interests include quantum computing, quantum information, and model checking.

LI YongMing was born in 1966. He received the Ph.D. degree from the Sichuan University. Currently, he is a Professor in the College of Computer Science at the Shaanxi Normal University, Xi'an, China. His research interests include computational intelligence, quantum logic, quantum computation, and quantum information.