几类非确定型量子程序的终止验证

雷红轩[1,2],彭家寅[1,2],刘 熠[1,2]
(1. 内江师范学院数学与信息科学学院,四川内江 641112; 2. 四川省高等学校数值仿真重点实验室,四川内江 641112)

摘 要: 程序验证是保证程序正确性的关键技术. 由于经典世界和量子世界的本质不同,经典程序验证的技术和工具不能直接应用到量子系统. 而量子程序设计语言是描述量子系统的一种新的形式化模型,量子程序的验证问题就显得更为迫切和必要. 本文首先讨论了量子通讯中常用的比特翻转、相位翻转、去极化、幅值阻尼、相位阻尼等信道作为特殊的非确定型量子程序从计算基态开始运行时的可达集合和终止集合等程序验证问题. 其次,把上述五种量子程序两两组合组成非确定型量子程序,根据这五种量子程序的可达集合之相似点,最终合并成三种非确定型量子程序,重点讨论了这三种非确定型量子程序从计算基态开始运行时的终止和发散等程序验证问题. 研究表明:这三种非确定型量子程序从计算基态 0 开始运行时都是终止的;而从计算基态 1 开始运行时:比特翻转信道和去极化信道组成的非确定型量子程序的终止和发散与分别刻画它们的两个参数有关;比特翻转信道和相位翻转信道组成的非确定型量子程序的终止和发散只与刻画比特翻转信道的参数有关;幅值阻尼信道和相位阻尼信道组成的非确定型量子程序是发散的,其发散条件与刻画量子信道的两个参数都没有关系. 本文的结果可以为量子信息安全中量子通讯协议的验证提供理论和技术支持.

关键词: 量子通讯; 量子程序; 程序验证; 信息安全
中图分类号: TP301.6 **文献标识码:** A **文章编号:** 0372-2112 (2016)12-2932-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.12.017

Termination Verification of Some Kinks Nondeterministic Quantum Programs

LEI Hong-xuan[1,2], PENG Jia-yin[1,2], LIU Yi[1,2]
(1. *School of Mathematics and Information Science of Neijiang Normal University, Neijiang, Sichuan* 641112, *China*;
2. *Key Laboratory of Numerical Simulation of Sichuan Province, Neijiang, Sichuan* 641112, *China*)

Abstract: Program verification is the key technology to ensure the correctness of the program. However, due to essential differences of the classical and quantum world, classical program verification techniques and tools cannot be applied directly to the quantum system. Since quantum programming language is a new formal model of quantum system, the verification problem of quantum program is more urgent and necessary. We investigate the program verification for the reachable set and the terminating set of specific nondeterministic quantum program described respectively by bit flip channel, phase flip channel, depolarizing channel, amplitude damping channel and phase damping channel starting from computational basic states in quantum communication systems. Then, we combine pairwise the above five quantum programs into nondeterministic quantum programs, and merge these nondeterministic quantum programs into three nondeterministic quantum programs in terms of the similarities of the reachable set of five quantum programs, and discuss the problem for termination and divergence of these three nondeterministic quantum programs starting from computational basic states. The results shows that these three nondeterministic quantum programs starting from computational basic state 0 are terminated, while starting from computational basic state 1, the termination and the divergence of nondeterministic quantum program consisted by bit flip channel and depolarizing channel relates to the two parameters describing two quantum channels, the termination and the divergence of nondeterministic quantum program consisted by bit flip channel and phase flip channel relates to one parameter describing bit flip channel, and nondeterministic quantum program consisted by amplitude damping channel and phase damping channel is divergence without the two parameters describing quantum channel. And the results provide theoretical and technical sup-

收稿日期:2015-07-06;修回日期:2015-11-06;责任编辑:覃怀银
基金项目:四川省教育厅重点科研项目(No. 14ZA0242);教育部数学与应用数学专业综合改革(No. ZG0464);四川省数学与应用数学专业综合改革(No. 01249);四川省教育厅科研创新团队基金(No. 15TD0027);四川省应用基础研究计划(No. 2015JY0120)

port for verification of quantum communication protocol in quantum information security.

Key words: quantum communication; quantum programs; program verification; information security

1 引言

Shor[1]关于大数的质因子分解算法以及 Grover[2]关于数据库搜索算法的相继出现,显示出量子计算在某些计算领域比经典计算更有效[3]. 当前,量子算法还处在较低水平的量子线路的探索阶段. 正如 Abramsky[4]所说的,高水平的概念化的方法对量子系统的设计、编程、推理是很必要的. 正如此,在过去的 20 多年中,多种量子程序语言被先后定义和提出. 比如,Knill[5]最先提出了设计量子程序语言,Ömer[6]第一次给出了真正的量子程序语言并对其进行了计算仿真,Selinger[7]指出一个量子程序由超算子描述. 正确性是程序的最重要的属性之一. 长期以来,如何保证程序的正确性、提高软件的可信度一直是计算机科学界高度关注的一个重要问题,也是推动计算机科学发展的主要动力之一. 由于量子通讯协议可以由量子程序表示,所以量子程序的验证问题就显得更为迫切和必要.

同时,一些量子过程代数也被先后提出,如 Gay 和 Nagarajan[8]提出了 CQP 代数,Feng 等[9]提出了 qCCS 代数,这些代数系统为量子通讯和非确定型程序建立了良好的模型. 最近,Li[10]等作者定义了一个语言独立的非确定型量子程序的模型,Yu[11]等作者提出了并发量子程序的概念和模型. 在这些模型中,量子程序是由有限个量子队列组成的,这些量子队列是由状态空间上的量子 Markov 链描述. 本文在上述工作和作者已有成果的基础上,首先讨论量子通讯中常用的比特翻转、相位翻转、去极化、幅值阻尼、相位阻尼等信道作为特殊的非确定型量子程序—确定型量子程序,从计算基态开始运行时的可达集合、终止集合、发散集合等情况. 其次按照可达集合重点讨论这五种信道按照一定的组合方式组成的三种非确定型量子程序从计算基态开始运行时的终止和发散情况,进一步为量子程序和量子协议的验证提供理论和技术支持.

2 基本概念

文中用到的有关量子计算的基本概念见文献[3]. 用 $D(H)$ 表示 Hilbert 空间 H 上所有密度算子之集. 设 $\boldsymbol{\rho}\in D(H)$,$\varepsilon$ 是一个超算子,$\{\boldsymbol{E}_i\}$ 是其运算元,则对任意的 $\boldsymbol{\rho}$,有 $\varepsilon(\boldsymbol{\rho})=\sum_i \boldsymbol{E}_i\boldsymbol{\rho}\boldsymbol{E}_i^\dagger$,且满足 $\sum_i \boldsymbol{E}_i^\dagger\boldsymbol{E}_i=\boldsymbol{I}$.

定义 1[10]　设 H 是一个有限维 Hilbert 空间,它也是量子程序的状态空间. 一个非确定型量子程序是二元组 $P=(\{\varepsilon_i\mid i=1,\cdots,m\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$,其中

(1)ε_i 是 H 上的超算子,$i=1,\cdots,m$;

(2)$\{\boldsymbol{M}_0,\boldsymbol{M}_1\}$ 是 H 上的测量算子.

一个非确定型量子程序的一个计算是随机地选取 m 个超算子中的一个组成的有限或无限的计算序列,在整个计算过程中,测量算子 $\{\boldsymbol{M}_0,\boldsymbol{M}_1\}$ 作用在每一步上,以决定程序是终止还是继续运行. 这里选取"yes-no"测量,当测量结果为 0 时,程序终止,此时程序状态进入一个终止空间;否则,当测量结果为 1 时,程序将进入下一步,继续完成保迹的超算子 ε.

程序 P 的执行表定义为集合

$$S=\{1,2,\cdots,m\}^\infty=\{s_1s_2\cdots s_k\cdots\mid s_k\in\{1,2,\cdots,m\},k\geqslant 0\} \tag{1}$$

程序 P 的有限执行表定义为集合

$$S_{\text{fin}}=\{1,2,\cdots,m\}^*=\bigcup_{n=0}^{\infty}\{1,2,\cdots,m\}^n \tag{2}$$

为方便起见,用 θ 表示空串. 对任意的 $s=s_1\cdots s_k\in S_{\text{fin}}$,用 $|s|$ 表示 s 的长度. 对每一个 $|s|\leqslant n$,$s(\leqslant n)$ 表示 s 的头部 $s_1s_2,\cdots,s_n$,也写 $s=s_1s_2\cdots\in S$ 的头部为

$$s(\leqslant n)=s_1s_2\cdots s_n\in S_{\text{fin}} \tag{3}$$

和尾部为

$$s(>n)=s_{n+1}s_{n+2}\cdots\in S \tag{4}$$

为了简单表示,用 T_i 表示如下的超算子

$$T_i(\boldsymbol{\rho})=\varepsilon_i(\boldsymbol{M}_1\boldsymbol{\rho}\boldsymbol{M}_1^\dagger),0\leqslant i\leqslant m \tag{5}$$

其中,$\boldsymbol{\rho}\in D(H)$. 进而,对任意的 $s=s_1s_2,\cdots,s_n\in S_{\text{fin}}$,写

$$T_s=T_{s_n}\circ\cdots\circ T_{s_2}\circ T_{s_1} \tag{6}$$

特别地,$T_\theta(\boldsymbol{\rho})=\boldsymbol{\rho}$. 设 $\boldsymbol{\rho}\in D(H)$ 为输入态,程序 P 按照执行表 $s=s_1s_2,\cdots,\in S$ 执行,在 n 步后程序的状态为 $T_{s(\leqslant n)}(\boldsymbol{\rho})$.

定义 2[10]　设非确定型量子程序的输入态为 $\boldsymbol{\rho}$,对任意一有限执行表 $s\in S_{\text{fin}}$,定义程序 P 在 s 内终止的概率为

$$t_s(\boldsymbol{\rho})=\sum_{n=0}^{|s|}\operatorname{tr}(\boldsymbol{M}_0T_{s(\leqslant n)}(\boldsymbol{\rho})\boldsymbol{M}_0^\dagger) \tag{7}$$

如果程序按照 $s=s_1s_2\cdots$ 执行,则程序在不超过 n 步终止的概率为 $t_{s(\leqslant n)}(\boldsymbol{\rho})$. 进而,程序在有限步终止的概率为

$$t_s(\boldsymbol{\rho})=\lim_{n\to\infty}t_{s(\leqslant n)}(\boldsymbol{\rho})=\sum_{n=0}^{\infty}\operatorname{tr}(\boldsymbol{M}_0T_{s(\leqslant n)}(\boldsymbol{\rho})\boldsymbol{M}_0^\dagger) \tag{8}$$

显然,$\operatorname{tr}(\boldsymbol{\rho})\geqslant t_s(\boldsymbol{\rho})$,且 $\operatorname{tr}(\boldsymbol{\rho})-t_s(\boldsymbol{\rho})$ 是程序在状态 $\boldsymbol{\rho}$ 运行执行表 s 时发散的概率.

对一个非确定型量子程序 P,沿着任意一个执行表 $s\in S$ 的执行都是可能的. 因此,下面给出在所有可能的执行路径上程序终止概率的定义如下:

定义 3[10]　从状态 $\boldsymbol{\rho}$ 开始运行的非确定型量子程序 P 的终止概率定义为 $t(\boldsymbol{\rho})=\inf\{t_s(\boldsymbol{\rho})\mid s\in S\}$.

定义 4[10]　(1)开始于状态 $\boldsymbol{\rho}$ 的非确定型量子程

序 P 的可达集合定义为 $R(\boldsymbol{\rho})=\{T_s(\boldsymbol{\rho})\mid s\in S_{\text{fin}}\}$.

(2)对任意的 $\boldsymbol{\rho}\in D(H)$,如果 $t(\boldsymbol{\rho})=\text{tr}(\boldsymbol{\rho})$,则称 $\boldsymbol{\rho}$ 是程序 P 的终止状态,简称为终态. 用 T 表示程序 P 的所有终态的集合,即 $T=\{\boldsymbol{\rho}\in D(H)\mid t(\boldsymbol{\rho})=\text{tr}(\boldsymbol{\rho})\}$.

(3)对任意的 $\boldsymbol{\rho}\in D(H)$,如果对某些 $s\in S$,有 $t_s(\boldsymbol{\rho})=0$,则称 $\boldsymbol{\rho}$ 是 P 的发散态. 用 D 表示程序 P 的所有发散态的集合,即 $D=\{\boldsymbol{\rho}\in D(H)\mid t_s(\boldsymbol{\rho})=0,\text{对某些 }s\in S\}$.

等式 $t(\boldsymbol{\rho})=\text{tr}(\boldsymbol{\rho})$ 被叫做非确定型量子程序 P 的终止条件. 这个条件是说,只要程序 P 从状态 $\boldsymbol{\rho}$ 开始,则它一定会在有限步内终止且终止概率为 1.

下面分别用 $\boldsymbol{I},\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}$ 表示单位矩阵、Pauli-$\boldsymbol{X}$ 矩阵、Pauli-$\boldsymbol{Y}$ 矩阵、Pauli-$\boldsymbol{Z}$ 矩阵. $H_2=\text{span}\{|0\rangle,|1\rangle\}$,$\boldsymbol{M}_0=|0\rangle\langle 0|$,$\boldsymbol{M}_1=|1\rangle\langle 1|$.

3 常用信道组成的确定型量子程序的可达集合和终态

为便于阅读,用 $\boldsymbol{E}_i,i=1,\cdots,5$ 和 $\varepsilon_i,i=1,\cdots,5$ 分别表示比特翻转、相位翻转、去极化、幅值阻尼、相位阻尼等信道的运算元和 Kraus 算子和表示(超算子).

3.1 比特翻转信道组成的确定型量子程序的可达集合和终态

比特翻转信道的运算元及其 Kraus 算子和表示分别为 $\boldsymbol{E}_{11}=\sqrt{p_1}I,\boldsymbol{E}_{12}=\sqrt{1-p_1}\boldsymbol{X}$ 和 $K_1(\boldsymbol{\rho})=\sum\limits_{i=1,2}\boldsymbol{E}_{1i}\boldsymbol{\rho}\boldsymbol{E}_{1i}^{\dagger}$,则由比特翻转信道组成的确定型量子程序为 $P=(\{K_1\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$.

经计算 P 从计算基态 $|0\rangle$ 或 $|1\rangle$ 运行时的可达集合分别为 $R(|0\rangle\langle 0|)=\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$ 和 $R(|1\rangle\langle 1|)=\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$,而 $|0\rangle,|1\rangle\in T,D=\varnothing$.

3.2 相位翻转信道组成的确定型量子程序的可达集合和终态

相位翻转信道的运算元和 Kraus 算子和表示为 $\boldsymbol{E}_{21}=\sqrt{p_2}\boldsymbol{I},\boldsymbol{E}_{22}=\sqrt{1-p_2}\boldsymbol{Z}$ 和 $K_2(\boldsymbol{\rho})=\sum\limits_{i=1,2}\boldsymbol{E}_{2i}\boldsymbol{\rho}\boldsymbol{E}_{2i}^{\dagger}$,则由相位翻转信道组成的确定型量子程序为 $P=(\{K_2\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$.

经计算 P 从计算基态 $|0\rangle$ 或 $|1\rangle$ 开始运行时的可达集合分别为 $R(|0\rangle\langle 0|)=\{|0\rangle\langle 0|\}$ 和 $R(|1\rangle\langle 1|=\{|1\rangle\langle 1|\}$. 同时,当 $\boldsymbol{\rho}=|0\rangle\langle 0|$ 时,由 $t(|0\rangle\langle 0|)=\text{tr}(\boldsymbol{M}_0|0\rangle\langle 0|\boldsymbol{M}_0^{\dagger})=1$ 知,$\boldsymbol{\rho}=|0\rangle\langle 0|\in T$;当 $\boldsymbol{\rho}=|1\rangle\langle 1|$ 时,由 $t(|0\rangle\langle 0|)=0$ 知,$\boldsymbol{\rho}=|1\rangle\langle 1|\in D$.

3.3 去极化信道组成的非确定型量子程序的可达集合和终态

去极化信道的运算元和 Kraus 算子和表示分别为 $\boldsymbol{E}_{31}=\dfrac{\sqrt{4-3p_3}}{2}\boldsymbol{I},\boldsymbol{E}_{32}=\dfrac{\sqrt{p_3}}{2}\boldsymbol{X},\boldsymbol{E}_{33}=\dfrac{\sqrt{p_3}}{2}\boldsymbol{Y},\boldsymbol{E}_{34}=\dfrac{\sqrt{p_3}}{2}\boldsymbol{Z}$ 和 $K_3(\boldsymbol{\rho})=\sum\limits_{i=1,2,3,4}\boldsymbol{E}_{3i}\boldsymbol{\rho}\boldsymbol{E}_{3i}^{\dagger}$,则由去极化信道组成的确定型量子程序为 $P=(\{K_3\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$.

经计算 P 从计算基态 $|0\rangle$ 或 $|1\rangle$ 运行时的可达集合均为 $R(|0\rangle\langle 0|)=R(|1\rangle\langle 1|)=\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$,而 $|0\rangle,|1\rangle\in T,D=\varnothing$.

3.4 幅值阻尼信道组成的确定型量子程序的可达集合和终态

幅值阻尼信道的运算元和 Kraus 算子和表示为 $\boldsymbol{E}_{41}=\begin{pmatrix}1&0\\0&\sqrt{1-p_4}\end{pmatrix}$,$\boldsymbol{E}_{42}=\begin{pmatrix}0&\sqrt{p_4}\\0&0\end{pmatrix}$ 和 $K_4(\boldsymbol{\rho})=\sum\limits_{i=1,2}\boldsymbol{E}_{4i}\boldsymbol{\rho}\boldsymbol{E}_{4i}^{\dagger}$,则由幅值阻尼信道组成的确定型量子程序为 $P=(\{K_4\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$.

经计算 P 从计算基态 $|0\rangle$ 或 $|1\rangle$ 开始运行时的可达集合分别为 $R(|0\rangle\langle 0|)=\{|0\rangle\langle 0|\}$ 和 $R(|1\rangle\langle 1|)=\{|1\rangle\langle 1|\}$. 同时,当取 $\boldsymbol{\rho}=|0\rangle\langle 0|,t(\boldsymbol{\rho})=\text{tr}(\boldsymbol{M}_0\boldsymbol{\rho}\boldsymbol{M}_0^{\dagger})=1,\boldsymbol{\rho}=|0\rangle\langle 0|\in T$;当 $\boldsymbol{\rho}=|1\rangle\langle 1|,t(\boldsymbol{\rho})=0,\boldsymbol{\rho}=|1\rangle\langle 1|\in D$.

3.5 相位阻尼信道组成的确定型量子程序的可达集合和终态

相位阻尼信道的运算元和 Kraus 算子和表示为 $\boldsymbol{E}_{51}=\begin{pmatrix}1&0\\0&\sqrt{1-p_5}\end{pmatrix}$,$\boldsymbol{E}_{52}=\begin{pmatrix}0&0\\0&\sqrt{p_5}\end{pmatrix}$ 和 $K_5(\boldsymbol{\rho})=\sum\limits_{i=1,2}\boldsymbol{E}_{5i}\boldsymbol{\rho}\boldsymbol{E}_{5i}^{\dagger}$,则由相位阻尼信道组成的确定型量子程序为 $P=(\{K_5\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\})$.

经计算 P 从计算基态 $|0\rangle$ 或 $|1\rangle$ 开始运行时的可达集合分别为 $R(|0\rangle\langle 0|)=\{|0\rangle\langle 0|\}$ 和 $R(|1\rangle\langle 1|)=\{|1\rangle\langle 1|\}$. 同时,当取 $\boldsymbol{\rho}=|0\rangle\langle 0|,t(\boldsymbol{\rho})=\text{tr}(\boldsymbol{M}_0\boldsymbol{\rho}\boldsymbol{M}_0^{\dagger})=1,\boldsymbol{\rho}=|0\rangle\langle 0|\in T$;当 $\boldsymbol{\rho}=|1\rangle\langle 1|,t(\boldsymbol{\rho})=0,\boldsymbol{\rho}=|1\rangle\langle 1|\in D$.

综上,在单量子比特空间 H_2 中,五种确定型量子程序从计算基态 $|0\rangle$ 或 $|1\rangle$ 开始运行时有如下结论:

(1)比特翻转信道 K_1 和去极化信道 K_3 从 $\{|0\rangle,|1\rangle\}$ 开始运行时的可达集合相同,即 $R(|0\rangle\langle 0|)=R(|1\rangle\langle 1|)=\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$,而 $|0\rangle,|1\rangle\in T,D=\varnothing$.

(2)相位翻转信道 K_2、幅值阻尼信道 K_4、相位阻尼信道 K_5 从 $|0\rangle$ 开始运行时的可达集合均为 $R(|0\rangle\langle 0|)=\{|0\rangle\langle 0|\}$,且 $|0\rangle\in T$;而从 $|1\rangle$ 开始运行时的可达集合均为 $R(|1\rangle\langle 1|)=\{|1\rangle\langle 1|\}$ 且 $|1\rangle\in D$,此时 $D\neq\varnothing$.

4 几种常用量子信道组成的非确定型量子程序

由上一节的分析,下面我们根据这五种确定型量

子程序的可达集合之相似点选取几种特殊的组合讨论这五种量子信道两两组合组成的非确定型量子程序从计算基态$\{|0\rangle,|1\rangle\}$开始运行时的终止和发散情况,即:

(1)比特翻转信道 K_1 和去极化信道 K_3 组成的非确定型量子程序;

(2)比特翻转信道 K_1 和相位翻转信道 K_2 组成的非确定型量子程序;

(3)幅值阻尼信道 K_4 和相位阻尼信道 K_5 组成的非确定型量子程序.

4.1 比特翻转信道和去极化信道组成的非确定型量子程序

比特翻转信道和去极化信道组成的非确定型量子程序为

$$P=(\{K_1,K_3\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\}) \tag{9}$$

4.1.1 K_1 执行 m 次后 K_3 执行 n 次

(*a*)当$\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_1(\leqslant m)s_3(\leqslant n)$从初态$|0\rangle\langle 0|$运行时是终止的.

(*b*)当$\boldsymbol{\rho}=|1\rangle\langle 1|$时:$T_{s_1(\leqslant m)}(\boldsymbol{\rho})=p_1^m|1\rangle\langle 1|+p_1^{m-1}(1-p_1)|0\rangle\langle 0|$,令$\boldsymbol{\rho}'=p_1^m|1\rangle\langle 1|+p_1^{m-1}(1-p_1)|0\rangle\langle 0|$,则

$$T_{s_3(\leqslant n)}(\boldsymbol{\rho}')=p_1^m\left(\frac{2-p_3}{2}\right)^{n-1}\left[\frac{2-p_3}{2}|1\rangle\langle 1|+\frac{p_3}{2}|0\rangle\langle 0|\right]$$

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=(1-p_1^m)+p_1^m\frac{p_3}{2}\left[1+\frac{2-p_3}{2}+\cdots+\left(\frac{2-p_3}{2}\right)^{n-1}\right].$$

对终止概率 $t(\boldsymbol{\rho})$的讨论如下:

(1)当 $p_1=1,p_3=0$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=0$$

即$\boldsymbol{\rho}=|1\rangle\langle 1|\in D$.

(2)当 $p_1=0$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1$$

即$\boldsymbol{\rho}=|1\rangle\langle 1|\in T$.

(3)$p_1=1,p_3\neq 0$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1-\left(\frac{2-p_3}{2}\right)^n,t(\boldsymbol{\rho})=1.$$

(4)$p_1\neq 1,p_3\neq 0$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1-\left(\frac{2-p_3}{2}\right)^n p_1^m$$

即当 $m\to\infty$,或 $n\to\infty$,或 $m,n\to\infty$ 时,$t(\boldsymbol{\rho})=1$.

(5)$p_1\neq 1,p_3=1$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1-\left(\frac{2-p_3}{2}\right)^n p_1^m$$

即当 $m\to\infty$,或 $n\to\infty$,或 $m,n\to\infty$ 时,$t(\boldsymbol{\rho})=1$.

(6)$0<p_1<1,0<p_3<1$ 时:

$$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1-\left(\frac{2-p_3}{2}\right)^n p_1^m$$

即当 $m\to\infty$,或 $n\to\infty$,或 $m,n\to\infty$ 时,$t(\boldsymbol{\rho})=1$.

(7)当 $p_1\neq 1,p_3=0$ 时:

$t_{s_1(\leqslant m)s_3(\leqslant n)}(\boldsymbol{\rho})=1-p_1^m,t(\boldsymbol{\rho})=1,m\to\infty$.

命题 1　比特翻转信道(K_1)和去极化信道(K_3)组成的非确定型量子程序 P 按执行表 $s=s_1(\leqslant m)s_3(\leqslant n)$运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=1,p_3=0$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$开始运行时是发散的;否则,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$开始运行时是终止的.

4.1.2 K_3 执行 m 次后 K_1 执行 n 次

(*a*)当$\boldsymbol{\rho}=|0\rangle\langle 0|$时:

$$T_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\rho\in T$$

即,非确定型量子程序 P 按执行表 $s=s_3(\leqslant m)s_1(\leqslant n)$从初态$|0\rangle\langle 0|$运行时是终止的.

(*b*)当$\boldsymbol{\rho}=|1\rangle\langle 1|$时:

$$T_{s_3(\leqslant m)}(\boldsymbol{\rho})=\left(\frac{2-p_3}{2}\right)^m|1\rangle\langle 1|+\left(\frac{2-p_3}{2}\right)^{m-1}\frac{p_3}{2}|0\rangle\langle 0|$$

令$\boldsymbol{\rho}'=\left(\frac{2-p_3}{2}\right)^m|1\rangle\langle 1|+\left(\frac{2-p_3}{2}\right)^{m-1}\frac{p_3}{2}|0\rangle\langle 0|$

则

$$T_{s_1(\leqslant n)}(\boldsymbol{\rho}')=\left(\frac{2-p_3}{2}\right)^m[p_1^n|1\rangle\langle 1|+p_1^{n-1}(1-p_1)|0\rangle\langle 0|],$$

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=\frac{p_3}{2}\left[1+\frac{2-p_3}{2}+\cdots+\left(\frac{2-p_3}{2}\right)^{m-1}\right]+\left(\frac{2-p_3}{2}\right)^m(1-p_1^n)$$

对终止概率 $t(\boldsymbol{\rho})$的讨论如下:

(1)当 $p_1=1,p_3=0$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=0$$

即$\boldsymbol{\rho}=|1\rangle\langle 1|\in D$.

(2)当 $p_1=0,p_3\neq 0$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1$$

即$\boldsymbol{\rho}=|1\rangle\langle 1|\in T$.

(3)当 $p_1=0,p_3=1$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1,t(\boldsymbol{\rho})=1.$$

(4)当 $p_1=1,p_3\neq 0$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1-\left(\frac{2-p_3}{2}\right)^m,t(\boldsymbol{\rho})=1,m\to\infty.$$

(5)当 $p_1\neq 1,p_3=1$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1,t(\boldsymbol{\rho})=1.$$

(6)当 $p_1=0,p_3=0$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1,t(\boldsymbol{\rho})=1.$$

(7)当 $0<p_1<1,0<p_3<1$ 时:

$$t_{s_3(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1-p_1^n\left(\frac{2-p_3}{2}\right)^m$$

即当 $m\to\infty$,或 $n\to\infty$,或 $m,n\to\infty$ 时,$t(\boldsymbol{\rho})=1$.

命题 2 比特翻转信道(K_1)和去极化信道(K_3)组成的非确定型量子程序 P 按执行表 $s=s_3(\leqslant m)s_1(\leqslant n)$ 运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=1,p_3=0$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$开始运行时是发散的;否则,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$开始运行时是终止的.

4.1.3 K_1 执行 1 次后 K_3 执行 1 次如此反复

(a)当 $\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_1s_3s_1s_3\cdots}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_1s_3s_1s_3\cdots$从初态$|0\rangle\langle 0|$运行时是终止的.

(b)初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$:

$$T_{s(\leqslant 2n)}(\boldsymbol{\rho})=\left(\frac{2-p_3}{2}\right)^n p_1^n|1\rangle\langle 1|+\left(\frac{2-p_3}{2}\right)^{n-1}\frac{p_3}{2}p_1^n|0\rangle\langle 0|,$$

$$t_{s(\leqslant 2n)}(\boldsymbol{\rho})=\left(\frac{2-2p_1+p_1p_3}{2}\right)\left[1+\frac{2-p_3}{2}p_1+\cdots+\left(\frac{2-p_3}{2}p_1\right)^{n-1}\right].$$

类似于命题 1 和命题 2 的讨论,有如下各结论.

命题 3 比特翻转信道(K_1)和去极化信道(K_3)组成的非确定型量子程序 P 按执行表 $s=s_1s_3s_1s_3\cdots$运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=1,p_3=0$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$开始运行时是发散的;否则,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$开始运行时是终止的.

4.1.4 K_3 执行 1 次后 K_1 执行 1 次如此反复

(a)当 $\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_3s_1s_3s_1\cdots}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_3s_1s_3s_1\cdots$从初态$|0\rangle\langle 0|$运行时是终止的.

(b)初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$:

$$T_{s(\leqslant 2n)}(\boldsymbol{\rho})=\left(\frac{2-p_3}{2}\right)^n p_1^n|1\rangle\langle 1|+\left(\frac{2-p_3}{2}\right)^{n-1}p_1^{n-1}(1-p_1)|0\rangle\langle 0|,$$

$$t_{s(\leqslant 2n)}(\boldsymbol{\rho})=\left(\frac{2-2p_1+p_1p_3}{2}\right)\left[1+\frac{2-p_3}{2}p_1+\cdots+\left(\frac{2-p_3}{2}p_1\right)^{n-1}\right].$$

命题 4 由比特翻转信道(K_1)和去极化信道(K_3)组成的非确定型量子程序 P 按执行表 $s=s_3s_1s_3s_1\cdots$运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=1,p_3=0$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$开始运行时是发散的;否则,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$开始运行时是终止的.

综上可得如下定理:

定理 1 设 P 是由比特翻转信道(K_1)和去极化信道(K_3)组成的非确定型量子程序,则 P 按任意的执行表 s 运行时,有如下结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=1,p_3=0$ 时,$t(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$开始运行时是发散的;否则,当 $p_1\neq 1$ 或 $p_3\neq 0$ 时,$t(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$开始运行时是终止的.

4.2 比特翻转信道和相位翻转信道组成的非确定型量子程序

比特翻转信道和相位翻转信道组成的非确定型量子程序为

$$P=(\{K_1,K_2\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\}) \tag{10}$$

4.2.1 K_1 执行 m 次后 K_2 执行 n 次

(a)当初态 $\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_1(\leqslant m)s_2(\leqslant n)}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_1(\leqslant m)s_2(\leqslant n)$ 从初态$|0\rangle\langle 0|$运行时是终止的.

(b)当初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$:$T_{s_1(\leqslant m)s_2(\leqslant n)}(\boldsymbol{\rho})=p_1^m|1\rangle\langle 1|$,$t_{s_1(\leqslant m)s_2(\leqslant n)}(\boldsymbol{\rho})=1-p_1^n$.

命题 5 非确定型量子程序 P 按执行表 $s=s_1(\leqslant m)s_2(\leqslant n)$ 运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=0$ 时,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$运行时是终止的;否则,当 $p_1=1$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$运行时是发散的.

4.2.2 K_2 执行 m 次后 K_1 执行 n 次

(a)当初态 $\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_2(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_2(\leqslant m)s_1(\leqslant n)$ 从初态$|0\rangle\langle 0|$运行时是终止的.

(b)当初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$:

$$T_{s_2(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=p_1^n|1\rangle\langle 1|+p_1^{n-1}(1-p_1)|0\rangle\langle 0|,$$

$$t_{s_2(\leqslant m)s_1(\leqslant n)}(\boldsymbol{\rho})=1-p_1^n.$$

命题 6 非确定型量子程序 P 按执行表 $s=s_2(\leqslant m)s_1(\leqslant n)$ 运行时,有下列结论:

(1)当初态为$|0\rangle\langle 0|$时是终止的;

(2)当初态为$|1\rangle\langle 1|$,且当 $p_1=0$ 时,$t_s(\boldsymbol{\rho})=1$,即程序从状态$|1\rangle\langle 1|$运行时是终止的;否则,当 $p_1=1$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态$|1\rangle\langle 1|$运行时是发散的.

4.2.3 K_1 执行 1 次后 K_2 执行 1 次如此反复

(a)当初态 $\boldsymbol{\rho}=|0\rangle\langle 0|$时:$T_{s_1s_2s_1s_2\cdots}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_2s_1s_2s_1\cdots$从初态$|0\rangle\langle 0|$运行时是终止的.

(*b*)当初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$ 时:

$$T_{s(\leqslant 2n)}(\boldsymbol{\rho})=p_1^n|1\rangle\langle 1|\ ,t_{s(\leqslant 2n)}(\boldsymbol{\rho})=1-p_1^n.$$

命题 7　非确定型量子程序 P 按执行表 $s=s_1s_2s_1s_2\cdots$ 运行时,有下列结论:

(1)当初态为 $|0\rangle\langle 0|$ 时是终止的;

(2)当初态为 $|1\rangle\langle 1|$,同时当 $p_1=0$ 时,$t_s(\boldsymbol{\rho})=1$,即程序从状态 $|1\rangle\langle 1|$ 运行时是终止的;否则,当 $p_1=1$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态 $|1\rangle\langle 1|$ 运行时是发散的.

4.2.4　K_2 执行 1 次后 K_1 执行 1 次如此反复

(*a*)当初态 $\boldsymbol{\rho}=|0\rangle\langle 0|$ 时:$T_{s_2s_1s_2s_1\cdots}(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 $s=s_2s_1s_2s_1\cdots$ 从初态 $|0\rangle\langle 0|$ 运行时是终止的.

(*b*)当初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$ 时:

$$T_{s(\leqslant 2n)}(\boldsymbol{\rho})=p_1^n|1\rangle\langle 1|\ ,t_{s(\leqslant 2n)}(\boldsymbol{\rho})=1-p_1^n.$$

命题 8　非确定型量子程序 P 按执行表 $s=s_2s_1s_2s_1\cdots$ 运行时,有下列结论:

(1)当初态为 $|0\rangle\langle 0|$ 时是终止的;

(2)当初态为 $|1\rangle\langle 1|$,且当 $p_1=0$ 时,$t_s(\boldsymbol{\rho})=1$,即程序从状态 $|1\rangle\langle 1|$ 运行时是终止的;否则,当 $p_1=1$ 时,$t_s(\boldsymbol{\rho})=0$,即程序从状态 $|1\rangle\langle 1|$ 运行时是发散的.

定理 2　设 P 是由比特翻转信道(K_1)和相位翻转信道(K_2)组成的非确定型量子程序,则程序 P 按任意执行表 s 运行时,有下列结论:

(1)当初态为 $|0\rangle\langle 0|$ 时是终止的;

(2)当初态为 $|1\rangle\langle 1|$,且当 $p_1=0$ 时,$t(\boldsymbol{\rho})=1$,即程序从状态 $|1\rangle\langle 1|$ 运行时是终止的;否则,当 $p_1=1$ 时,$t(\boldsymbol{\rho})=0$,即程序从状态 $|1\rangle\langle 1|$ 运行时是发散的;

(3)当初态为 $|1\rangle\langle 1|$ 时,程序 P 的终止和发散只与比特翻转信道(K_1)的参数 p_1 有关.

从上面的定理可以看到,比特翻转信道(K_1)和相位翻转信道(K_2)组成的非确定型量子程序 P 的终止和发散只与比特翻转信道(K_1)的参数 p_1 有关,与相位翻转信道(K_2)的参数 p_2 没有关系,这和比特翻转信道(K_1)单独作为确定型量子程序时终止和发散的结论一致.

4.3　幅值阻尼信道和相位阻尼信道组成的非确定型量子程序

幅值阻尼信道和相位阻尼信道组成的非确定型量子程序为

$$P=(\{K_4,K_5\},\{\boldsymbol{M}_0,\boldsymbol{M}_1\}) \tag{11}$$

分别选取执行表 s 为 $s'=s_4(\leqslant m)s_5(\leqslant n)$,$s''=s_5(\leqslant m)s_4(\leqslant n)$,$s'''=s_4s_5s_4s_5\cdots$,$s''=s_5s_4s_5s_4\cdots$ 经计算均有如下的结果:

(*a*)当初态 $\boldsymbol{\rho}=|0\rangle\langle 0|$ 时:$T_s(\boldsymbol{\rho})=0,t(\boldsymbol{\rho})=1,\boldsymbol{\rho}\in T$. 即,非确定型量子程序 P 按执行表 s 从初态 $|0\rangle\langle 0|$ 运行时是终止的.

(*b*)当初态 $\boldsymbol{\rho}=|1\rangle\langle 1|$ 时:

$$T_s(\boldsymbol{\rho})=(1-p_4)^l|1\rangle\langle 1|,t(\boldsymbol{\rho})=0,\boldsymbol{\rho}\in D,$$

其中 l 为幅值阻尼信道 K_4 执行的次数.

定理 3　设 P 是由幅值阻尼信道(K_4)和相位阻尼信道(K_5)组成的非确定型量子程序,则程序 P 按任意执行表 s 运行时,有下列结论:

(1)当初态为 $|0\rangle\langle 0|$ 时是终止的;

(2)当初态为 $|1\rangle\langle 1|$,$t(\boldsymbol{\rho})=0$,即程序从状态 $|1\rangle\langle 1|$ 开始运行时是发散的.

5　结束语

终止条件是研究循环程序的一个非常重要但又极其困难的课题. 事实上一般量子循环的终止是不可判定的. 本文对几类非确定型量子程序的终止和发散进行了详细的讨论,此研究对量子程序的设计和量子协议的设计都有很好的帮助和启迪作用,但对非确定型量子程序的研究还有很多的理论和实验需要完善和补充,例如对于五种常用量子信道两两组成的非确定型量子程序在别的测量算子,如 $M_0=|+\rangle\langle +|$,$M_1=|-\rangle\langle -|$ 下的终止和发散情况,及 H_2 空间中两个以上常用量子信道组合组成的非确定型量子程序的终止发散的情况如何我们在另文中加以讨论.

参考文献

[1] P W Shor. Algorithms for quantum computation: discrete logarithms and factoring[A]. Proc. 35th Annual Symp. on Foundations of Computer Science[C]. Los Alamitos, CA: IEEE Press, 1994. 124 – 134.

[2] L Grover. A fast quantum mechanical algorithm for database search[A]. Proc 28th Annual ACM Symp on the Theory of Computing[C]. New York: ACM Press, 1996. 212 – 219.

[3] M A Nielsen, I L C′huang. Quantum Computation and Quantum Information[M]. Cambridge: Cambridge University Press, 2000.

[4] S Abramsky. High-level methods for quantum computation and information[A]. Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS′04)[C]. USA: IEEE Computer Society, 2004. 410 – 414.

[5] E H Knill. Conventions for Quantum Pseudocode[R]. USA: Los Alamos National Laboratory, 1996.

[6] Bömer. A Procedural Formalism for Quantum Computing[D]. Vienna: Department of Theoretical Physics, Technical University of Vienna, 1998.

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

[8] S J Gay, R Nagarajan. Communicating quantum processes, annual symposium on principles of programming languages [A]. Proceedings of the 32nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages [C]. USA: Programming Language, 2005. 145 – 157.

[9] Y Feng, R Y Duan, M S Ying. Bisimulation for quantum processes [A]. Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL) [C]. New York: ACM Press, 2011. 523 – 534.

[10] Y J Li, N K Yu, M S Ying. Termination of nodeterministic quantum programs [J]. Acta Informatica, 2014, 51(1): 1 – 24.

[11] N K Yu, M S Ying. Reachability and termination analysis of concurrent quantum programs [J]. Lecture Notes in Computer Science, 2012, 7454: 69 – 83.

[12] M S Ying, N K Yu, Y Feng, R Y Duan. Verification of quantum programs [J]. Sci Comput Program, 2013, 78(9): 1679 – 1700.

[13] 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.
LEI Hong-xuan, XI Zheng-jun, LI Yong-ming. Some properties of genaralized quantum loop program [J]. Acta Electronica Sinica, 2013, 41(4): 727 – 732. (in Chinese)

[14] 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.
LEI Hong-xuan, XI Zheng-jun, LI Yong-ming. Commutativity of quantum weakest liberal precondition and its properties [J]. Journal of Software, 2013, 24(5): 933 – 941. (in Chinese)

[15] 林运国,雷红轩,李永明. 量子马尔可夫链安全性模型检测[J]. 电子学报,2014,42(11):2191 – 2197.
LIN Yun-guo, LEI Hong-xuan, LI Yong-ming. Model checking of safety property over quantum markov chain [J]. Acta Electronica Sinica, 2014, 42(11): 2191 – 2197. (in Chinese)

作者简介

雷红轩 男,1967 年出生于陕西洋县,博士,教授,主要研究领域为自动机理论,量子程序验证和量子模型检测.
E-mail: hongxuan_lei@163.com

彭家寅 男,1962 出生于四川资中县,博士,教授,主要研究领域为量子信息处理.
E-mail: pengjiayin62226@163.com

刘 熠 男,1979 年出生于四川仪陇县,博士,副教授,主要研究领域为智能信息处理.
E-mail: liuyiyl@126.com