几种量子程序终止的有效验证

雷红轩[1,2] 席政军[1] 李永明[1]

(陕西师范大学计算机科学学院 西安 710062)[1] (内江师范学院数学与信息科学学院 内江 641112)[2]

摘 要 基于文献[18]提出的量子程序验证方法,讨论了单量子比特系统上比特翻转、去极化、幅值阻尼、相位阻尼等信道刻画的量子程序的验证,通过选取不同的可观测算子对程序终止的情况进行了详细的讨论。研究表明,由这些量子信道所描述的量子程序的终止情况不仅依赖于输入态的选取,还依赖于可观测算子的选取。

关键词 量子程序,超算子,终止概率,程序验证

中图法分类号 TP301.6 **文献标识码** A

Valid Verification of Termination for Some Quantum Programs

LEI Hong-xuan[1,2] XI Zheng-jun[1] LI Yong-ming[1]

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)[1]

(School of Mathematics and Information Science, Neijiang Normal University, Neijiang 641112, China)[2]

Abstract Using the verification method for quantum programs proposed in [18], the verification of quantum programs on the single qubit system described by bit flip channel, depolarizing channel, amplitude damping channel and phase damping channel was investigated, and the termination conditions of a quantum program were discussed in detail by selecting the different observable operators. It shows that the termination conditions of the quantum program described by quantum channel not only depends on the selection of input state, but also depends on the selection of observable operators.

Keywords Quantum programs, Super-operator, Termination probability, Program verification

1 引言

从 20 世纪 80 年代早期以来,各种量子程序协议被先后提出,量子密码系统已经广泛应用于 Quantique、MagiQ 技术、SmartQuantum 和 NEC 中[1]。量子通讯比经典通讯最显著的优势就是它的安全性,但在设计阶段要想保证协议的正确性是很难的。由于量子通讯协议可以表示成量子程序,因此量子程序的验证问题就显得更为迫切。

1994 年,Shor[2] 提出了著名的量子因子分解算法。1996 年,Grover[3] 给出了进行数据搜索的量子搜索算法。这些算法表明量子计算在某些计算领域比经典计算更有效。当前,量子算法还处在较低水平的量子线路的阶段。最近一些学者[4-8]开始研究量子程序语言的设计和语义。Apt, Olderog[9] 在其著作中详细地介绍了序列和并发程序的验证理论和技术。Sharir, Pnueli 和 Hrat[10] 讨论了概率程序的验证问题,给出了称为 Sharir-Pnueli-Hart 方法的验证方法。Papanikolao[11] 研究了模型检测量子协议。Akatov[12] 讨论了量子程序验证的逻辑。特别是最近,应明生教授[18] 提出了由量子 Markov 链所刻画的量子程序验证的思想和方法,称其为量子 Sharir-Pnueli-Hart 方法,该方法将量子程序在终态终止的概率计算归约到在初态的概率计算上。本文对上述文献提出的量子程序的验证方法给出了一个算法,对量子通讯中常用的比特翻转、去极化、幅值阻尼、相位阻尼等信道所刻画的量子程序在选取不同的可观测算子时终止的情况进行了详细讨论。

2 量子 Sharir-Pnueli-Hart 方法

本文用到的有关量子计算的基本概念见文献[1]。用 $D(H)$ 表示 Hilbert 空间 H 上所有密度算子之集。算子的 Löwner 序定义为:$A \sqsubseteq B$ 当且仅当 $B-A$ 是一个正算子。设 M 是一个算子,如果 $M^{+}=M$,则称 M 为 Hermite 算子,其中 M^{+} 表示 M 的共轭转置。量子系统的一个可观测算子是一个 Hermite 算子。

定义 1[1] 设 ε 是 H 上的线性算子空间中的一个线性算子,如果 ε 满足下列两个条件,则称 ε 为 H 上的超算子:

(1) $\mathrm{tr}[\varepsilon(\rho)] \leqslant \mathrm{tr}(\rho)$, $\forall \rho \in D(H)$;

(2) 完全正性:设 H_R 是一个辅助 Hilbert 空间,如果 A 是 $H_R \otimes H$ 上的正算子,则 $(I_R \otimes \varepsilon)(A)$ 也是正的,其中 I_R 是

到稿日期:2012-02-03 返修日期:2012-05-22 本文受国家自然科学基金(60873119)资助。

雷红轩(1967—),男,博士生,副教授,主要研究方向为自动机理论、量子程序验证和量子模型检测,E-mail:leihx2004@yahoo.com.cn;席政军(1983—),男,博士生,主要研究方向为量子计算、量子信息论与非局域性;李永明(1966—),男,博士,教授,博士生导师,主要研究方向为计算智能、模糊系统分析、量子逻辑、量子计算、模型检测。

H_R 的单位算子。

如果条件(1)加强到 $\forall \rho\in D(H)$，$\mathrm{tr}[\varepsilon(\rho)]=\mathrm{tr}(\rho)$，则称 ε 是保迹的。

用 $CP(H)$ 表示 H 上的所有超算子之集。

ε 是 H 上的超算子，当且仅当存在一组运算元 $\{E_i\}$ 满足下列条件：

(1) $\varepsilon(\rho)=\sum_i E_i\rho E_i^+$，$\forall \rho\in D(H)$；

(2) $\sum_i E_i^+E_i\sqsubseteq I$，当 ε 是保迹的超算子时取等号，其中 I 是 H 的单位算子[1,18]。

定义 2[18] 设 $\varepsilon,\varepsilon^*\in CP(H)$，且 ε^* 把 Hermite 算子映射成 Hermite 算子。如果对任意的 Hermite 算子 M，$\forall \rho\in D(H)$，有

$$\mathrm{tr}[M\varepsilon(\rho)]=\mathrm{tr}[\varepsilon^*(M)\rho]$$

则称 ε 和 ε^* 是(Schrödinger-Heisenberg)对偶的。

设 ε 有算子和表示 $\varepsilon(\rho)=\sum_i E_i\rho E_i^+$，$\forall \rho\in D(H)$，则对任意的 Hermite 算子 M，有

$$\varepsilon^*(M)=\sum_i E_i^+ME_i$$

定义 3[18] 一个量子 Markov 链是一个三元组 (H,ε,ρ_0)，其中

(1) H 是 Hilbert 空间；

(2) ε 是保迹的超算子；

(3) ρ_0 是密度算子。

假定程序有一个终止空间。在每执行完一步后，检查程序是否结束，这里选取测量算子为“yes-no”测量，即 $\{M_0,M_1\}$ 测量算子，其中 $M_0=|0\rangle\langle 0|$，$M_1=|1\rangle\langle 1|$。也就是说，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。

为了方便表示，定义超算子：$\forall \rho\in D(H)$，$\varepsilon_i(\rho)=M_i\rho M_i^+$，$i=0,1$。这样，程序的执行过程完全由量子 Markov 链所描述，经计算可得程序的终态[18]：

$$\rho^*=\sum_{n=0}^{\infty}[\varepsilon_0\circ(\varepsilon\circ\varepsilon_1)^n](\rho_0)$$

量子 Sharir-Pnueli-Hart 方法[18](简记为 QSPHM)：为了计算正的可观测算子 P 在程序的终态 ρ^* 的平均值 $\langle P\rangle_{\rho^*}$，只需要找到一个正算子 Q 满足条件：

$(QV_1)\ \langle M_0^+PM_0+M_1^+QM_1\rangle_{\rho_0}<\infty$；

$(QV_2)\ \varepsilon^*(M_0^+PM_0+M_1^+QM_1)=Q$；

$(QV_3)\ \lim\limits_{n\to\infty}\mathrm{tr}(Q[\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n](\rho_0))=0$。

那么计算 $\langle P\rangle_{\rho^*}$ 的问题可以归约到计算可观测算子 $M_0^+PM_0+M_1^+QM_1$ 在程序的初态 ρ_0 的平均值 $\langle M_0^+PM_0+M_1^+QM_1\rangle_{\rho_0}$，即等式

$$(QC)\ \langle P\rangle_{\rho^*}=\langle M_0^+PM_0+M_1^+QM_1\rangle_{\rho_0}$$

成立。

对以上 QSPHM，下面给出单量子比特系统中量子程序验证时计算 $\langle P\rangle_{\rho^*}$ 的算法：

第一步 选定初态 ρ_0 和正的可观测算子 P；

第二步 取算子 $Q=\lambda|\varphi\rangle\langle\varphi|+\mu|\psi\rangle\langle\psi|(\lambda,\mu\geqslant 0)$，计算 $M_0^+PM_0+M_1^+QM_1$；

第三步 根据条件 (QV_1)，(QV_2)，(QV_3) 选定 Q；

第四步 计算 $\langle M_0^+PM_0+M_1^+QM_1\rangle_{\rho_0}$。

其中上述算法中 $\{|\varphi\rangle,|\psi\rangle\}$ 为 H_2 的一组标准正交基。

3 几种信道终止的判定

本文用 I,X,Y,Z 分别表示 $\mathbb{C}^2$ 上的单位矩阵、Pauli-X、Pauli-Y、Pauli-Z 矩阵，即

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},X=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}。$$

设 $\rho_0\in D(H_2)$，其中 $\rho_0=|\varphi_0\rangle\langle\varphi_0|$，$|\varphi_0\rangle=\alpha|0\rangle+\sqrt{1-\alpha^2}|1\rangle$ 为单量子比特，α 为实数。假设正算子 $Q=\lambda|\varphi\rangle\langle\varphi|+\mu|\psi\rangle\langle\psi|(\lambda,\mu\geqslant 0)$，记 $N=M_0^+PM_0+M_1^+QM_1$。

下面取 $P=|0\rangle\langle 0|$ 和 $P=|1\rangle\langle 1|$，对比特翻转、去极化、幅值阻尼、相位阻尼等信道所刻画的量子程序的终止情况分别讨论如下。

1. 比特翻转信道

比特翻转信道的运算元为 $E_{10}=\sqrt{p}I$，$E_{11}=\sqrt{1-p}X$，该信道将量子比特的状态以概率 $1-p$ 从 $|0\rangle$ 翻转到 $|1\rangle$(或者相反)，$0\leqslant p\leqslant 1$。它的 Kraus 算子和为

$$\varepsilon(\rho_0)=E_{10}\rho_0E_{10}^+E_{11}\rho_0E_{11}^+$$

(a) 取 $P=|0\rangle\langle 0|$，经计算，得

$N=|0\rangle\langle 0|+k|1\rangle\langle 1|$，且

$\varepsilon^*(N)=[p+(1-p)k]|0\rangle\langle 0|+[pk+(1-p)]|1\rangle\langle 1|$，其中 $k=\lambda|\langle\varphi|1\rangle|^2+\mu|\langle\psi|1\rangle|^2$。

由条件 (QV_2) $\varepsilon^*(N)=Q$，即有

$$k=\langle 1|Q|1\rangle=\langle 1|\varepsilon^*(N)|1\rangle=pk+(1-p)$$

即

$$(1-p)k=1-p \tag{1a}$$

再经过简单的计算可得

$$\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n(\rho_0)=(1-\alpha^2)p^n|1\rangle\langle 1|$$

$$\mathrm{tr}(Q(\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n)(\rho_0))=(1-\alpha^2)p^nk$$

分析如下：(i) 当 $|\alpha|=1$ 时，(QV_3) 成立，即当 $\rho=|0\rangle\langle 0|$ 为计算基态时，程序终止的概率为

$$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$$

(ii) 当 $|\alpha|\neq 1$，$p=1$ 时，由 (QV_3) 成立知 $k=0$，此时 $N=|0\rangle\langle 0|$，程序终止的概率为

$$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\langle\varphi_0|N|\varphi_0\rangle=\alpha^2$$

(iii) 当 $0<p<1$，$|\alpha|\neq 1$ 时，(QV_3) 成立，从式(1a)知 $k=1$，此时 $N=I$，程序终止的概率为

$$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\langle\varphi_0|N|\varphi_0\rangle=1$$

(b) 取 $P=|1\rangle\langle 1|$，类似地计算可得

$N=k|1\rangle\langle 1|$，且

$$\varepsilon^*(N)=(1-p)k|0\rangle\langle 0|+pk|1\rangle\langle 1|,(1-p)k=0 \tag{1b}$$

分析如下：(i) 当 $|\alpha|=1$ 时，(QV_3) 成立，即当 $\rho=|0\rangle\langle 0|$ 为计算基态时，程序终止的概率为

$$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$$

(ii) 当 $|\alpha|\neq 1$，$p=1$ 时，由 (QV_3) 成立知 $k=0$，此时 $N=$

0，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\langle\varphi_0|N|\varphi_0\rangle=0$

(iii) 当 $0<p<1$，$|\alpha|\neq1$ 时，(QV_3)成立，从式(1b)知 $k=0$，此时 $N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\langle\varphi_0|N|\varphi_0\rangle=0$

从以上(a)，(b)的分析可以看到，对于某些正算子 P，程序不可能终止。

2. 去极化信道

去极化信道是一类重要的量子噪声，它对一个单量子比特以概率 p 使量子比特去极化。去极化信道的运算元为 $E_{20}=\sqrt{1-\frac{3}{4}p}I$，$E_{21}=\frac{\sqrt{p}}{2}X$，$E_{22}=\frac{\sqrt{p}}{2}Y$，$E_{23}=\frac{\sqrt{p}}{2}Z$，$0\leqslant p\leqslant1$。它的 Kraus 算子和为

$\varepsilon(\rho_0)=E_{20}\rho_0E_{20}^{+}+E_{21}\rho_0E_{21}^{+}+E_{22}\rho_0E_{22}^{+}+E_{23}\rho_0E_{23}^{+}$

(a) 取 $P=|0\rangle\langle0|$，类似地计算可得：$N=|0\rangle\langle0|+k|1\rangle\langle1|$，且 $\varepsilon^*(N)=\frac{1}{2}|0\rangle\langle0|+\left(1-\frac{1}{2}p\right)k|1\rangle\langle1|$，其中 $k=\lambda|\langle\varphi|1\rangle|^2+\mu|\langle\psi|1\rangle|^2$。

由条件(QV_2) $\varepsilon^*(N)=Q$，即有

$$k=\langle1|Q|1\rangle=\left(1-\frac{1}{2}p\right)k,\ pk=0 \tag{2a}$$

经过简单的计算可得

$$\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n(\rho_0)=(1-\alpha^2)\left(1-\frac{1}{2}p\right)^n|1\rangle\langle1|$$

$$\mathrm{tr}(Q(\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n)(\rho_0))=(1-\alpha^2)\left(1-\frac{1}{2}p\right)^nk$$

分析如下：(i) 当 $0<p<1$ 时，(QV_3)成立，由式(2a) $pk=0$ 得 $k=0$，$N=|0\rangle\langle0|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2$

(ii) 当 $|\alpha|=1$，$p\neq0$ 时，(QV_3)成立，此时 $\rho=|0\rangle\langle0|$ 为计算基态，由(2a)可知 $k=0$，$N=|0\rangle\langle0|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2=1$

(iii) 当 $|\alpha|\neq1$，$p=0$ 时，从式(2a)知 $k=0$ 时，(QV_3)成立，此时 $N=|0\rangle\langle0|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2$

(iV) 当 $|\alpha|=1$，$p=0$ 时，(QV_3)成立，从式(2a)知 k 为任意值，$N=|0\rangle\langle0|+k|1\rangle\langle1|$，于是程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$

(b) 取 $P=|1\rangle\langle1|$，类似地计算可得

$N=k|1\rangle\langle1|$，且

$$\varepsilon^*(N)=\frac{1}{2}pk|0\rangle\langle0|+\left(1-\frac{1}{2}p\right)k|1\rangle\langle1|,$$

$$pk=0 \tag{2b}$$

分析如下：(i) 当 $0<p<1$ 时，(QV_3)成立，由式(2b)得 $k=0$，$N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(ii) 当 $|\alpha|=1$，$p\neq0$ 时，(QV_3)成立，此时 $\rho=|0\rangle\langle0|$ 为计算基态，由(2b)知 $k=0$，$N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2=0$

(iii) 当 $|\alpha|\neq1$，$p=0$ 时，从式(2b)知当 $k=0$ 时，(QV_3)成立，此时 $N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(iV) 当 $|\alpha|=1$，$p=0$ 时，(QV_3)成立，从式(2b)知 k 为任意值，$N=k|1\rangle\langle1|$，于是程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=k(1-\alpha^2)$

3. 幅值阻尼信道

幅值阻尼是噪声的理想模型，这个模型刻画了出现于量子力学系统中噪声的许多重要特性。幅值阻尼信道的运算元为 $E_{30}=\begin{pmatrix}1&0\\0&\sqrt{1-\gamma}\end{pmatrix}$，$E_{31}=\begin{pmatrix}0&\sqrt{\gamma}\\0&0\end{pmatrix}$，其中 $\gamma(0\leqslant\gamma\leqslant1)$可认为是丢失一个光子的概率[1]。它的 Kraus 算子和为

$\varepsilon(\rho_0)=E_{30}\rho_0E_{30}^{+}+E_{31}\rho_0E_{31}^{+}$

(a) 取 $P=|0\rangle\langle0|$，类似地计算可得 $N=|0\rangle\langle0|+k|1\rangle\langle1|$，且 $\varepsilon^*(N)=|0\rangle\langle0|+(k+(1-\gamma)k)|1\rangle\langle1|$，其中 $k=\lambda|\langle\varphi|1\rangle|^2+\mu|\langle\psi|1\rangle|^2$。

由条件(QV_2) $\varepsilon^*(N)=Q$，即有

$k=\langle1|Q|1\rangle=\langle1|\varepsilon^*(N)|1\rangle=k+(1-\gamma)k$，即

$$(1-\gamma)k=0 \tag{3a}$$

经过简单的计算可得

$\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n(\rho_0)=(1-\alpha^2)(1-\gamma)^n|1\rangle\langle1|$，

$tr(Q(\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n)(\rho_0))=(1-\alpha^2)(1-\gamma)^nk$

分析如下：(i) 当 $0<\gamma<1$ 时，(QV_3)成立，由式(3a)得 $k=1$，$N=I$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$

(ii) 当 $\gamma=0$，$|\alpha|\neq1$ 时，只有当 $k=0$ 时(QV_3)成立，此时 $N=|0\rangle\langle0|$，序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2$

(iii) 当 $|\alpha|=1$，$\gamma\neq0$ 时，(QV_3)成立，从式(3a)知 $k=1$，$N=I$，即 $\rho_0=|0\rangle\langle0|$ 为计算基态时，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$

(iV) 当 $|\alpha|=1$，$\gamma=0$ 时，(QV_3)成立，从式(3a)知 $k=0$，此时 $N=|0\rangle\langle0|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$

(b) 取 $P=|1\rangle\langle1|$，类似地计算可得

$N=k|1\rangle\langle1|$，且 $\varepsilon^*(N)=(1-\lambda)k|1\rangle\langle1|$，

$$\gamma k=0 \tag{3b}$$

分析如下：(i) 当 $0<\gamma<1$ 时，(QV_3)成立，由式(3b)得 $k=0$，$N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(ii) 当 $\gamma=0$，$|\alpha|\neq1$ 时，只有当 $k=0$ 时(QV_3)成立，此时 $N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(iii) 当 $|\alpha|=1$，$\gamma\neq0$ 时，(QV_3)成立，由式(3b)知 $k=0$，$N=0$，即 $\rho_0=|0\rangle\langle0|$ 为计算基态时，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(iV) 当 $|\alpha|=1$，$\gamma=0$ 时，(QV_3)成立，从式(3b)知 k 任意，此时 $N=k|1\rangle\langle1|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=k(1-\alpha^2)$

4. 相位阻尼信道

相位阻尼是纯粹量子力学性质的噪声过程，它描述没有能量损失下的量子信息的丢失。相位阻尼信道的运算元为 $E_{40}=\begin{pmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{pmatrix}$，$E_{41}=\begin{pmatrix}0 & 0\\ 0 & \sqrt{\gamma}\end{pmatrix}$，其中 $\gamma(0\leqslant\gamma\leqslant1)$ 可以认为是来自系统的一个光子没有能量损失的散射的概率[1]。它的 Kraus 算子和为

$\varepsilon(\rho_0)=E_{40}\rho_0E_{40}^{\dagger}+E_{41}\rho_0E_{41}^{\dagger}$

(a) 取 $P=|0\rangle\langle0|$，类似地计算可得 $N=|0\rangle\langle0|+k|1\rangle\langle1|$，且 $\varepsilon^*(N)=|0\rangle\langle0|+k|1\rangle\langle1|$，其中 $k=\lambda|\langle\varphi|1\rangle|^2+\mu|\langle\psi|1\rangle|^2$。

由条件(QV_2) $\varepsilon^*(N)=Q$，即有

$$k=\langle1|Q|1\rangle=\langle1|\varepsilon^*(N)|1\rangle=k \tag{4a}$$

经过简单的计算可得

$\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n(\rho_0)=(1-\alpha^2)|1\rangle\langle1|$，

$\mathrm{tr}(Q(\varepsilon_1\circ(\varepsilon\circ\varepsilon_1)^n)(\rho_0))=(1-\alpha^2)k$

分析如下：(i) 当$|\alpha|=1$，即当 $\rho_0=|0\rangle\langle0|$ 为计算基态时，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=1$

(ii) 当$|\alpha|\neq1$ 时，只有 $k=0$，(QV_3) 成立，此时 $N=|0\rangle\langle0|$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=\alpha^2$。

(b) 取 $P=|1\rangle\langle1|$，类似地计算可得

$N=k|1\rangle\langle1|$，且 $\varepsilon^*(N)=k|1\rangle\langle1|$，

$$k=\langle1|Q|1\rangle=\langle1|\varepsilon^*(N)|1\rangle=k \tag{4b}$$

分析如下：(i) 当$|\alpha|=1$，即 $\rho_0=|0\rangle\langle0|$ 为计算基态时，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

(ii) 当$|\alpha|\neq1$ 时，只有 $k=0$，(QV_3) 成立，此时 $N=0$，程序终止的概率为

$\langle P\rangle_{\rho^*}=\langle N\rangle_{\rho_0}=0$

从以上的分析讨论我们看到，如果选取可观测算子 $P=|0\rangle\langle0|$，则以上讨论的 4 种量子信道所描述的量子程序终止的概率不是 1 就是 α^2，当输入态 $\rho_0=|0\rangle\langle0|$ 为计算基态时，4 种程序终止的概率都为 1，这说明量子程序终止的情况和输入态的选取有关系。然而，当选取可观测算子 $P=|1\rangle\langle1|$ 时，4 种程序终止的概率除去极化信道和幅值阻尼信道中各出现一次不可判定外全为 0，即不终止。同时，我们也选取了 $P=|+\rangle\langle+|$ 为可观测算子，讨论的结果与选 $P=|0\rangle\langle0|$ 时一致，这说明量子程序终止的判定和可观测算子 P 的选取有极大关系。

结束语 本文对文献[18]提出的量子程序的验证方法给出了计算可观测算子终态平均值的算法，分别就量子通讯中常用的比特翻转、去极化、幅值阻尼、相位阻尼等信道所刻画的量子程序的终止情况进行了讨论。研究表明：这 4 种量子信道所描述的量子程序的终止情况不但依赖于输入态的选取，还与可观测算子的选取有极大关系。因此，我们在量子程序设计或量子通讯协议设计中就要考虑这些因素，以避免量子程序不能终止的情况发生。如何用所讨论的验证算法去验证如 BB84 这样的协议，我们将在另文中给出。

参 考 文 献

[1] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge University Press, Cambridge, 2000

[2] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]// Proceedings, 35th Annual Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Press, 1994: 124-134

[3] Grover L. A fast quantum mechanical algorithm for database search[C]// Proceedings, 28th Annual ACM Symposium on the Theory of Computing. 1996: 212-219

[4] Knill EH. Conventions for quantum pseudocode[R]. LAUR-96-2724. 1996

[5] Ömer B. A procedural formalism for quantum computing[D]. Department of theoretical Physics, Technical University of Vienna, 1998

[6] Sanders J W, Zuliani P. Quantum programming [C]// Proceedings, Mathematics of Program Construction 2000, LNCS 1837. 2000: 80-99

[7] Zuliani P. Quantum programming [D]. Oxford University, 2001

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

[9] Apt KR, Olderog ER. Verification of Sequential and Concurrent Programs[M]. New York: Springer-Verlag, 1997

[10] Sharir M, Pnueli A, Hrat S. Verification of probabilistic programs[J]. SIAM Journal of Computing, 1984, 13: 292-314

[11] Papanikolaou NK. Model Checking Quantum Protocols[D]. Department of Computer Science, University of Warwick, 2008

[12] Akatov D. The Logic of Quantum Program Verification[D]. Oxford University Computing Laboratory, 2005

[13] de Alfaro L. How to specify and verify the long-run average behavior of probabilistic systems[C]// Proceedings of the Annual IEEE Symposium on Logic in Compter Science (LICS). 1998: 454-465

[14] Feng Yuan, Duan Run-yao, Ji Zheng-feng, et al. Probabilistic bisimulations for quantum processes[J]. Information and Computation, 2007, 205: 1608-1639

[15] Feng Yuan, Duan Run-yao, Ji Zheng-feng, et al. Proof rules for the correctness of quantum programs[J]. Theoretical Computer Science, 2007, 386: 581-600

[16] Ying Ming-sheng, Duan Run-yao, Ji Zheng-feng. An algebra of quantum process[J]. ACM Transactions on Computation Logic, 2009, 10(3): 1-36

[17] Ying Ming-sheng, Feng Yuan. Quantum loop programs[J]. Acta Informatica, 2010, 47(4): 221-250

[18] Ying Ming-sheng, Yu Neng-kun, Feng Yuan, et al. Verification of Quantum programs[OL]. arXiv: 1106.4063, 2011