arXiv:2302.07973v1 [cs.LO] 15 Feb 2023

非确定性量子程序验证

Yuan
FengYuan.Feng@uts.edu.au
悉尼科技大学 澳大利亚

Yingte
X
uYingte.Xu@student.uts.edu.au
悉尼科技大学 澳大利亚

摘要

非确定性选择是一种有用的程序构造，它提供了一种描述程序行为的方式，而无需指定可能实现的细节。它支持程序的逐步细化，这种方法已被证明对软件开发很有用。非确定性也已引入量子编程，且非确定性量子程序的终止性已得到广泛分析。本文超越终止性分析，研究非确定性量子程序的验证，其中性质由相关希尔伯特空间上的厄米算子集合给出。本文提出了用于部分正确性和完全正确性的 Hoare 型逻辑系统，结果表明，这些系统相对于相应的语义正确性既可靠又相对完备。为展示这些证明系统的实用性，我们分析了一些量子算法，例如量子纠错方案、Deutsch 算法和非确定性量子游走。最后，我们实现了一个证明助手原型，以辅助对非确定性量子程序进行自动推理。

CCS 概念

• **计算理论** → **指称语义**；**公理语义**；**霍尔逻辑**；**程序验证**；**前置条件与后置条件**；**断言**。

关键词

量子编程、非确定性、程序验证、霍尔逻辑

ACM 参考格式：
Yuan Feng 和 Yingte Xu。2023年。《非确定性量子程序的验证》。载于 第 *28* 届 *ACM* 编程语言与操作系统架构支持国际会议论文集，第 *3* 卷（*ASPLOS '23*），*2023*年*3*月*25*日至*29*日，加拿大不列颠哥伦比亚省温哥华。ACM，纽约州纽约，18页。https://doi.org/10.1145/3582016.3582039

1 引言

在编程语言中引入非确定性，使人们能够用同一种语言描述规约及其可能的实现。它自然支持程序的逐步细化技术，而这一技术已被证明在计算机软件开发中十分有用 [1, 17, 19]。从验证的角度来看，它提供了一种方法，可以在抽象规约完全实现之前对其正确性进行推理 [5],从而能够在软件开发的最早阶段发现错误。

兼具非确定性选择和概率选择的程序已在 [8, 14, 15, 18] 中得到研究。有趣的是，正如 [8], 所指出的，描述非确定性与概率选择如何交互，有两种自然的模型。将非确定性和概率程序的执行视为与恶意对手进行的博弈，最能说明这种差异。在关系模型中，对手会在运行时执行期间作出非确定性选择，并利用截至该时刻已经发生的所有概率选择。相比之下，提升模型中的对手必须在编译时、程序实际执行之前作出所有非确定性选择。 [8] 证明，关系模型中的程序具有许多良好的代数性质，有助于静态分析和编译器设计 [9]。

多年前，非确定性也被引入量子编程。Zuliani [30] 扩展了量子守卫命令语言 qGCL [22]，加入了非确定性选择构造，以便对反事实计算 [16] 和量子混态系统进行建模与推理。非确定性量子程序的终止性分析最早在 [12],中得到研究，其中程序以一种与语言无关的方式描述：一个非确定性量子程序仅由一组具有相同希尔伯特空间的确定性量子马尔可夫链（数学上表示为超算子）以及一个用于判断程序是否已终止的二结果测量组成。后来，研究者使用线性排序超鞅技术，将终止性分析扩展到一种同时包含恶魔式和天使式非确定性的量子编程语言[11]。

尽管 [11, 12], 中已对终止性进行了分析，文献中却很少涉及非确定性量子程序的验证。本文考虑一种用于量子程序的扩展 while 语言，其中包含一个用于二元（恶魔式）非确定性选择的构造。本文的主要贡献包括：

- 一种非确定性量子程序的指称语义，其形式类似于概率情形中的提升模型。这一设计决策的依据是：在量子情形下，关系模型无法得到令人满意的定义，部分原因在于，与给定密度算子相关联的纯态系综并不唯一。

- 基于其指称语义的非确定性量子程序的部分正确性和完全正确性。与[11, 12], 相比，我们的正确性概念更加

允许出于个人或课堂用途免费制作本作品全部或部分内容的数字或纸质副本，但前提是不得为牟利或商业利益制作或分发副本，且副本首页必须包含本声明和完整引文。对于并非由作者持有版权的本作品组成部分，必须尊重其版权。注明出处后可以摘录。以其他方式复制、再版、发布到服务器或分发至列表，均须事先获得特定许可和/或支付费用。请向 permissions@acm.org 申请许可。
ASPLOS '23，*2023*年*3*月*25*日至*29*日，加拿大不列颠哥伦比亚省温哥华©
2023年版权归所有者/作者所有。出版权已授权 ACM。ACM ISBN 978-1-4503-9918-0/23/03...$15.00https://doi.org/10.1145/3582016.3582039

广泛，能够描述超出量子程序终止性的更广泛性质。

- 相对于部分正确性和完全正确性，本文提出了既可靠又相对完备的霍尔型逻辑系统。本文还探讨了说明性示例，并实现了一个原型工具，展示这些逻辑系统在证明某些量子算法正确性方面的用途，例如量子纠错方案、Deutsch 算法和非确定性量子游走。

本文其余部分安排如下。第 2 节回顾后续讨论将用到的一些量子计算基本概念。本文所讨论的非确定性量子程序的语法和指称语义见第 3 节。第 4 节是本文的主体部分，我们将在此详细阐述量子态断言以及非确定性量子程序的部分正确性和完全正确性。本文提出了针对这两种正确性概念的证明系统，并证明它们既可靠又相对完备。第 5 节探讨说明性示例，以展示这些证明系统的有效性。第 6 节介绍一个证明助手原型，该原型实现了本文开发的验证技术。最后，第 7 节总结全文，并指出若干未来研究课题。

2 量子计算背景

本节旨在统一本文将用到的一些线性代数和量子力学记号。有关背景知识的详细介绍，请参阅 [20, 第 2]章。

设 H 为有限维希尔伯特空间。遵循量子计算领域的惯例，H 中的向量用狄拉克形式表示为 $|\psi\rangle$。两个向量 $|\psi\rangle$ 和 $|\phi\rangle$ 的内积和外积分别记作 $\langle\psi|\phi\rangle$ 和 $|\psi\rangle\langle\phi|$。令 $\mathcal{L}(\mathcal{H})$ 表示 H 上线性算子的集合。记 $\mathrm{tr}(A) = \sum_{i\in I}\langle\psi_i|A|\psi_i\rangle$ 为 $A \in \mathcal{L}(\mathcal{H})$ 的迹，其中 $\{|\psi_i\rangle : i \in I\}$ 是 H 的一个（任意）标准正交基。A的伴随记作 $A^\dagger$，它是 $\mathcal{L}(\mathcal{H})$ 中唯一满足对所有 $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ 都有 $\langle\psi|A|\phi\rangle = \langle\phi|A^\dagger|\psi\rangle^*$ 的线性算子。这里，对于复数 z，z^*表示其共轭。若算子 $A \in \mathcal{L}(\mathcal{H})$ 满足以下条件，则称其为：(1) 厄米算子，若 $A^\dagger = A$；(2) 酉算子，若$A^\dagger A = I_{\mathcal{H}}$，其中 H 是 H 上的恒等算子；(3) 正算子，若对所有 $|\psi\rangle \in \mathcal{H}$，均有 $\langle\psi|A|\psi\rangle \geq 0$。每个厄米算子 A都有谱分解形式 $A = \sum_{i\in I}\lambda_i|\psi_i\rangle\langle\psi_i|$，其中 $\{|\psi_i\rangle : i \in I\}$ 构成 H 的一个标准正交基。$\mathcal{L}(\mathcal{H})$ 上的 Löwner（偏）序 $\sqsubseteq$定义为：当且仅当 $B - A$ 为正算子时，令 $A \sqsubseteq B$成立。

设 H1 和 H2 是两个有限维希尔伯特空间，$\mathcal{H}_1\otimes\mathcal{H}2$ 是它们的张量积。设 $A_i \in \mathcal{L}(\mathcal{H}_i)$。$A_1$ 和 A_2的张量积记为 $A_1\otimes A_2$，它是 $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}2)$ 中的一个线性算子，满足 $(A_1\otimes A_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A_1|\psi_1\rangle) \otimes (A_2|\psi_2\rangle)$，对所有 $|\psi_i\rangle \in \mathcal{H}_i$ 均成立。该定义可线性扩展到 $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}2)$。为简化记号，我们常将 $|\psi_1\rangle \otimes |\psi_2\rangle$ 写作 $|\psi_1\rangle|\psi_2\rangle$。

从 L(H1) 到 L(H2) 的线性算子 E 称为<style id="1">超算子。如果它将 H1 上的正算子映射为 H2 上的正算子，则称其为 (1)正；如果对于所有有限维希尔伯特空间 H，$I_{\mathcal{H}} \otimes E$ 都是正的，则称其为 (2)完全正，其中 $I_{\mathcal{H}}$是 $\mathcal{L}(\mathcal{H})$ 上的恒等超算子；(3)保迹（分别为迹非增）是指，对于任意正算子 $A \in \mathcal{L}(\mathcal{H}1)$，$\mathrm{tr}(E(A)) = \mathrm{tr}(A)$（分别为 $\mathrm{tr}(E(A)) \leq \mathrm{tr}(A)$）。

根据*Kraus* 表示定理 [10],，从 $\mathcal{L}(\mathcal{H}1)$ 到 $\mathcal{L}(\mathcal{H}2)$ 的超算子 E 是完全正的，当且仅当存在从 H1 到 H2 的线性算子 $\{E_i : i \in I\}$，称为 E 的*Kraus* 算子，使得对所有 $A \in \mathcal{L}(\mathcal{H}1)$，$E(A) = \sum_{i\in I} E_i A E_i^\dagger$。此外，E 是保迹的（分别地，迹非增的），当且仅当 $\sum_{i\in I} E_i^\dagger E_i = I_{\mathcal{H}^1}$（分别地，$\sum_{i\in I} E_i^\dagger E_i \sqsubseteq I_{\mathcal{H}_1}$）。E 的伴随 记为 $E^\dagger$，它是一个从 $\mathcal{L}(\mathcal{H}2)$ 映回 $\mathcal{L}(\mathcal{H}1)$ 的完全正超算子，其 Kraus 算子为 $\{E_i^\dagger : i \in I\}$。容易验证，对任意 $A \in \mathcal{L}(\mathcal{H}1)$ 和 $B \in \mathcal{L}(\mathcal{H}2)$，$\mathrm{tr}(E(A)\cdot B) = \mathrm{tr}(A\cdot E^\dagger(B))$。

以下为简便起见，除非另有说明，所有超算子均假设为完全正且迹非增。给定张量积空间 $\mathcal{H}_1 \otimes \mathcal{H}2$，关于 H2 的偏迹记为 $\mathrm{tr}_{\mathcal{H}_2}$，它是从 $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}2)$ 到 $\mathcal{L}(\mathcal{H}1)$ 的超算子，满足对于任意 $|\psi_i\rangle, |\phi_i\rangle \in \mathcal{H}_i, i = 1, 2$，

$$\mathrm{tr}_{\mathcal{H}_2}(|\psi_1\rangle\langle\phi_1| \otimes |\psi_2\rangle\langle\phi_2|) = \langle\phi_2|\psi_2\rangle|\psi_1\rangle\langle\phi_1|.$$

同样，该定义可线性扩展到 $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}2)$。

根据冯·诺伊曼的量子力学形式体系，[27],任何具有有限自由度的量子系统都对应一个有限维希尔伯特空间 H，称为其状态空间。当 H 的维数为 2 时，这种系统称为量子比特，它类似于经典计算中的比特。系统的纯态由 H 中的归一化向量描述。当系统以概率 $p_i\, i \in I$处于状态 $|\psi_i\rangle$ 时，称其处于混合状态，该状态由 H 上的密度算子$\sum_{i\in I} p_i|\psi_i\rangle\langle\psi_i|$表示。显然，密度算子是正的，且迹为 1。本文遵循 Selinger 的惯例，[23] 将部分密度算子（即迹不大于 1 的正算子）视为（未归一化的）量子态。直观地说，部分密度算子ρ表示一个合法的量子态 $\rho/\mathrm{tr}(\rho)$，其出现概率为 $\mathrm{tr}(\rho)$。用 $\mathcal{D}(\mathcal{H})$ 表示 H 上部分密度算子的集合。复合系统（例如由多个量子比特组成的量子系统）的状态空间，是其各组成部分状态空间的张量积。对于任意 ρ in $\mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}2)$，偏迹 $\mathrm{tr}_{\mathcal{H}_1}(\rho)$ 和 $\mathrm{tr}_{\mathcal{H}_2}(\rho)$ 分别是 ρ 在 H2 和 H1 上的约化量子态。

封闭量子系统的演化 由其状态空间上的酉算子描述：若系统在 t_1 和t_2 时的状态分别为 ρ_1 和 ρ_2，则 $\rho_2 = U\rho_1U^\dagger$，其中 U为某个酉算子。本文中常用的酉算子包括泡利-X、 Y和 Z、哈达玛 H，以及受控非门（CNOT）算子 CX，它们相对于计算基的矩阵表示分别如下：

$$X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y \triangleq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

and

$$H \triangleq \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ CX \triangleq \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

一个（投影）量子测量规则 M由状态空间H中的一组投影算子$\{P_i : i \in O\}$（特征值为0或1的厄米算子）描述，其中 O 是

测量结果集合。要求测量算子 P_i'满足完备性方程$\sum_{i\in O} P_i = I_{\mathcal{H}}$。如果系统在测量前处于状态 ρ，那么观测到结果 i 的概率为 $p_i = \mathrm{tr}(P_i\rho)$，测量后系统的状态变为 $\rho_i = P_i\rho P_i/p_i$，只要 $p_i > 0$。有时我们用L(H)中的厄米算子 M（称为可观测量）来表示投影测量。具体来说，令

$$M = \sum_{m\in spec(M)} mP_m$$

其中，$spec(M)$ 是 M 的特征值集合，而 P_m 是与 m 相关联的特征子空间上的投影算子。由 M 确定的投影测量为 $\{P_m : m \in spec(M)\}$。注意，根据迹函数的线性性，在状态 ρ 上测量 M 时，测量结果的期望值计算如下：

$$\sum_{m\in spec(M)} m\cdot \mathrm{tr}(P_m\rho) = \mathrm{tr}(M\rho).$$

最后，（不一定是封闭的）物理系统中可能发生的动力学由保迹超算子描述。典型示例包括酉变换 $\mathrm{E}_U(\rho) \quad U\rho U^\dagger$，以及在考虑所有测量后态时由测量引起的状态变换。更具体地说，演化

$$\mathcal{E}_{\mathcal{M}}(\rho) \triangleq \sum_{i\in O} p_i\rho_i = \sum_{i\in O} P_i\rho P_i$$

是一个超算子。

记号约定。为简化记号，全文采用以下约定。

- 对于有限维希尔伯特空间 H 中的纯态 $|\psi\mathrm{i}$，我们用 $[|\psi\mathrm{i}]$ 表示其对应的（秩为 1 的）密度算子；也就是说，$[|\psi\mathrm{i}]$，$|\psi\mathrm{ih}\psi|$。

- 我们用下标标明状态、算子或超算子所作用的量子系统。例如，$|\psi\mathrm{i}_q$或 $[|\psi\mathrm{i}_q]$表示量子比特 q 的纯态 $|\psi$，而CX_{q_1,q_2}表示 CNOT 算子，其中 q_1是控制量子比特，q_2是目标量子比特。此处，对于任意 $x, y \in\{0,1\}$，$CX|x\mathrm{i}|y\mathrm{i} = |x\mathrm{i}|x\oplus y\mathrm{i}$，且 $\oplus$表示异或。此外，对于一个 d $|i \quad 0 \le$维希尔伯特空间，用 $i \le d-1$ { i : } 表示其标准基（或计算基）。

- 约定将任意超算子与其在更大希尔伯特空间上的柱扩张视为相同（即将其与剩余子系统上的恒等超算子作张量积）。换言之，通过将 E 与 $\mathrm{I}_{\mathcal{H}}\otimes$E 视为相同，可将从 L(H1) 到 L(H2) 的 E 看作从 L(H⊗H1) 到 L(H⊗H2) 的算子，其中 H 为任意希尔伯特空间。特别地，任意值 $p \in [0,1]$（0 维空间上的超算子）都可看作任意有限组 V量子比特上的 $p\cdot \mathrm{I}_V$on D(H_V)。

- 约定将对单个元素的操作逐元素地扩展到集合。例如，设 $\mathbb{E}$ 和 $\mathbb{F}$ 是两个超算子集合。那么

$$\mathbb{E}\circ\mathcal{E} + \mathbb{F}\circ\mathcal{F} \triangleq \{\mathcal{E}'\circ\mathcal{E} + \mathcal{F}'\circ\mathcal{F} : \mathcal{E}' \in \mathbb{E}, \mathcal{F}' \in \mathbb{F}\}$$

其中 ∘ 表示超算子复合；也就是说，对于所有 ρ，E ∘ F (ρ) = E(F (ρ))。

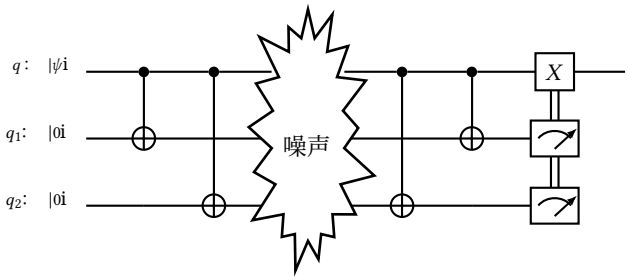

图 1：一种量子纠错方案，可纠正三个量子比特中任意一个发生的比特翻转错误。

3 非确定性量子程序

我们扩展 [6, 28] 中定义的纯量子 while 语言，以描述具有非确定性选择的量子程序。令$\mathcal{V}$为一个有限的（量子比特类型）量子变量集合，其元素记作 q，r，$\cdots$。对于 V的任意子集$\mathcal{V}$，令

$$\mathcal{H}_V \triangleq \bigotimes_{q\in V} \mathcal{H}_q,$$

其中，$\mathrm{H}_q \simeq$ H2 是与 q 关联的二维希尔伯特空间。由于我们使用下标来区分与不同量子变量关联的希尔伯特空间，因此它们在张量积中的顺序无关紧要。

3.1 语法

非确定性量子程序由以下规则定义：

$$S ::= \textbf{skip} \mid \textbf{abort} \mid \bar{q} := 0 \mid \bar{q} \mathrel{*}= U \mid S_0; S_1 \mid S_0 \square S_1 \mid \textbf{if } \mathcal{M}[\bar{q}] \textbf{ then } S_1 \textbf{ else } S_0 \textbf{ end} \mid \textbf{while } \mathcal{M}[\bar{q}] \textbf{ do } S \textbf{ end}$$

其中 S，S_0 和 S_1 是非确定性量子程序，$\bar{q}$、$q_1 \quad q_n$ 、……、是一个由互不相同的量子比特类型变量组成的（有序）元组，而 U 是酉算子，M ={P_0，P_1} 分别是 $\mathrm{H}_{\bar{q}}$ 上的二结果投影测量。有时我们也用 $\bar{q}$ 表示（无序）集合 {q_1，q_2，……、q_n}。令 $qv(S)$ 表示 S 中量子变量的集合。

这些程序构造都是标准的，待稍后给出指称语义后，其含义便会清楚。直观而言，**空操作** 是一条空操作语句，**中止** 会终止计算，且不会到达任何有效状态；$\bar{q} := 0$ 将系统 $\bar{q}$ 中的每个量子比特初始化为|0i，$\bar{q} \mathrel{*}= U$ 在系统 $\bar{q}$上应用酉算子 U，$S_0;S_1$ 是 S_0与 S_1的顺序组合，而 $S_0 \square S_1$则非确定性地选择执行 S_0或 S_1。条件语句**if**M $[\bar{q}]$ **then** S_1**else** S_0**end**和 while 语句**while**M$[\bar{q}]$**do** S**end**的行为类似于它们的经典对应物，不同之处在于，它们使用对 $\bar{q}$进行M测量的结果来决定后续操作。这些量子测量通常会改变其作用对象系统的状态。这与经典程序形成对比，因为经典程序中不存在这类副作用。

例3.1（作为非确定性程序的量子纠错方案）。纠错码广泛用于在量子通信中保护量子信息免受噪声影响

信道中或量子计算过程中。最简单的纠错码称为三量子比特翻转码，它将每个量子比特态$\alpha_0|0\rangle + \alpha_1|1\rangle$编码为一个三量子比特态 $\alpha_0|000\rangle + \alpha_1|111\rangle$（编码过程的电路实现见图 *1*左侧部分）。随后，三个量子比特都通过一个含噪量子信道，该信道会以某个较小的概率翻转量子比特（即对其施加 *Pauli-X* 算子，使其将$|0\rangle$ 变为 $|1\rangle$，并将 $|1\rangle$ 变为 $|0\rangle$）。为简单起见，我们假设三个量子比特中至多有一个发生翻转，但不知道是哪一个。有趣的是，通过应用适当设计的纠错过程（如图 *1*右侧部分所示），可以完美地检测并纠正该错误。

如果我们用非确定性选择来建模未知噪声，那么量子纠错方案（包括编码、引入错误和解码过程）可以写成如下的非确定性量子程序：

$$
\begin{aligned}
&\mathit{ErrCorr} \triangleq \\
&\quad q_1,\ q_2 := 0;\ q,\ q_1 *= CX;\ q,\ q_2 *= CX;\ \textbf{空操作} \\
&\quad \square\ q *= X \square\ q_1 *= X \square\ q_2 *= X;\ q,\ q_2 *= CX;\ q,\ q_1 *= CX;\ \textbf{如果}\ \mathcal{M}[q_2]\ \textbf{则如果}\ \mathcal{M}[q_1]\ \textbf{则}\ q *= X\ \textbf{结束}\ \textbf{结束}
\end{aligned}
$$

这里 CX 的 *CNOT* 是受控非门，$\mathcal{M}$ 表示按照计算基进行测量 $\{|0\rangle, |1\rangle\}$，而命令 $\textbf{if}\ \mathcal{M}[r]\ \textbf{then}\ S\ \textbf{end}$ 是 $\textbf{if}\ \mathcal{M}[r]\ \textbf{then}\ S\ \textbf{else skip end}$的缩写。非确定性语句对错误发生的四种不同可能性进行建模：无错误，分别在第一个、第二个和第三个量子比特上发生比特翻转错误。与顺序组合类似，我们假设（并将在给出形式语义后予以论证）非确定性选择既满足左结合律，也满足右结合律。

3.2 指称语义

本小节旨在为非确定性量子程序定义指称语义，该语义是通过提升 [6, 28] 中介绍的确定性程序的语义而得到的。

给定一个有限维希尔伯特空间 H，令 $\mathrm{S}(\mathrm{H})$ 表示 H 上超算子的集合。注意，关于如下定义的序 $\preceq$，$\mathrm{S}(\mathrm{H})$ 是一个完备偏序集（CPO）：$\mathrm{E} \preceq \mathrm{F}$ 当且仅当存在一个超算子 G，使得 $\mathrm{F} = \mathrm{E} + \mathrm{G}$。下面的引理表明，这个偏序与通过将扩展希尔伯特空间上密度算子的 Löwner序逐点提升而定义的偏序相同。

引理 3.1. 对于任意 $\mathcal{E}、\mathcal{F} \in \mathcal{S}(\mathcal{H})$，$\mathcal{E} \preceq \mathcal{F}$ 当且仅当对于任意辅助希尔伯特空间 $\mathcal{H}_\prime$ 以及任意 $\rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}_\prime)$，

$$\mathcal{E}(\rho) \sqsubseteq \mathcal{F}(\rho).$$

证明。必要性部分很容易。对于充分性部分，注意映射 $\mathrm{G} \triangleq \mathrm{F} - \mathrm{E}$ 是线性的、迹非增且完全正的。因此，它也是一个超算子。□

$$
\begin{aligned}
[\![\textbf{skip}]\!] &= \{1\} \\
[\![\textbf{abort}]\!] &= \{0\} \\
[\![\bar{q} := 0]\!] &= \left\{ Set^0_{\bar{q}} \right\} \\
[\![\bar{q} *= U]\!] &= \left\{ \mathcal{U}_{\bar{q}} \right\} \\
[\![S_0; S_1]\!] &= [\![S_1]\!] \circ [\![S_0]\!] \\
[\![S_0 \square S_1]\!] &= [\![S_0]\!] \cup [\![S_1]\!] \\
[\![\textbf{if}\ \mathcal{M}[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}]\!] &= [\![S_0]\!] \circ \mathcal{P}^0_{\bar{q}} + [\![S_1]\!] \circ \mathcal{P}^1_{\bar{q}} \\
[\![\textbf{while}\ \mathcal{M}[\bar{q}]\ \textbf{do}\ S\ \textbf{end}]\!] &= \\
&\left\{ \sum_{i=0}^{\infty} \mathcal{P}^0_{\bar{q}} \circ \eta_i \circ \mathcal{P}^1_{\bar{q}} \circ \ldots \eta_1 \circ \mathcal{P}^1_{\bar{q}} : \eta \in [\![S]\!]^{\mathbb{N}} \right\}
\end{aligned}
$$

图 2：非确定性量子程序的指称语义。

令*Prog* 为所有非确定性量子程序的集合。对于任意 $S \in \mathit{Prog}$，其指称语义 $[\![S]\!]$ 是 $\mathrm{S}(\mathrm{H}_{qv(S)})$ 中超算子的集合，其归纳定义见图2；其中$\mathrm{M}_{P^i_{\bar{q}} \rho P^i_{\bar{q}}}$ $\mathrm{P}^0_{\bar{q}}$ $\mathrm{U}_{\bar{q}}$ $|\bar{q}| = n$ $\rho = \{P^0, P^1\}$、$\mathrm{P}^i_{\bar{q}}$, $i = 0, 1$ 是满足 $\mathrm{P}^i_{\bar{q}}(\ )$ 的超算子，而*Set*和 U with 均为超算子，满足$Set^0_{\bar{q}}(\rho) = \sum_{i=0}^{2^n-1} |0\rangle_{\bar{q}}\langle i|\rho|i\rangle_{\bar{q}}\langle 0|$，并且对于所有 $\rho \in \mathrm{D}(\mathrm{H}_{\mathcal{V}})$，$\mathrm{U}_{\bar{q}}(\rho) = U_{\bar{q}} \rho U^\dagger_{\bar{q}}$。回顾一下，确定性量子程序的语义是单个超算子。我们借鉴经典程序设计理论中广泛采用的思想，在非确定性量子程序的语义中使用超算子集合来表示非确定性。

定义非确定性量子程序指称语义的一种更优雅的方法，是考虑幂域，其元素是满足某些闭包性质的超算子子集。例如，while循环的语义便是该幂域上某个斯科特连续函数的最小不动点。然而，由于本文的主要目标是为非确定性量子程序开发验证技术，我们决定采用当前的定义，因为对于没有域理论背景的普通读者而言，这种定义更直观、更易理解。

请注意，按照我们的记号约定，对于任意 $V \supseteq qv(S)$，$[\![S]\!]$ 也可以视为 $\mathrm{S}(\mathrm{H}_V)$ 的子集。例如，对于任意 $V \subseteq \mathrm{V}$，$[\![\textbf{skip}]\!]$ 中的数字 1 可以视为恒等超算子 $\mathrm{I}_{\mathcal{H}_V}$。类似地，$[\![\textbf{abort}]\!]$ 中的数字 0 可以表示作用于任意量子比特系统上的零超算子。此外，请注意，对于任意输入 ρ，$0(\rho)$ 都是零密度算子。这准确地体现了这样一种直觉：对任何输入施加**abort** 都无法产生任何有效的量子态。

由于四种基本命令 **空操作**、**中止**、$\bar{q} := 0$, $\bar{q} *= U$ 都是确定性的，因此它们的语义集合只包含一个表示相应量子操作的超算子。还要回顾一下，我们用下标 $\bar{q}$ 表示量子操作所作用的量子比特系统。$S_0; S_1$ 的语义定义为 $[\![S_1]\!]$ 和 $[\![S_0]\!]$ 的（逐元素）复合。这遵循了 [8] 中为非确定性

概率程序提出的提升模型。我们将在第 3.3 节详细阐述采用这种提升模型（而非关系模型）的原因。

对于 $[\![\textbf{若}\ \mathrm{M}[\bar{q}]\ \textbf{则}\ S_1\ \textbf{否则}\ S_0\ \textbf{结束}]\!]$,，我们必须使用相应的测量超算子来组合 S_0 和 S_1 的语义。具体而言，对于任意输入态 ρ，若测量返回 0，则测量后态变为 $\mathrm{P}_{\bar{q}}^0(\rho)$，并且 $[\![S_0]\!]$ 中的一个超算子将作用于该状态。测量结果为 1 的情形类似。最后，必须将两个分支得到的（部分）密度算子相加，以构成整个语句的输出态，因为这两个分支是以概率方式（由于测量）而非非确定性地选择的。

最后，在 $[\![\textbf{当}\ \mathrm{M}[\bar{q}]\ \textbf{执行}\ S\ \textbf{结束}]\!]$,中，由于循环体 S可能包含非确定性选择，我们使用一个调度器 η 来指定在while循环的每次迭代中选取 $[\![S]\!]$ 中的哪个超算子。为简化记号，我们用 η_i表示 $\eta(i)$，即第 i 次迭代中选取的超算子。对于每个 $n \geq 0$，该超算子

$$\mathcal{F}_n^{\eta} \triangleq \sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^0 \circ \eta_i \circ \mathcal{P}_{\bar{q}}^1 \circ \ldots \eta_1 \circ \mathcal{P}_{\bar{q}}^1 \tag{1}$$

取循环体 S 在调度器 η 下的前 n 次执行所得结果。显然，序列 $\mathrm{F}_n^{\eta}, n \geq 0$ 在 $\preceq$下是非递减的。因此，最小上界 $\hat{\mathrm{O}}_{n\geq 0} \mathrm{F}_n^{\eta}$ 是良定义的；当使用 η 来消解 S 中的非确定性时，它就是 $\textbf{while}\,\mathrm{M}[\bar{q}]\,\textbf{do}\ S\textbf{end}$ 的语义。

例3.2。 我们重新 *рассмотр*量子纠错方案，该方案在例 3.1 中给出。首先，容易看出

$$[\![ErrCorr]\!] = \left\{\left(\mathcal{X}_q \circ \mathcal{P}_{q_1,q_2}^{11} + \mathcal{P}_{q_1,q_2}^{\neq 11}\right) \circ \mathcal{CX}_{q,q_1} \circ \mathcal{CX}_{q,q_2} \circ \mathcal{U} \circ \mathcal{CX}_{q,q_2} \circ \mathcal{CX}_{q,q_1} \circ \mathcal{Set}_{q_1,q_2}^0 : \mathcal{U} \in \{\mathcal{I}, \mathcal{X}_q, \mathcal{X}_{q_1}, \mathcal{X}_{q_2}\}\right\}$$

其中，$\mathcal{X}$ 和$\mathcal{CX}$ 分别是与酉算子 X 和 CX 对应的超算子。此外，

$$\mathcal{P}^{11}(\rho) = |11\rangle\langle 11|\rho|11\rangle\langle 11|$$

and

$$\mathcal{P}^{\neq 11}(\rho) = \sum_{(i,j)\neq(1,1)} |ij\rangle\langle ij|\rho|ij\rangle\langle ij|$$

对于所有 $\rho \in \mathcal{D}(\mathcal{H}_2 \otimes \mathcal{H}_2)$。也就是说，$\mathcal{P}_{q_1,q_2}^{11}$ 表示测量规则$\mathcal{M}[q_2]$ 和$\mathcal{M}[q_1]$ 均得到 *1* 时所对应的超算子，而$\mathcal{P}_{q_1}^{\neq 11},_{q_2}$ 表示其他情况。

对于任意输入态 $|\psi i_q|\psi' i_{q_1,q_2}$其中 $|\psi i = \alpha_0|0i + \alpha_1|1i$ 且$|\psi' i \in H_2 \otimes H2$，尽管指称语义 $[\![ErrCorr]\!]$,作用于 $|\psi i_q|\psi' i_{q_1,q_2}$ 时有四种不同的超算子，但最终量子态 $|\psi i_q|ij i_{q_1,q_2}$, $i, j = 0, 1$ 在量子比特 q 上具有相同的约化状态 $|\psi i$，而这恰好是 q 上的输入态。由此观察可知，该纠错方案已成功纠正了三个量子比特中任意一个可能发生的比特翻转错误。

下一个引理给出了 while 循环指称语义的递归描述。对于任意调度器 $\eta \in [\![S]\!]^{\mathbb{N}}$，我们定义 $\eta^{\rightarrow} \in [\![S]\!]^{\mathbb{N}}$ 为从 η_2开始的 η 后缀；也就是说，对于所有 $i \geq 1$，都有$\eta_i^{\rightarrow} = \eta_{i+1}$。

引理3.2。 令$\textbf{while} \triangleq \textbf{while}\,\mathcal{M}[\bar{q}]\,\textbf{do}\ S\textbf{end}$。那么对于任意$\eta \in [\![S]\!]^{\mathbb{N}}$ 和 $n \geq 0$,

$$\mathcal{F}_{n+1}^{\eta} = \mathcal{P}_{\bar{q}}^0 + \mathcal{F}_n^{\eta^{\rightarrow}} \circ \eta_1 \circ \mathcal{P}_{\bar{q}}^1. \tag{2}$$

其中 $\mathcal{F}_n^{\eta}$定义如公式 (1)所示。因此，

$$[\![\textbf{while}]\!] = \mathcal{P}_{\bar{q}}^0 + [\![\textbf{while}]\!] \circ [\![S]\!] \circ \mathcal{P}_{\bar{q}}^1. \tag{3}$$

证明。公式 (2) 可通过对 n使用归纳法轻易证明，进而可得公式 (3) 中的'⊆'部分。对于'⊇'部分，令 $\mathrm{G} \in \mathrm{P}_{\bar{q}}^0 +[\![\textbf{While}]\!] \circ [\![S]\!] \circ \mathrm{P}_{\bar{q}}^1$。则存在 $\eta \in [\![S]\!]^{\mathbb{N}}$ 和 $\mathrm{E} \in [\![S]\!]$，使得 $\mathrm{G} = \mathrm{P}_{\bar{q}}^0 + \hat{\mathrm{O}}_{n\geq 0} \mathrm{F}_n^{\eta} \circ \mathrm{E} \circ \mathrm{P}_{\bar{q}}^1$。令 $\eta' \in [\![S]\!]^{\mathbb{N}}$，其中 $\eta'_1 = \mathrm{E}$ 且对所有 $i \geq 1$ 都有 $\eta'_{i+1} = \eta_i$。然后容易通过归纳法证明，对于任意 $n \geq 1$,

$$\mathcal{F}_n^{\eta'} = \mathcal{P}_{\bar{q}}^0 + \mathcal{F}_n^{\eta} \circ \mathcal{E} \circ \mathcal{P}_{\bar{q}}^1.$$

因此，$\mathrm{G} = \hat{\mathrm{O}}_{n\geq 0} \mathrm{F}_n^{\eta'}$ 也属于 $[\![\textbf{While}]\!]$。 □

3.3 量子程序语义的不同方法

本小节旨在解释我们在定义非确定性量子程序语义时所作的设计决策。

3.3.1 纯态语义与混合态语义。请注意，在文献中，定义确定性量子程序语义有两种不同的方法。一种基于纯态 [2, 21, 22, 24, 26],，其中程序的含义是在假设其作用于纯态的前提下定义的。随后可以使用谱分解等方法将该语义扩展到混合态。具体而言，若 $\rho = \sum_{i\in I} p_i|\psi_i\rangle\langle\psi_i|$，且程序 S 将 $|\psi_i\rangle$ 映射为 $|\psi_{ii}\rangle$，那么在 ρ 上执行 S 后得到的最终（混合）状态为 $\sum_{i\in I} p_i|\psi_{ii}\rangle\langle\psi_{i'_i}|$。与之相反，另一种方法基于混合态 [4, 6, 23, 28]。也就是说，程序的语义直接在混合态上定义，无需扩展。

当所考虑的程序是确定性的时，选择纯态语义还是混合态语义并无区别。这是因为确定性量子程序的语义是一个超算子，它对密度算子的凸组合是线性的。因此，将这两种方法应用于混合态时，确实会得到确定性量子程序相同的语义。然而，对于非确定性量子程序而言，情况并非如此，因为此时一个程序通常对应一组超算子，而非单个超算子。因此，纯态语义的凸组合不会得到与混合态语义相同的结果。为了说明这一点，我们来看一个简单的例子。

例3.3。 设 S 是一个定义如下的非确定性量子程序：

$$S \triangleq \textbf{skip} \square\, q *= X$$

于是，根据图 2 可得 $[\![S]\!] = \{1, \mathcal{X}_q\}$。因此，

$$\begin{aligned} [\![S]\!]([|0\rangle]_q) &= \{[|0\rangle]_q, [|1\rangle]_q\} \\ [\![S]\!]([|1\rangle]_q) &= \{[|0\rangle]_q, [|1\rangle]_q\} \\ [\![S]\!]([|+\rangle]_q) &= \{[|+\rangle]_q\} \end{aligned} \tag{4}$$

$$[\![S]\!](|-\rangle_q) = \{|-\rangle_q\}$$

其中 $|\pm\rangle \quad \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$，最后一个等式是根据以下事实得出的：$[X|-\rangle] = [-|-\rangle] = [|-\rangle]$；也就是说，在量子态的密度算符表示中，全局相位会消失。

假设我们采用纯态方法来定义我们的指称语义，并通过对纯态语义取凸组合将其扩展到混合态。回想一下，在$\mathcal{H}_2$中，

$$\frac{I}{2} = \frac{1}{2}([|0\rangle] + [|1\rangle]) = \frac{1}{2}([|+\rangle] + [|-\rangle]). \tag{5}$$

那么，根据式(4) 中的前两个等式，我们可以推导出

$$[\![S]\!](I_q/2) = \{[|0\rangle]_q, [|1\rangle]_q, I_q/2\},$$

而根据式(4) 中的后两个等式，我们则会得到

$$[\![S]\!](I_q/2) = \{I_q/2\}$$

而不是上述结果。也就是说，混合态的扩展语义将无法得到良好定义。

请注意，经典程序不存在这种不一致，因为与密度算子可以表示不同的纯态系综这一事实不同（式 (5) 中的例子）适用于 $I/2$，经典状态的任意概率分布都有唯一的表示形式（即底层经典状态的凸组合）。

3.3.2 关系模型与提升模型。 正如 [8], 所指出的，非确定性概率程序自然可以有两种不同的语义模型：关系模型和提升模型。直观地说，在提升模型中，非确定性程序在语义上被视为一组确定性程序；而在关系模型中，则通过考虑概率与非确定性之间的干涉来定义专门的语义。这两种模型之间的差异，在它们对程序顺序组合的处理方式上体现得最为明显。具体而言，设 Σ 为经典状态空间，其元素记作 $s, t,$ 等。为简单起见，假设 Σ 可数。设 S 和 T 为非确定性概率程序。回顾一下， S 在关系模型中的语义 $[\![S]\!]_{\mathbf{r}}$ 是一个映射，将 Σ 中的状态映射到 Σ 上的概率分布集合。对于任意 $s \in \Sigma$，顺序组合 $S;T$ 的语义定义为

$$[\![S;T]\!]^{\mathbf{r}}(s) = \left\{ \sum_{t\in\Sigma} \mu(t) \cdot \nu_t : \mu \in [\![S]\!]^{\mathbf{r}}(s), \forall t.\nu_t \in [\![T]\!]^{\mathbf{r}}(t) \right\}. \tag{6}$$

也就是说， $[\![S;T]\!]_{\mathbf{r}}(s)$ 中的每个概率分布，都是先选择一个属于 $[\![S]\!]_{\mathbf{r}}(s)$ 的分布 μ，然后对每个状态t选择一个属于$[\![T]\!]_{\mathbf{r}}(t)$ 的分布 ν_t，最后对 ν_t 作凸组合得到的，其中 ν_t 的权重由 $\mu(t)$ 给出。与此相反，提升模型中 S 的语义 $[\![S]\!]_{\mathbf{l}}$ 是一个确定性分布变换器集合，它将 Σ 中的状态映射为 Σ 上的概率分布。$S;T$ 的提升语义定义为

$$[\![S;T]\!]^{\mathbf{l}} = \left\{ g \circ f : f \in [\![S]\!]^{\mathbf{l}}, g \in [\![T]\!]^{\mathbf{l}} \right\} \tag{7}$$

其中$g \circ f$按标准方式定义：$(g \circ f)(s) = \acute{\mathrm{I}}_{t\in\Sigma} f(s)(t) \cdot g(t)$。尽管这两种模型都有充分的动机，但[8] 指出，关系模型更可取，因为它具有更多良好的代数性质。

显然，图 2 中的定义与公式 (7) 中提升模型的风格相同。为了说明为何为非确定性量子程序定义关系语义会带来问题，让我们从博弈的角度仔细考察公式 (6) 中 $[\![S;T]\!]_{\mathbf{r}}$ 的定义。直观地说，对于每个 $t \in \Sigma$，如果当前程序状态为 t，则对手会从$[\![T]\!]_{\mathbf{r}}(t)$ 中选择 ν_t。请注意，只有假设运行时能够精确确定任意时刻的程序状态，对手才能利用这一信息作出选择，这种说法才有意义。然而，由于密度算子可以表示不同的纯态系综，这一假设在量子情形下未必成立。为了更清楚地说明这一点，我们来看下面的例子。

例3.4。 设 S 定义如例*3.3* 所示，且

$$T \triangleq q := 0;\ q *= H;\ \textbf{measure}\ q$$
$$T_{\pm} \triangleq q := 0;\ \textbf{measure}_{\pm}\ q$$

此处，命令测量规则 q 是 *if M0,1*$[q]$ *then* 空操作 *else* 空操作 *end* 的缩写，而 *M0,1* 表示按照计算基 *{|0i |1i}* 进行的测量。类似地，测量规则$_{\pm}$ q是 *if* $M_{\pm}[q]$ *then* 空操作 *else* 空操作 *end* 的缩写，而 $M_{\pm}$ 表示按照标准正交基 *{|+i |–i}* 进行的测量。注意， T和 $T_{\pm}$ 都是确定性的。显然，对于 *D(Hq)* 中满足 *tr(ρ)* = 1 的任意输入态ρ， T 的输出态是系综$\left(|0i : 12, |1i : \frac{1}{2}\right)$，也可以视为在 $|0i$ 和 $|1i$ 之间均匀取值的概率分布。类似地，对于相同的输入态 ρ， $T_{\pm}$ 的输出态是系综 $\left(|+i : 12, |-i : \frac{1}{2}\right)$，即在 $|+i$ 和 $|-i$ 之间均匀取值的概率分布。如果我们采用关系语义 $[\![\cdot]\!]r$，将混合量子态视为纯态上的概率分布，那么我们可以得到

$$[\![T]\!]^{\mathbf{r}}(\rho) = \left\{ \left(|0\rangle : \frac{1}{2}, |1\rangle : \frac{1}{2} \right) \right\},$$
$$[\![T_{\pm}]\!]^{\mathbf{r}}(\rho) = \left\{ \left(|+\rangle : \frac{1}{2}, |-\rangle : \frac{1}{2} \right) \right\}.$$

请注意，这两个系综虽然概率分布形式不同，但物理上不可区分；参见式(5)。因此， $[\![T]\!]_{\mathbf{r}} = [\![T_{\pm}]\!]_{\mathbf{r}}$。

现在，考虑 T和 $T_{\pm}$ 的顺序组合，分别配以 S。与式(6)类似，我们可以得到

$$\begin{aligned}[\![T;S]\!]^{\mathbf{r}}(\rho) &= \frac{1}{2} \cdot [\![S]\!]^{\mathbf{r}}([|0\rangle]) + \frac{1}{2} \cdot [\![S]\!]^{\mathbf{r}}([|1\rangle]) \\ &= \frac{1}{2} \cdot \{|0\rangle, |1\rangle\} + \frac{1}{2} \cdot \{|0\rangle, |1\rangle\} \\ &= \left\{ (|0\rangle : 1), (|1\rangle : 1), \left(|0\rangle : \frac{1}{2}, |1\rangle : \frac{1}{2} \right) \right\}\end{aligned}$$

while

$$\begin{aligned}[\![T_{\pm};S]\!]^{\mathbf{r}}(\rho) &= \frac{1}{2} \cdot [\![S]\!]^{\mathbf{r}}([|+\rangle]) + \frac{1}{2} \cdot [\![S]\!]^{\mathbf{r}}([|-\rangle]) \\ &= \frac{1}{2} \cdot \{|+\rangle\} + \frac{1}{2} \cdot \{|-\rangle\} = \left\{ \left(|+\rangle : \frac{1}{2}, |-\rangle : \frac{1}{2} \right) \right\}.\end{aligned}$$

在密度算子语言中，我们可以说，从 ρ, $[\![T;\ S]\!]_{\mathbf{r}}$ 开始，可能非确定性地输出 $|0\rangle$、 $|1\rangle$ 或 $\frac{I}{2}$ $\left(= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right)$，而 $[\![T_{\pm};\ S]\!]_{\mathbf{r}}$ 只能输出$\frac{I}{2}$

$\left(=\frac{1}{2}|+\rangle\langle+|+\frac{1}{2}|-\rangle\langle-|\right)$尽管其中也存在非确定性选择。换句话说，$[\![T;\ S]\!]_{\mathrm{r}}\neq[\![T_{\pm};\ S]\!]_{\mathrm{r}}$，尽管$[\![T]\!]_{\mathrm{r}}=[\![T_{\pm}]\!]_{\mathrm{r}}$。这非常不可取，因为语义可组合性是语言设计的一项自然要求。

4 非确定性量子程序验证

回想一下，在验证（确定性或非确定性）概率程序时，常见的做法是将期望——即线性函数 $f\colon \Sigma\to[0,1]$，其中 Σ 是经典状态的集合——作为断言。这样，程序便可视为一个期望变换器，将后置期望映射为其最大前置期望。确定性和非确定性概率程序能够使用相同形式的断言，原因在于，期望集合相对于逐点偏序构成一个完备格，其中上确界和下确界也按逐点方式定义。因此，该集合在取下确界的运算下封闭，而此运算对应于（恶意）非确定性。

为了描述量子态的理想性质，我们沿用在确定性量子程序验证中将厄米算子视为量子谓词的方法

$$\mathcal{P}(\mathcal{H}_{\mathcal{V}})\triangleq\{M\in\mathcal{L}(\mathcal{H}_{\mathcal{V}}):0\sqsubseteq M\sqsubseteq I\}.$$

。请注意，任何厄米算子 $M\in\mathrm{P}(\mathrm{HV})$ 都会诱导一个线性函数 $f_M\colon \mathrm{D}(\mathrm{HV})\to[0,1]$，定义为对任意 ρ，令 $f_M(\rho)=\mathrm{tr}(M\rho)$。值得注意的是，回顾第 2 节可知，$\mathrm{tr}(M\rho)$ 正是测量状态 ρ 上的可观测量 M 时所得结果的期望值。如果 M 表示量子系统的某种理想性质，那么自然可以将其解释为 ρ 满足 M 的程度。

然而，集合 $\mathrm{P}(\mathrm{H}\mathcal{V})$ 虽然是一个链完备偏序集（CPO），却并不构成格。因此，它不足以表达非确定性量子程序的验证。本文简单地取 $\mathrm{A}, 2^{\mathcal{P}(\mathcal{H}_{\mathcal{V}})}$，即 $\mathrm{P}(\mathrm{H}\mathcal{V})$ 的子集所构成的集合，并以 Θ、Ψ、$\cdots$ 表示其中的元素，作为量子断言的集合。显然，按照通常的子集序，它构成一个完备格。当 $\Theta=\{M\}$ 是单元素集合时，我们简记 Θ 为 M。我们还将作用于厄米算子的运算逐元素地扩展到量子断言上。例如，设 E 是一个超算子，则 $\mathrm{E}(\Theta)$ 表示集合 $\{\mathrm{E}(M):M\in\Theta\}$。

定义 4.1. 给定一个密度算子 $\rho\in\mathcal{D}(\mathcal{H}_{\mathcal{V}})$ 和一个量子断言 $\Theta\in\mathcal{A}$，将 ρ 满足 Θ 的期望定义为$\mathrm{Exp}(\rho\models\Theta)\triangleq$下确界$_{M\in\Theta}\,\mathrm{tr}(M\rho)$。

上述定义中 $\mathrm{Exp}(\rho\models\Theta)$ 的下确界反映了对满足度的悲观观点：在可能存在恶魔式非确定性的情况下，它给出了 ρ 满足 Θ 的有保证的期望满足度。

4.1 正确性公式

通常，程序正确性用正确性公式表示，其形式为 $\{\Theta\}\ S\ \{\Psi\}$，其中 S 是一个量子程序，而 Θ 和 Ψ 是 A 中的量子断言。

定义4.2。设 $S\in\mathit{Prog}$，且 $\Theta,\ \Psi\in\mathrm{A}$。

(1) 若正确性公式 $\{\Theta\}\ S\{\Psi\}$ 满足完全正确性意义下的真，记作 $\models_{tot}\{\Theta\}\ S\{\Psi\}$，则对于任意 $\rho\in\mathcal{D}(\mathcal{H}\mathcal{V})$，

$$\mathrm{Exp}(\rho\models\Theta)\le\inf\left\{\mathrm{Exp}(\sigma\models\Psi):\sigma\in[\![S]\!](\rho)\right\}.$$

(2) 如果正确性公式 $\{\Theta\}\ S\{\Psi\}$ 在部分正确性意义下成立，记作 $\models_{par}\{\Theta\}\ S\{\Psi\}$，是指对任意$\rho\in\mathcal{D}(\mathcal{H}\mathcal{V})$，

$$\mathrm{Exp}(\rho\models\Theta)\le\inf\{\mathrm{Exp}(\sigma\models\Psi)+\mathrm{tr}(\rho)-\mathrm{tr}(\sigma):\sigma\in[\![S]\!](\rho)\}.$$

直观地说，$\models_{\text{完全正确性}}\{\Theta\}\ S\{\Psi\}$成立，当且仅当从任意初始状态出发，任意可能的最终态对后置条件 Ψ 的有保证的期望满足度都以下界为初始状态对前置条件 Θ 的有保证的期望满足度。对于部分正确性的情形，我们将非终止概率 $\mathrm{tr}(\rho)-\mathrm{tr}(\sigma)$ 考虑在内，从而放宽下界。容易看出，当 S 是确定性的，且 Θ 和 Ψ 都只包含一个量子谓词时，上述定义便化为 [28] 中针对确定性量子程序的相应定义。

例 4.1. 例 *3.1* 中比特翻转量子纠错方案的正确性可表述如下：对于任意 $|\psi\rangle\in\mathcal{H}_q$，

$$\models_{tot}\left\{|\psi\rangle_q\langle\psi|\right\}\ ErrCorr\ \left\{|\psi\rangle_q\langle\psi|\right\}. \tag{8}$$

为理解等式(8) 如何体现了量子比特 q 的（任意）状态已成功免受可能发生的比特翻转错误的影响这一直观含义，请注意，等式(8) 意味着

$$1=\langle\psi|\psi\rangle\langle\psi|\psi\rangle\le\inf\left\{\langle\psi|\sigma|\psi\rangle:\sigma\in[\![ErrCorr]\!](|\psi\rangle\langle\psi|)\right\}.$$

因此 $\sigma=|\psi\rangle\langle\psi|$ 对所有 $\sigma\in[\![ErrCorr]\!](|\psi\rangle\langle\psi|)$均成立。

注意，对于 $*\in\{tot,par\}$，若存在 $M\in\Theta$使得$\models_*\{M\}\ S\{N\}$ 对所有 $N\in\Psi$均成立，则 $\models_*\{\Theta\}\ S\{\Psi\}$。然而，反过来并不成立。以下是一个反例。令 $\mathrm{V}\triangleq\{q\}$、$\Theta$、$\{|0\mathrm{i}q\mathrm{h}0|,|1\mathrm{i}q\mathrm{h}1|\}$、$\Psi$、$\{I_q/2\}$，且 S 为 **空操作**。注意，对于任意 $\rho\in\mathrm{D}(\mathrm{H}\mathcal{V})$，$\mathrm{tr}(|0\mathrm{i}q\mathrm{h}0|\rho)+\mathrm{tr}(|1\mathrm{i}q\mathrm{h}1|\rho)=\mathrm{tr}(\rho)$。因此

$$\mathrm{Exp}(\rho\models\Theta)=\min\left\{\mathrm{tr}(|0\rangle_q\langle0|\rho),\mathrm{tr}(|1\rangle_q\langle1|\rho)\right\}\le\frac{\mathrm{tr}(\rho)}{2}=\mathrm{Exp}(\rho\models\Psi),$$

因此 $\models_*\{\Theta\}\ S\{\Psi\}$。然而，$\models_*\left\{|0\mathrm{i}q\mathrm{h}0|\right\}\ S\ \left\{I_q/2\right\}$和 $\models_*\left\{|1\mathrm{i}q\mathrm{h}1|\right\}\ S\ \left\{I_q/2\right\}$均不成立。要看出前者这一点，我们注意到

$$\mathrm{Exp}\left(|0\rangle_q\langle0|\models|0\rangle_q\langle0|\right)=1\not\le1/2=\mathrm{Exp}\left(|0\rangle_q\langle0|\models I_q/2\right).$$

对于后者，我们可以取 $|1\mathrm{i}q\mathrm{h}1|$ 作为初始态。

下面给出一些关于完全正确性和部分正确性的基本事实。

引理 4.1. 设 $S\in\mathit{Prog}$、Θ 和 Ψ 均为量子断言。
(1) 若 $\models_{tot}\{\Theta\}\ S\{\Psi\}$，则 $\models_{par}\{\Theta\}\ S\{\Psi\}$；*(2)* $\models_{tot}\{0\}\ S\{\Psi\}$ 且 $\models_{par}\{\Theta\}\ S\{I\}$；*(3)* 若对所有 i 都有 $\models_*\{\Theta_i\}\ S\{\Psi_i\}$，则 $\models_*\{\bigsqcap_i\Theta_i\}\ S\{\bigsqcap_i\Psi_i\}$，其中 $*\in\{tot,par\}$。

证明。条款 (1) 直接由以下事实得出：对于所有 $\sigma\in[\![S]\!](\rho)$，$\mathrm{tr}(\sigma)\le\mathrm{tr}(\rho)$；条款 (3) 由定义得出；条款 (2) 则由以下观察得出：对于任意 $M\in\Theta$，$\mathrm{tr}(M\rho)\le\mathrm{tr}(\rho)$。□

(Skip) $$\{\Theta\}\ \textbf{skip}\ \{\Theta\}$$

(Abort) $$\{I\}\ \textbf{abort}\ \{0\}$$

(Init) $$\left\{\sum_{i=0}^{2^n-1}|i\rangle_{\bar{q}}\langle 0|\Theta|0\rangle_{\bar{q}}\langle i|\right\}\ \bar{q}:=0\ \{\Theta\}$$

(Unit) $$\left\{U_{\bar{q}}^{\dagger}\Theta U_{\bar{q}}\right\}\ \bar{q}\ *\!=U\ \{\Theta\}$$

(Seq) $$\frac{\{\Theta\}\ S_0\ \{\Theta'\},\ \{\Theta'\}\ S_1\ \{\Psi\}}{\{\Theta\}\ S_0;S_1\ \{\Psi\}}$$

(NDet) $$\frac{\{\Theta\}\ S_0\ \{\Psi\},\ \{\Theta\}\ S_1\ \{\Psi\}}{\{\Theta\}\ S_0\ \square\ S_1\ \{\Psi\}}$$

(Meas) $$\frac{\{\Theta_1\}\ S_1\ \{\Psi\},\ \{\Theta_0\}\ S_0\ \{\Psi\}}{\left\{\mathcal{P}_{\bar{q}}^0(\Theta_0)+\mathcal{P}_{\bar{q}}^1(\Theta_1)\right\}\ \textbf{if}\ \mathcal{M}[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}\ \{\Psi\}}$$

(While) $$\frac{\{\Theta\}\ S\ \left\{\mathcal{P}_{\bar{q}}^0(\Psi)+\mathcal{P}_{\bar{q}}^1(\Theta)\right\}}{\left\{\mathcal{P}_{\bar{q}}^0(\Psi)+\mathcal{P}_{\bar{q}}^1(\Theta)\right\}\ \textbf{while}\ \mathcal{M}[\bar{q}]\ \textbf{do}\ S\ \textbf{end}\ \{\Psi\}}$$

(Imp) $$\frac{\Theta\sqsubseteq_{inf}\Theta',\ \{\Theta'\}\ S\ \{\Psi'\},\ \Psi'\sqsubseteq_{inf}\Psi}{\{\Theta\}\ S\ \{\Psi\}}$$

(Union) $$\frac{\{\Theta_i\}\ S\ \{\Psi_i\}\ \text{for all}\ i\in I}{\{\bigcup_{i\in I}\Theta_i\}\ S\ \{\bigcup_{i\in I}\Psi_i\}}$$

图 3：部分正确性的证明系统。

作为本小节的总结，我们通过规定若对于任意 ρ，$\inf_{M\in\Theta}\mathrm{tr}(M\rho)\le\inf_{N\in\Psi}\mathrm{tr}(N\rho)$，则 $\Theta\sqsubseteq_{\text{下确界}}\Psi$，来定义量子断言之间的预序。以下引理对我们后续的讨论很有用。

引理 4.2. (1) 设 $\mathcal{E}$ 为一个超算子，且 $\Theta\sqsubseteq$下确界 Ψ。那么 $\mathcal{E}^\dagger(\Theta)\sqsubseteq$下确界 $\mathcal{E}^\dagger(\Psi)$。回想一下，$\mathcal{E}^\dagger$ 是$\mathcal{E}$的伴随超算子。(2) 若对所有 i，$\Theta_i\sqsubseteq$下确界 Ψ_i，则 $\bigcup_i\Theta_i\sqsubseteq$下确界 $\bigcup_i\Psi_i$。

证明。由 $\sqsubseteq_{\text{下确界}}$ 的定义可轻易得出。 □

4.2 证明系统

霍尔逻辑的核心是一个由公理和证明规则组成的证明系统，它支持以语法为导向的模块化程序正确性推理。本节将为非确定性量子程序提出一种霍尔逻辑。

部分正确性。我们在图 3 中提出一个用于量子程序部分正确性的证明系统，它是对 [28] 中为确定性量子程序引入的霍尔逻辑系统的自然扩展。

为了帮助理解图3中给出的规则，我们将它们与经典程序中对应的规则进行比较。规则 (Skip)、(Abort)、(Seq)、(NDet)、(Imp) 与相应的经典规则形式相同。注意，对于任意纯态 $|\psi\rangle$，$\mathrm{tr}(I\cdot|\psi\rangle\langle\psi|)=1$，且 $\mathrm{tr}(0\cdot|\psi\rangle\langle\psi|)=0$。因此，量子谓词$I$和 0 分别与经典断言中的**真**和**假**起着类似的作用。规则 (Init) 和 (Unit) 是经典赋值规则的对应规则，可以从后往前更好地理解。例如，(Unit) 表示，要保证后置条件 Ψ，只需将 $U^\dagger_{\bar{q}}\Theta U_{\bar{q}}$作为前置条件。

回顾经典条件语句的证明规则

$$\frac{\{p\wedge B\}\ S_1\ \{q\},\ \{p\wedge\neg B\}\ S_0\ \{q\}}{\{p\}\ \textbf{if}\ B\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}\ \{q\}}. \tag{9}$$

由于量子断言缺少合取，我们的证明规则（Meas）采用了另一种形式：在应用相应的测量超算子后，将 $\textbf{if}\,\mathcal{M}[\bar{q}]\,\textbf{then}\ S_1\ \textbf{else}\ S_0\,\textbf{end}$ 两个分支的前置条件相加。注意，$p=(p\wedge B)\vee(p\wedge\neg B)$。因此，（Meas）确实是式（9）中规则的推广。受 [28], 量子断言 $\mathcal{P}_{\bar{q}}^0(\Psi)+\mathcal{P}_{\bar{q}}^1(\Theta)$ 的启发，规则（While）中的该断言充当 while循环的循环不变式。最后，我们引入规则（Union），以组合同一量子程序的不同正确性公式，这与经典程序的合取规则相仿。

若正确性公式 $\{\Theta\}\ S\{\Psi\}$ 可以从证明系统中推导出来，则记作 $\vdash_{par}\{\Theta\}\ S\{\Psi\}$。

定理 4.1。 图 3 中的证明系统对于非确定性量子程序的部分正确性而言，既是可靠的，也是相对完备的。

证明。（概要）与 [28], 类似，此处证明的关键思路是为量子程序定义最弱自由前置条件的概念。具体而言，对于任意非确定性量子程序S和后置条件 $\Psi\in\mathrm{A}$，我们构造一个量子断言，记作 $wlp.S.\Psi$，它是所有有效前置条件中最弱（或按 $\sqsubseteq_{inf}$ 计最大的）一个。换言之，对于任意 $\Theta\in\mathrm{A}$，$\vDash_{par}\{\Theta\}\ S\{\Psi\}$ 当且仅当 $\Theta\sqsubseteq_{inf}wlp.S.\Psi$。

现在，为了证明我们的逻辑系统的可靠性，只需根据 S 的结构进行归纳，并证明只要 $\vdash_{par}\{\Theta\}\ S\{\Psi\}$，就有 $\Theta\sqsubseteq_{inf}wlp.S.\Psi$。对于完备性部分，我们需要再次通过结构归纳证明 $\vdash_{par}\{wlp.S.\Psi\}\ S\{\Psi\}$。更多细节请参见附录 B。 □

完全正确性。秩函数在证明 while 循环程序的完全正确性时发挥着核心作用。回顾一下，在经典情形中，秩函数会将循环体执行过程中每个可达状态映射到一个良基有序集合中的元素（例如非负整数集合），并且该值会在每次循环迭代后严格递减。我们用于证明 while 循环完全正确性的规则也高度依赖排序断言这一概念。下面的定义受到 [7] 中提出的相应概念的启发。不过，这里我们必须考虑循环体中可能出现的非确定性选择。

定义 4.3. 设$\widehat{\Theta}$ 是一个量子断言。若对于每个 η，量子谓词集合 $\left\{R_i^\eta:\ i\ge 0,\eta\in[\![S]\!]^{\mathbb{N}}\right\}$ 满足以下条件，则称其为$\widehat{\Theta}$-排序断言，对应于 $\textbf{While}\ \mathcal{M}[\bar{q}]\,\textbf{do}\,S\,\textbf{end}$：

(1) $\widehat{\Theta}\sqsubseteq_{inf}R_0^\eta$;

(2) *the sequence* $R_i^\eta, i\ge 0$, *is decreasing with respect to* $\sqsubseteq$; *that is,* $R_0^\eta\sqsupseteq R_1^\eta\sqsupseteq\ldots$. *Furthermore,* $\bigwedge_i R_i^\eta=0$;

(3) 对于任意 $i \geq 0$ 和 $\rho \in \mathcal{D}(\mathcal{H}v)$,

$$\mathrm{tr}\left(R_i^{\eta\rightarrow} \cdot \left(\eta_1 \circ \mathcal{P}_{\bar{q}}^1(\rho)\right)\right) \leq \mathrm{tr}\left(R_{i+1}^{\eta} \cdot \rho\right). \tag{10}$$

这也可以更简洁地写作

$$\mathcal{P}_{\bar{q}}^1 \circ \eta_1^{\dagger}\left(R_i^{\eta\rightarrow}\right) \sqsubseteq R_{i+1}^{\eta}. \tag{11}$$

b 从下文的规则（WhileT）可以看出， Θ 通常被视为我们所关注的正确性公式的前置条件，同时也是**while** $\mathrm{M}[\bar{q}]$ **do** S **end**的循环不变式。 Θ排序断言的基本思想是为 bΘ提供一系列上界。我们将在下文对此进行更详细的解释。

为简单起见，假设 $\mathrm{b}\Theta = \mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)$，其中量子谓词为 M，断言为 Θ。令$M_0^{\eta} = 0$ 和$M_i^{\eta}, i \geq 1$为表示 M 最弱前置条件的量子谓词，其中循环体仅执行 $i-1$ 次；也就是说，对于任意 ρ,

$$\mathrm{tr}\left(M_i^{\eta} \cdot \rho\right) = \mathrm{tr}\left(M \cdot \mathcal{F}_{i-1}^{\eta}(\rho)\right)$$

其中 $\mathcal{F}_i^{\eta}$ 由公式（1）定义。 $\widehat{\ }\Theta$-排序断言 R_i^{η} 的目标是确保

$$\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta) \sqsubseteq_{inf} M_i^{\eta} + R_i^{\eta}. \tag{12}$$

定义 4.3 的条款（1）确立了 $i = 0$的界，而条款（3）与假设 $\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)$ 是循环不变式相结合，保证公式（12）对所有 i 都归纳成立。这可由引理3.2证明。最后，由于条款（2），当 i 趋于无穷时，只有 M_i^{η} 充当上界，这反过来意味着，关于 while $\mathrm{M}[\bar{q}]$do Send，$\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)$ 是完全正确性意义下的有效前置条件。

借助排序断言的概念，我们可以将完全正确性中 while 循环的规则（WhileT）表述如下：

$$\text{(WhileT)} \quad \frac{\{\Theta\}\ S\ \left\{\mathcal{P}_{\bar{q}}^0(\Psi) + \mathcal{P}_{\bar{q}}^1(\Theta)\right\} \qquad \mathcal{P}_{\bar{q}}^0(\Psi) + \mathcal{P}_{\bar{q}}^1(\Theta)\text{-ranking assertion exists}}{\left\{\mathcal{P}_{\bar{q}}^0(\Psi) + \mathcal{P}_{\bar{q}}^1(\Theta)\right\}\ \textbf{while}\ \mathcal{M}[\bar{q}]\ \textbf{do}\ S\ \textbf{end}\ \{\Psi\}}$$

完全正确性的证明系统定义方式与部分正确性相同，只是将规则（While）替换为（WhileT），并将规则（Abort）替换为

$$\text{(AbortT)} \qquad \{0\}\ \textbf{abort}\ \{0\}.$$

我们记作 $\vdash_{\text{完全}} \{\Theta\}\ S\ \{\Psi\}$，表示正确性公式 $\{\Theta\}\ S\ \{\Psi\}$ 可以通过完全正确性的证明系统推导得出。同样，我们可以证明完全正确性证明系统的可靠性和相对完备性。

定理 4.2。 对于非确定性量子程序的完全正确性，该证明系统既是可靠的，也是相对完备的。

证明。（概要）这里证明的核心思想仍然是定义量子程序的最弱前置条件这一概念。

使用排序断言来确立规则（WhileT）可靠性的基本思想，已在定义4.3下方作了直观讨论。对于完备性部分，我们可以证明量子谓词集

$$R_i^{\eta} = \sum_{k=i}^{\infty} \mathcal{P}_{\bar{q}}^1 \circ \eta_1^{\dagger} \circ \ldots \circ \mathcal{P}_{\bar{q}}^1 \circ \eta_k^{\dagger} \circ \mathcal{P}_{\bar{q}}^0(I),$$

表示 while 循环在执行 i次循环体后的终止概率，构成一个恰当的排序断言，从而证明 $\vdash_{\text{完全}} \{wp.\textbf{while}.\Theta\}\ \textbf{while}\ \{\Theta\}$。更多详情请参阅附录 B。 □

5 个案例研究

为说明上一节所介绍的证明系统的有效性，我们使用这些系统验证一些简单的量子算法和协议。

5.1 三量子比特量子纠错方案

回顾示例4.1 ，三量子比特量子纠错方案的正确性可表述如下：对于任意$|\psi\mathrm{i} = \alpha_0|0\mathrm{i} + \alpha_1|1\mathrm{i} \in \mathrm{H}2$,

$$\models_{tot} \left\{|\psi\rangle_q\langle\psi|\right\}\ ErrCorr\ \left\{|\psi\rangle_q\langle\psi|\right\}. \tag{13}$$

首先注意到，根据规则（空操作）和（酉变换规则），

$$\begin{aligned}
&\vdash_{tot} \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}\ \textbf{skip}\ \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}\\
&\vdash_{tot} \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}\ q *= X\ \{[\alpha_0|100\rangle + \alpha_1|011\rangle]\}\\
&\vdash_{tot} \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}\ q_1 *= X\ \{[\alpha_0|010\rangle + \alpha_1|101\rangle]\}\\
&\vdash_{tot} \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}\ q_2 *= X\ \{[\alpha_0|001\rangle + \alpha_1|110\rangle]\}.
\end{aligned}$$

设 M_i、 $1 \leq i \leq 4$ 分别为上述给出的四个后置条件。那么根据（Imp），对于每个 $S \in \{$**空操作** $q *= X$， $q_1 *= X$， $q_2 *= X\}$，我们有，

$$\left\{[\alpha_0|000\rangle + \alpha_1|111\rangle]_{q,q_1,q_2}\right\}\ S\ \{M_1 + M_2 + M_3 + M_4\}.$$

因此，我们得到如下证明概要：

$$\begin{aligned}
&\left\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q\right\}\\
&q_1, q_2 := 0;\\
&\left\{[\alpha_0|000\rangle + \alpha_1|100\rangle]_{q,q_1,q_2}\right\} && (Init)\\
&q, q_1 *= CX;\\
&\left\{[\alpha_0|000\rangle + \alpha_1|110\rangle]_{q,q_1,q_2}\right\} && (Unit)\\
&q, q_2 *= CX;\\
&\left\{[\alpha_0|000\rangle + \alpha_1|111\rangle]_{q,q_1,q_2}\right\} && (Unit)\\
&\textbf{skip} \square\ q *= X \square\ q_1 *= X \square\ q_2 *= X;\\
&\{[\alpha_0|000\mathrm{i} + \alpha_1|111\mathrm{i}] + [\alpha_0|001\mathrm{i} + \alpha_1|110\mathrm{i}]\\
&\quad + [\alpha_0|010\rangle + \alpha_1|101\rangle] + [\alpha_0|100\rangle + \alpha_1|011\rangle]\} && (NDet)\\
&q,\ q_2 *= CX;\\
&\{[\alpha_0|000\rangle + \alpha_1|110\rangle] + [\alpha_0|001\rangle + \alpha_1|111\rangle]\\
&\quad + [\alpha_0|010\rangle + \alpha_1|100\rangle] + [\alpha_0|101\rangle + \alpha_1|011\rangle]\} && (Unit)\\
&q, q_1 *= CX;\\
&\left\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes ([|00\rangle] + [|01\rangle] + [|10\rangle])_{q_1,q_2}\right.
\end{aligned}$$

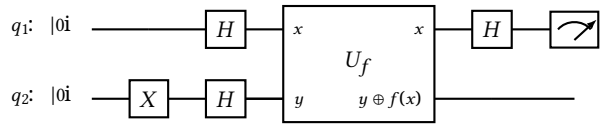

图 4：Deutsch 算法的量子电路。

$$+[\alpha_0|1\rangle+\alpha_1|0\rangle]_q\otimes[|11\rangle]_{q_1,q_2}\big\} \qquad (Unit)$$

若 $\mathcal{M}[q_2]$ **则**

$\{[\alpha_0|0\rangle+\alpha_1|1\rangle]\otimes[|0\rangle]+[\alpha_0|1\rangle+\alpha_1|0\rangle]\otimes[|1\rangle]\}$

如果 $\mathcal{M}[q_1]$ **则**

$\big\{[\alpha_0|1\rangle+\alpha_1|0\rangle]_q\big\}$

$q *= X$

$\big\{[\alpha_0|0\rangle+\alpha_1|1\rangle]_q\big\}$ $(Unit)$

end

$\big\{[\alpha_0|0\rangle+\alpha_1|1\rangle]_q\big\}$ $(Meas)$

end

$\big\{[\alpha_0|0\rangle+\alpha_1|1\rangle]_q\big\}$ $(Meas)$

根据逻辑系统的可靠性，这就完成了对公式（13）的证明。

5.2 Deutsch 算法

Deutsch 算法 [3] 是最早展示量子计算带来加速的量子算法之一。给定一个布尔函数 f: $\{0,1\}\to\{0,1\}$，Deutsch 算法只需对 f 求值一次，就能判断 $f(0)$ 是否等于 $f(1)$。在该算法的传统描述中，会使用一个量子预言机U_f，将任意状态 $|x\rangle\otimes|y\rangle$ 映射为状态 $|x\rangle\otimes|y\oplus f(x)\rangle$，其中 x、$y\in\{0,1\}$。Deutsch 算法的电路如图 4 所示。它声称，如果测量结果为 0，则 f 为常数（即 $f(0)=f(1)$）；否则，则声称 f 是平衡的（即 $f(0)\neq f(1)$）。

现在我们说明如何将 Deutsch 算法描述为一个非确定性量子程序，以及如何验证其正确性。为此，我们注意到

$$U_f=\begin{cases} I_2\otimes I_2 & \text{if } f(0)=f(1)=0;\\ I_2\otimes X & \text{if } f(0)=f(1)=1;\\ CX & \text{if } f(0)=0 \text{ and } f(1)=1;\\ C^0X & \text{if } f(0)=1 \text{ and } f(1)=0.\end{cases}$$

其中 CX 是受控非门，而 $C^0X=(X\otimes I_2)\cdot CX\cdot(X\otimes I_2)$ 表示在第一个量子比特为 $|0\rangle$ 的条件下，对第二个量子比特应用 X门。在前两种情况下，f是常量；而在后两种情况下，f是平衡的。于是，Deutsch 算法可以写成

$Deutsch \triangleq$

$q_1,q_2 := 0;$

$q_1 *= H;\ q_2 *= X;\ q_2 *= H;$

if $\mathcal{M}_{0,1}[q]$ **then**

$(q_1,q_2 *= CX)\ \square\ (q_1,q_2 *= C^0X)$

else

skip $\square\ (q_2 *= X)$

end

$q_1 *= H;$

measure q_1

这里我们引入一个辅助量子比特 q，其初始态未知，并使用 q 上的测量结果来选择 f(或者等价地，U_f)。注意，对于每个测量结果，U_f都有两种可能性，我们用这两者之间的非确定性选择来表示。语句**测度** q_1 的定义与例3.4 相同。很容易根据规则 (酉变换规则) 和 (测量规则) 证明，对于任意量子断言 Θ，下面的正确性公式均成立：

$$\big\{|0\rangle_{q_1}\langle 0|\Theta|0\rangle_{q_1}\langle 0|+|1\rangle_{q_1}\langle 1|\Theta|1\rangle_{q_1}\langle 1|\big\}\ \textbf{measure}\ q_1\ \{\Theta\}.$$

注意，算法结束时，q 和 q_1 都处于计算基 {|0⟩,|1⟩}中的某一个。于是，Deutsch 算法的正确性可以表述如下：

$$\models_{tot}\{I\}\ Deutsch\ \big\{(|00\rangle\langle 00|+|11\rangle\langle 11|)_{q,q_1}\big\}. \qquad (14)$$

也就是说，程序终止时 q_1 中编码的（经典）信息与 q中编码的信息一致，因此能正确判断 $f(0)$是否等于 $f(1)$。

为证明式（14），我们首先由（酉变换规则）注意到

$\vdash_{tot}\big\{[|0\rangle_q|+-\rangle_{q_1,q_2}]\big\}\ \textbf{skip}\ \big\{[|0\rangle_q|+-\rangle_{q_1,q_2}]\big\}$

$\vdash_{tot}\big\{[|0\rangle_q|+-\rangle_{q_1,q_2}]\big\}\ q_2 *= X\ \big\{[|0\rangle_q|+-\rangle_{q_1,q_2}]\big\}$

$\vdash_{tot}\big\{[|1\rangle_q|+-\rangle_{q_1,q_2}]\big\}\ q_1,q_2 *= CX\ \big\{[|1\rangle_q|--\rangle_{q_1,q_2}]\big\}$

$\vdash_{tot}\big\{[|1\rangle_q|+-\rangle_{q_1,q_2}]\big\}\ q_1,q_2 *= C^0X\ \big\{[|1\rangle_q|--\rangle_{q_1,q_2}]\big\}$

其中 $|\pm\rangle$ $\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$。于是我们得到如下证明概要：

$\{I\}$

$q_1,\ q_2 := 0;$

$\{[|00\rangle]_{q_1,\ q_2}\}$ $(Init),(Seq)$

$q_1 *= H;\ q_2 *= X;\ q_2 *= H;$

$\big\{[|0+-\rangle]_{q,q_1,q_2}+[|1+-\rangle]_{q,q_1,q_2}\big\}$ $(Unit),(Seq)$

如果 $\mathcal{M}_{0,\ 1}[q]$ **那么**

$\big\{[|1+-\rangle]_{q,q_1,q_2}\big\}$

$(q_1,q_2 *= CX)\ \square\ (q_1,q_2 *= C^0X)$

$\big\{[|1--\rangle]_{q,q_1,q_2}\big\}$ $(NDet)$

else

$\big\{[|0+-\rangle]_{q,q_1,q_2}\big\}$

空操作 $\square\ (q_2 *= X)$

$\big\{[|0+-\rangle]_{q,q_1,q_2}\big\}$ $(NDet)$

end

$\big\{[|0+-\rangle]_{q,q_1,q_2}+[|1--\rangle]_{q,q_1,q_2}\big\}$ $(Imp),(Meas)$

$\big\{[|0+\rangle]_{q,q_1}+[|1-\rangle]_{q,q_1}\big\}$ (Imp)

$q_1 *= H;$

$\big\{[|00\rangle]_{q,q_1}+[|11\rangle]_{q,q_1}\big\}$ $(Unit)$

测度 q_1

$$\{[|00\rangle]_{q,q_1} + [|11\rangle]_{q,q_1}\} \qquad (Meas)$$

最后，由我们的逻辑系统的可靠性可得，式（14）。

5.3 非确定性量子游走

为了说明我们的逻辑系统在量子循环方面的实用性，我们考虑 [12] 中所述的、在具有四个顶点的圆上的非确定性量子游走的一个修订版本。该游走使用一个双量子比特系统，由 q_1 和 q_2 组成，作为其主系统。它从初始态 $|00\mathrm{i}$ 开始，并且在游走的每一步中，依次应用以下两个酉漫步算子

$$W_1 \triangleq \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & -1 & 1 \end{pmatrix}, \quad W_2 \triangleq \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 0 & 1 \\ -1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & -1 & -1 \end{pmatrix}$$

于 q_1 和 q_2 上。这里，W_1 和 W_2 是相对于 $\mathrm{H}_{q_1,\ q_2}$ 的计算基 $\{|00\mathrm{i}\ |0\mathrm{i}\ |10\mathrm{i}\ |11\mathrm{i}\}$ 写出的。然而，应用这些酉漫步算子的顺序是非确定性选择的。我们进一步假设，在由 $|10\mathrm{i}$ 张成的子空间处存在一个吸收边界；也就是说，在每个游走步骤之后，进行投影测量 $\mathrm{M} = \{P_0,\ P_1\}$，其中

$$P_0 \triangleq |10\rangle\langle 10|, \qquad P_1 \triangleq I_4 - |10\rangle\langle 10|$$

被应用。如果观察到与 P_0 对应的结果，整个过程就会终止；否则将继续执行下一步行走。

该行走可以描述为以下非确定性程序：

$$\begin{aligned} &QWalk \triangleq \\ &\quad q_1, q_2 := 0; \\ &\quad \textbf{while } \mathcal{M}[q_1, q_2] \textbf{ do} \\ &\qquad (q_1, q_2 *= W_1;\ q_1, q_2 *= W_2) \\ &\quad \square \quad (q_1, q_2 *= W_2;\ q_1, q_2 *= W_1) \\ &\quad \textbf{end} \end{aligned}$$

文献 [12] 已证明，若在每次迭代中始终选择非确定性选择的左分支，则$QWalk$ 不会终止。从 $W_2W_1|00\mathrm{i} = |00\mathrm{i}$这一事实可以很容易看出这一点。接下来，我们将使用针对非确定性量子程序的证明系统给出一个更强的结果：事实上，在非确定性选择的任何调度器下，$QWalk$ 都不会终止！为简单起见，在下面的讨论中，我们省略断言和超算子中的下标 $\{q_1, q_2\}$。

首先请注意，这一非终止性可以表述如下：

$$\models_{par} \{I\}\ QWalk\ \{0\}. \qquad (15)$$

原因是，根据定义42(2)，当且仅当对于任意 $\rho \in \mathrm{D}(\mathrm{H}_{q_1,q_2})$ 和 $\sigma \in [\![QWalk]\!](\rho)$，等式 (15) 成立，

$$\mathrm{tr}(\rho) \le \mathrm{tr}(\rho) - \mathrm{tr}(\sigma).$$

因此 $\mathrm{tr}(\sigma) = 0$，这意味着从任意 ρ 开始，$QWalk$ 到达任意有效量子态的概率为 0。

为证明式（15），我们首先根据规则（酉变换规则）计算 that

$$\left\{[|00\rangle] + \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right]\right\}$$
$$q_1, q_2 *= W_1;$$
$$\left\{\left[\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle)\right] + \left[\frac{1}{\sqrt{6}}(-|01\rangle + 2|10\rangle + |11\rangle)\right]\right\}$$
$$q_1, q_2 *= W_2;$$
$$\left\{[|00\rangle] + \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right]\right\}$$

and

$$\left\{[|00\rangle] + \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right]\right\}$$
$$\left\{\left[\frac{1}{3}(-|00\rangle + 2|01\rangle + 2|11\rangle)\right] + \left[\frac{1}{3\sqrt{2}}(4|00\rangle + |01\rangle + |11\rangle)\right]\right\}$$
$$q_1, q_2 *= W_2;$$
$$\left\{\left[\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle - |11\rangle)\right] + \left[\frac{1}{\sqrt{6}}(2|00\rangle - |01\rangle + |11\rangle)\right]\right\}$$
$$q_1, q_2 *= W_1;$$
$$\left\{[|00\rangle] + \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right]\right\}$$

现在令 $N = [|00\mathrm{i}] + \mathrm{h}\frac{1}{\sqrt{2}}(|0\,1\mathrm{i} + |1\,1\mathrm{i})\mathrm{i}$，并令 S 为 **QWalk**的**while** 循环体。注意，$\mathrm{P}^0(0) = 0$ 且 $\mathrm{P}^1(N) = N$，其中对于 $i = 0, 1$，P^i 是仅含一个 Kraus 算子的超算子。于是根据（NDet）可得

$$\vdash_{par} \{N\}\ S\ \{\mathcal{P}^0(0) + \mathcal{P}^1(N)\} \qquad (16)$$

最后，我们有

$$\begin{aligned} &\{I\} \\ &q_1, q_2 := 0; \\ &\left\{[|00\rangle] + \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right]\right\} \qquad (Init) \\ &\textbf{当 } \mathcal{M}[q_1, q_2] \textbf{ 时执行} \\ &(q_1,\ \ q_2 *= W_1;\ \ q_1,\ \ q_2 *= W_2)\ \square\ (q_1,\ \ q_2 *= W_2;\ \ q_1, \\ &q_2 *= W_1)\textbf{结束} \\ &\{0\} \qquad (While), Eq.\ (16) \end{aligned}$$

根据可靠性定理 4.1，由此完成了对等式（15）的证明。

6 原型工具实现

上一节通过几个示例展示了我们的证明系统的实用性。可以看出，即使对于这样简单的程序，执行形式化验证也十分繁琐（尽管属于常规工作），并且涉及大量的矩阵运算。为了减轻用户的负担，使其能够专注于更具挑战性的部分，例如为 while 循环指定不变量，我们实现了一个原型证明助手 NQPV，用于自动完成验证过程中的常规工作。目前，NQPV 仅支持部分正确性；完全正确性的验证将作为未来的工作。

NQPV 是一个纯 Python 项目，不依赖 Isabelle 和 Coq 等现有定理证明器。我们综合考虑了以下因素后作出这一决定：(1) Python 及其各种库提供了强大的矩阵运算能力，便于我们计算量子程序的前置条件和后置条件，并轻松确定量子断言之间的 $\sqsubseteq_{inf}$ 关系；(2) NQPV 的主要目的是展示我们提出的逻辑系统的实用性，因此易用性是我们的首要考虑。Python 的流行度和丰富的矩阵库使得描述量子程序和断言既方便又自然；

(3) 在 Python 中进行符号验证较为困难，这限制了 NQPV 能够表达和验证的量子程序。不过作为回报，在 NQPV 中大多数验证步骤都可以自动完成。

NQPV 依赖以下 Python 包：用于语法分析的 ply、用于算子计算的 numpy，以及用于半定规划求解器的 cvxpy。NQPV 使用一种简单的语言来定义和管理算子与证明项。

6.1 用户输入

NQPV 将第 4.1 节中定义的正确性公式作为输入。不过，为了自动证明 while 程序，每当遇到 while 结构时，还需要提供循环不变式。作为示例，我们重新 рассмотр第 5.3节中的量子游走示例。代码如下：

```
定义 invN: =加载 "invN.npy" 结束
// 导入更多算子.....
def pf := 证明 [q1 q2]: { I[q1]};[q1 q2]:=0; { inv :
invN [q1 q2]}; while MQWalk [q1 q2]do ( [
q1 q2]*=W1; [q1 q2]*=W2 # [q1 q2]*=W2; [
q1 q2]*=W1 ) end ; { Zero [q1]} end show pf
end
```

这里的酉算子W1、W2 以及测量规则MQWalk 定义于第5.3节，用户应将它们作为numpy 矩阵输入。请注意，一些标识符（例如 I 和Zero）已保留，用于表示常用的酉算子、厄米算子和测量规则。此外，用户为 while 程序指定的循环不变量（invN，本例中的不变量）也应为numpy 矩阵。

除了描述量子游走行为的主程序外，上述代码还包含另外两行 { I[q1]} 和 { Zero[q1] }，分别表示程序的前置条件和后置条件。因此，证明项的主体 pf 确实描述了式（15）中给出的正确性公式。最后，关键字 inv 标记循环不变式，而最后一行的 show 命令会输出 NQPV 生成的证明概要。

为了进一步简化使用，NQPV 也允许用户省略前置条件，只指定后置条件。在这种情况下，NQPV 会根据给定的后置条件和用户提供的循环不变量，输出其能够计算出的最弱前置条件。

6.2 验证过程

成功解析输入后，NQPV 会依据图 3 中的逻辑系统自动逐步构造证明。其策略是从整个程序的后置条件出发，反向计算最弱前置条件。对于 while 循环，NQPV 会检查用户提供的循环不变式是否有效。

最后，助手会比较验证条件和用户提出的前置条件（详情将在下一小节中介绍），然后生成最终结果。下面再次展示 NQPV 对量子游走示例的输出：

```
proof [q1 q2]: { I[q1]}; { VAR2[q1 q2]}; // 验
证条件[q1 q2]:=0; { invN[q1 q2] }; { inv: invN [
q1 q2]}; while MQWalk [q1 q2]do { invN[q1
q2] }; ( { invN[q1 q2]}; [q1 q2]*=W1 ; {
VAR0[q1 q2]}; [q1 q2]*=W2 # { invN[q1 q2]};
[q1 q2]*=W2 ; { VAR1[q1 q2]}; [q1 q2]*=
W1 )
```

```
结束 ;
{ 零 [q1]}
```

如图所示，每个子程序语句都标注了相应的前置条件和后置条件。其中一些已经定义，例如 invN。其他算子（如 VAR0）由 NQPV 生成，用于表示证明概要中使用的谓词。使用 show 命令可以显示这些算子的详细信息。例如，在此示例中执行 show VAR2 end，将返回双量子比特恒等算子，这意味着由给定后置条件和循环不变式确定的验证条件为 I[q1 q2]（因此，原始正确性公式有效）。

除了检查正确性公式是否有效外，NQPV 还可以验证用户提供的算子是否确实是循环不变式。例如，如果我们将第 invN[q1 q2] 节代码中的 6.1 改为 P0[q1]，其中 P0 = $|0\rangle\langle 0|$，就会收到一条错误消息：

```
错误:
序关系不满足:
    { P0[q1]}  <={ VAR0[q1 q2]VAR3[q1 q2]} ...

错误: 谓词"{ P0[q1]}"不是
     有效的循环       不变式。
...
```

6.3 确定 $\sqsubseteq_{inf}$ 关系

验证正确性公式的关键步骤之一，是确定两个断言（量子谓词集）是否满足 $\sqsubseteq_{inf}$ 关系。为便于实现，我们假设 NQPV 中允许的所有量子断言都是有限的。

引理 6.1。 设 Θ 和 Ψ 是有限量子谓词集。那么 $\Theta \sqsubseteq_{inf} \Psi$ 当且仅当对任意 $N \in \Psi$，

$$\forall \rho \in \mathcal{D}(\mathcal{H}_\mathcal{V}), \exists M \in \Theta, \mathrm{tr}(M\rho) \leq \mathrm{tr}(N\rho).$$

证明。由 Θ 和 Ψ 的有限性，

$\Theta \sqsubseteq_{inf} \Psi$

$$\Leftrightarrow \forall \rho \in \mathcal{D}(\mathcal{H}_\mathcal{V}), \min_{M\in\Theta} \mathrm{tr}(M\rho) \le \min_{N\in\Psi} \mathrm{tr}(N\rho)$$
$$\Leftrightarrow \forall \rho \in \mathcal{D}(\mathcal{H}_\mathcal{V}), \forall N \in \Psi, \exists M \in \Theta, \mathrm{tr}(M\rho) \le \mathrm{tr}(N\rho)$$
$$\Leftrightarrow \forall N \in \Psi, \forall \rho \in \mathcal{D}(\mathcal{H}_\mathcal{V}), \exists M \in \Theta, \mathrm{tr}(M\rho) \le \mathrm{tr}(N\rho). \quad \square$$

根据引理 6.1，我们有以下算法来确定对于有限集合 Θ 和 Ψ，$\Theta \sqsubseteq_{\text{下确界}} \Psi$：

- 如果 $\Theta = \{M\}$ 是单元素集合，那么 $\Theta \sqsubseteq_{\text{下确界}} \Psi$ 当且仅当 $M \sqsubseteq N$ 对所有 $N \in \Psi$ 都成立。只需检查 $N - M$ 的特征值是否均为非负数即可。
- 否则，对于每个 $N \in \Psi$，我们尝试求解以下半定规划问题：

$$\begin{array}{ll} \text{minimize} & 0 \\ \text{subject to} & \forall M \in \Theta, \mathrm{tr}(N\rho) \le \mathrm{tr}(M\rho) - \epsilon \\ & 0 \sqsubseteq \rho \end{array}$$

这里的 ϵ 是用户定义的精度，它足够小且为正数。MOSEK 和 CVX 等半定规划求解器要求这一条件。引入 ϵ 的另一个原因是使可行域闭合，从而使整个问题成为一个半定规划问题。显然，如果任一 $|\Psi|$ 半定规划问题返回一个解，那么 $\Theta \not\sqsubseteq_{\text{下确界}} \Psi$。然而，由于精度参数的存在，即使没有一个半定规划问题返回解，我们也无法确定 $\Theta \sqsubseteq_{\text{下确界}} \Psi$ 是否成立。尽管如此，只要将 ϵ 设得足够小，得到错误答案的概率就可以忽略不计。

6.4 相关工具

也可以在 Isabelle 和 Coq 等交互式定理证明器中进行程序验证。首个用于量子程序的定理证明器是 QHLProver [13], , 它使用 Isabelle/HOL 实现了 [28] 中的程序逻辑。CoqQ [29] 则在 Coq 中实现了相同的逻辑，并对线性算子采用通用且抽象的表示。Qrhl-tool [25] 是嵌入在 Isabelle 中的验证工具，支持对量子程序进行关系验证。

为了进行公平比较，我们从以下几个方面考察 NQPV 与现有工具之间的差异（我们仅以 CoqQ 为例，因为 QHLProver 和 Qrhl-tool 的构建方式与 CoqQ 类似）：

可靠性。对于 CoqQ，不仅定义了推理规则，还在 Coq 中证明了它们相对于指称语义（也在 CoqQ 中形式化定义）的可靠性。相比之下，NQPV 并未检查推理规则的可靠性。尽管如此，我们已在定理4.1中给出了逻辑系统可靠性的严谨证明。

表达能力。 现有工具只能处理确定性的量子程序，而我们的原型实现支持非确定性的量子程序。另一方面，如同定理证明器中的做法，CoqQ 可以处理符号；而如同 Python 中的做法，NQPV 只允许数值项。特别是，CoqQ 适用于验证 Grover 算法等一般性（即具有任意数量量子比特的）算法，因为在 CoqQ 中量子比特的数量以符号形式出现。

自动化。 由于 CoqQ 对线性算子的抽象表示，许多量子谓词的性质并不容易证明，必须由用户加以证明。不过，NQPV 可以利用功能强大的 Python 库，因此许多证明无需用户协助即可自动完成。因此，NQPV 的证明脚本通常比 CoqQ 中编写的证明短得多。

易用性。 借助 Coq 库 MathComp，CoqQ 直接基于希尔伯特空间开发了线性算子的抽象表示，并提供了一种使用带标签的 Dirac 记号描述它们的智能方式。因此，CoqQ 的用户应当具备足够的 Coq 知识，尤其是其中线性算子和计算机程序的规定方式。在 NQPV 中，算子被具体地给定为 numpy 矩阵，程序则以普通 Python 程序员熟悉的自然方式表示。如本节开头所述，我们选择这种简便的路径来实现原型，因为我们的主要目的在于说明逻辑系统的效用，而非开发一个功能完备的验证工具。

性能。 CoqQ 的性能取决于所提供的证明，而 NQPV 的性能则取决于计算后端；在最坏情况下，其复杂度随量子比特数量呈指数增长。相比之下，在 CoqQ 中验证一般的 Grover 算法只需几秒，而在 NQPV 中验证 13 量子比特的 Grover 算法则需要 90 秒。

7 结论

本文研究了允许非确定性选择的量子程序。这类程序的指称语义通过提升确定性量子程序的语义来定义；我们认为，这是在量子情形下定义非确定性的唯一自然方式。为实现验证，我们将相关希尔伯特空间上的厄米算子集合视为量子态的断言，并分别针对部分正确性和完全正确性提出了两种证明系统。我们证明，这两种证明系统相对于相应的正确性概念都是可靠且相对完备的。我们分析了一些简单的量子算法和协议，例如三量子比特比特翻转量子纠错方案、Deutsch 算法和非确定性量子游走，以展示这些证明系统的实用性。此外，我们还实现了一个轻量级证明助手原型，用于辅助非确定性量子程序的自动推理。

未来的工作中，我们将研究如何利用非确定性选择构造以及本文提出的验证技术来进行量子程序细化。如何将天使式非确定性纳入其中，也是未来值得研究的有趣课题。

致谢

作者感谢 Mingsheng Ying 教授和李三江教授进行的启发性讨论。本研究部分得到了中国国家重点研发计划项目（项目编号：2018YFA0306704）和澳大利亚研究理事会项目（项目编号：DP220102059）的资助。YX 也获得了悉尼量子学院的部分资助。

最弱（宽松）前置条件语义

本节以最弱（自由）前置条件的形式，为非确定性量子程序介绍一种替代语义。事实证明，这种语义等价于第 3.2 节给出的指称语义。更重要的是，最弱（自由）前置条件语义为证明我们逻辑系统的可靠性和完备性提供了一种强有力的证明技术，如下一节所示。

设 $S \in Prog$。 最弱前置条件语义 $wp.S$和 最弱自由前置条件语义 $wlp.S$的 S都是从 $2^{\mathcal{A}} \to 2^{\mathcal{A}}$中归纳定义的，如图 5所示。为简化记号，我们用 xp 表示 wp 或 wlp，只要它们都适用即可。

这些定义与 [28] 中给出的确定性量子程序定义相似。同样，由于循环体 S中可能存在非确定性选择，我们在 **while** $\mathrm{M}[\bar{q}]$ **do** S**end** 的最弱（自由）前置条件语义中纳入了调度器 $\eta \in [\![S]\!]^{\mathbb{N}}$。

下面的引理展示了量子程序的指称语义与最弱（自由）前置条件语义之间的对偶关系。

引理 A.1. 设 $S \in Prog$、 $\rho \in \mathcal{D}(\mathcal{HV})$ 是量子谓词， Θ 是量子断言。那么

(1) $wp.S.M = \left\{\mathcal{E}^\dagger(M) : \mathcal{E} \in [\![S]\!]\right\}$;
(2) $wlp.S.M = \left\{\mathcal{E}^\dagger(M) + I - \mathcal{E}^\dagger(I) : \mathcal{E} \in [\![S]\!]\right\}$;
(3) $\mathrm{Exp}(\rho \models wp.S.\Theta) = \inf\left\{\mathrm{Exp}(\sigma \models \Theta) : \sigma \in [\![S]\!](\rho)\right\}$;
(4) $\mathrm{Exp}(\rho \models wlp.S.\Theta) =$
$\inf\left\{\mathrm{Exp}(\sigma \models \Theta) + \mathrm{tr}(\rho) - \mathrm{tr}(\sigma) : \sigma \in [\![S]\!](\rho)\right\}$.

证明。我们通过对 S 的结构进行归纳法来证明条款 (1)。根据定义，基础情形很容易证明。在归纳步骤中，我们仅以以下两种情况为例。

• 设 S，**如果** $\mathcal{M}[\bar{q}]$**则** S_1 **否则** S_0 **结束**。那么

$$\begin{aligned}
&wp.S.M \\
&= \mathcal{P}^1_{\bar{q}}(wp.S_1.M) + \mathcal{P}^0_{\bar{q}}(wp.S_0.M) \\
&= \left\{\mathcal{P}^1_{\bar{q}} \circ \mathcal{F}^\dagger(M) : \mathcal{F} \in [\![S_1]\!]\right\} + \left\{\mathcal{P}^0_{\bar{q}} \circ \mathcal{E}^\dagger(M) : \mathcal{E} \in [\![S_0]\!]\right\} \\
&= \left\{(\mathcal{F} \circ \mathcal{P}^1_{\bar{q}} + \mathcal{E} \circ \mathcal{P}^0_{\bar{q}})^\dagger(M) : \mathcal{E} \in [\![S_0]\!], \mathcal{F} \in [\![S_1]\!]\right\} \\
&= \left\{\mathcal{G}^\dagger(M) : \mathcal{G} \in [\![S]\!]\right\}.
\end{aligned}$$

• 设 S，while $\mathrm{M}[\bar{q}]$ 执行 S' 结束。对于任意 $\eta \in [\![S]\!]^{\mathbb{N}}$ 和 $i \geq 0$，令 M_i^η 按图 5 中针对 $wp.$(while $\mathrm{M}[\bar{q}]$ 执行 S' 结束)$.M$ 的定义来定义，并令 F_i^η 按图 2 中针对 [[while $\mathrm{M}[\bar{q}]$ 执行 S' 结束]] 的定义来定义。首先，根据引理3.2，通过对 i 进行归纳法，很容易证明

$$\forall i \geq 0,\ \forall \eta \in [\![S']\!]^{\mathbb{N}},\ M_i^\eta = (\mathcal{F}_i^\eta)^\dagger(M). \tag{17}$$

因此我们有

$$\bigvee_{i\geq 0} M_i^\eta = \bigvee_{i\geq 0} \left(\mathcal{F}_i^\eta\right)^\dagger (M) = \left(\bigvee_{i\geq 0} \mathcal{F}_i^\eta\right)^\dagger (M),$$

and so

$$wp.S.M = \left\{\bigvee_{i\geq 0} M_i^\eta : \eta \in [\![S']\!]^{\mathbb{N}}\right\} = \left\{\mathcal{E}^\dagger(M) : \mathcal{E} \in [\![S]\!]\right\}$$

根据 $[\![S]\!]$的定义。

条款（2）的证明类似；证明 **While** $\mathcal{M}[\bar{q}]$**执行** S'**结束** 这一情形时，唯一的区别是，我们不必证明等式（17），而是需要证明

$$\forall i \geq 0,\ \forall \eta \in [\![S']\!]^{\mathbb{N}},\ I - M_i^\eta = (\mathcal{F}_i^\eta)^\dagger(I - M)$$

其中，M_i^η 的定义方式与图 5中的类似，但适用于$wlp.$（**while** $\mathrm{M}[\bar{q}]$ **do** S' **end**）$.M$。不过，通过对 i进行归纳也很容易证明这一点。

对于条款 (3)，我们计算

$$\begin{aligned}
\mathrm{Exp}(\rho \models wp.S.\Theta) &= \inf\left\{\mathrm{tr}(M\rho) : N \in \Theta, M \in wp.S.N\right\} \\
&= \inf\left\{\mathrm{tr}(\mathcal{E}^\dagger(N)\rho) : N \in \Theta, \mathcal{E} \in [\![S]\!]\right\} \\
&= \inf\left\{\mathrm{tr}(N\mathcal{E}(\rho)) : N \in \Theta, \mathcal{E} \in [\![S]\!]\right\} \\
&= \inf\left\{\mathrm{tr}(N\sigma) : N \in \Theta, \sigma \in [\![S]\!](\rho)\right\} \\
&= \inf\left\{\mathrm{Exp}(\sigma \models \Theta) : \sigma \in [\![S]\!](\rho)\right\}
\end{aligned}$$

其中，第二个等式由条款 (1) 得出。最后，条款 (4) 通过类似的论证由 (2) 得出。□

下一个引理表明，while 程序的最弱（自由）前置条件是 A 上某个函子的一个不动点。

引理 A。 $2^{M \quad \Theta =}$。对于任意量子谓词 $xp.$，令 $(\mathbf{while}\ \mathcal{M}[\bar{q}]\ \mathbf{do}\ S\ \mathbf{end}).M$。则

$$\Theta = \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}(xp.S.\Theta).$$

证明。 设 **while** $\triangleq$**while** $\mathcal{M}[\bar{q}]$**do** S**end**。那么

$$\begin{aligned}
&wp.\mathbf{while}.M \\
&= \left\{\mathcal{E}^\dagger(M) : \mathcal{E} \in [\![\mathbf{while}]\!]\right\} \\
&= \left\{\mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}} \circ \mathcal{F}^\dagger \circ \mathcal{G}^\dagger(M) : \mathcal{F} \in [\![S]\!], \mathcal{G} \in [\![\mathbf{while}]\!]\right\} \\
&= \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(wp.S.\left\{\mathcal{G}^\dagger(M) : \mathcal{G} \in [\![\mathbf{while}]\!]\right\}\right) \\
&= \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(wp.S.\left(wp.\mathbf{while}.M\right)\right)
\end{aligned}$$

其中，第二个等式由式（3）得出，其余等式均由引理 A.1(1) 得出。对于 wlp 的情形，证明类似。□

最后，为结束本节，我们证明一个对后续讨论有用的引理。

引理 A.3。 对于任意正确性公式 $\{\Theta\}\ S\ \{\Psi\}$，
(1)$\models_{tot} \{\Theta\}\ S\ \{\Psi\}$ 当且仅当 $\Theta \sqsubseteq_{inf}\ wp.S.\Psi$;
(2)$\models_{par} \{\Theta\}\ S\ \{\Psi\}$ 当且仅当 $\Theta \sqsubseteq_{inf}\ wlp.S.\Psi$。

证明。对于条款（1），我们计算

$$\begin{aligned}
&\models_{tot} \{\Theta\}\ S\ \{\Psi\} \\
&\Leftrightarrow \forall \rho, \mathrm{Exp}(\rho \models \Theta) \leq \inf\left\{\mathrm{Exp}(\sigma \models \Psi) : \sigma \in [\![S]\!](\rho)\right\} \\
&\Leftrightarrow \forall \rho, \mathrm{Exp}(\rho \models \Theta) \leq \mathrm{Exp}(\rho \models wlp.S.\Psi) \\
&\Leftrightarrow \forall \rho, \inf\left\{\mathrm{tr}(M\rho) : M \in \Theta\right\} \leq \inf\left\{\mathrm{tr}(N\rho) : N \in wlp.S.\Psi\right\} \\
&\Leftrightarrow \Theta \sqsubseteq_{inf}\ wp.S.\Psi
\end{aligned}$$

其中，第二个等价关系来自引理A 1(3)，而第三个来自式（8）。条款（2）中 wlp的情形类似。□

$$xp.\mathbf{skip}.M = M \qquad xp.(\bar{q} *= U).M = U_{\bar{q}}^{\dagger} M U_{\bar{q}}$$

$$xp.(\bar{q} := 0).M = \sum_{i=0}^{2^n-1} |i\rangle_{\bar{q}}\langle 0|M|0\rangle_{\bar{q}}\langle i| \qquad xp.S.\Theta = \bigcup_{M\in\Theta} xp.S.M$$

$$xp.(S_0; S_1).M = xp.S_0.(xp.S_1.M) \qquad xp.(S_0 \square S_1).M = xp.S_0.M \cup xp.S_1.M$$

$$wlp.\mathbf{abort}.M = \{I\} \qquad wp.\mathbf{abort}.M = \{0\}$$

$$xp.(\mathbf{if}\ \mathcal{M}[\bar{q}]\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0\ \mathbf{end}).M = \mathcal{P}_{\bar{q}}^1(xp.S_1.M) + \mathcal{P}_{\bar{q}}^0(xp.S_0.M)$$

$$wlp.(\mathbf{while}\ \mathcal{M}[\bar{q}]\ \mathbf{do}\ S\ \mathbf{end}).M = \left\{ \bigwedge_{i\geq 0} M_i^{\eta} : \eta \in [\![S]\!]^{\mathbb{N}} \right\} \text{ where for each } \eta,\ M_0^{\eta} \triangleq I, \text{ and for any } i \geq 0,$$

$$M_{i+1}^{\eta} = \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1\left(\eta_1^{\dagger}\left(M_i^{\eta^{\rightarrow}}\right) + I - \eta_1^{\dagger}(I)\right)$$

$$wp.(\mathbf{while}\ \mathcal{M}[\bar{q}]\ \mathbf{do}\ S\ \mathbf{end}).M = \left\{ \bigvee_{i\geq 0} M_i^{\eta} : \eta \in [\![S]\!]^{\mathbb{N}} \right\} \text{ where for each } \eta,\ M_0^{\eta} \triangleq 0, \text{ and for any } i \geq 0,$$

$$M_{i+1}^{\eta} = \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1\left(\eta_1^{\dagger}\left(M_i^{\eta^{\rightarrow}}\right)\right)$$

Fig图5：量子程序的最弱（宽松）前置条件语义，其中 $xp \in \{wp,\ wlp\}$.

B 证明细节

B.1 定理证明 4.1

可靠性：我们只需证明图 3中的每条规则在部分正确性的意义下都是有效的。以规则（While）为例；其他规则更简单。根据（Union），只需考虑特殊情形 $\Psi = \{M\}$ 其中 M是某个量子谓词。令

$$\vDash_{par} \{\Theta\}\ S\ \left\{\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)\right\}.$$

于是 $\Theta \sqsubseteq_{\text{下确界}} wlp.S.\left(\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)\right)$。现在我们对 i 进行归纳证明：

$$\forall i \geq 0, \forall \eta \in [\![S]\!]^{\mathbb{N}},\ \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta) \sqsubseteq_{inf} M_i^{\eta}$$

其中 M_i^{η}的定义见图 5中关于 wlp语义的 **while** $\triangleq$**while** $[\bar{q}]$ **执行** S**结束**。当 $i = 0$时，情况显然。接下来计算

$$\begin{aligned}
&\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)\\
&\sqsubseteq_{inf} \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1\left(wlp.S.\left(\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)\right)\right)\\
&\sqsubseteq_{inf} \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1\left(wlp.S.M_i^{\eta^{\rightarrow}}\right)\\
&\sqsubseteq_{inf} \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1\left(\eta_1^{\dagger}\left(M_i^{\eta^{\rightarrow}}\right) + I - \eta_1^{\dagger}(I)\right)\\
&= M_{i+1}^{\eta},
\end{aligned}$$

其中，第一个不等式由引理 42(1) 得出，第二个不等式由归纳假设以及 $wlp.S$关于$\sqsubseteq_{inf}$ 的单调性得出，第三个不等式则由引理 A.1 以及 $\eta_1 \in [\![S]\!]$得出。因此

$$\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta) \sqsubseteq_{inf} wlp.\mathbf{while}.M,$$

因此

$$\vDash_{par} \left\{\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)\right\}\ \mathbf{while}\ \{M\}$$

由引理 A.3。

完备性：由引理 A.3 和 (Imp) 规则，只需证明对于任意 Θ 和 $S\prime$,

$$\vdash_{par} \left\{wlp.S'.\Theta\right\}\ S'\ \{\Theta\}.$$

同样，我们以循环的情况为例。对于任意 $M \in \Theta$，令 Ψ, $wlp.\mathbf{while}.M$。根据归纳法，有 $\vdash_{par}\{wlp.S.\Psi\}\ S\{\Psi\}$ 。注意，根据引理 A.2， $\Psi = \mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(wlp.S.\Psi)$ 。于是，根据规则（While），有 $\vdash_{par}\{\Psi\}\ \mathbf{while}\ \{M\}$。最后，所需结果

$$\vdash_{par} \{wlp.\mathbf{while}.\Theta\}\ \mathbf{while}\ \{\Theta\}$$

由（Union）和引理 42(2) .

B.2 定理证明 4.2

可靠性：我们只需证明证明系统中的每条规则在完全正确性的意义下都是有效的。以规则（WhileT）为例。同样，由（Union）可知，只需考虑以下特殊情形：对于某个量子谓词 M，有 $\Psi = \{M\}$。令

$$\vDash_{tot} \{\Theta\}\ S\ \left\{\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)\right\},$$

并且 $\{R_i^{\eta}\colon\ i \geq 0, \eta \in [\![S]\!]^{\mathbb{N}}\}$ 是关于 **当** $\mathrm{M}[\bar{q}]$ **执行** S**结束** 的 $\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)$-排序断言。则 $\Theta \sqsubseteq_{\text{下确界}} wp.S.\left(\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta)\right)$。现在我们通过对 i 进行归纳法来证明

$$\forall i \geq 0, \forall \eta \in [\![S]\!]^{\mathbb{N}},\ \mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta) \sqsubseteq_{inf} M_i^{\eta} + R_i^{\eta}$$

其中，M_i^{η}的定义如图5所示，适用于**while** $\mathrm{M}[\bar{q}]$ **do** S**end**的 wp 语义。当 $i = 0$来自假设 $\mathrm{P}_{\bar{q}}^0(M) + \mathrm{P}_{\bar{q}}^1(\Theta) \sqsubseteq_{inf} R_0^{\eta}$时，接下来我们计算

$$\mathcal{P}_{\bar{q}}^0(M) + \mathcal{P}_{\bar{q}}^1(\Theta)$$

$$\sqsubseteq_{inf} \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(wp.S.\left(\mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}(\Theta)\right)\right)$$
$$\sqsubseteq_{inf} \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(wp.S.\left(M_i^{\eta\rightarrow} + R_i^{\eta\rightarrow}\right)\right)$$
$$\sqsubseteq_{inf} \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(\eta_1^\dagger\left(M_i^{\eta\rightarrow}\right)\right) + \mathcal{P}^1_{\bar{q}}\left(\eta_1^\dagger\left(R_i^{\eta\rightarrow}\right)\right)$$
$$\sqsubseteq_{inf} M^\eta_{i+1} + R^\eta_{i+1},$$

其中，第一个不等式由引理 42(1) 得出，第二个不等式由归纳假设以及 $wp.S$ 关于 $\sqsubseteq$ $\eta_1 \in_{inf}$ 单调A。以及 $[\![S]\!]$，第三个不等式由引理 得出，11最后一个不等式由公式 ( ) 得出。因此

$$\mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}(\Theta) \sqsubseteq_{inf} wp.(\textbf{while } \mathcal{M}[\bar{q}] \textbf{ do } S \textbf{ end}).M$$

注意到 $\acute{O}_i R_i^\eta = 0$ 对任意 η均成立，因此

$$\vDash_{tot} \left\{\mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}(\Theta)\right\} \textbf{ while } \mathcal{M}[\bar{q}] \textbf{ do } S \textbf{ end } \{M\}$$

根据引理 A.3。

完备性：根据引理 A.3 和 (Imp) 规则，只需证明对于任意 Θ 和 $S\prime$，

$$\vdash_{tot} \{wp.S'.\Theta\}\ S'\ \{\Theta\}.$$

同样，我们以 while 循环的情形为例。设 while $\triangleq$while M$[\bar{q}]$ do Send 和 $M \in \Theta$。根据归纳法，有 $\vdash$tot $\{wp.S.\Psi\}$ $S\{\Psi\}$，其中 Ψ, $wp.$while$.M$。另由引理 A.2 可知， $\Psi = \mathrm{P}^0_{\bar{q}}(M) + \mathrm{P}^1_{\bar{q}}(wp.S.\Psi)$。为完成证明，我们需要构造一个用于 while 的 Ψ- 排序断言。

对于任意 $\eta \in [\![S]\!]^{\mathbb{N}}$ 和 $k \geq 0$，令

$$R^\eta_k = \sum_{i=k}^{\infty} \mathcal{P}^1_{\bar{q}} \circ \eta_1^\dagger \circ \ldots \circ \mathcal{P}^1_{\bar{q}} \circ \eta_i^\dagger \circ \mathcal{P}^0_{\bar{q}}(I). \tag{18}$$

我们要证明，满足定义 R^η_k 中条件的集合4.3。首先，我们对 i 进行归纳，证明

$$\forall i \geq 0, \forall \eta \in [\![S]\!]^{\mathbb{N}},\ M^\eta_i \sqsubseteq R^\eta_0 \tag{19}$$

其中 M^η_i 按图 5 中对 $wp.$**的定义**$.M$，这进而意味着 $\Psi \sqsubseteq_{inf} R^\eta_0$。式（19）中 $i = 0$ 的基例显然成立，因为 $M^\eta_0 = 0$。进一步计算可得

$$\begin{aligned} M^\eta_{i+1} &= \mathcal{P}^0_{\bar{q}}(M) + \mathcal{P}^1_{\bar{q}}\left(\eta_1^\dagger\left(M_i^{\eta\rightarrow}\right)\right) \\ &\sqsubseteq \mathcal{P}^0_{\bar{q}}(I) + \mathcal{P}^1_{\bar{q}}\left(\eta_1^\dagger\left(R_0^{\eta\rightarrow}\right)\right) \\ &= R^\eta_0. \end{aligned}$$

对于定义4 3的第二个条件，我们注意到由式（18）可得，$R^\eta_{k+1} \sqsubseteq R^\eta_k$和 $\acute{O}_k R^\eta_k = 0$。此外，很容易看出$R^\eta_{k+1} = \mathrm{P}^1_{\bar{q}}\left(\eta_1^\dagger\left(R_k^{\eta\rightarrow}\right)\right)$。

现在使用规则(WhileT)，我们有 $\vdash_{总计}$ $\{\Psi\}$ 当 $\{M\}$。最后，得到所需结果

$$\vdash_{tot} \{wp.\textbf{while}.\Theta\}\ \textbf{while}\ \{\Theta\}$$

由（Union）和引理 4.2（2）。

C 制品附录

C.1 摘要

NQPV 是一个用于非确定性量子程序的验证助手原型。它以数值形式实现了部分正确性的验证逻辑，其可靠性由理论和实验保证。它是一个 Python 项目，依赖 numpy、cvxpy 和 ply 软件包。论文中的三个示例——三量子比特比特翻转量子纠错方案、Deutsch 算法和量子游走——均以数值方式编码并经过验证。评估过程集成在一个循序渐进的 Jupyter 笔记本中。它展示了该工具能够检查程序语法、自动计算验证条件、检查前置条件是否满足该条件，并在满足时返回正确性公式的证明概要。与基于 Coq 或 Isabelle 等定理证明器的其他验证工具相比，NQPV 的表达能力较弱，但自动化程度更高。整个评估可在配备 32 GB 内存的计算机上完成。

C.2 制品检查清单（元信息）

- **算法：** 非确定性量子程序验证。 • **运行环境：** Python 3。该项目使用 Python 3.9 开发。
- **指标：** 程序和量子断言的表达能力；验证的自动化程度；验证较大程序所需的时间和内存消耗。
- **输出：** 数值验证条件已保存到计算机文件中。
- **实验：** 集成在 Jupyter 笔记本中。
- **大约需要多少磁盘空间？：** 只有性能测试会消耗资源。本文中的实验使用 8 GB 空间即可。
- **大约需要多少时间来准备工作流程？：** 5 分钟。
- **大约需要多少时间来完成实验？：** 浏览 Jupyter 笔记本需要 15 分钟。 • **是否公开提供：** 是，在 GitHub、Zenodo 和 PyPI 上均可获取。
- 2 0 **代码许可（如公开提供）：**
- Apache- 。**是否已存档（请提供数字对象标识符）：** https://doi.org/ 。/ 10.5281 zenodo.7564087

C.3 描述

C.3.1 如何访问。这是一个托管在 GitHub 上的 Python 项目：https://github.com/Luci 为进行评估，请克隆“文章发布版”。项目本身约有 1 MB 大小。

该项目也已作为 Python 包发布在 PyPI 上：https://pypi.org/project/NQP

C.3.2 硬件依赖项。只有性能测试较为消耗资源。配备 32 GB 内存和 8 GB 磁盘存储的笔记本电脑足以进行评估。

C.3.3 软件依赖项。Python 包：用于矩阵计算的 numpy、用于半定规划求解器的 cvxpy，以及用于语法解析的 ply。

C.4 安装

使用源代码进行实验：

(1) 准备 Python 3 环境（本项目使用 Python 3.9 开发）。
(2) 使用以下命令安装软件包依赖项：pip install cvxpy ply (3) 克隆 NQPV 项目或下载“文章发布版”。

(4) 在项目根目录打开控制台，并使用 python test_install.py 运行测试脚本。如果未报告错误，则表示安装成功。将 NQPV 作为 Python 软件包安装：运行命令 pip install NQPV

C.5 实验流程

在源代码根目录中找到 Jupyter 笔记本 evaluate.ipynb。该笔记本简要介绍了此工具，并整合了论文中所有示例的验证实验。

每项实验都使用一个包含 NQPV 程序代码的 .nqpv 文件，以及一个用于准备算子并调用验证的 .py Python 脚本。

C.6 评估和预期结果

论文中的三个示例——三量子比特比特翻转量子纠错方案、Deutsch 算法和量子游走——均在 Jupyter 笔记本中编码为程序代码。该笔记本还包含一些示例，用以展示 NQPV 拒绝错误正确性声明的能力。所需的算子（特殊的酉算子或测量）已准备好并保存为 NumPy 矩阵。

预期验证将自动完成，并打印出证明概要。我们可以使用 show 命令检查证明概要中的每个中间条件。每个示例的验证条件都会与给定的前置条件进行比较。

最后，给出了 NQPV 在较大量子比特数上的性能测试。对于 Grover 算法，NQPV 需要数分钟和 32 GB 内存才能完成对 13 量子比特情况的验证。

C.7 实验定制

笔记本中的示例展示了如何在 NQPV 中描述验证任务的语法。

要进行定制实验，我们可以：
（1）在 example.nqpv 文件中编写验证任务。该文件包含待验证的程序、前置条件和后置条件，以及循环不变量。（2）准备一个 Python 脚本，将 example.nqpv 中使用的算子生成为二进制 numpy 矩阵文件。然后使用命令 nqpv.verify("example.nqpv") 调用验证。（3）运行 Python 脚本执行验证。（4）获得证明概要后，修改 example.nqpv，并重复上述步骤，以在验证过程中打印条件。

为避免路径错误，应在 NQPV 源代码的根文件夹中进行上述实验，或使用通过 PyPI 安装的 NQPV。

C.8 注释

macOS 用户可能会遇到 cmake 软件包导致的安装错误。遇到这种情况时，请先运行 pip install cmake，然后手动将 cmake 添加到 PATH，最后安装 NQPV。

我们建议使用 conda 创建新的实验环境。该部署也已在 Linux 云服务器上进行测试。

参考文献

[1] Ralph-Johan Back 和 Joakim Wright。2012。《细化演算：系统介绍》。Springer Science & Business Media。[2] Yuxin Deng、Yuan Feng 和 Ugo Dal Lago。2015。《余归纳与量子 λ 演算》。载于第 26 届国际并发理论会议。427–440。[3] David Deutsch。1985。《量子理论、丘奇–图灵原理与通用量子计算机》。载于《伦敦皇家学会会刊 A：数学与物理科学》400 卷第 1818 期（1985），97–117。[4] Ellie D'Hondt 和 Prakash Panangaden。2006。《量子最弱前置条件》。《计算机科学数学结构》16 卷第 3 期（2006），429–451。[5] Edsger Wybe Dijkstra、Edsger Wybe Dijkstra、Edsger Wybe Dijkstra、Etats-Unis Informaticien 和 Edsger Wybe Dijkstra。1976。《程序设计规范》。Prentice-Hall Englewood Cliffs。[6] Yuan Feng、Runyao Duan、Zhengfeng Ji 和 Mingsheng Ying。2007。《量子程序正确性的证明规则》。《理论计算机科学》386 卷第 1–2 期（2007），151–166。[7] Yuan Feng 和 Mingsheng Ying。2021。《含经典变量的量子霍尔逻辑》。《ACM 量子计算汇刊》2 卷第 4 期（2021），1–43。[8] Jifeng He、Karen Seidel 和 Annabelle McIver。1997。《守卫命令语言的概率模型》。《计算机程序设计科学》28 卷第 2–3 期（1997），171–192。[9] CAR Hoare、He Jifeng 和 Augusto Sampaio。1993。《编译器设计的范式方法》。《信息学学报》30 卷第 8 期（1993），701–739。[10] Karl Kraus、Arno Böhm、John D Dollard 和 WH Wootters。1983。《状态、效应与操作：量子理论的基本概念》。《物理学讲义》190（1983）。[11] Yangjia Li 和 Mingsheng Ying。2017。《量子程序终止问题的算法分析》。载于《ACM 程序设计语言会议录》。ACM，纽约，纽约州，美国，1–29。[12] Yangjia Li、Nengkun Yu 和 Mingsheng Ying。2014。《非确定性量子程序的终止性》。《信息学学报》51 卷第 1 期（2014），1–24。[13] Junyi Liu、Bohua Zhan、Shuling Wang、Shenggang Ying、Tao Liu、Yangjia Li、Mingsheng Ying 和 Naijun Zhan。2019。《使用量子霍尔逻辑对量子算法进行形式化验证》。Springer，Cham，187–207。https://doi.org/10 1007 978 3 030 25543 5 _ 12 。 / - - - - { } Annabelle McIver 、[14] Carroll Morgan 和 Charles Carroll Morgan。2005。《概率系统的抽象、细化与证明》。Springer Science & Business Media。[15] A K McIver 和 Carroll Morgan。2001。《概率恶魔程序的部分正确性》。《理论计算机科学》266 卷第 1–2 期（2001 年 9 月），513–541。https://doi.org/10 1016 0304 3975 00 00208 5 。 /s - ( ) - Graeme Mitchison 和 Richard Jozsa。[16] 2001。《反事实计算》。《伦敦皇家学会会刊 A 辑：数学、物理与工程科学》457 卷第 2009 期（2001），1175–1193。[17] Carroll Morgan。1993。《细化演算》。载于《程序设计演算》。Springer，3–52。[18] Carroll Morgan、Annabelle McIver 和 Karen Seidel。1996。《概率谓词变换器》。《ACM 程序设计语言与系统汇刊（TOPLAS）》18 卷第 3 期（1996），325–353。[19] Joseph M Morris。1987。《逐步细化与程序演算的理论基础》。《计算机程序设计科学》9 卷第 3 期（1987），287–306。[20] Michael A Nielsen 和 Isaac Chuang。2002。《量子计算与量子信息》。剑桥大学出版社。[21] Michele Pagani、Peter Selinger 和 Benoît Valiron。2014。《将定量语义应用于高阶量子计算》。载于第 41 届 ACM SIGPLAN-SIGACT 编程语言原理研讨会论文集。647–658。[22] Jeff W Sanders 和 Paolo Zuliani。2000。《量子编程》。载于国际程序构造数学会议。Springer，80–99。[23] Peter Selinger。2004。《迈向量子编程语言》。《计算机科学数学结构》14 卷第 4 期（2004），527–586。[24] Peter Selinger 和 Benoît Valiron。2006。《具有经典控制的量子计算 λ 演算》。《计算机科学数学结构》16 卷第 3 期（2006），527–552。[25] Dominique Unruh。2019。《量子关系霍尔逻辑》。《ACM 程序设计语言会议录》3 卷，POPL（2019），1–31。https://doi.org/10 1145 3290346 。 / André Van Tonder。《量子计算的 λ 演算》。[26] 2004。《SIAM 计算杂志》33 卷第 5 期（2004），1109–1135。[27] John Von Neumann。1955。《量子力学的数学基础》。普林斯顿大学出版社，普林斯顿，新泽西州。[28] Mingsheng Ying。2012。《量子程序的弗洛伊德–霍尔逻辑》。《ACM 程序设计语言与系统汇刊（TOPLAS）》33 卷第 6 期（2012），1–49。

[29] Li Zhou、Gilles Barthe、Pierre-Yves Strub、Junyi Liu 和 Mingsheng Ying。2022。*CoqQ*：量子程序的基础验证。arXiv。https://doi.org/10.48550/arXiv.2207.11350

[30] Paolo Zuliani。2004年。非确定性量子编程。载于 第二届量子编程语言国际研讨会论文集。179–195。

收稿日期：2022年10月20日；录用日期：2023年1月19日