

Quantum Weakest Preconditions for Reasoning about Expected Runtimes of Quantum Programs

量子程序期望运行时间的量子最弱前置条件推理

刘君毅, 周立, Gilles Barthe, 应明生

Accepted by 37th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), 2022

联系方式: liujy@ios.ac.cn

研究背景

量子计算机的硬件在近年取得了重大的突破, Google和中科大都分别在超导量子芯片上实现了量子优越性的实验。然而, 目前超导量子芯片的退相干时间很短, 每次运行量子程序的时间都非常有限。为此, 我们需要分析量子程序所需要的运行时间, 以判断其是否能在当前的量子设备上有效地运行。

论文摘要

在这篇论文中, 我们研究了量子程序的期望运行时间。受到近期关于概率程序的工作[1]启发, 我们给出了一种关于量子程序期望运行时间的量子最弱前置条件演算。我们证明了量子程序 S 在初态为 ρ 时的期望运行时间 $ERT[S](\rho)$ 可以用一个量子力学中的可观测量 $ert[S]$ 在 ρ 上的期望值 $\text{tr}(ert[S] \cdot \rho)$ 来表示。基于这一发现, 我们提出了一种计算有限维状态空间中量子程序期望运行时间的方法。借此, 我们计算了包括量子伯努利工厂算法在内几个量子程序的期望运行时间。特别地, 我们还解决了量子随机游走的期望运行时间这一公开问题。

主要结果

我们首先证明了在有限维Hilbert空间中, 对期望运行时间有限的初态, 量子程序的期望运行时间可以由一个可观测量的期望值表示:

定理1. 对于量子程序 S 和初态 ρ , 如果 $ERT[S](\rho) < \infty$, 那么

$$ERT[S](\rho) = \text{tr}(ert[S] \cdot \rho)$$

这一定理说明可观测量 $ert[S]$ 完全描述了量子程序 S 在期望运行有限的状态上所需的运行时间。这意味着给定满足要求的初态 ρ , 我们不需要运行量子程序 S , 而只需要计算 $\text{tr}(ert[S] \cdot \rho)$ 就能得到 S 在 ρ 上的期望运行时间。而为了能够应用上述结论, 我们还需要判断一个初态的期望运行时间是否有限。之前的工作[2]发现在量子程序以1的概率终止的状态构成了状态空间上的一个线性子空间。在此基础上, 我们证明了在有限维Hilbert空间中, 量子程序以1的概率终止等价于期望运行时间有限。

定理2. 对于量子程序 S 和初态 ρ , 有 $ERT[S](\rho) < \infty$ 当且仅当 S 在以 ρ 为初态时以1的概率终止。

将上面两个定理结合, 我们就得到了有限维Hilbert空间上量子程序期望运行时间的一个完整刻画。要计算量子程序 S 在初态 ρ 上的期望运行时间, 我们只需要先判断 S 在 ρ 上是否以1的概率终止, 如果终止的概率小于1, 那么 S 的期望运行时间无限; 如果终止的概率等于1, 那么 S 的期望运行时间就等于 $\text{tr}(ert[S] \cdot \rho)$ 。

在 $ert[S]$ 的计算中, 当程序 S 包含循环时会需要计算矩阵序列的极限, 直接求解会比较困难。为此, 我们参考了[3]中方法, 利用超算子矩阵表示的性质给出了一种实用的计算方法。利用这一方法, 我们计算出了带吸收壁的量子随机游走在任意初态下期望运行时间的一个解析解, 解决了一个公开问题。

参考文献

- [1] Kaminski B L, Katoen J P, Matheja C, et al. Weakest precondition reasoning for expected run-times of probabilistic programs[C]//European Symposium on Programming. Springer, 2016: 364-389.
- [2] Zhou L, Yu N, Ying M. An applied quantum Hoare logic[C]//Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation. 2019: 1149-1162.
- [3] Ying M, Yu N, Feng Y, et al. Verification of quantum programs[J]. Science of Computer Programming, 2013, 78(9): 1679-1700.