

迎新报告

姓名: 刘君毅
导师: 应明生

2019 年 9 月 8 日

研究方向

- 量子程序设计语言
- 量子程序的形式化研究

2018-2019 学年主要研究成果:

- Formal verification of quantum algorithms using quantum Hoare logic, Junyi Liu, Bohua Zhan, Shuling Wang, Shenggang Ying, Tao Liu, Yangjia Li, Mingsheng Ying and Naijun Zhan.
- Expected runtimes of quantum programs.

Hoare Logic

经典的 Hoare Logic 用于验证程序的正确性.

- While Program:

$S ::= \text{skip} \mid u := t \mid S_1; S_2 \mid \text{if } B \text{ then } S_1 \text{ else } S_2 \mid \text{while } B \text{ do } S$

- Hoare triple:

$\{P\}S\{Q\}$

- Example:

$\{x \geq 0\}x := x + 1\{x > 0\}$

Quantum Hoare Logic¹

- Quantum While Program:

$$S ::= \text{skip} \mid \bar{q} := U\bar{q} \mid S_1; S_2 \mid \text{measure } M[\bar{q}] : \bar{S} \\ \mid \text{while } M[\bar{q}] = 1 \text{ do } S$$

- Quantum Predicate:

P is a quantum predicate $\Leftrightarrow P$ and $(I - P)$ are both positive

- Hoare triple:

$$\{P\}S\{Q\}$$

where P, Q are quantum predicates and S is a quantum while program.

- Example:

$$\{|0\rangle_q\langle 0|\}q := H[q]\{|+\rangle_q\langle +|\}$$

¹Mingsheng Ying. “Floyd–hoare logic for quantum programs”. In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 33.6 (2011), p. 19.

Grover's Algorithm²

Given $f: \{0, 1, \dots, N-1\} \rightarrow \{0, 1\}$, find x such that $f(x) = 1$.

- Example: SAT.
- Classical Algorithm: $O(N)$ queries of f .
- Grover's Algorithm: $O(\sqrt{N})$ quantum queries of f .

²Lov K Grover. "A fast quantum mechanical algorithm for database search". In: *arXiv preprint quant-ph/9605043* (1996).

我们在交互式证明环境 Isabelle 中形式化了 Quantum Hoare Logic 并在这一框架下验证了 Grover's Algorithm 的一类情形. 据我们所知, 这是首个在交互式证明环境下非平凡量子算法的形式化证明.

我们对 Quantum Hoare Logic 的形式化同时也是一个验证量子程序正确性的框架.

其他贡献:

- Isabelle 下 Hermitian 矩阵可对角化的形式证明.
- Isabelle 下有限维有界单调线性算子序列极限存在性的形式证明.
- Quantum Hoare Logic partial correctness 完备性和可靠性的形式化证明.

研一学习建议

- 目标: 弄懂专业名词, 拓宽视野.
 - 个人推荐:
 - 代数基础
 - 高等分析基础
- 适合没有数学背景的同学.
- 对感兴趣的内容, 可以在 Google 和 Youtube 搜索相应的国外课程录像, 通常能找到内容较深质量较高的课程.
 - 学英语.

个人体会

- 什么事情是自己想做的?
- 什么东西是自己觉得有价值的?
- 学想学的东西.
- 做想做 (且别人没做过) 的事.
- 有目的地练习.

谢谢