ISCAS 中国科学院软件研究所学术年会'2022 暨计算机科学国家重点实验室开放周 学术论文

互不交并行量子程序的证明系统

李杨佳

计算机科学国家重点实验室

yangjia@ios.ac.cn

论文：Mingsheng Ying, Li Zhou, Yangjia Li and Yuan Feng, A proof system for disjoint parallel quantum programs, TCS 2022

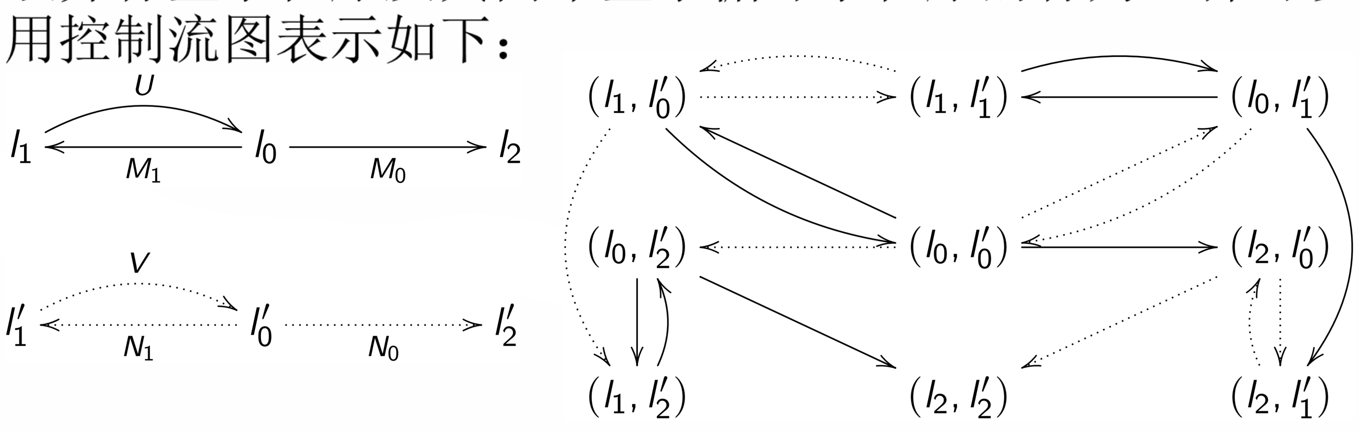
问题背景

并行量子程序的行为由其顺序子程序的行为复合而成。

以如下的并行量子程序为例：

$$\textbf{while } M[q]=1 \textbf{ do } U[q] \textbf{ od} \parallel \textbf{while } N[q]=1 \textbf{ do } V[q] \textbf{ od}$$

该并行量子程序及其两个量子循环子程序的行为，都可以用控制流图表示如下：



并行量子程序的特点：执行路径和运行结果具有不确定性

顺序量子程序的Hoare逻辑 (Ying, 2011)

$$\{precondition\}\ \mathrm{QP}\ \{postcondition\}$$

前后条件：量子断言 $X=X^*, 0\sqsubseteq X\sqsubseteq I$

逻辑公式间的推理：

$$\frac{\{A\}P_1\{B\},\ B\Rightarrow C, \{C\}P_2\{D\}}{\{A\}P_1;P_2\{D\}}$$

研究目标：并行量子程序的Hoare逻辑

$$\{A\}\ P_1 \parallel \cdots \parallel P_n\ \{B\}$$

$P_1,\cdots,P_n$为顺序量子程序，从它们各自的正确性出发，证明整体程序的正确性。

应用：并行量子算法具有广泛应用，需要验证其正确性

研究难点

经典并行程序的证明方法：并行程序的整体性质可以从各个子程序的性质获得

$$\frac{\{A_i\}P_i\{B_i\}\quad \text{for } i=1,\cdots,n}{\{\bigwedge_{i=1}^n A_i\}P_1\parallel\cdots\parallel P_n\{\bigwedge_{i=1}^n B_i\}}\quad (R.PC)$$

$\{A_i\}P_i\{B_i\}$ 通过的顺序程序的证明方法得到，只要这些证明是 interference free 的，那么$(R.PC)$ 成立。这是由 Owicki & Gries (1976) 和 Lamport (1977) 各自独立提出的方法。

量子情形下 Owicki-Gries 和 Lamport 方法失效！

反例：$\{0.5I\}\ X\ [q] \parallel q:=|0\rangle; H[q]\ \{|0\rangle\langle 0|\}$

为用QGL方法证明上式，需找到 W 来证明：

$$\{0.5I\}\ q:=|0\rangle;\ \{W\}\ (X\ [q] \parallel H[q])\ \{|0\rangle\langle 0|\}$$

这要求：$0\sqsubseteq W\sqsubseteq |+\rangle\langle +|, |-\rangle\langle -|$，并且

$$\langle 0|W|0\rangle\geq 0.5$$

但很容易验证，这样的算子 W 是不存在的！

程序行为的复杂性

分析并行量子程序需要处理以下两类对象的耦合：

(1) 连续的状态空间用以刻画量子线性叠加特性

(2) 离散集合的划分用以描述程序执行中的不确定选择

这使得并行量子程序的行为更加复杂，现有分析方法可能失效。以如下并行量子程序为例：

$$\textbf{while } M[q]=1 \textbf{ do } U[q] \textbf{ od}\ \parallel\ V[q]$$

其中 $M=\{M_0=|2\rangle\langle 2|, M_1=|0\rangle\langle 0|+|1\rangle\langle 1|\}$,

$$U=|+\rangle\langle +|+e^{i\pi c}|-\rangle\langle -|+|2\rangle\langle 2|,$$

$$V=|1\rangle\langle 0|+|2\rangle\langle 1|+|0\rangle\langle 2|.$$

分析可知，对初始态 $q=|0\rangle$，程序的终止概率集合为

$$\{(1-\cos n\pi c)/2 | n\geq 0\}$$

特别的，当c为无理数时，这是一个区间 [0,1] 上的稠密集，其上确界 1 可任意逼近但永远无法取得，因此无法定义其最弱前置条件，这与顺序量子程序的情形有本质不同。

主要结果

针对互不交并行量子程序的证明开展研究：

$$\{A\}\ P_1\parallel\cdots\parallel P_n\ \{B\}$$

其子程序 $P_1,\cdots,P_n$ 之间两两都不共享变量。主要有两种情形：

(1)简单情形：A 和 B 为可分算子。利用以下推理规则可以证明 A 和 B 都为张量积形式的情形：

$$\frac{\{A_i\}P_i\{B_i\}\quad \text{for } i=1,\cdots,n}{\{\bigotimes_{i=1}^n A_i\}P_1\parallel\cdots\parallel P_n\{\bigotimes_{i=1}^n B_i\}}\quad (R.PC.P)$$

进一步，将张量积形式的算子进行凸组合，就可以得到一般的可分算子。

(2)复杂情形：A 和 B 中存在量子纠缠。这一情形下，并行程序整体的性质无法直接表示为子程序性质的复合，是研究中的难点。

成果：我们提出了两种完备的证明方法来处理这一情形。

方法一：辅助变量法。该方法通过以下三个步骤完成：

(1) 引入变量。对程序中的每个变量 q 都引入一个辅助变量 q'，q' 具有和 q 一致的数据类型 (也即状态空间维数相同)。

(2) 形成纠缠。证明每个子程序的性质 $\{A_i\}P_i\{B_i\}$，其中 A_i 和 B_i 不仅包含 P_i 中的变量 q_i，还包含对应的辅助变量 q_i'，并且在两种变量之间形成纠缠。运用规则 $(R.PC.P)$ 得到整体程序的性质：

$$\{A'=\bigotimes_{i=1}^n A_i\}P_1\parallel\cdots\parallel P_n\{B'=\bigotimes_{i=1}^n B_i\}$$

(3) 消去变量。选择辅助变量上的一个消去操作 $\mathcal{E}$ 同时作用在前后条件上得到：$A=\mathcal{E}(A')$， $B=\mathcal{E}(B)$。

方法二：纠缠转换法

利用 Gurvits & Barnum (2003) 的结果，可以选择足够小的系数 $\epsilon>0$，可以使得 $(1-\epsilon)I+\epsilon A$ 与 $(1-\epsilon)I+\epsilon B$ 都成为可分的，即使 A 和 B都是纠缠的。进一步利用可分情形的技术可以证明：

$$\{(1-\epsilon)I+\epsilon A\}\ P_1\parallel\cdots\parallel P_n\ \{(1-\epsilon)I+\epsilon B\}$$

以下证明规则把纠缠的情形归约为可分的情形：

$$\frac{\{(1-\epsilon)I+\epsilon A\}P\{(1-\epsilon)I+\epsilon B\}}{\{A\}P\{B\}}$$