基于期望的量子关系Hoare逻辑

李杨佳

计算机科学国家重点实验室

yangjia@ios.ac.cn

论文：Yangjia Li and Dominique Unruh, Quantum Relational Hoare Logic with Expectations，ICALP 2021

研究背景

程序验证基本方法：Hoare逻辑

$$\{x \geq 0\}\ \text{SQRT}\ \{y^2 = x\}$$

逻辑公式间的推理：

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

量子程序Hoare逻辑 [Ying, TOPLAS'12]

$$\{precondition\}\ \text{QP}\ \{postcondition\}$$

前后条件：量子断言

$$X = X^*, 0 \leq X \leq I$$

经典程序的关系Hoare逻辑

$$\{A\}\ P_1 \sim P_2\ \{B\}$$

含义：$(input_1, input_2) \vDash A \Rightarrow (output_1, output_2) \vDash B$

概率程序：分布μ_1, μ_2的耦合μ

$$\text{Proj}_1(\mu) = \mu_1, \text{Proj}_2(\mu) = \mu_2$$

1. 定性分析：$(\mu_1, \mu_2) \vDash A \Leftrightarrow \mu \vDash A$ 对某个耦合μ成立
2. 定量分析：$(\mu_1, \mu_2) \vDash A \stackrel{\text{def}}{=} \max_{\mu} \chi_A(\mu)$

量子程序的关系Hoare逻辑

$$\{A\}\ Q_1 \sim Q_2\ \{B\}$$

Q_1, Q_2为量子程序，A, B为耦合空间上的算子。

定性分析 [Unruh, POPL'19]

$$tr(A\rho_{in}) = 1 \Rightarrow tr(B\rho_{out}) = 1$$

A, B为投影算子：$X = X^*X$

问题：定量分析?

A, B为量子期望：$X = X^*, X \geq 0$

应用：密码安全性验证

$$\{=_A\}\ Q_1 \sim Q_2\ \{=_A\}$$

主要成果

基于期望的量子Hoare逻辑（EQRHL）公式定义：

$$\{A\}\ Q_1 \sim Q_2\ \{B\}\quad \text{iff}$$

$\forall \rho_{in} \in \text{SEP}(H^{\otimes 2}), \exists \rho_{out} \in \text{SEP}(H^{\otimes 2})$ s.t.

(1) $tr_2(\rho_{out}) = [\![Q_1]\!](tr_2(\rho_{in}))$;

(2) $tr_2(\rho_{out}) = [\![Q_1]\!](tr_2(\rho_{in}))$;

(3) $tr(A\rho_{in}) \leq tr(B\rho_{out})$.

这里假定Q_1, Q_2为终止的量子程序。

一般情形：Q_1, Q_2为可能不终止的量子程序。

典型例子：$\{(1-\epsilon)A\}$ **skip** ~ 0.999**skip** $\{A\}$

解决方案：新增状态$\perp$表示不终止

$$[\![Q']\!](\rho) \stackrel{\text{def}}{=} [\![Q]\!](\rho) + [1 - tr[\![Q]\!](\rho)]P_\perp$$

则Q'在$H \oplus |\perp\rangle$上总是终止的，转而考虑

$$\{A\}\ Q_1' \sim Q_2'\ \{B\}$$

部分正确性: $\{A+T\}\ Q_1' \sim Q_2'\ \{B+T\}$

$$T \stackrel{\text{def}}{=} I \otimes P_\perp + P_\perp \otimes I - P_{\perp\perp}$$

推理规则

$$\textsc{Skip}\ \frac{}{\{A\}\ \underline{\textbf{skip}} \sim \underline{\textbf{skip}}\ \{A\}} \qquad \textsc{Apply1}\ \frac{}{\{(U\ \underline{\textbf{on}}\ \mathbf{X}_1)^*\mathsf{A}(U\ \underline{\textbf{on}}\ \mathbf{X}_1)\}\ \underline{\textbf{apply}}\ U\ \underline{\textbf{to}}\ \mathbf{X} \sim \underline{\textbf{skip}}\ \{\mathsf{A}\}}$$

$$\textsc{ExFalso}\ \frac{}{\{0\}\ \mathbf{c} \sim \mathfrak{d}\ \{\mathsf{B}\}} \qquad \textsc{Init1}\ \frac{}{\{\mathrm{id}_{\mathbf{X}_1} \otimes (\psi^* \otimes \mathrm{id}_{-\mathbf{X}_1})\mathsf{A}(\psi \otimes \mathrm{id}_{-\mathbf{X}_1})\}\ \mathbf{X} \leftarrow \psi \sim \underline{\textbf{skip}}\ \{\mathsf{A}\}}$$

$$\textsc{Seq}\ \frac{\{\mathsf{A}\}\ \mathbf{c}_1 \sim \mathfrak{d}_1\ \{\mathsf{B}\} \qquad \{\mathsf{B}\}\ \mathbf{c}_2 \sim \mathfrak{d}_2\ \{\mathsf{C}\}}{\{\mathsf{A}\}\ \mathbf{c}_1; \mathbf{c}_2 \sim \mathfrak{d}_1; \mathfrak{d}_2\ \{\mathsf{C}\}} \qquad \textsc{Conseq}\ \frac{\mathsf{A}' \leq \mathsf{A} \qquad \{\mathsf{A}\}\ \mathbf{c} \sim \mathfrak{d}\ \{\mathsf{B}\} \qquad \mathsf{B} \leq \mathsf{B}'}{\{\mathsf{A}'\}\ \mathbf{c} \sim \mathfrak{d}\ \{\mathsf{B}'\}}$$

$$\textsc{Sym}\ \frac{\{\mathsf{A}\}\ \mathbf{c} \sim \mathfrak{d}\ \{\mathsf{B}\}}{\{\mathsf{SWAP}^* \cdot \mathsf{A} \cdot \mathsf{SWAP}\}\ \mathfrak{d} \sim \mathbf{c}\ \{\mathsf{SWAP}^* \cdot \mathsf{B} \cdot \mathsf{SWAP}\}} \qquad \textsc{Scale}\ \frac{\{\mathsf{A}\}\ \mathbf{c} \sim \mathfrak{d}\ \{\mathsf{B}\} \qquad \lambda \in [0,1]}{\{\lambda\mathsf{A}\}\ \mathbf{c} \sim \mathfrak{d}\ \{\lambda\mathsf{B}\}}$$

$$\textsc{If1}\ \frac{\{\mathsf{A}_T\}\ \mathbf{c}_T \sim \mathfrak{d}\ \{\mathsf{B}\} \qquad \{\mathsf{A}_F\}\ \mathbf{c}_F \sim \mathfrak{d}\ \{\mathsf{B}\}}{\{\downarrow^*_{\mathsf{true}}(\mathsf{A}_T) + \downarrow^*_{\mathsf{false}}(\mathsf{A}_F)\}\ \underline{\textbf{if}}\ M[\mathbf{X}]\ \underline{\textbf{then}}\ \mathbf{c}_T\ \underline{\textbf{else}}\ \mathbf{c}_F \sim \mathfrak{d}\ \{\mathsf{B}\}}$$

$$\textsc{JointIf9}\ \frac{\{\mathsf{A}_{t,u}\}\ \mathbf{c}_t \sim \mathfrak{d}_u\ \{\mathsf{B}\}\ \text{for } t,u \in \{\mathsf{true}, \mathsf{false}\}}{\{\textstyle\sum_{t,u \in \{\mathsf{true},\mathsf{false}\}} \downarrow^*_{t,u}(\mathsf{A}_{t,u})\}\ \underline{\textbf{if}}\ M[\mathbf{X}]\ \underline{\textbf{then}}\ \mathbf{c}_{\mathsf{true}}\ \underline{\textbf{else}}\ \mathbf{c}_{\mathsf{false}} \sim \underline{\textbf{if}}\ N[\mathbf{Y}]\ \underline{\textbf{then}}\ \mathfrak{d}_{\mathsf{true}}\ \underline{\textbf{else}}\ \mathfrak{d}_{\mathsf{false}}\ \{\mathsf{B}\}}$$

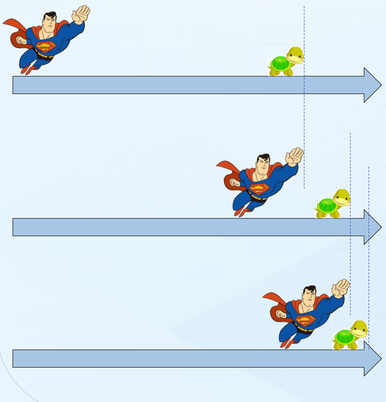
$$\textsc{JointIf}\ \frac{\{\mathsf{A}_{\mathsf{true}}\}\ \mathbf{c}_{\mathsf{true}} \sim \mathfrak{d}_{\mathsf{true}}\ \{\mathsf{B}\} \qquad \{\mathsf{A}_{\mathsf{false}}\}\ \mathbf{c}_{\mathsf{false}} \sim \mathfrak{d}_{\mathsf{false}}\ \{\mathsf{B}\}}{\{\downarrow^*_{\mathsf{true},\mathsf{true}}(\mathsf{A}_{\mathsf{true}}) + \downarrow^*_{\mathsf{false},\mathsf{false}}(\mathsf{A}_{\mathsf{false}})\}\ \underline{\textbf{if}}\ M[\mathbf{X}]\ \underline{\textbf{then}}\ \mathbf{c}_{\mathsf{true}}\ \underline{\textbf{else}}\ \mathbf{c}_{\mathsf{false}} \sim \underline{\textbf{if}}\ N[\mathbf{Y}]\ \underline{\textbf{then}}\ \mathfrak{d}_{\mathsf{true}}\ \underline{\textbf{else}}\ \mathfrak{d}_{\mathsf{false}}\ \{\mathsf{B}\}}$$

$$\textsc{While1}\ \frac{\{\mathsf{A}\}\ \mathbf{c} \sim \underline{\textbf{skip}}\ \{\downarrow^*_{\mathsf{true}}(\mathsf{A}) + \downarrow^*_{\mathsf{false}}(\mathsf{B})\} \qquad \underline{\textbf{while}}\ M[\mathbf{X}]\ \underline{\textbf{do}}\ \mathbf{c}\ \text{is terminating}}{\{\downarrow^*_{\mathsf{true}}(\mathsf{A}) + \downarrow^*_{\mathsf{false}}(\mathsf{B})\}\ \underline{\textbf{while}}\ M[\mathbf{X}]\ \underline{\textbf{do}}\ \mathbf{c} \sim \underline{\textbf{skip}}\ \{\mathsf{B}\}}$$

$$\textsc{JointWhile}\ \frac{\{\mathsf{A}\}\ \mathbf{c} \sim \mathfrak{d}\ \{\downarrow^*_{\mathsf{true},\mathsf{true}}(\mathsf{A}) + \downarrow^*_{\mathsf{false},\mathsf{false}}(\mathsf{B})\} \qquad \underline{\textbf{while}}\ M[\mathbf{X}]\ \underline{\textbf{do}}\ \mathbf{c}\ \text{or}\ \underline{\textbf{while}}\ N[\mathbf{Y}]\ \underline{\textbf{do}}\ \mathfrak{d}\ \text{is terminating}}{\{\downarrow^*_{\mathsf{true},\mathsf{true}}(\mathsf{A}) + \downarrow^*_{\mathsf{true},\mathsf{false}}(\mathsf{B})\}\ \underline{\textbf{while}}\ M[\mathbf{X}]\ \underline{\textbf{do}}\ \mathbf{c} \sim \underline{\textbf{while}}\ N[\mathbf{Y}]\ \underline{\textbf{do}}\ \mathfrak{d}\ \{\mathsf{B}\}}$$

应用实例

芝诺效应：超人"永远"追不上乌龟！



量子芝诺效应：量子空间中观察者可以"定住"超人！(飞矢不动)

通过EQRHL验证量子芝诺效应：

$$\left\{\left(\cos\frac{\pi}{2n}\right)^{2n} I\right\}\ Q_1 \sim Q_2\ \{=_y\}$$

其中：$Q_1 \stackrel{\text{def}}{=} y \leftarrow |0\rangle$; **apply** R^n **to** y

$Q_2 \stackrel{\text{def}}{=} x \leftarrow 0; y \leftarrow |0\rangle$; **while** $(x < n)$ **do** $\{INC(x);$ **if** $P_{\phi_x}[y]\}$

$$R = \begin{pmatrix} \cos\frac{\pi}{2n} & -\sin\frac{\pi}{2n} \\ \sin\frac{\pi}{2n} & \cos\frac{\pi}{2n} \end{pmatrix}.$$

关键：量子操作R的作用可以通过量子测量P_{ϕ_x}来实现。

意义：对量子芝诺效应的第一个形式化证明！