ISCAS 中国科学院软件研究所学术年会暨重点实验室科技活动周 2025 第十届

学术论文

Complete Quantum Relational Hoare Logics from Optimal Transport Duality
基于最优传输对偶性的完备量子关系Hoare逻辑

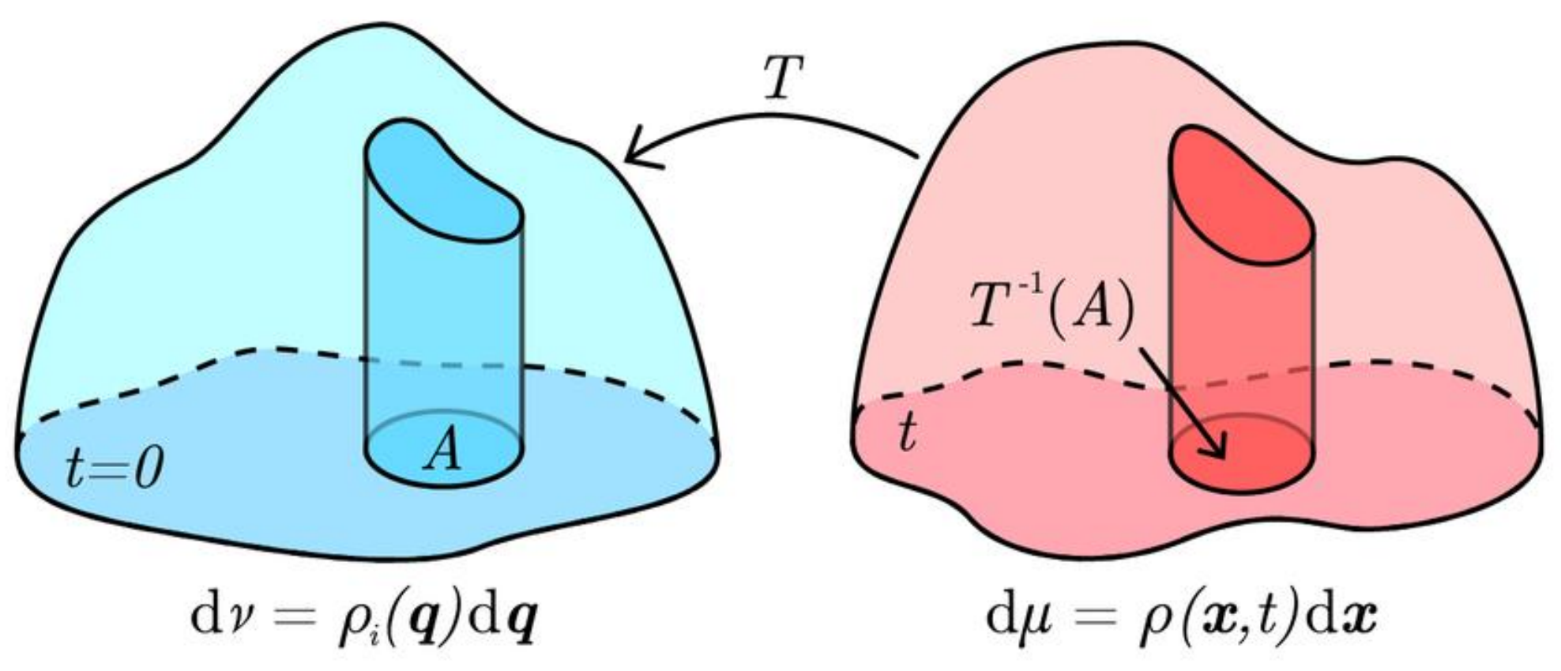
Gilles Barthe（MPI），高敏博（中科院软件所），
Theo Wang（剑桥大学），周立（中科院软件所）

Fortieth Annual ACM/IEEE Symposium on
Logic in Computer Science (LICS), 2025

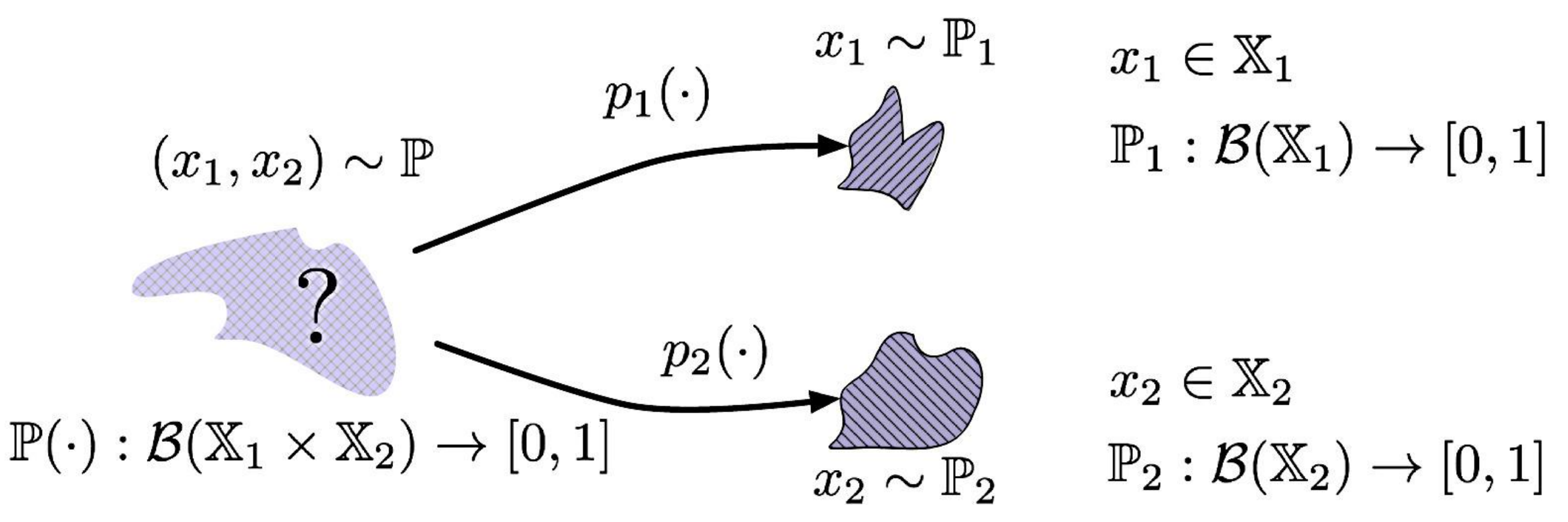
联系方式：高敏博 gaomb@ios.ac.cn
周立 zhouli@ios.ac.cn

研究背景与动机

- 关系Hoare逻辑是分析两个程序之间关系的重要工具，一般形式为：$\vdash \{P\}\ S_1 \sim S_2\ \{Q\}$。
- 在量子计算中，有效性（validity）基于“量子耦合”定义。
- 现有系统虽能推理，但缺乏完备性（completeness）保证。
- 最优输运的耦合和对偶理论为程序逻辑提供了有力工具。



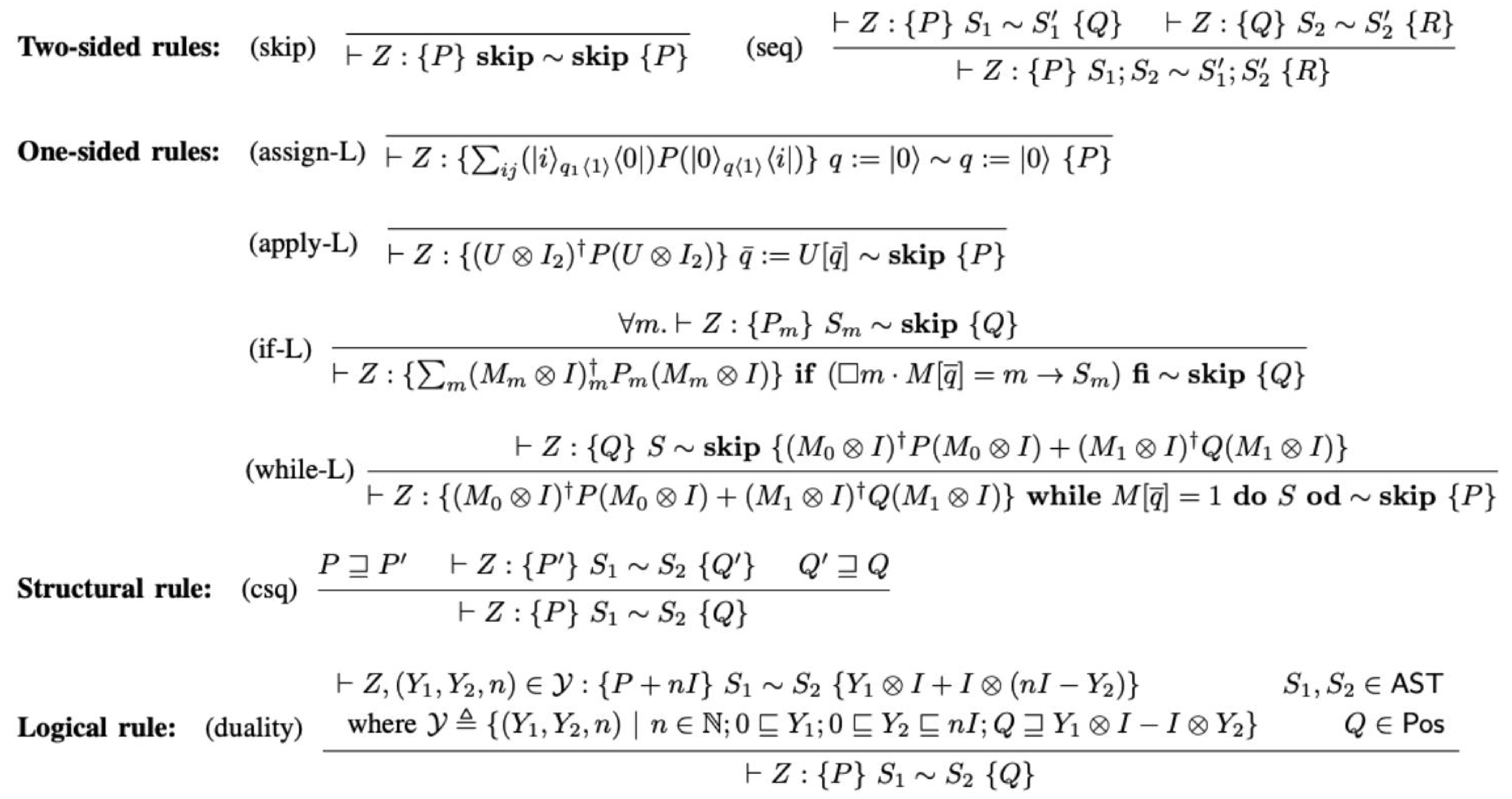
最优输运示意图



概率耦合示意图

主要贡献

- 一个完备的量子关系Hoare逻辑系统（qOTL）
  - 三个组成部分：
    - 标准结构规则（例如对每个构造的单边规则）；
    - 对偶规则：基于量子最优传输的对偶性；
    - 双边规则（非完备性所必需，但增强可用性）。
- 引入无限值断言
  - 正半定算符的拓展，引入可含正无穷的本征值；
  - 可统一处理量子逻辑中的“投影断言”和“数量断言”。
- 应用示例与性质刻画
  - 量子程序等价判定；
  - 描述量子距离度量（迹距离、钻石距离、Wasserstein 距离）；
  - 非干扰与差分隐私的量子版本刻画；
  - 完备性对概率程序的 eRHL 系统也有启发。



Two-sided rules: (skip)
$$\frac{}{\vdash Z : \{P\}\ \mathbf{skip} \sim \mathbf{skip}\ \{P\}}$$

(seq)
$$\frac{\vdash Z : \{P\}\ S_1 \sim S_1'\ \{Q\} \qquad \vdash Z : \{Q\}\ S_2 \sim S_2'\ \{R\}}{\vdash Z : \{P\}\ S_1; S_2 \sim S_1'; S_2'\ \{R\}}$$

One-sided rules: (assign-L)
$$\frac{}{\vdash Z : \{\sum_{ij} (|i\rangle_{q_1\langle 1\rangle}\langle 0|) P (|0\rangle_{q\langle 1\rangle}\langle i|)\}\ q := |0\rangle \sim q := |0\rangle\ \{P\}}$$

(apply-L)
$$\frac{}{\vdash Z : \{(U \otimes I_2)^\dagger P (U \otimes I_2)\}\ \bar{q} := U[\bar{q}] \sim \mathbf{skip}\ \{P\}}$$

(if-L)
$$\frac{\forall m. \vdash Z : \{P_m\}\ S_m \sim \mathbf{skip}\ \{Q\}}{\vdash Z : \{\sum_m (M_m \otimes I)^\dagger_m P_m (M_m \otimes I)\}\ \mathbf{if}\ (\square m \cdot M[\overline{q}] = m \to S_m)\ \mathbf{fi} \sim \mathbf{skip}\ \{Q\}}$$

(while-L)
$$\frac{\vdash Z : \{Q\}\ S \sim \mathbf{skip}\ \{(M_0 \otimes I)^\dagger P (M_0 \otimes I) + (M_1 \otimes I)^\dagger Q (M_1 \otimes I)\}}{\vdash Z : \{(M_0 \otimes I)^\dagger P (M_0 \otimes I) + (M_1 \otimes I)^\dagger Q (M_1 \otimes I)\}\ \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od} \sim \mathbf{skip}\ \{P\}}$$

Structural rule: (csq)
$$\frac{P \sqsupseteq P' \qquad \vdash Z : \{P'\}\ S_1 \sim S_2\ \{Q'\} \qquad Q' \sqsupseteq Q}{\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}}$$

Logical rule: (duality)
$$\frac{\begin{array}{ll} \vdash Z, (Y_1, Y_2, n) \in \mathcal{Y} : \{P + nI\}\ S_1 \sim S_2\ \{Y_1 \otimes I + I \otimes (nI - Y_2)\} & S_1, S_2 \in \mathsf{AST} \\ \text{where } \mathcal{Y} \triangleq \{(Y_1, Y_2, n) \mid n \in \mathbb{N}; 0 \sqsubseteq Y_1; 0 \sqsubseteq Y_2 \sqsubseteq nI; Q \sqsupseteq Y_1 \otimes I - I \otimes Y_2\} & Q \in \mathsf{Pos} \end{array}}{\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}}$$

Fig. 1. Rules for qOTL

qOTL逻辑规则