Complete Quantum Relational Hoare Logics from Optimal Transport Duality

Gilles Barthe*†, Minbo Gao‡, Theo Wang§, Li Zhou*¶
†MPI for Security and Privacy, Germany and IMDEA Software Institute, Spain, gilles.barthe@mpi-sp.org
‡ Institute of Software, CAS, China[1] and University of Chinese Academy of Sciences, China, gaomb@ios.ac.cn
§University of Cambridge, United Kingdom, tcw57@cam.ac.uk
¶ Institute of Software, CAS, China[1], zhouli@ios.ac.cn

***Abstract*—We introduce a quantitative relational Hoare logic for quantum programs. Assertions of the logic range over a new infinitary extension of positive semidefinite operators. We prove that our logic is sound, and complete for bounded postconditions and almost surely terminating programs. Our completeness result is based on a quantum version of the duality theorem from optimal transport. We also define a complete embedding into our logic of a relational Hoare logic with projective assertions.**

I. Introduction

Relational Hoare logics are program logics used to reason about relationships between programs. Typically, their judgments are of the form $\{P\}\ S_1 \sim S_2\ \{Q\}$, where S_1 and S_2 are programs, and P and Q are relational assertions, traditionally known as pre- and postcondition. In this paper, we consider the setting where S_1 and S_2 are quantum programs in the pure qWhile language. In this setting, it is natural to define validity based on quantum couplings. Indeed, there exist several proof systems that support a rich set of proof rules and are sound w.r.t. coupling-based notions of validity [1]–[3]. These proof systems have been used to reason about quantum processes and quantum security. However, the proof-theoretic foundations of these proof systems remain unexplored. In particular, there is no prior account of the completeness of these systems. The challenge with completeness arises from the existential nature of coupling-based reasoning: validity of a Hoare judgment $\{P\}\ S_1 \sim S_2\ \{Q\}$ asserts the existence of a suitable coupling, called witness coupling, between (output states of) S_1 and S_2. Therefore, the completeness of the proof system is intuitively equivalent to proving that the rules of the proof system suffice to build all valid couplings between two programs. Unfortunately, it seems difficult to establish a direct argument of this kind. One reason is that proof rules are compositional and allow to build couplings that respect the structure of programs, so it seems plausible that the proof rules are incomplete. In this paper, we do not attempt a direct proof of completeness. Rather, we observe that one can achieve completeness by leveraging a duality theorem for quantum couplings. Our approach follows and generalises the work of Avanzini et al. [4] on completeness for probabilistic relational Hoare logics.

Contributions: The main contribution of this paper is a complete proof system for almost surely terminating programs and positive semi-definite (PSD) assertions. The proof system contains three parts. The first part is a minimalistic, standard, set of rules—concretely, one left and right rule for each construct, two-sided rules for skip and sequential composition, and a rule of consequence w.r.t. the usual Löwner order $\sqsubseteq$ on assertions. We prove that this set of rules is complete for split postconditions, i.e. postconditions of the form $Q_1 \otimes I + I \otimes Q_2$, where Q_1 and Q_2 are unary assertions. The proof follows by classic structural induction on programs—for technical considerations that will be explained later, the proof also requires that validity be defined using a new variant of quantum coupling, called partial coupling, of independent interest. The second part is a new structural rule, called the duality rule. The validity of the (duality) rule is based on a quantum duality theorem, akin to the celebrated Kantorovich-Rubinstein duality theorem for the probabilistic setting. The main benefit of the rule is that it allows to reduce a judgment of the form

$$\{P\}\ S_1 \sim S_2\ \{Q\}$$

to a judgment of the form

$$\{P\}\ S_1 \sim S_2\ \{Q_1 \otimes I - I \otimes Q_2\}$$

where informally Q_1 and Q_2 are quantified universally over all unary assertions such that $Q_1 \otimes I - I \otimes Q_2 \sqsubseteq Q$. Therefore, the duality rules allow us to reduce the proof of a judgment with an arbitrary postcondition to the validity of a judgment with a split postcondition, for which the standard rules suffice. The third part of the logic are two-sided proof rules. These proof rules are important for the usability of the logic and are present in prior works, but are not needed for completeness, and will only be discussed briefly in the paper.

The second contribution of the paper is an alternative interpretation of our proof system where assertions are drawn from an infinite-valued generalization of PSD operators. The logic remains sound for all postconditions and complete for all bounded postconditions—provided one restricts the (dual) rule to bounded postconditions. However, the main benefit of this generalization is that it provides a means to unify

*Corresponding authors: Gilles Barthe, Li Zhou
[1]Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China

projective assertions, used e.g. in [1], and positive semi-definite operators. As an application, we provide a complete embedding into our logic of a relational Hoare logic with projective predicates.

Finally, we leverage our completeness theorems to characterize some properties of interest. We give two characterizations of program equivalence. The first characterization is based on (finite-valued) positive semi-definite assertions and uses tools from stable quantum optimal transport. The second characterization is based on projective assertions (and infinite-valued predicates). We also present characterizations of quantum distance measures (trace distance and Wasserstein semi-distance), diamond norm for programs, non-interference and quantum differential privacy. Finally, as a contribution of independent interest, we prove that the recently proposed relational Hoare logic eRHL for probabilistic programs [4] is complete for all bounded postconditions and AST programs.

Summary of contributions

In summary, the main contributions of the paper are:

- a sound and complete relational program logic for quantum programs (Theorem VI.3, Theorem VI.7);
- a complete semantic embedding of quantum relational Hoare logics using projective predicates using infinite-valued predicates (Proposition VII.2);
- characterizations of observational equivalence (Theorem VIII.1), trace distance and diamond norm (Proposition VIII.3 and Theorem VIII.6), Wasserstein distance (Theorem VIII.8), non-interference (Theorem VIII.13), and quantum differential privacy (Theorem VIII.16);
- a proof of completeness for the eRHL relational program logic for probabilistic programs (Proposition IX.2).

II. Notation and Preliminaries

We assume basic familiarity to quantum computing (see standard textbook [5]) and set the scene with some notations.

a) Quantum states and maps: Let $\mathcal{H}$ be a Hilbert space. We define $\mathcal{D}(\mathcal{H})$ and $\mathcal{D}^1(\mathcal{H})$ to be the set of partial density operators (i.e. positive semi-definite (PSD) operators with trace ≤ 1) and density operators (i.e. partial density operators with trace 1) over $\mathcal{H}$, respectively. Intuitively, $\mathcal{D}(\mathcal{H})$ represents the subdistributions over pure states in $\mathcal{H}$ and $\mathcal{D}^1(\mathcal{H})$ contains only the full distributions. Furthermore, we write $\mathcal{QC}(\mathcal{H})$ and $\mathcal{QO}(\mathcal{H})$ for the set of quantum channels (CPTP maps) and quantum operations (trace-nonincreasing CP maps) over $\mathcal{H}$. We use the former to interpret all almost surely terminating quantum programs and the latter to represent general quantum programs. Obviously, $\mathcal{QC}(\mathcal{H}) \subsetneq \mathcal{QO}(\mathcal{H})$.

b) Quantum predicates: We define $\mathcal{S}(\mathcal{H})$ and $\mathsf{Pos}(\mathcal{H})$ to be respectively the closed subspaces (equivalently the orthogonal projectors) and the PSD operators on $\mathcal{H}$. Subspaces can be used as a 'discrete' predicate: a state $\rho \in \mathcal{D}(\mathcal{H})$ satisfies $X \in \mathcal{S}(\mathcal{H})$ if $\mathrm{supp}(\rho) \subseteq X$. General PSD operators are used as bounded quantitative predicates: the 'extent' to which ρ satisfies $P \in \mathsf{Pos}(\mathcal{H})$ is defined to be $\mathrm{tr}(P\rho)$. Commonly used predicates in the work include: the 'symmetric' predicate $P_{sym}[\mathcal{H}] = \frac{1}{2}(I + \mathsf{SWAP}[\mathcal{H}])$ (we sometimes denote it as $=_{\mathrm{sym}}$) where $\mathsf{SWAP}[\mathcal{H}] = \sum_{ij} |ij\rangle\langle ji|$, and parameter $\mathcal{H}$ is omitted if it is clear from the context; and the 'anti-symmetric' predicate $P^{\perp}_{sym}$, i.e., the complement of the projector P_{sym}, $P^{\perp}_{sym}[\mathcal{H}] = \frac{1}{2}(I - \mathsf{SWAP}[\mathcal{H}])$. Note that both $P_{sym}[\mathcal{H}]$ and $P^{\perp}_{sym}[\mathcal{H}]$ are in $\mathcal{S}(\mathcal{H} \otimes \mathcal{H})$.

c) Infinite-valued predicates: In this work, we introduce a novel notion of possibly infinite-valued quantitative predicates, denoted $\mathsf{Pos}^{\infty}(\mathcal{H})$, by allowing positive operators to have an eigenspace corresponding to eigenvalue $+\infty$. In other words, any $A \in \mathsf{Pos}^{\infty}(\mathcal{H})$ has an eigenvalue decomposition $\{(\lambda_i, X_i)\}_i$ where $\lambda_i \in \mathbb{R}^{+\infty} \triangleq [0, +\infty]$, the non-zero eigenspaces X_i are pairwise orthogonal, and $\sum_i X_i = I$. As a convention, we define $(+\infty)\cdot 0 = 0 \cdot (+\infty) = 0$, $(+\infty) + a = a + (+\infty) = +\infty$ for $a \in \mathbb{R}^{+\infty}$, and $+\infty \leq +\infty$. We now extend the definitions of various operations on PSD operators to $\mathsf{Pos}^{\infty}(\mathcal{H})$. Firstly, for any $|\psi\rangle$, the inner product $\langle\psi|A|\psi\rangle$ is defined as $\langle\psi|A|\psi\rangle \triangleq \sum_i \lambda_i \langle\psi|X_i|\psi\rangle$. This definition allows us to extend all the operations and constructions on PSD operators that this work relies on to the infinite-valued case. For example, the extended Löwner order is defined by $A_1 \sqsubseteq A_2$ if for all $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle \leq \langle\psi|A_2|\psi\rangle$. We refer the reader to the appendix for more details on the supported operations (see Definition A.6). Finally, for $X \in \mathcal{S}(\mathcal{H})$ and $A \in \mathsf{Pos}^{\infty}(\mathcal{H})$, we define $X \mid A \triangleq A + (+\infty \cdot X^{\perp}) \in \mathsf{Pos}^{\infty}(\mathcal{H})$. This will be useful for enforcing assertion-based, projective preconditions in the quantitative setting.

For compactness reasons, in this paper, we present the technical development of our results in terms of the more general infinite-valued predicates. The proofs of all theorems and propositions are provided in the appendix of the full version [6].

III. Quantum Couplings

We review basic definitions and theorems of quantum couplings and quantum optimal transport.

A. Basic Definitions and Duality Theorems

In probability theory, probabilistic couplings are a powerful tool for reasoning about different ways of correlating two distributions. A coupling of two distributions d_1, d_2 is a joint distribution with d_1, d_2 as its respective marginals. Quantum couplings are the quantum analogue of probabilistic couplings; instead of (sub)distributions, they relate (partial) density operators.

Definition III.1 (Quantum Coupling)**.** *Let $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ be two partial density operators. A coupling between ρ_1 and ρ_2 is a partial density operator $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that $\mathrm{tr}_2(\rho) = \rho_1$ and $\mathrm{tr}_1(\rho) = \rho_2$. We write $\rho : \langle\rho_1, \rho_2\rangle$.*

Strassen's theorem [7] provides a necessary and sufficient condition for the existence of a coupling with respect to a given relation. Zhou *et al.* [8] lift Strassen's theorem to the quantum setting. Their theorem relates a quantum lifting (where for any subspace X, a lifting $\rho_1 X^{\#} \rho_2$ is witnessed by couplings of

the form $\rho : \langle \rho_1, \rho_2 \rangle$ such that $\mathrm{supp}(\rho) \subseteq X$) to a universally quantified property that reasons about ρ_1 and ρ_2 separately. Their proof is based on semi-definite programming (SDP), a common technique in quantum computing and information theory. It turns out that the same technique can be generalized to accommodate for a more general, 'quantitative' version of liftings, as stated below.

Definition III.2 (Quantum Lifting with Defects)**.** *Let $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$, and $\epsilon \in \mathbb{R}^{+\infty}$ be a defect. Let $X \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Then $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is called a witness of the lifting $\rho_1 X^{\#}_{\epsilon} \rho_2$, iff $\rho : \langle \rho_1, \rho_2 \rangle$ and $\mathrm{tr}(X\rho) \leq \epsilon$.*

Note that for any subspace X, $\rho_1 X^{\#} \rho_2$ iff $\rho_1 (X^{\perp})^{\#}_0 \rho_2$.

Theorem III.3 (Quantum Strassen's Theorem with Defects)**.** *For any $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ with $\mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$, for any defect $\epsilon \in \mathbb{R}^{+\infty}$ and for any $X \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, the following are equivalent:*

1) *$\rho_1 X^{\#}_{\epsilon} \rho_2$;*
2) *For any $Y_1 \in \mathsf{Pos}(\mathcal{H}_1)$ and $Y_2 \in \mathsf{Pos}(\mathcal{H}_2)$ such that $X \sqsupseteq Y_1 \otimes I_2 - I_1 \otimes Y_2$, $\mathrm{tr}(Y_1\rho_1) \leq \mathrm{tr}(Y_2\rho_2) + \epsilon$.*

The setting of the primal and dual problems in the proof is essentially the same as in [8], [9].

B. Partial Couplings

The following fact is a basic consequence of the definition of quantum couplings.

Lemma III.4 (Trace Equivalence)**.** *Let $\rho : \langle \rho_1, \rho_2 \rangle$. Then, $\mathrm{tr}(\rho) = \mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$.*

It follows that partial density operators can be coupled only if they have the same trace. This basic fact is a limiting factor for coupling-based relational Hoare logics. In particular, it limits our ability to reason about pairs of non-trace-preserving quantum operations (e.g. quantum programs with while loops). To address this limitation, we draw ideas from [4] ($\star$-couplings) and [3] (quantum $\perp$-memories) and introduce the concept of partial couplings (see Proposition B.3 for precise relationship between $\star$-couplings and partial couplings).

Definition III.5 (Partial Coupling)**.** *For $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$, we say $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is a partial coupling of ρ_1 and ρ_2, written $\rho : \langle \rho_1, \rho_2 \rangle_p$, if:*

$$\mathrm{tr}_2(\rho) \sqsubseteq \rho_1, \quad \mathrm{tr}_1(\rho) \sqsubseteq \rho_2, \quad \mathrm{tr}(\rho_1) + \mathrm{tr}(\rho_2) \leq 1 + \mathrm{tr}(\rho).$$

The first two inequalities say that the coupling ρ is partial: it represents a correlation between parts of the marginal state ρ_1, ρ_2, and leaves another part of the states uncorrelated. The last inequality is a requirement on the uncorrelated parts of the marginal states. It can be decomposed into two inequalities:

$$\mathrm{tr}(\rho_1 - \mathrm{tr}_2(\rho)) \leq 1 - \mathrm{tr}(\rho_2), \quad \mathrm{tr}(\rho_2 - \mathrm{tr}_1(\rho)) \leq 1 - \mathrm{tr}(\rho_1).$$

Explained using programming language terms, the first inequality says that the probability of the uncorrelated part of the first system, $\mathrm{tr}(\rho_1 - \mathrm{tr}_2(\rho))$, should not exceed the probability of non-termination in the second system, $1 - \mathrm{tr}(\rho_2)$. The meaning of the second inequality can be obtained by symmetry.

Obviously, any coupling is a partial coupling, i.e., $\rho : \langle \rho_1, \rho_2 \rangle$ implies $\rho : \langle \rho_1, \rho_2 \rangle_p$. In the case where ρ_1, ρ_2 are density operators, any partial coupling is also a coupling, i.e., $\rho : \langle \rho_1, \rho_2 \rangle_p$ implies $\rho : \langle \rho_1, \rho_2 \rangle$ if $\mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2) = 1$. Partial coupling is preserved under (sub-)convex combination and scalar multiplication (see Proposition B.4). A variant of duality theorem for partial coupling is established via SDP (see Theorem B.5).

IV. Quantum Optimal Transport

One of the applications of quantum coupling is to reason about relational properties of quantum states and thus quantum channels and operations. We first review the basic concept of quantum optimal transport and then show how it can be used to characterize the equivalence of quantum channels.

A. Basic Definitions

The optimal transport problem [10] is a classical optimization problem. Its goal is to minimize the transportation cost of goods from sources to sinks. The optimal transport problem has a natural formulation based on probabilistic couplings. In this section, we review a quantum version of optimal transport. We mainly follow [9].

Definition IV.1 (Partial Quantum Optimal Transport (c.f. [9]))**.** *For a given cost function $C \in \mathsf{Pos}^{\infty}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ and two states $\rho_1 \in \mathcal{D}(\mathcal{H}_1), \rho_2 \in \mathcal{D}(\mathcal{H}_2)$, the quantum optimal transport*

$$T_C(\rho_1, \rho_2) \triangleq \min_{\rho : \langle \rho_1, \rho_2 \rangle_p} \mathrm{tr}(C\rho),$$

where ρ is ranging over all partial couplings of ρ_1 and ρ_2.

The minimum can be attained because the set of partial couplings is an non-empty, closed and convex set (see Proposition C.1). Whenever ρ_1 and ρ_2 are (total) density operators, every partial coupling is a coupling, and therefore, $T_C(\rho_1, \rho_2) = \min_{\rho : \langle \rho_1, \rho_2 \rangle} \mathrm{tr}(C\rho)$.

The basic properties of QOT have been systematically studied, see [9] for a comprehensive review. For example, QOT is jointly convex on its input (see Proposition C.2).

B. QOT under Data Processing

The original definition of QOT studies the relationship between quantum *states*. In this work, we go one step further and ask: can QOT be used to represent and evaluate the relationship between quantum *state transformers* (i.e. quantum channels or operations)? To answer this question, we study how QOT evolves 'under data processing'.

Definition IV.2. *Let $C_i, C_o \in \mathsf{Pos}^{\infty}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ be input and output cost functions respectively. We say that a pair of quantum operations $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o iff $T_{C_o}(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq T_{C_i}(\rho_1, \rho_2)$ hold for all possible inputs $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$.*

The following lemma shows that it is sufficient to check contractivity on inputs $\rho_1 \in \mathcal{D}^1(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_2)$.

Lemma IV.3 (Alternative Characterization)**.** *Given two quantum operations $\mathcal{E}_1 \in \mathcal{QO}(\mathcal{H}_1), \mathcal{E}_2 \in \mathcal{QO}(\mathcal{H}_2)$, input and output costs C_i and C_o, the following statement are equivalent:*

1) *$(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o;*
2) *For all $\rho_1 \in \mathcal{D}^1(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_2)$,*

$$T_{C_o}(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq T_{C_i}(\rho_1, \rho_2).$$

Whenever reasoning about two quantum channels, the condition can be simplified as follows:

Lemma IV.4 (Contractivity for Quantum Channels)**.** *Suppose $\mathcal{E}_1 \in \mathcal{QC}(\mathcal{H}_1), \mathcal{E}_2 \in \mathcal{QC}(\mathcal{H}_2)$ are two quantum channels. Then $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o if and only if for every $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, there exists a coupling $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1(\rho)) \rangle$ such that $\mathrm{tr}(C_i \rho) \geq \mathrm{tr}(C_o \sigma)$.*

The next proposition establishes key properties of contractivity.

Proposition IV.5. *Contractivity satisfies several desired properties for data processing:*

1) *Backward. $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. $(\mathcal{E}_1^\dagger \otimes \mathcal{E}_2^\dagger)(C)$ and C. Here, $\mathcal{E}^\dagger$ is the dual of $\mathcal{E}$, which satisfies $\mathrm{tr}(A\mathcal{E}(B)) = \mathrm{tr}(\mathcal{E}^\dagger(A)B)$ for all linear operator A, B[1].*
2) *Consequence. Suppose $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i' and C_o', and $C_i' \sqsubseteq C_i$, $C_o \sqsubseteq C_o'$, then $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o.*
3) *Sequential composition. Suppose $(\mathcal{E}_1, \mathcal{E}_1')$ is contractive w.r.t. C_i and C_m, and $(\mathcal{E}_2, \mathcal{E}_2')$ is contractive w.r.t. C_m and C_o, then $(\mathcal{E}_2 \circ \mathcal{E}_1, \mathcal{E}_2' \circ \mathcal{E}_1')$ is contractive w.r.t. C_i and C_o.*

Here, $\circ$ is the composition of two quantum operations, i.e., for all ρ, $(\mathcal{E}_1 \circ \mathcal{E}_2)(\rho) \triangleq \mathcal{E}_1(\mathcal{E}_2(\rho))$.

The (Backward) property asserts that every pair of quantum channels is contractive w.r.t. an output cost and its pre-image under some form of relational pre-image. The (Consequence) property states that one can strengthen the input cost or weaken the output cost in the style of the rule of consequence. The (Sequential composition) property states that contractivity is compositional.

Additionally, our formulation of QOT under data processing allows us to translate the previous duality result about quantum states (Theorem III.3) to the following duality theorem about quantum operations. Specifically, we show that contractivity w.r.t. C_i and C_o is equivalent to contractivity w.r.t. a split output cost function. The duality theorem is carefully stated to match our assumptions, in particular that C_o is positive. It is also restricted to the case that C_o is finite.

Theorem IV.6 (Duality under Data Processing)**.** *Suppose $\mathcal{E}_1$ and $\mathcal{E}_2$ are quantum channels and costs $C_i \in \mathsf{Pos}^\infty$ and $C_o \in \mathsf{Pos}$ (i.e., C_o is finite). Then the following statements are equivalent:*

1) *$(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o;*
2) *for all $(Y_1, Y_2, n) \in \mathcal{Y}$, $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. $C_i + nI$ and $Y_1 \otimes I + I \otimes (nI - Y_2)$, where $\mathcal{Y} \triangleq \{(Y_1, Y_2, n) \mid n \in \mathbb{N}; 0 \sqsubseteq Y_1; 0 \sqsubseteq Y_2 \sqsubseteq nI; C_o \sqsupseteq Y_1 \otimes I - I \otimes Y_2\}$.*

This formalization will be instrumental in reducing arbitrary judgments to judgments with split postconditions.

C. Characterizing Equivalence

The symmetric and anti-symmetric predicates are standard tools used to characterize equivalence of quantum *states* [1], [2]: indeed, two states ρ_1, ρ_2 are equal iff there a (non-quantitative) lifting of the form $\rho_1 (=_{\mathrm{sym}})^\# \rho_2$. In this section, by lifting this tool to the setting of QOT under data processing, we give a complete characterization of equivalence between quantum *channels*. This is a significant result: as we shall see in Theorem VIII.1, it directly leads to the first complete characterization of program equivalence in quantum relational Hoare logics only using finite-valued PSD predicates.

Our starting point is the instantiation of QOT under data processing with $C_o = C_i = P^\perp_{sym}$, studied in [9], [11]–[13]. For simplicity, we write T instead of $T_{P^\perp_{sym}}$. It is clear that T encapsulates some notion of equivalence: $T(\rho, \sigma) = 0$ if and only if $\rho = \sigma$, given ρ, σ density operators. However, T cannot fully capture equivalence under data processing, because it is not contractive under general quantum channels [12], i.e. $T(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq T(\rho, \sigma)$ does not always hold for every $\mathcal{E}$. Indeed, it does hold for tensoring with an arbitrary quantum state [9], i.e., $\mathcal{E} : \rho \mapsto \rho \otimes \gamma$, but not for the partial trace. This makes it difficult to completely reason about the equivalence of data processing operations using the current definition of T.

Fortunately, [12] proposed a stabilized version of T, defined by $T_s \triangleq \inf_\gamma T(\rho \otimes \gamma, \sigma \otimes \gamma)$ by extending (tensoring) with an arbitrary auxiliary state γ, which satisfies several desired properties such as joint convexity, and

- (Invariance under tensor product)

$$T_s(\rho \otimes \gamma, \sigma \otimes \gamma) = T_s(\rho, \sigma).$$

- (Contractivity under data processing) For $\mathcal{E} \in \mathcal{QC}$,

$$T_s(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq T_s(\rho, \sigma).$$

Surprisingly, it turns out that $T_s(\rho, \sigma) = T\big(\rho \otimes \frac{I}{2}, \sigma \otimes \frac{I}{2}\big)$. The proof is technical and employs techniques like the Haar measure; we leave the details to Appendix H, and provide some intuition. Intuitively, this fact can be understood from two perspectives: 1) the quantum marginal problem, such as the monogamy of entanglement [14], implies that extending the state can yield more couplings and therefore $T_s(\rho, \sigma) \leq T(\rho, \sigma)$ and 2) extending it by a maximally mixed qubit is sufficient to produce all couplings that minimize optimal transport on the cost function $P^\perp_{sym}$, instead of ranging over all γ. These properties give a complete criterion for checking the equivalence of two quantum channels:

[1]For any super-operator $\mathcal{E}$, its dual $\mathcal{E}^\dagger$ is another super-operator. Whenever $\mathcal{E}$ is a quantum operation with Kraus operator $\{E_i\}$, then $\mathcal{E}^\dagger$ has Kraus representation $\{E_i^\dagger\}$.

Proposition IV.7. *Two quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ are equivalent if and only if for all density operators ρ_1, ρ_2, $T_s(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq T_s(\rho_1, \rho_2)$.*

While [12] already gives a precise characterization of T_s in terms of QOT, as a semi-definite program, we rephrase it as the following duality theorem:

Proposition IV.8 (Duality for Stabilized QOT)**.** *Given $\rho_1, \rho_2 \in \mathcal{D}^1(\mathcal{H})$ and $\epsilon \in \mathbb{R}^+$, the following are equivalent:*

1) *$T_s(\rho_1, \rho_2) \leq \epsilon$;*
2) *For all $Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2)$ such that $P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)$, it holds that:*

$$\mathrm{tr}(\mathrm{tr}_2(Y_1)\rho_1) \leq \mathrm{tr}(\mathrm{tr}_2(Y_2))\rho_2) + \epsilon.$$

This property is crucial for establishing a judgment characterizing program equivalence (see Theorem VIII.1), as T_s itself cannot be directly encoded within our program logic. It additionally allows us to use a split postcondition and thus make the judgment completely derivable (Theorem VI.6) without first applying the duality rule.

V. Quantum Programs

We now present the syntax and semantics of the quantum programs considered in this paper.

A. Syntax

We choose to use the quantum **while**-language defined in [15], [16]. We assume a finite set **qVar** of quantum variables and use $q, q_0, q_1, q_2, \ldots$ to denote them. The finite-dimensional state Hilbert space of a quantum variable q is denoted $\mathcal{H}_q$.

A quantum register is a finite sequence of distinct quantum variables. The state space of a quantum register $\overline{q} = q_0 \ldots q_n$ is then the tensor product $\mathcal{H}_{\overline{q}} = \bigotimes_{i=0}^{n} \mathcal{H}_{q_i}$.

Definition V.1 (Syntax [15])**.** *The set **qProgs** of quantum **while**-programs is defined by the following syntax:*

$$S ::= \mathbf{skip} \mid S_1; S_2 \mid q := |0\rangle \mid \overline{q} := U[\overline{q}] \quad (1)$$
$$\mid \mathbf{if}\ (\square m \cdot M[\overline{q}] = m \to S_m)\ \mathbf{fi} \quad (2)$$
$$\mid \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od} \quad (3)$$

The constructs **skip** and sequential composition $S_1; S_2$ are similar to their counterparts in the classical or probabilistic **while**-programs. The initialization $q := |0\rangle$ sets the quantum register q to the basis state $|0\rangle$. The statement $\overline{q} := U[\overline{q}]$ means that unitary transformation U is performed on the quantum register $\overline{q}$. The construct in (2) is a quantum generalization of classical case statement. In the execution, measurement $M = \{M_m\}$ is performed on $\overline{q}$, and then a subprogram S_m will be selected according to the outcome of the measurement. The statement in (3) is a quantum generalization of **while**-loop, where the measurement M has only two possible outcomes: if the outcome is 0, the program terminates, and if the outcome 1 occurs, the program executes the loop body S and then continues the loop.

B. Semantics

For each quantum program S, we write $var(S) \subseteq V$ for the set of all variables $q \in$ **qVar** appearing in S. The Hilbert space of program S is the tensor product $\mathcal{H}_S = \bigotimes_{q \in var(S)} \mathcal{H}_q$.

We interpret each program S denotationally as a complete positive trace non-increasing map $[\![S]\!] \in \mathcal{QO}(\mathcal{H}_S)$ as follows:

Definition V.2 (Denotational Semantics [15])**.** *For any input state $\rho \in \mathcal{H}_S$, we have:*

1) $[\![\mathbf{skip}]\!](\rho) = \rho$;
2) $[\![q := |0\rangle]\!](\rho) = \sum_n |0\rangle_q\langle n|\rho|n\rangle_q\langle 0|$;
3) $[\![\overline{q} := U[\overline{q}]]\!](\rho) = U_{\overline{q}}\rho U^{\dagger}_{\overline{q}}$;
4) $[\![S_1; S_2]\!](\rho) = [\![S_2]\!]([\![S_1]\!](\rho))$;
5) $[\![\mathbf{if}(\square m \cdot M[\overline{q}] = m \to S_m)\mathbf{fi}]\!](\rho)$ $= \sum_m [\![S_m]\!](M_m \rho M_m^{\dagger})$;
6) *for loop* $\mathbf{while}[M, S] \equiv \mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ S\ \mathbf{od}$*:*

$$[\![\mathbf{while}[M, S]]\!](\rho) = \bigsqcup_{k=0}^{\infty} [\![\mathbf{while}^{(k)}[M, S]]\!](\rho),$$

where $\mathbf{while}^{(k)}[M, S]$ is the k-fold iteration of the loop **while***:*

$$\begin{cases} \mathbf{while}^{(0)}[M, S] \equiv \textbf{\textit{abort}}, \\ \mathbf{while}^{(k+1)}[M, S] \\ \equiv \mathbf{if}\ M[\overline{q}] = \ 0 \to \mathbf{skip} \\ \quad \square \qquad\quad 1 \to S; \mathbf{while}^{(k)}[M, S]\ \mathbf{fi} \end{cases}$$

*for $k \geq 0$, $\bigsqcup$ stands for the least upper bound in the CPO of partial density operators with the Löwner order $\sqsubseteq$ (see [16], Lemma 3.3.2), and **abort** is a program that never terminates so that $[\![\textbf{\textit{abort}}]\!](\rho) = \mathbf{0}$ for all ρ.*

In the special case where $[\![S]\!] \in \mathcal{QC}(\mathcal{H}_S)$, we say that S is almost-surely terminating (AST), or simply write $S \in \mathsf{AST}$.

VI. A Quantum Relational Hoare Logic

We now present qOTL, a quantum relational Hoare logic similar to [2] extended with logical variables, and prove its soundness. As we shall see in Section VI-B, this extension is crucial to enabling our completeness results.

A. Definition

In qOTL, judgments are of the form

$$\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$$

where predicates $P, Q \in \mathsf{Pos}^{\infty}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, i.e., are infinite-valued positive semi-definite operators over $\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2}$, parameterized over Z, and S_1, S_2 are programs. Validity of the judgment is defined using partial couplings.

Definition VI.1 (qOTL Validity)**.** *The judgment $\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ is valid, written*

$$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\},$$

if for every $z \in Z$, and $\rho \in \mathcal{D}^1(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, there exists a partial coupling σ for $\langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle_p$ such that

$$\mathrm{tr}(P_z\rho) \geq \mathrm{tr}(Q_z\sigma).$$

We usually write P (resp Q) instead of P_z (resp Q_z) when there is no ambiguity.

Whenever S_1, S_2 are AST programs, the partial coupling σ is a coupling (see Lemma D.3), which is consistent or similar to previous works [1], [2].

Validity can be recast in terms of contractivity, which allows us to investigate it from a QOT view.

Lemma VI.2. *$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ if and only if for all $z \in Z$, $(\llbracket S_1 \rrbracket, \llbracket S_2 \rrbracket)$ is contractive w.r.t. P and Q.*

Fig. 1 introduces a minimal set of proof rules of our logic. Our set of proof rules contains so-called one-sided rules for initialization, unitaries, conditionals and loops. We only show left rules; there exists a similar right rule for each construct. We note that the one-sided rules are the obvious counterparts of the usual rules for quantum Hoare logic [15]; for instance, the rule for while loops requires users to provide a loop invariant. Besides, our proof system features the usual two-sided rules for skip and sequential compositions. Lastly, our proof system features two structural rules. The (csq) rule is the rule of consequence; it is based on Löwner order. The (duality) rule is an application of the duality theorem, and is used to reduce postconditions to universally quantified split postconditions. Note that the rule requires that the postcondition Q is bounded, i.e. $Q \in \mathsf{Pos}$ rather than $Q \in \mathsf{Pos}^\infty$. In particular, our core set of rules does not feature additional two sided-rules. We discuss two-sided rules in Section VI-C.

Also, we showcase concrete examples in Appendix G.

B. Soundness and Completeness

Every derivable judgment is valid.

Theorem VI.3 (Soundness)**.** *If $\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$, then $\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$.*

Conversely, one can prove completeness for bounded postconditions and AST programs. The proof is divided into two main steps. First, we establish completeness result for *split postconditions*, i.e., postconditions of the form $Q_1 \otimes I_2 + I_1 \otimes Q_2$. With this result in place, we can then leverage duality to derive completeness for all AST programs, and bounded postconditions.

The first step towards completeness is to show some form of one-sided weakest precondition for AST programs.

Lemma VI.4 (One-Sided Weakest Preconditions)**.** *For every AST program S, we have*

$$\vdash Z : \{(\llbracket S \rrbracket^\dagger \otimes I)(Q)\}\ S \sim \mathbf{skip}\ \{Q\}.$$

The lemma is proved by structural induction on the program S. One can then lift the results to the case of two programs.

Lemma VI.5 (Two-Sided Weakest Preconditions)**.** *For every AST programs S_1, S_2, we have*

$$\vdash Z : \{(\llbracket S_1 \rrbracket^\dagger \otimes \llbracket S_2 \rrbracket^\dagger)(Q)\}\ S_1 \sim S_2\ \{Q\}.$$

Now we are ready to give our completeness result.

Theorem VI.6 (Completeness for Split Postconditions)**.** *For every AST programs S_1, S_2, we have:*

$$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q_1 \otimes I + I \otimes Q_2\}$$

implies

$$\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q_1 \otimes I + I \otimes Q_2\}.$$

Using the duality theorem, we can then derive that qOTL is complete for all terminating programs with finite postconditions.

Theorem VI.7 (Completeness for Terminating Programs)**.** *For every AST S_1, S_2 programs and bounded predicate $Q \in \mathsf{Pos}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, we have: $\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ implies $\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$.*

Proof. The desired judgment follows from an application of the duality rule and the provability of:

$$\begin{aligned}\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\} \iff \\ \vdash Z, (Y_1, Y_2, n) \in \mathcal{Y} : \{P + nI\} \\ S_1 \sim S_2\ \{Y_1 \otimes I + I \otimes (nI - Y_2)\}\end{aligned}$$

where $\mathcal{Y}$ is defined as in Theorem IV.6 with $C_i = P$ and $C_o = Q$. Provability of the latter follows from completeness for split postconditions. □

C. Two-Sided Rules

This part considers two-sided rules. Such rules are not needed for completeness. However, they allow to carry lockstep reasoning about structurally similar programs, and typically lead to simpler and more intuitive derivations. For example, it may be easier to establish the equivalence of two loops using a two-sided loop rule rather than using twice a one-sided loop rule, simply because a two-sided loop rule may use the loop invariant that the two loop bodies preserve state equivalence. However, it can be challenging to define sound and expressive two-sided proof rules for control-flow constructs. For instance, [2] uses two-sided rules that involve measurement conditions and entailment between measurement conditions—where these entailments are proved by semantic means. In this section, we show that these rules remain sound for infinite-valued predicates, and we further show how our formalism yields some proof rules to reason about measurement conditions.

Definition VI.8 (Measurement Condition and Entailment, c.f. [2])**.** *Suppose $M = \{M_1, \cdots, M_k\}$ and $N = \{N_1, \cdots, N_k\}$ are two measurements with the same output set. We say two states $\rho, \sigma \in \mathcal{D}$ satisfy the measurement condition $M \approx N$, written $(\rho, \sigma) \vDash M \approx N$, if for all i, $\mathrm{tr}(M_i \rho M_i^\dagger) = \mathrm{tr}(N_i \sigma N_i^\dagger)$.*

Let Γ and Γ' be sets of measurement conditions. We further define the entailment relation of two programs S_1, S_2 between Γ and Γ', written $\Gamma \overset{(S_1,S_2)}{\vDash} \Gamma'$, if for all $\rho, \sigma \in \mathcal{D}^1$ such that $(\rho, \sigma) \vDash \Gamma$, it holds $(\llbracket S_1 \rrbracket(\rho), \llbracket S_2 \rrbracket(\sigma)) \vDash \Gamma'$.

Two-sided rules: (skip) $\dfrac{}{\vdash Z : \{P\}\ \mathbf{skip} \sim \mathbf{skip}\ \{P\}}$ (seq) $\dfrac{\vdash Z : \{P\}\ S_1 \sim S_1'\ \{Q\} \qquad \vdash Z : \{Q\}\ S_2 \sim S_2'\ \{R\}}{\vdash Z : \{P\}\ S_1; S_2 \sim S_1'; S_2'\ \{R\}}$

One-sided rules: (assign-L) $\dfrac{}{\vdash Z : \{\sum_i (|i\rangle_{q_1\langle 1\rangle}\langle 0|) P (|0\rangle_{q\langle 1\rangle}\langle i|)\}\ q := |0\rangle \sim \mathbf{skip}\ \{P\}}$

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

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

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

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

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

Fig. 1. Rules for qOTL

Checking the entailment relation involves the program constructions is highly nontrivial [2]. In fact, the proposed method in [2] is based on the semantics of the programs. Here, we give a complete characterization so that checking entailment itself can be done using program logic.

Theorem VI.9. *For AST programs S_1, S_2, and measurements $M = \{M_1, \cdots, M_k\}$ and $N = \{N_1, \cdots, N_k\}$, the following are equivalent:*

1) $\emptyset \overset{(S_1,S_2)}{\models} M \approx N$;
2) $\models (Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, n) \in \mathcal{Y}_k : \{nI\} S_1 \sim S_2$
$\{(\sum_i M_i^\dagger Y_i M_i) \otimes I + I \otimes [nI - (\sum_i N_i^\dagger Z_i N_i)]\}$

where $\mathcal{Y}_k = \{(Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, n) \mid$
$\forall i,\ 0 \sqsubseteq Y_i,\ 0 \sqsubseteq Z_i \sqsubseteq nI, Y_i \otimes I - I \otimes Z_i \sqsubseteq 0,$
$\forall j \neq i,\ Y_i \otimes I - I \otimes Z_j \sqsubseteq I\}$.

We further define measurement properties as side conditions to set up two-sided rules for **if** and **while**. Our definition unifies Def. 5.4 and 7.2 in [2] (see Proposition E.3).

Definition VI.10 (Measurement Property, c.f. [2])**.** *Let $M = \{M_1, \cdots, M_k\}$ and $N = \{N_1, \cdots, N_k\}$ be measurements, and let $\{Q_j\}_{j=1}^m$ be a set of infinite-valued PSD predicates. Then, we write $\Gamma \models Z : \{P\} M \approx N \{Q_j\}$ if for all $\rho, \sigma \in \mathcal{D}^1$ such that $(\rho, \sigma) \models \Gamma$ and $z \in Z$, if $T_P(\rho, \sigma) < +\infty$, there exist couplings $\delta_j : \langle M_j \rho M_j^\dagger, N_j \sigma N_j^\dagger \rangle$ for each j, such that:*

$$T_P(\rho, \sigma) \geq \sum_j \mathrm{tr}(Q_j \delta_j).$$

We can now defined two-sided rules in Fig. 2 and prove their soundness.

Theorem VI.11 (Soundness of Two-Sided Rules)**.** *The extra rules for qOTL in Fig. 2 are sound regarding the notion of validity.*

VII. Infinite-Valued and Projective Predicates

It might seem curious why we chose to present everything in terms of infinite-valued predicates. What exactly do they buy us? In this section, we answer this question by showcasing the expressiveness of infinite-valued predicates, by showing how it enables a complete semantic embedding of projector-based quantum relational Hoare logics in qOTL. In the context of qOTL, this gives us complete characterisations of non-trivial properties like program equivalence, for free. In the wider field of quantum program logics, this gives us a general way of unifying the two types of predicates (projective and quantitative) in the same logic.

A. Projective Predicates

Our logic, qOTL, follows a quantitative paradigm: we use (generalised) positive semi-definite operators as predicates, and reason about the 'extent' to which quantum states satisfy those predicates by the expectations of the operators over the states. The alternative approach, followed by [1], [17] and parts of [2], uses subspaces (or equivalently projectors) as assertions: a state ρ satisfies $X \in \mathcal{S}(\mathcal{H})$ if $\mathrm{supp}(\rho) \subseteq X$. In the setting of quantum relational Hoare logics, this corresponds to a notion of validity as follows:

Definition VII.1 (Logic for Projective Predicates)**.** *We write $\models_{\mathsf{pqRHL}} \{X\}\ S_1 \sim S_2\ \{Y\}$, where $X, Y \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, if for any initial state ρ with $\mathrm{supp}(\rho) \subseteq X$, there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho)) \rangle$ such that $\mathrm{supp}(\sigma) \subseteq Y$.*

This formulation has several advantages compared to its quantitative counterpart: the resulting logic often has simpler rules, and several non-trivial properties have much simpler formulations. Crucially, this is possible only because pqRHL allows one to enforce *projective preconditions*, i.e., membership of the initial state in a particular subspace. For example,

Extra rules:

$$\text{(if)}\ \frac{\Gamma \vDash Z : \{P\}M \approx M'\{R_k\} \qquad \forall k,\ \vdash Z : \{R_k\}\ S_k \sim S'_k\ \{Q\}}{\Gamma \vdash Z : \{P\}\ \textbf{if}\ (\square k \cdot M[\overline{q}] = k \to S_k)\ \textbf{fi} \sim \textbf{if}\ (\square k \cdot M'[\overline{q}] = k \to S'_k)\ \textbf{fi}\ \{Q\}}$$

$$\text{(while)}\ \frac{\vDash Z : \{P\}M \approx M'\{Q_0, Q_1\} \qquad \vdash Z : \{Q_1\}\ S \sim S'\ \{P\}}{\vdash Z : \{P\}\ \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \textbf{od} \sim \textbf{while}\ M'[\overline{q}] = 1\ \textbf{do}\ S'\ \textbf{od}\ \{Q_0\}}$$

$$\text{(seq+)}\ \frac{\Gamma \vdash Z : \{P\}\ S_1 \sim S'_1\ \{Q\} \qquad \Gamma' \vdash Z : \{Q\}\ S_2 \sim S'_2\ \{R\} \qquad \Gamma \overset{(S_1, S'_1)}{\vDash} \Gamma'}{\Gamma \vdash Z : \{P\}\ S_1; S_2 \sim S'_1; S_2\ \{R\}}$$

Fig. 2. Extra two-side rules for qOTL.

equivalence between two programs S_1, S_2, or, equivalently, the property that $\forall \rho \in \mathcal{D}(\mathcal{H}).[\![S_1]\!](\rho) = [\![S_2]\!](\rho)$ can be expressed as the judgement $\vDash_{\mathsf{pqRHL}} \{=_{\text{sym}}\}\ S_1 \sim S_2\ \{=_{\text{sym}}\}$, where importantly, the precondition $=_{\text{sym}}$ forces the arbitrary initial state ρ to satisfy $\mathrm{tr}_2(\rho) = \mathrm{tr}_1(\rho)$. Unfortunately, similar constraints on the initial state/coupling are not known to be expressible in the bounded quantitative case. As a consequence, it takes much more effort to characterise properties like program equivalence using only positive semi-definite operators as predicates, as we will later show in theorem VIII.1.

B. Enforcing Projective Preconditions Using Infinite-Valued Predicates

It turns out that things are different when we allow infinite-valued predicates. Consider a qOTL judgement of the form $\vDash \{P\}\ S_1 \sim S_2\ \{Q\}$ where P is of the form $X|A = \infty \cdot X^{\perp} + A$. For any initial coupling ρ, if $\mathrm{supp}(\rho) \subseteq X$, then the judgement acts as if $P = A$; if $\mathrm{supp}(\rho) \not\subseteq X$ however, then the judgement is rendered trivially true. In other words, $X|A$ is the same thing as a normal quantitative precondition A constrained by a projective precondition X! A direct consequence of this insight is a semantic embedding of pqRHL in qOTL as follows:

Proposition VII.2. *For AST programs S_1, S_2, and $X, Y \in \mathcal{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ be projectors. The following holds:*

$$\vDash \{X \mid 0\}\ S_1 \sim S_2\ \{Y^{\perp}\} \iff \vDash_{\mathsf{pqRHL}} \{X\}\ S_1 \sim S_2\ \{Y\}.$$

Noting that the postcondition here is bounded, by the completeness theorem (Theorem VI.7), we directly obtain a complete embedding of the projector logic into our logic for AST programs, as shown in the following theorem.

Theorem VII.3. *For AST programs S_1, S_2, and $X, Y \in \mathcal{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ be projectors, we can completely characterise any property defined by the judgement $\vDash_{\mathsf{pqRHL}} \{X\}\ S_1 \sim S_2\ \{Y\}$ in* qOTL.

Therefore, as a corollary, we obtain a complete characterisation of program equivalence for AST programs – this has not been achieved so far in existing quantitative quantum relational Hoare logics [2], [3].

C. Wider Consequences

Infinite-valued predicates provide a general recipe for unifying quantitative and projective quantum predicates. We have seen how it works in the relational case; the same approach also works in the non-relational case. Indeed, if we define a quantum Hoare logic using projective predicates:

Definition VII.4. *Let S be a* qWhile *program and $X, Y \in \mathcal{S}(\mathcal{H}_S)$. We define $\vDash_{\mathsf{pqHL}} \{X\}\ S\ \{Y\}$ to mean $\forall \rho \in \mathcal{D}(\mathcal{H}_S).\ \mathrm{supp}(\rho) \subseteq X \implies \mathrm{supp}[\![S]\!](\rho) \subseteq Y$.*

A logic similar to [15] but using infinite-valued quantitative predicates can also be defined:

Definition VII.5. *Let S be a program and $P, Q \in \mathsf{Pos}^{\infty}(\mathcal{H}_S)$. We define $\vDash_{\mathsf{iqHL}} \{P\}\ S\ \{Q\}$ to mean $\forall \rho \in \mathcal{D}(\mathcal{H}_S).\ \mathrm{tr}(P\rho) \geq \mathrm{tr}(Q[\![S]\!]\rho)$.*

Following a similar reasoning, we could conclude a semantic embedding result:

Theorem VII.6. *For an AST program S, and $X, Y \in \mathcal{S}(\mathcal{H}_S)$, the following holds:*

$$\vDash_{\mathsf{pqHL}} \{X\}\ S\ \{Y\} \iff \vDash_{\mathsf{iqHL}} \{X \mid 0\}\ S\ \{Y^{\perp}\}.$$

Note that this is not the first or the unique possible embedding of pqHL in a quantitative quantum Hoare logic. In fact, in the simple, non-relational case, the naive embedding is complete [18]:

$$\vDash_{\mathsf{pqHL}} \{X\}\ S\ \{Y\} \iff \vDash_{\mathsf{qHL}} \{X^{\perp}\}\ S\ \{Y^{\perp}\},$$

where qHL is a special case of iqHL where all predicates are bounded. The advantage of our approach lies in its generality: it works even when the naive embedding does not apply, as is the case of (quantum) relational logics [2].

VIII. Applications

We present more applications of our completeness results in characterizing non-trivial relational properties, including quantum non-interference, quantum differential privacy, as well as an alternative characterization of equivalence that only needs bounded predicates. Interestingly, most of these results are direct consequences of completeness for split postconditions and do not require the duality rule.

A. Program Equivalence

In the previous section, we showed how equivalence can be characterized with the help of infinite-valued predicates. But can we do it only with bounded quantitative predicates? This question is of particular interest, for it allows us to obtain a

complete characterization of equivalence with a more minimal extension to existing quantum relational Hoare logics [2]. We show that this is indeed possible, and it relies on deep results in QOT.

Theorem VIII.1. *Let S_1, S_2 be AST programs acting on the same Hilbert spaces, $\mathcal{H}_{S_1} = \mathcal{H}_{S_2} = \mathcal{H}$. S_1 and S_2 are semantically equivalent, i.e., $[\![S_1]\!] = [\![S_2]\!]$, if and only if,*

$$\vdash (Y_1,Y_2,n) \in \mathcal{Y} : \{nI + P^{\perp}_{sym}\} \\ S_1 \sim S_2\{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}. \quad (4)$$

where $\mathcal{Y} = \{(Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2), n \in \mathbb{N}) \mid 0 \sqsubseteq Y_1, 0 \sqsubseteq 2Y_2 \sqsubseteq nI, P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)\}$.

Proof. Immediate consequence of Theorem VI.6 and Proposition IV.8. □

Therefore, the fragment of qOTL using only finite-valued predicates is complete for program equivalence for AST programs.

B. Trace Distance and Diamond Norm

Another application of our completeness result for split postconditions would be a notion of completeness with respect to the diamond norm of quantum channels, which builds upon the encoding of the trace distance – the quantum analogue of the total variation distance. The diamond norm is closely related to channel discrimination, as it quantifies the maximum probability of successfully distinguishing between two quantum channels in a single-shot scenario with the help of auxiliary systems. As such, it serves as the foundation in reasoning about the robustness [19] and error analysis [20] of quantum programs, particularly important in the current noisy intermediate-scale quantum (NISQ) era and beyond [21]. We first recall some relevant definitions and properties.

Definition VIII.2 (Trace Distance (see e.g. [22] Definition 9.1.2))**.** *Let ρ_1, ρ_2 be density operators over $\mathcal{H}$. Then their trace distance is defined as $\mathsf{TD}(\rho, \sigma) \triangleq \frac{1}{2}\|\rho - \sigma\|_1$, where $\|\cdot\|_1$ is the trace norm defined by $\|M\|_1 = \mathrm{tr}(\sqrt{M^\dagger M})$.*

Trace distance is also referred to as a quantum generalisation of total variation distance, as it can be alternatively characterised by the maximum (see Lemma 9.1.1 in [22]): $\mathsf{TD}(\rho, \sigma) = \max_{0 \sqsubseteq P \sqsubseteq I} \mathrm{tr}(P(\rho - \sigma))$.

We have the following characterization of the trace distance.

Proposition VIII.3 (Encoding of Trace Distance)**.** *The following are equivalent for all AST programs S_1, S_2 such that[2] $\mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $\mathsf{TD}([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \leq \mathrm{tr}(\Phi_1\rho_1) + \mathrm{tr}(\Phi_2\rho_2)$ *for all $z \in Z$ and $\rho_1 X^{\#} \rho_2$, for some given subspace X;*
2) $\vDash 0 \sqsubseteq P \sqsubseteq I : \{X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2)\}\ S_1 \sim S_2\ \{P \otimes I + I \otimes (I - P)\}$.

We now introduce the notion of diamond norms of quantum channels.

[2]We could also just ask all programs to be interpreted over $\mathcal{H} = \mathcal{H}_{\text{all variables}}$, or over $\mathcal{H} = \mathcal{H}_{var(S_1) \cup var(S_2)}$.

Definition VIII.4 (Diamond Norm, Definition 8 in [23])**.** *Let $\Phi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$ be a linear transformation, where $M_n(\mathbb{C})$ denote the set of $n \times n$ complex matrices, and let $id_n : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ be the identity map. Then, the diamond norm (also known as the completely bounded trace norm) of Φ is given by $\|\Phi\|_\diamond = \max_{X;\|X\|_1 \leq 1} \|(\Phi \otimes id_n)X\|$.*

The diamond norm induces the diamond distance. For completely positive, trace non-increasing maps $\mathcal{E}_1$ and $\mathcal{E}_2$ with domain $\mathsf{Pos}(\mathcal{H})$, their diamond distance could be written as

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_\diamond = \max_{\rho \in \mathcal{D}^1(\mathcal{H} \otimes \mathcal{H})} \|(\mathcal{E}_1 \otimes \mathcal{I})(\rho) - (\mathcal{E}_2 \otimes \mathcal{I})(\rho)\|_1,$$

where $\mathcal{I}$ is the identity quantum channel on $\mathcal{H}$. Now, consider setting $X = P_{sym}[\mathcal{H} \otimes \mathcal{H}]$, and $\Phi_1 = \Phi_2 = cI/2$ in Proposition VIII.3, where $c \geq 0$ is a constant. The property we are trying to encode becomes

$$\mathsf{TD}((([\![S_1]\!] \otimes \mathcal{I})(\rho_1), ([\![S_2]\!] \otimes \mathcal{I})(\rho_2)) \leq c, \quad \forall \rho_1 (=_{sym})^{\#} \rho_2.$$

Noting that $\rho_1 (=_{sym})^{\#} \rho_2$ iff $\rho_1 = \rho_2$, this gives an encoding of the diamond distance between $[\![S_1]\!]$ and $[\![S_2]\!]$, which we formally stated as follows.

Proposition VIII.5 (Encoding of Diamond Norm)**.** *Let $c \in \mathbb{R}^+$. The following are equivalent for all AST programs S_1, S_2 such that $\mathcal{H} = \mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $\|[\![S_1]\!] - [\![S_2]\!]\|_\diamond \leq 2c$;
2) $\vDash 0 \sqsubseteq P \sqsubseteq I_{\mathcal{H} \otimes \mathcal{H}} : \{P_{sym}[\mathcal{H} \otimes \mathcal{H}] \mid (1 + c)I\}\ S_1 \sim S_2\ \{P \otimes I + I \otimes (I - P)\}$.

Theorem VIII.6 (Completeness with respect to Diamond Norm)**.** *The* qOTL *is complete with respect to diamond norm, for AST programs.*

Comparison to [19], [20]: The program logic introduced in [19], [20] provides a sound method for reasoning about the upper bound of (Q, λ)-diamond norm between a noisy program and its ideal counterpart. However, its completeness remains unknown. Theorem VIII.6 can be extended to establish complete reasoning for the upper bound of $(X, 1)$-diamond norm where $X \in \mathcal{S}(\mathcal{H})$ is a subspace.

C. Quantum Wasserstein Semi-Distance

The Wasserstein metric, also known as the earth mover's distance, is a measure of distance between two probability distributions. It is important because it characterizes the minimal cost required to transform one probability distribution into the other in the context of optimal transport. Several quantum generalizations of the Wasserstein metric have been proposed. However, so far, these generalizations have only been shown to satisfy the properties of a semi-distance for density matrices. In this work, we adopt the following definition of the quantum Wasserstein semi-distance discussed in [9].

Let $\rho, \sigma \in \mathcal{D}^1(\mathcal{H})$ be two density operators. Their quantum 2-Wasserstein semi-distance $W(\rho, \sigma)$ is defined as $W(\rho, \sigma) = \sqrt{T(\rho, \sigma)}$, where $T(\rho, \sigma) = T_{P^{\perp}_{sym}}(\rho, \sigma)$ is the QOT between ρ and σ with the cost function $P^{\perp}_{sym}$, see Section IV-C for details.

Verifying properties of programs related to the above quantum Wasserstein semi-distance can be easily encoded in our logic. Specifically, we investigate the Lipschitz property of programs with respect to the quantum Wasserstein semi-distance. This property asserts that the quantum Wasserstein semi-distance between a program's outputs is bounded by the quantum Wasserstein semi-distance between its inputs scaled by a constant λ. This property can be directly encoded and verified in our logic:

Proposition VIII.7 (Encoding of Quantum Wasserstein Semi-Distance)**.** *Let $\lambda > 0$. The following are equivalent for all AST programs S_1, S_2 such that $\mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $W([\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))) \leq \lambda \cdot W(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho))$ *for all $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$;*
2) $\vDash \{\lambda^2 P^{\perp}_{sym}\}\ S_1 \sim S_2\ \{P^{\perp}_{sym}\}$.

Theorem VIII.8 (Completeness with respect to Quantum Wasserstein Semi-Distance)**.** *The* qOTL *is complete with respect to the Lipschitz property of quantum Wasserstein semi-distance for AST programs.*

D. Quantum Non-Interference

Another application of our logic involves characterizing the concept of quantum non-interference. Intuitively, non-interference refers to a critical property where the actions of one group of agents in a computer system do not influence the actions of another group of agents. This concept was later extended to quantum settings in [24]. The key components for defining quantum non-interference in their work include quantum computer systems, a pseudo-distance for measuring output distributions, and the degree of interference. We introduce these notions as follows.

Definition VIII.9 (Definition 3.1 in [24])**.** *A quantum system is a 6-tuple $\mathbb{S} = \langle \mathcal{H}, \rho_0, A, C, do, measure \rangle$, where*

- *$\mathcal{H}$ is a Hilbert space specifying the state space;*
- *$\rho \in \mathcal{D}(\mathcal{H})$ specifying the initial state;*
- *A is a set of agents;*
- *C is a set of commands;*
- *$do = \{\mathcal{E}_{a,c} | a \in A \text{ and } c \in C\}$ is a set of trace-preserving operations $\mathcal{E}_{a,c}$ which describes how states are updated when agent a executes command c;*
- *$measure = \{\mathbb{M}_a | a \in A\}$ is a collection of sets of POVM measurements, where each $\mathbb{M}_a$ is allowable for agent a.*

The quantum non-interference influence is measured by the following pseudo distance $d_{\mathbb{M}}$ induced by POVM measurements $\mathbb{M}$. Let $d(p, q)$ denote the total variation distance between two probability distributions p and q over the sample space X. For a density operator ρ and a POVM measurement $E = \{E_\lambda | \lambda \in \Lambda\}$, we define the probability distribution $p_{E,\rho}$ as $p_{E,\rho}(\lambda) = \mathrm{tr}(E_\lambda \rho)$. The pseudo distance $d_{\mathbb{M}}$ is formalized as follows.

Definition VIII.10 (Definition 3.2 in [24])**.** *The pseudo distance $d_{\mathbb{M}}$ between two density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ induced by a set of POVM measurements $\mathbb{M}$ is defined as*

$$d_{\mathbb{M}}(\rho, \sigma) = \sup_{E \in \mathbb{M}} d(p_E(\rho), p_E(\sigma)).$$

For each agent $a \in A$ in a quantum system $\mathbb{S}$, we write $d_a = d_{\mathbb{M}_a}$ for the pseudo distance defined by the set $\mathbb{M}_a$ of POVM measurements.

Let $G \subseteq A$ be a group of agents, $D \subseteq A$ be a set of commands. For a sequence of actions $\alpha = \alpha_1 \alpha_2 \cdots \alpha_n \in (A \times C)^*$, we define a function $\mathsf{purge}_{G,D}$ for α that removes the actions in D by the agents in group G. In other words, $\mathsf{purge}_{G,D}(\alpha) = \alpha'_1 \alpha'_2 \cdots \alpha'_n$, where $\alpha'_i = \epsilon$ (the empty action) if $\alpha'_i = (a_i, c_i)$ with $a_i \in G$ and $c_i \in D$, and $\alpha'_i = \alpha_i$ otherwise. The degree of (non-) interference is measured by the pseudo distance $d_{\mathbb{M}}$ between the state operated by the original actions and the state operated by the purged actions.

Definition VIII.11 (Interference Degree, Definition 3.3 in [24])**.** *For a quantum system $\mathbb{S} = \langle \mathcal{H}, \rho_0, A, C, do, measure \rangle$, let $G_1, G_2 \subseteq A$ be two groups of agents, and $D \subseteq C$ be a set of commands. Then, the degree that agents in G_1 with commands D interfere agents in G_2 is*

$$Int(G_1, D | G_2) = \sup_{\substack{\alpha \in (A \times C)^*, \\ a \in G_2}} \{d_a(\mathcal{E}_\alpha(\rho_0), \mathcal{E}_{\mathsf{purge}_{G_1,D}(\alpha)}(\rho_0))\}$$

If $Int(G_1, D | G_2) = 0$, we will denote this as $G_1, D : | G_2$.

For a quantum system $\mathbb{S} = \langle \mathcal{H}, \rho_0, A, C, do, measure \rangle$ with an initial state $\rho_0 = |0\rangle\langle 0|$, we represent trace-preserving operations $\mathcal{E}_{a,c}$ as corresponding AST programs $S_{a,c}$, and sequence of actions α as AST programs S_α. The following and theorem shows the quantum non-interference property can be encoded and verified using our logic.

Proposition VIII.12 (Encoding of Quantum Non-Interference)**.** *For a quantum system $\mathbb{S} = \langle \mathcal{H}, \rho_0, A, C, do, measure \rangle$ with $\rho_0 = |0\rangle\langle 0|$, let $G_1, G_2 \subseteq A$ be two groups of agents, and $D \subseteq C$ be a set of commands. The following are equivalent:*

- *$G_1, D : | G_2$.*
- *$\forall \alpha \in (A \times C)^*$,*

$$\vDash a \in G_2, E = \{E_\lambda | \lambda \in \Lambda_E\} \in \mathbb{M}_a, T \subseteq \Lambda_E :$$
$$\{I\}\ q := |0\rangle; S_\alpha \sim q := |0\rangle; S_{\mathsf{purge}_{G_1,D}(\alpha)}\ \{M\},$$

where $M = M_T \otimes I + I \otimes (I - M_T)$ with $M_T = \sum_{\lambda \in T} E_\lambda$.

Theorem VIII.13 (Completeness with respect to Quantum Non-Interference)**.** *The* qOTL *is complete with respect to the quantum non-interference property for AST programs.*

E. Quantum Differential Privacy

Finally, with the help of infinite-valued predicates, we can characterize a quantum version of differential privacy. Differential privacy is a mathematical framework about providing statistical properties about datasets while preserving private information of individual objects. The core intuition behind differential privacy is that the output distributions of a program should remain nearly indistinguishable when run on two "neighboring" inputs, usually differing only by a single

element. This concept has been successfully extended to quantum computing, resulting in the development of related but distinct notions of quantum differential privacy. These notions, as explored in works such as [25], [26], primarily differ in how they define and characterize "neighboring inputs". In this paper, we adopt the following definition proposed in [25].

Definition VIII.14 (Quantum Differential Privacy, Definition 3 in [25])**.** *Let $\varepsilon, \delta > 0$ be constants. A quantum operation $\mathcal{E}$ on an n-qubit system is (ε, δ)-differentially private, if for every POVM $M = \{M_m\}_{m \in \mathsf{Out}(m)}$, every set $A \subseteq \mathsf{Out}(m)$, and every input ρ, σ that differs at most one qubit (i.e., there exists $i \in [n]$ that $\mathrm{tr}_i(\rho) = \mathrm{tr}_i(\sigma)$), it holds that $\Pr[\mathcal{E}(\rho) \in_M A] \leq \exp(\varepsilon) \cdot \Pr(\mathcal{E}(\sigma) \in_M A) + \delta$, where $\Pr(\rho \in_M A) = \sum_{m \in A} \mathrm{tr}(M_m \rho)$.*

Let S be some quantum program that corresponds to the quantum operation $\mathcal{E}$. We could verify whether $\mathcal{E}$, or equivalently $[\![S]\!]$, is (ε, δ)-differentially private in our logic, as implied by the following proposition and theorem.

Proposition VIII.15 (Encoding of Differential Privacy)**.** *The following are equivalent for all AST programs S_1 on an n-qubit system:*

1) *$[\![S]\!]$ is (ε, δ)-differentially private;*
2) *$\vDash i \in [n], 0 \sqsubseteq M \sqsubseteq I : \{P_{i,sym} \mid (\exp(\varepsilon) + \delta) I\}\ S \sim S\ \{M \otimes I + \exp(\varepsilon) I \otimes (I - M)\}$.*

Here $P_{i,sym} = P_{sym}[\mathcal{H}_{[n]-i}] \otimes (I_{i\langle 1\rangle} \otimes I_{i\langle 2\rangle})$ for $i \in [n]$.

Theorem VIII.16 (A Complete Characterization of Quantum Differential Privacy)**.** *The* qOTL *is complete with respect to the quantum differential privacy property for AST programs.*

IX. Probabilistic Duality

There is a variety of relational program logics for probabilistic programs [4], [27]–[29]. Similar to the quantum case, validity of these logics is based on probabilistic couplings, their completeness has remained an open problem. Recent work by Avanzini *et al*. [4] defines a quantitative relational Hoare logic, called eRHL, and shows that it achieves completeness for non-trivial classes of properties. Their proof of completeness leverages a notion of split post-condition similar to ours. However, their work lacks a general completeness theorem. We show that their logic is in fact complete for bounded postconditions. Completeness follows from the classic Kantorovich-Rubinstein duality. Our phrasing of the theorem is stated w.r.t. positive functions c_1 and c_2, to match the assumption that assertions in eRHL take positive values.

Theorem IX.1 (Kantorovich-Rubinstein Duality)**.** *Let μ, ν be discrete probability distributions over X and Y respectively, and let $c : X \times Y \to [0, +\infty)$ be a bounded function. Then*

$$\inf_{\theta \in \Gamma(\mu,\nu)} \mathbb{E}_\theta[c] = \sup_{(n,c_1,c_2) \in \mathcal{W}} (\mathbb{E}_\mu[c_1] + \mathbb{E}_\nu[c_2] - n)$$

where $\Gamma(\mu, \nu)$ denotes the set of probabilistic couplings of μ and ν and $(n, c_1, c_2) \in \mathcal{W}$ iff for every $x \in X$ and $y \in Y$, we have $0 \leq c_1(x), c_2(y)$ and $c_1(x) + c_2(y) \leq c(x, y) + n$.

It follows that every bounded post-condition is logically equivalent to a universally quantified split post-condition—where in the probabilistic setting a split post-condition is simply the addition of two unary assertions on the first and second state respectively. Therefore eRHL is complete for all bounded postconditions.

Proposition IX.2. eRHL *is complete for all AST programs and bounded postconditions.*

Note that completeness does not require adding a duality rule, due to a difference of settings. Indeed, eRHL features a very general rule of consequence, which allows using arbitrary theorems from the theory of couplings.

Interestingly, [4] establishes a completeness theorem for judgments of the pRHL logic, using Strassen's theorem [7]. This is very similar in spirit to our use of the duality theorem. In fact, Strassen's theorem can be seen as a specialized variant of the duality theorem for boolean-valued cost functions. Furthermore, note that [4] uses the Kantorovich-Rubinstein duality to prove that eRHL characterizes Kantorovich distance, but fails to establish a link with completeness.

X. Related work and Discussion

A. Quantum Relational Hoare Logics

Our logic can be seen as a generalization of Barthe *et al*.'s rqPD [2]. It differs with rqPD in three ways: we consider possibly infinite-valued positive predicates (instead of finite-valued and subunital ones), we consider an upper-bounding instead of a lower-bounding semantics, and we allow for logical variables. That said, rqPD can be semantically embedded in our logic as follows:

Proposition X.1. *Let S_1, S_2 be AST programs and $0 \sqsubseteq P, Q \sqsubseteq I$ be predicates. Then $\vDash_{\mathsf{rqPD}} \{P\}\ S_1 \sim S_2\ \{Q\}$ iff $\vDash \{I - P\}\ S_1 \sim S_2\ \{I - Q\}$.*

Moreover, most of our proof rules are adapted from rqPD's rules, and it turns out that straightforwardly generalizing rqPD's one-sided rules to our setting is sufficient to achieve completeness without needing two-sided rules with complex semantic conditions like measurement conditions. Nevertheless, the said rules being still sound and potentially more usable, we adapt them and further show that measurement conditions can be reasoned about *within* our logic.

Barthe *et al*. [2] also discuss a logic using projective (instead of quantitative) predicates similar to pqRHL, as well as an incomplete embedding of that logic into rqPD. This work achieves a complete embedding with the help of infinite-valued predicates.

Another line of work [1], [3] is based on separable couplings (instead of general couplings like in [2] and our work). Unruh [1] defines the first sound relational program logic for quantum programs based on projective predicates and separable couplings. The primary motivation for using separable couplings is that it is possible to prove soundness of a frame rule. Li and Unruh [3] define an expectation-based variant of [1]. The soundness of their logic is also proved with a

notion of validity based on separable couplings. Interestingly, the motivation for using separable couplings in this case is soundness—there is no frame rule in this logic. Neither of these logics are known to be complete.

Comparing our logic to separable-coupling-based ones is not the focus of our work. As already extensively discussed by [2] and [3], while similar sets of proof rules can be sound for both general-coupling-based and separable-coupling-based notions of validity, it is unclear how these notions of validity actually relate to each other. Moreover, it is unclear whether it is possible to adapt ideas in our work (like Strassen's theorem) to obtain similar completeness results.

Finally, in [17], Yan *et al*. study approximative relational reasoning by giving a logic similar to [2]'s projective logic, but based on approximate couplings (where a ρ is an ϵ-coupling of ρ_1 and ρ_2 if both $\mathsf{TD}(\rho_1, \mathrm{tr}_2(\rho))$ and $\mathsf{TD}(\rho_2, \mathrm{tr}_1(\rho))$ are upper-bounded by ϵ, where TD is the trace distance). In comparsion, while our logic is quantitative and completely characterizes various distance metrics like the Wasserstein semi-distance, we do require couplings to be exact. It would indeed be interesting to explore how expressive our logic is for approximative reasoning compared to their work.

B. Quantum Optimal Transport

Over the past decades, efforts have been made to generalize the optimal transport problem to the quantum setting. Early attempts [30] defined the cost between two quantum states using the (probabilistic) Monge distance based on their corresponding Husimi distributions, and then explored the physical consequences including unitary evolution and decoherence [31]. More recent approaches have framed quantum optimal transport in terms of expectations over couplings. Specifically, given quantum states ρ_1 and ρ_2, they have studied the expectation $\mathrm{tr}(C\rho)$ over possible "couplings" ρ of ρ_1 and ρ_2, for both general and specific types of costs:

[32] explored the QOT based on quantum coupling (Definition III.1 but on continuous space), with the cost specified as energies involving position and momentum operators, primarily for investigating applications in quantum mean-field theory and its classical limits. Related results include such as inequalities involving QOT and related potentials or metrics [32], [33], Kantorovich type duality theorem [34], and showing that QOT can be cheaper than the classical one [35].

Another approach [36], [37] examines QOT from a view of changing one state to another, i.e, focusing on the properties of quantum channels $\mathcal{E}$ that satisfy $\mathcal{E}(\rho_1) = \rho_2$. It was shown that there is a one-to-one correspondence between such channels and the couplings of $\langle \rho_1^T, \rho_2 \rangle$, offering an alternative definition of couplings. They further studied the cost function $\sum_i (R_i \otimes I_2 - I_1 \otimes R_i^T)^2$, and established related entropic and concentration inequalities [38], [39], with an application showing the limitations of Variational Quantum Algorithms in the presence of noise [38].

In addition to special cost functions, prior works have systematically explored the general properties and associated metrics or distances in quantum optimal transport (QOT) [9], [40], [41]. For instance, [12] introduced a stable version of QOT, as briefly summarized in Section IV. This line of research aligns closely with our objectives, as we prioritize the general relational properties of program states over specific costs or physically oriented properties.

C. Reasoning about Program Equivalence

Outside of quantum relational Hoare logics, reasoning techniques about equivalence between quantum programs/circuits have been widely studied.

Several lines of works create axiomatizations of program equivalence in the form of equational theories. Similarly to our work, they look at notions of quantum computing with *existing* and well-defined denotational semantics, with respect to which they would prove properties like soundness and completeness. However, they only focus on program equivalence and have a very different goal of enabling equational reasoning. One line of work stems from the categorical quantum mechanics (CQM) programme [42]–[44] and leverages categorical formalisms developed therein to produce string-diagrammatic axiomatizations of quantum theory like the ZX calculus and others [45]–[47]. Similarly to these calculi, [48] develop a tool for reasoning about expressions formally written in Dirac notation. Other works, including ours, have a specific focus on quantum computing (CP and trace non-decreasing maps), a proper subset of quantum theory (CP maps). In [49], Staton presents an algebraic theory of qubit quantum computing and proved that it completely axiomatizes a standard model of quantum computation. Recently, [50] complements [49] by giving an equational theory for unitary quantum circuits that is complete for various gate sets, by extending Π, a model of classical reversible computing.

Other works focus on models of quantum computation (e.g. quantum concurrency) that do not yet have a readily available notion of program equivalence. Quantum process calculi [51]–[54], for instance, model quantum concurrency by extending classical process calculi with quantum primitives. Several notions of behavioural equivalence were then developed based on bisimulation. However, as [53] points out, each of these proposals is subtly different from the others, and there is not yet a consensus on which is the right one. Compared to our work, quantum bisimulation handles a richer programming language, but once again only handles equivalence.

XI. Conclusion

We have defined a sound and complete relational proof system for quantum programs. Our proof system achieves completeness from the duality theorem of quantum optimal theorem. In addition, with the help of infinite-valued predicates, we have given a complete embedding of projective assertions into our logic.

Acknowledgment

This research was supported by the National Key R&D Program of China under Grant No. 2023YFA1009403.

References

[1] D. Unruh, "Quantum relational hoare logic," Proceedings of the ACM on Programming Languages, vol. 3, no. POPL, p. 1–31, Jan. 2019. [Online]. Available: http://dx.doi.org/10.1145/3290346

[2] G. Barthe, J. Hsu, M. Ying, N. Yu, and L. Zhou, "Relational proofs for quantum programs," Proc. ACM Program. Lang., vol. 4, no. POPL, Dec. 2019.

[3] Y. Li and D. Unruh, "Quantum Relational Hoare Logic with Expectations," in Proceedings of the 48th International Colloquium on Automata, Languages, and Programming, vol. 198, 2021, pp. 136:1–136:20.

[4] M. Avanzini, G. Barthe, D. Davoli, and B. Grégoire, "A quantitative probabilistic relational hoare logic," Proc. ACM Program. Lang., vol. 9, no. POPL, Jan. 2025. [Online]. Available: https://doi.org/10.1145/3704876

[5] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010.

[6] G. Barthe, M. Gao, T. Wang, and L. Zhou, "Complete quantum relational Hoare logics from optimal transport duality (extended version)," 2025. [Online]. Available: https://arxiv.org/abs/2501.15238

[7] V. Strassen, "The existence of probability measures with given marginals," The Annals of Mathematical Statistics, pp. 423–439, 1965. [Online]. Available: http://projecteuclid.org/euclid.aoms/1177700153

[8] L. Zhou, S. Ying, N. Yu, and M. Ying, "Strassen's theorem for quantum couplings," Theoretical Computer Science, vol. 802, pp. 67–76, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397519305225

[9] S. Cole, M. Eckstein, S. Friedland, and K. Życzkowski, "On quantum optimal transport," Mathematical Physics, Analysis and Geometry, vol. 26, no. 2, p. 14, Jun 2023. [Online]. Available: https://doi.org/10.1007/s11040-023-09456-7

[10] G. Monge, "Mémoire sur la théorie des déblais et des remblais," Mem. Math. Phys. Acad. Royale Sci., pp. 666–704, 1781.

[11] R. Bistroń, M. Eckstein, and K. Życzkowski, "Monotonicity of a quantum 2-wasserstein distance," Journal of Physics A: Mathematical and Theoretical, vol. 56, no. 9, p. 095301, feb 2023. [Online]. Available: https://dx.doi.org/10.1088/1751-8121/acb9c8

[12] A. Müller-Hermes, "On the monotonicity of a quantum optimal transport cost," 2022. [Online]. Available: https://arxiv.org/abs/2211.11713

[13] L. Zhou, N. Yu, S. Ying, and M. Ying, "Quantum earth mover's distance, a no-go quantum Kantorovich–Rubinstein theorem, and quantum marginal problem," Journal of Mathematical Physics, vol. 63, no. 10, p. 102201, 10 2022. [Online]. Available: https://doi.org/10.1063/5.0068344

[14] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," Physical Review A, vol. 69, no. 2, p. 022309, 2004.

[15] M. Ying, "Floyd–hoare logic for quantum programs," ACM Trans. Program. Lang. Syst., vol. 33, no. 6, Jan. 2012. [Online]. Available: https://doi.org/10.1145/2049706.2049708

[16] ——, Foundations of Quantum Programming, 1st ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2016.

[17] P. Yan, H. Jiang, and N. Yu, "Approximate relational reasoning for quantum programs," in Computer Aided Verification, A. Gurfinkel and V. Ganesh, Eds. Cham: Springer Nature Switzerland, 2024, pp. 495–519.

[18] L. Zhou, N. Yu, and M. Ying, "An applied quantum hoare logic," in Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, ser. PLDI 2019. New York, NY, USA: Association for Computing Machinery, 2019, p. 1149–1162. [Online]. Available: https://doi.org/10.1145/3314221.3314584

[19] S.-H. Hung, K. Hietala, S. Zhu, M. Ying, M. Hicks, and X. Wu, "Quantitative robustness analysis of quantum programs," Proc. ACM Program. Lang., vol. 3, no. POPL, Jan. 2019. [Online]. Available: https://doi.org/10.1145/3290344

[20] R. Tao, Y. Shi, J. Yao, J. Hui, F. T. Chong, and R. Gu, "Gleipnir: toward practical error analysis for quantum programs," in Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, ser. PLDI 2021. New York, NY, USA: Association for Computing Machinery, 2021, p. 48–64. [Online]. Available: https://doi.org/10.1145/3453483.3454029

[21] J. Preskill, "Quantum Computing in the NISQ era and beyond," Quantum, vol. 2, p. 79, Aug. 2018. [Online]. Available: https://doi.org/10.22331/q-2018-08-06-79

[22] M. M. Wilde, Quantum Information Theory, 2nd ed. Cambridge University Press, 2017.

[23] D. Aharonov, A. Kitaev, and N. Nisan, "Quantum circuits with mixed states," in Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, ser. STOC '98. New York, NY, USA: Association for Computing Machinery, 1998, p. 20–30. [Online]. Available: https://doi.org/10.1145/276698.276708

[24] M. Ying, Y. Feng, and N. Yu, "Quantum information-flow security: Noninterference and access control," in 2013 IEEE 26th Computer Security Foundations Symposium, 2013, pp. 130–144.

[25] S. Aaronson and G. N. Rothblum, "Gentle measurement of quantum states and differential privacy," in Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, 2019, p. 322–333.

[26] L. Zhou and M. Ying, "Differential privacy in quantum computation," in 2017 IEEE 30th Computer Security Foundations Symposium (CSF), 2017, pp. 249–262.

[27] G. Barthe, B. Grégoire, and S. Zanella Béguelin, "Formal certification of code-based cryptographic proofs," in Proceedings of the 36th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 2009, p. 90–101.

[28] A. Aguirre, G. Barthe, J. Hsu, B. L. Kaminski, J. Katoen, and C. Matheja, "A pre-expectation calculus for probabilistic sensitivity," Proc. ACM Program. Lang., vol. 5, no. POPL, pp. 1–28, 2021. [Online]. Available: https://doi.org/10.1145/3434333

[29] S. O. Gregersen, A. Aguirre, P. G. Haselwarter, J. Tassarotti, and L. Birkedal, "Asynchronous probabilistic couplings in higher-order separation logic," Proc. ACM Program. Lang., vol. 8, no. POPL, pp. 753–784, 2024. [Online]. Available: https://doi.org/10.1145/3632868

[30] K. Zyczkowski and W. Slomczynski, "The monge distance between quantum states," Journal of Physics A: Mathematical and General, vol. 31, no. 45, p. 9095, nov 1998. [Online]. Available: https://dx.doi.org/10.1088/0305-4470/31/45/009

[31] ——, "The monge metric on the sphere and geometry of quantum states," Journal of Physics A: Mathematical and General, vol. 34, no. 34, p. 6689, aug 2001. [Online]. Available: https://dx.doi.org/10.1088/0305-4470/34/34/311

[32] F. Golse, C. Mouhot, and T. Paul, "On the mean field and classical limits of quantum mechanics," Communications in Mathematical Physics, vol. 343, no. 1, pp. 165–205, Apr. 2016.

[33] F. Golse and T. Paul, "Quantum and Semiquantum Pseudometrics and applications," Journal of Functional Analysis, 2022. [Online]. Available: https://hal.science/hal-03136855

[34] E. Caglioti, F. Golse, and T. Paul, "Towards Optimal Transport for Quantum Densities," Annali della Scuola Normale Superiore di Pisa, Classe di Scienze, 2022. [Online]. Available: https://hal.science/hal-01963667

[35] ——, "Quantum optimal transport is cheaper," Journal of Statistical Physics, vol. 181, no. 1, pp. 149–162, Oct. 2020.

[36] G. De Palma and D. Trevisan, "Quantum optimal transport with quantum channels," Annales Henri Poincaré, vol. 22, no. 10, pp. 3199–3234, Oct. 2021.

[37] ——, Quantum Optimal Transport: Quantum Channels and Qubits. Cham: Springer Nature Switzerland, 2024, pp. 203–239. [Online]. Available: https://doi.org/10.1007/978-3-031-50466-2_4

[38] G. De Palma, M. Marvian, C. Rouzé, and D. S. França, "Limitations of variational quantum algorithms: A quantum optimal transport approach," PRX Quantum, vol. 4, p. 010309, Jan 2023. [Online]. Available: https://link.aps.org/doi/10.1103/PRXQuantum.4.010309

[39] G. D. Palma and D. Pastorello, "Quantum concentration inequalities and equivalence of the thermodynamical ensembles: an optimal mass transport approach," 2024. [Online]. Available: https://arxiv.org/abs/2403.18617

[40] S. Friedland, M. Eckstein, S. Cole, and K. Życzkowski, "Quantum monge-kantorovich problem and transport distance between density matrices," Physical Review Letters, vol. 129, p. 110402, Sep 2022.

[41] L. Zhou, N. Yu, S. Ying, and M. Ying, "Quantum earth mover's distance, a no-go quantum kantorovich–rubinstein theorem, and quantum marginal problem," Journal of Mathematical Physics, vol. 63, no. 10, p. 102201, 10 2022. [Online]. Available: https://doi.org/10.1063/5.0068344

[42] S. Abramsky and B. Coecke, "A categorical semantics of quantum protocols," 2007. [Online]. Available: https://arxiv.org/abs/quant-ph/0402130

[43] B. Coecke and A. Kissinger, Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning. Cambridge University Press, 2017.

[44] C. Heunen and J. Vicary, Categories for Quantum Theory: An Introduction. Oxford University Press, 11 2019. [Online]. Available: https://doi.org/10.1093/oso/9780198739623.001.0001

[45] B. Coecke and R. Duncan, "Interacting quantum observables," in Automata, Languages and Programming, L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 298–310.

[46] M. Backens and A. Kissinger, "Zh: A complete graphical calculus for quantum computations involving classical non-linearity," Electronic Proceedings in Theoretical Computer Science, vol. 287, p. 23–42, Jan. 2019. [Online]. Available: http://dx.doi.org/10.4204/EPTCS.287.2

[47] A. Hadzihasanovic, "A diagrammatic axiomatisation for qubit entanglement," 2015. [Online]. Available: https://arxiv.org/abs/1501.07082

[48] Y. Xu, G. Barthe, and L. Zhou, "Automating equational proofs in dirac notation," Proc. ACM Program. Lang., vol. 9, no. POPL, Jan. 2025. [Online]. Available: https://doi.org/10.1145/3704878

[49] S. Staton, "Algebraic effects, linearity, and quantum programming languages," in Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, ser. POPL '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 395–406. [Online]. Available: https://doi.org/10.1145/2676726.2676999

[50] J. Carette, C. Heunen, R. Kaarsgaard, and A. Sabry, "With a few square roots, quantum computing is as easy as pi," Proceedings of the ACM on Programming Languages, vol. 8, no. POPL, p. 546–574, Jan. 2024. [Online]. Available: http://dx.doi.org/10.1145/3632861

[51] M. Lalire and P. Jorrand, "A process algebraic approach to concurrent and distributed quantum computation: Operational semantics," 2004. [Online]. Available: https://arxiv.org/abs/quant-ph/0407005

[52] S. Gay and R. Nagarajan, "Communicating quantum processes," 2004. [Online]. Available: https://arxiv.org/abs/quant-ph/0409052

[53] L. Ceragioli, F. Gadducci, G. Lomurno, and G. Tedeschi, "Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers," Proc. ACM Program. Lang., vol. 8, no. POPL, jan 2024. [Online]. Available: https://doi.org/10.1145/3632885

[54] M. Ying, Y. Feng, R. Duan, and Z. Ji, "An algebra of quantum processes," 2010. [Online]. Available: https://arxiv.org/abs/0707.0330

[55] G. Barthe, J. Hsu, M. Ying, N. Yu, and L. Zhou, "Relational proofs for quantum programs," Proceedings of the ACM on Programming Languages, vol. 4, no. POPL, Dec. 2019.

[56] A. A. Mele, "Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial," Quantum, vol. 8, p. 1340, 2024.

[57] C. Villani, Optimal transport – Old and new. Springer Berlin, Heidelberg, 2008, vol. 338.

APPENDIX A
DEFERRED PROOFS IN "NOTATIONS AND PRELIMINARIES" SECTION

We first briefly review some basic concepts and propositions in linear algebra and quantum computing.

Quantum States. The state space of a quantum system is described by a complex Hilbert space $\mathcal{H}$, which we ususally assume to be finite-dimensional. A pure state is a unit (column) vector in the Hilbert space. For example, an d-dimensional quantum state in $\mathbb{C}^d$ has the form

$$v = (v_0, v_1, v_2, \ldots, v_{d-1})^\intercal,$$

usually denoted as $|v\rangle$ with the Dirac symbol $|\cdot\rangle$. The computational basis of $\mathbb{C}^d$ is denoted as $\{|i\rangle\}_{i=0}^{d-1}$, where the j-th coordinate of $|i\rangle$ is 1 if $j = i$, and 0 otherwise. The inner product between states $|u\rangle$ and $|v\rangle$ is denoted as $\langle u|v\rangle$, which is the standard inner product in the Hilbert space, where $\langle u|$ stands for the conjugate transpose of $|u\rangle$. Let $|u\rangle \in \mathbb{C}^{d_1}$ and $|v\rangle \in \mathbb{C}^{d_2}$ be two states. Their tensor product, written as $|u\rangle \otimes |v\rangle$, or $|u\rangle|v\rangle$ in short, is defined to as the following vector $|u\rangle|v\rangle = (u_0v_0, u_0v_1, u_0v_2, \ldots, u_{d_1}v_{d_2})^\intercal$.

A quantum bit (or qubit for short), is a quantum state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$, with $|\alpha|^2 + |\beta|^2 = 1$. An n-qubit state is in the Hilbert space of dimension 2^n.

Let $\mathcal{H}$ be a d-dimensional Hilbert space. The (linear) operators on $\mathcal{H}$ are just $d \times d$ matrices. For an operator A, the trace of A, $\mathrm{tr}(A)$ is defined as $\sum_{j=0}^{d-1}\langle j|A|j\rangle$. It can be shown that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ and thus $\mathrm{tr}(UAU^\dagger) = \mathrm{tr}(A)$ holds for linear operators A, B and unitary operator U, meaning that the trace of an operator does not rely on the choice of basis. A density operator ρ in $\mathcal{H}$, is a positive semi-definite operator with trace 1. Applying the spectral decomposition theorem, we could write it as $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$, meaning that it can be regarded as a distribution over pure states. We could also regard pure states $|\phi\rangle$ as rank 1 density matrices $|\phi\rangle\langle\phi|$. We call a positive semi-definite operator with trace no more than 1 a partial density operator.

Quantum Operations. Evolutions on pure quantum states on $\mathcal{H}$ are described by the unitary operators U on $\mathcal{H}$ with $UU^\dagger = U^\dagger U = I$. Given any state $|\phi\rangle$, the evolution of U gives $U|\phi\rangle$. A more general concept of quantum operations is quantum channel, which could be seen as completely-positive and trace-preserving linear maps from the set of density operators in a Hilbert space into another set of density operators in some Hilbert space. For a linear map $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(H)$, we say it is completely positive if for all $\mathcal{H}'$, the map $\mathcal{E} \otimes I$ maps positive semi-definite operators on $\mathcal{H} \otimes \mathcal{H}'$ to positive semi-definite operators, and it is trace-preserving if $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\rho)$ for any density operator ρ.

In this work, we only consider projective measurements. For a projective measurement $\mathcal{M} = \{P_i\}$, we require all the P_i's are projectors, and $\sum_i P_i = I$. Given any density operator ρ, after performing the projective measurement $\mathcal{M} = \{P_i\}$, we will observe the event i with probability $\mathrm{tr}(P_i\rho)$, with the post measured state $P_i\rho P_i/\mathrm{tr}(P_i\rho)$.

An observable, or a quantum predicate, is a positive semi-definite operator on $\mathcal{H}$. For an observable A, its spectral decomposition can be written as $A = \sum \lambda P_\lambda$, where P_λ is the projector onto the eigenspace corresponding to the eigenvalue λ. The expection of A in a state ρ is given by $\sum \lambda\,\mathrm{tr}(P_\lambda\rho) = \mathrm{tr}(A\rho)$.

The notion partial trace is a special quantum operation that discard the state of a system. Formally, for the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, we define partial trace over $\mathcal{H}_1$, written as tr_1 as a mapping from $\mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ to $\mathsf{Pos}(\mathcal{H}_2)$, that satisfies

$$\mathrm{tr}_1(A) = \sum_i (\langle i| \otimes I)A(|i\rangle \otimes I)$$

where $|i\rangle$ ranges over all computational basis of $\mathcal{H}_1$.

For more introductions and explanations of the above notions, we refer the readers to [5].

We now introduce some concepts that are useful in the study of quantum programs.

The Löwner order is a partial order of positive semi-definite operators, defined as follows: for $A, B \in \mathsf{Pos}(\mathcal{H})$, $A \sqsubseteq B$ if and only if $B - A$ is positive semi-definite.

Definition A.1 (Support)**.** *Let $P \in \mathsf{Pos}(\mathcal{H})$ be a positive semi-definite operator. Then, the support of P, denoted as* $\mathrm{supp}(P)$*, is the subspace of $\mathcal{H}$ that are spanned by the eigenvectors of P associated with non-zero eigenvalues.*

Definition A.2. *Let $\mathcal{H}$ be a Hilbert space, X and Y be its subspaces. The join of X and Y is defined as $X \vee Y = \overline{\mathrm{span}\{X \cup Y\}}$, where $\bar{\cdot}$ represents the operation of taking the topological closure. The meet of X and Y is defined as $X \wedge Y = X \cap Y$. The orthogonal complement of X is $X^\perp = \{|\psi\rangle \in \mathcal{H} || \psi\rangle \perp |\phi\rangle, \forall |\phi\rangle \in X\}$.*

Here are some of the properties of the support that are needed for proofs in the subsequent parts.

Proposition A.3 (Properties of the Support)**.** *We have the following properties:*

- *Let $P, Q \in \mathsf{Pos}(\mathcal{H})$, then* $\mathrm{supp}(P + Q) = \mathrm{supp}(P) \vee \mathrm{supp}(Q)$*;*
- *Let X_1 and X_2 be subspaces of a Hilbert space $\mathcal{H}$, then $\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$ for any CP maps $\mathcal{E}$.*

Infinite-valued predicates.

In the following, we introduce the basic notions that are related to the infinite-valued predicates. We first formally define the notion of infinite-valued predicates as follows.

Definition A.4 (Infinite-Valued Predicates)**.** *Given a Hilbert space $\mathcal{H}$, A is called an infinite-valued predicate on $\mathcal{H}$, if it has a unique spectral decomposition $\{(\lambda_i, X_i)\}_i$, where $\lambda_i \in \mathbb{R}^{+\infty}$ are its eigenvalues, X_i's are projections onto eigenspaces that are pairwise orthogonal, with $\sum_i X_i = I$.*

The set of all infinite-valued predicates is denoted as $\mathsf{Pos}^\infty(\mathcal{H})$.

For the arithmetic operations related to the $+\infty$, we make the conventions that $(+\infty)\cdot 0 = 0\cdot(+\infty) = 0$, $(+\infty) + a = a + (+\infty) = +\infty$ for $a \in \mathbb{R}^{+\infty}$, $0/0 = 0$ (this is used in normalization of quantum states, i.e., $\rho = \mathrm{tr}(\rho)(\rho/\mathrm{tr}(\rho))$ even if $\rho = 0$), and $+\infty \leq +\infty$.

The following lemma enables us to represent the infinite-valued predicates as two parts, namely the "finite" and "infinite" part.

Lemma A.5. *For any $A \in \mathsf{Pos}^\infty(\mathcal{H})$, it can be uniquely represented as (P_A, X_A), written $A \triangleq (P_A, X_A)$, where $P_A \in \mathsf{Pos}(\mathcal{H})$, $X_A \in \mathcal{S}(\mathcal{H})$ such that $P_A X_A = 0$, and we will write it as $A = P_A + (+\infty \cdot X_A)$.*

Proof. Suppose $A = \sum_j \lambda_j X_j$. We set $P_A = \sum_{j:\lambda_j<+\infty} \lambda_j X_j$ and $X_A = \sum_{j:\lambda_j=+\infty} X_j$. It is clear that $P_A X_A = 0$. Now we prove the uniqueness. Suppose A could also be written as $P'_A + \infty \cdot X'_A$. We first prove $X_A = X'_A$. If not, there must exist a non-zero vector $|\psi\rangle \in X_A \cap X'^{\perp}_A$, which satisfies $\langle\psi|A|\psi\rangle = \langle\psi|P_A|\psi\rangle + \infty\langle\psi|X_A|\psi\rangle = +\infty$, and $\langle\psi|A|\psi\rangle = \langle\psi|P'_A|\psi\rangle + \infty\langle\psi|X'_A|\psi\rangle = \langle\psi|P'_A|\psi\rangle < +\infty$, a contradiction. Then, we have $P_A = X_A^\perp A X_A^\perp = X_A'^\perp A X_A'^\perp = P'_A$ as we desired. □

Here we introduces some basic operations for infinite-valued predicates:

Definition A.6 (Operations of Infinite-Valued Predicate)**.** *The basic operations of infinite-valued predicates can be defined as follows.*

- *The addition for two infinite-valued predicates A_1, A_2 is:*

$$A_1 + A_2 \triangleq \left(X^\perp \left(P_{A_1} + P_{A_2}\right) X^\perp, X\right),$$

  where $X = X_{A_1} \vee X_{A_2}$.
- *The tensor product for two infinite-valued predicates A_1, A_2 is*

$$A_1 \otimes A_2 \triangleq \left(P_{A_1} \otimes P_{A_2}, X\right),$$

  where $X = (\mathrm{supp}\,(P_{A_1}) \otimes X_{A_2}) \vee (X_{A_1} \otimes \mathrm{supp}\,(P_{A_2})) \vee (X_{A_1} \otimes X_{A_2})$.
- *For any $|\psi\rangle \in \mathcal{H}$ and $A \in \mathsf{Pos}^\infty(\mathcal{H})$ with spectral decomposition $\{(\lambda_i, X_i)\}$, the inner product $\langle\psi|A|\psi\rangle$ is defined as*

$$\langle\psi|A|\psi\rangle \triangleq \sum_i \lambda_i \langle\psi|X_i|\psi\rangle.$$

- *For a density operator $\rho \in \mathcal{D}(\mathcal{H})$, its expectation value on an infinite-valued predicate A is*

$$\mathrm{tr}(A\rho) \triangleq \begin{cases} \mathrm{tr}(P_A\rho), & \text{if } X_A\rho = 0 \\ \infty, & \text{otherwise} \end{cases}$$

- *For subspace X, $X \mid A \triangleq X \cdot A \cdot X + (+\infty \cdot X^\perp)$, or equivalently, $X \mid A \triangleq ((X \vee X_A^\perp) P_A (X \vee X_A^\perp), X^\perp \vee X_A)$.*

Lemma A.7 (Basic Properties of Operations of Infinite-Valued Predicates)**.** *We have the following properties for $A, A_1, A_2 \in \mathsf{Pos}^\infty(\mathcal{H})$:*

- *Scalar product cA for $c \in \mathbb{R}^{+\infty}$ is defined such that for all $|\psi\rangle$, $\langle\psi|cA|\psi\rangle = c\langle\psi|A|\psi\rangle$.*
- *Addition $A_1 + A_2$ such that for all $|\psi\rangle \in \mathcal{H}$, $\langle\psi|(A_1 + A_2)|\psi\rangle = \langle\psi|A_1|\psi\rangle + \langle\psi|A_2|\psi\rangle$.*
- *Tensor product $A_1 \otimes A_2$ such that for all $|\psi_1\rangle, |\psi_2\rangle$, $(\langle\psi_1| \otimes \langle\psi_2|)(A_1 \otimes A_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (\langle\psi_1|A_1|\psi_1\rangle) \cdot (\langle\psi_2|A_2|\psi_2\rangle)$.*
- *Let M be a linear operator with $\mathcal{H}$ as its domain, $M^\dagger A M$ can be defined such that for all $|\psi\rangle$, $\langle\psi|(M^\dagger A M)|\psi\rangle = \langle\phi|A|\phi\rangle$ where $|\phi\rangle = M|\psi\rangle$.*
- *For $P \in \mathsf{Pos}$ with decomposition $P = \sum_i a_i |\psi_i\rangle\langle\psi_i|$ ($0 \leq a_i$), the trace is $\mathrm{tr}(AP) = \sum_i a_i \langle\psi_i|A|\psi_i\rangle$. Note that the value is unique for any decomposition.*
- *For $\mathcal{E} \in \mathcal{QO}$ (more generally, CP maps) with Kraus operators $\{E_i\}$, $\mathcal{E}^\dagger(A) = \sum_i E_i^\dagger A E_i$. Note that it is unique for arbitrary Kraus operators.*
- *$A_1 = A_2$ if for all $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle = \langle\psi|A_2|\psi\rangle$.*

- $A_1 \sqsubseteq A_2$ *if for all* $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle \leq \langle\psi|A_2|\psi\rangle$.

For readability, we postpone the proof of the above lemma to Appendix J.

Lemma A.8 (Algebraic Properties)**.** *In the following, let* $a, b, c \in \mathbb{R}^{+\infty}$, $A, A_1, A_2 \in \mathsf{Pos}^\infty$, $M, M_1, M_2, \cdots \in \mathcal{L}$, *and* $P, P_1, P_2 \cdots \in \mathsf{Pos}$. *We have the following properties:*

- $0A = 0$, $1A = A$, $a(bA) = (ab)A$;
- $0 + A = A + 0 = A$, $A_1 + A_2 = A_2 + A_1$, $A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$;
- $0 \otimes A = A \otimes 0 = 0$, $A_1 \otimes (A_2 \otimes A_3) = (A_1 \otimes A_2) \otimes A_3$;
- $A \otimes (cA_1 + A_2) = c(A \otimes A_1) + (A \otimes A_2)$; $(cA_1 + A_2) \otimes A = c(A_1 \otimes A) + (A_2 \otimes A)$;
- $0^\dagger A 0 = 0$, $M_2^\dagger(M_1^\dagger A M_1)M_2 = (M_1 M_2)^\dagger A (M_1 M_2)$; $M^\dagger(cA_1 + A_2)M = c(M^\dagger A_1 M) + M^\dagger A_2 M$;
- $(M_1 \otimes M_2)^\dagger (A_1 \otimes A_2)(M_1 \otimes M_2) = (M_1^\dagger A_1 M_1) \otimes (M_2^\dagger A_2 M_2)$;
- $\mathrm{tr}(A(cP_1 + P_2)) = c\,\mathrm{tr}(AP_1) + \mathrm{tr}(AP_2)$; $\mathrm{tr}((cA_1 + A_2)P) = c\,\mathrm{tr}(A_1 P) + \mathrm{tr}(A_2 P)$;
- $\mathrm{tr}((A_1 \otimes A_2)(P_1 \otimes P_2)) = \mathrm{tr}(A_1 P_1)\,\mathrm{tr}(A_2 P_2)$; $\mathrm{tr}((M^\dagger A M)P) = \mathrm{tr}(A(MPM^\dagger))$.
- $\mathrm{tr}((A \otimes I)P) = \mathrm{tr}(A\,\mathrm{tr}_2(P))$; $\mathrm{tr}((I \otimes A)P) = \mathrm{tr}(A\,\mathrm{tr}_1(P))$;
- $\mathrm{tr}(A|\phi\rangle\langle\phi|) = \langle\phi|A|\phi\rangle$.
- $A_1 = A_2$ *iff for all* $P \in \mathsf{Pos}$ *(or* $P \in \mathcal{D}$*) such that* $\mathrm{tr}(A_1 P) = \mathrm{tr}(A_2 P)$;
- $A_1 \sqsubseteq A_2$ *iff for all* $P \in \mathsf{Pos}$ *(or* $P \in \mathcal{D}$*) such that* $\mathrm{tr}(A_1 P) \leq \mathrm{tr}(A_2 P)$;
- $A_1 \sqsubseteq A_2$ *implies* $M^\dagger A_1 M \sqsubseteq M^\dagger A_2 M$; $A_1 \sqsubseteq A_2$ *and* $A_3 \sqsubseteq A_4$ *implies* $cA_1 + A_3 \sqsubseteq cA_2 + A_4$.

As direct corollaries, for CP map $\mathcal{E}, \mathcal{E}_1, \mathcal{E}_2$,

- $\mathrm{tr}(A\mathcal{E}(P)) = \mathrm{tr}(\mathcal{E}^\dagger(A)P)$; $A_1 \sqsubseteq A_2$ *implies* $\mathcal{E}(A_1) \sqsubseteq \mathcal{E}(A_2)$;
- $(c\mathcal{E}_1 + \mathcal{E}_2)(A) = c\mathcal{E}_1(A) + \mathcal{E}_2(A)$; $\mathcal{E}(cA_1 + A_2) = c\mathcal{E}(A_1) + \mathcal{E}(A_2)$;
- $\mathcal{E}_2(\mathcal{E}_1(A)) = (\mathcal{E}_2 \circ \mathcal{E}_1)(A)$; $(\mathcal{E}_1 \otimes \mathcal{E}_2)(A_1 \otimes A_2) = \mathcal{E}_1(A_1) \otimes \mathcal{E}_2(A_2)$.

For readability, we postpone the proof of the above lemma to Appendix J.

APPENDIX B
DEFERRED PROOFS IN "QUANTUM COUPLING" SECTION

Theorem B.1 (Theorem III.3)**.** *For any* $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ *and* $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ *with* $\mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$, *for any defect* $\epsilon \in \mathbb{R}^{+\infty}$ *and for any* $X \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, *the following are equivalent:*

1) $\rho_1 X_\epsilon^\# \rho_2$;
2) *For any* $Y_1 \in \mathsf{Pos}(\mathcal{H}_1)$ *and* $Y_2 \in \mathsf{Pos}(\mathcal{H}_2)$ *such that* $X \sqsupseteq Y_1 \otimes I_2 - I_1 \otimes Y_2$, *it holds that*

$$\mathrm{tr}(Y_1\rho_1) \leq \mathrm{tr}(Y_2\rho_2) + \epsilon$$

Proof. If $\epsilon = +\infty$, then both (1) and (2) trivially hold. So we consider the case that $\epsilon \in \mathbb{R}^+$, i.e., ϵ is finite.

- $(1 \implies 2)$. Suppose $\rho_1 X_\epsilon^\# \rho_2$, let $\rho : \langle\rho_1, \rho_2\rangle$ be the witness such that $\mathrm{tr}(X\rho) \leq \epsilon$. Then for any Hermitian Y_1, Y_2, if $X \geq Y_1 \otimes I - I \otimes Y_2$, we have $\mathrm{tr}(Y_1\rho_1) = \mathrm{tr}((Y_1 \otimes I)\rho) \leq \mathrm{tr}((X + I \otimes Y_2)\rho) \leq \mathrm{tr}((I \otimes Y_2)\rho) + \epsilon = \mathrm{tr}(Y_2\rho_2) + \epsilon$, where the second last step uses the assumption.
- $(2 \implies 1)$. In this part of the proof, we write $\langle A, B\rangle$ to mean the Hilbert-Schmidt inner product $\langle A, B\rangle \triangleq \mathrm{tr}(A^\dagger B)$. The original proof [8] considers a semi-definite program (Φ, A, B). The primal formulation is that of maximising $\langle A, Z\rangle$, subject to $\Phi(Z) = B, Z \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, and the dual one is that of minimising $\langle B, Y\rangle$ subject to $\Phi^\dagger(Y) \geq A, Y \in \mathsf{Herm}(\mathcal{H}_1 \oplus \mathcal{H}_2)$, where:

$$A = I - X, B = \begin{pmatrix} \rho_1 & \\ & \rho_2 \end{pmatrix}$$
$$\Phi(Z) = \begin{pmatrix} \mathrm{tr}_2(Z) & \\ & \mathrm{tr}_1(Z) \end{pmatrix}$$
$$\Phi^\dagger(Y) = \Phi^\dagger \begin{pmatrix} Y_1 & \cdot \\ \cdot & Y_2 \end{pmatrix} = Y_1 \otimes I_2 + I_1 \otimes Y_2$$

The above formulation can be shown to satisfy strong duality, meaning that the optima for the primal and dual problems exist and are equal.

Then, let us consider for all Hermitians $Y_1 \in \mathsf{Herm}(\mathcal{H}_1)$, $Y_2 \in \mathsf{Herm}(\mathcal{H}_2)$ satisfying $Y_1 \otimes I_2 + I_1 \otimes Y_2 \geq I - X$, observe that

$$\begin{aligned}\langle B, Y\rangle &= \mathrm{tr}(Y_1\rho_1 + Y_2\rho_2) \\ &= \mathrm{tr}(Y_2'\rho_2) - \mathrm{tr}(Y_1'\rho_1) + \mathrm{tr}(\rho_1) \\ &\geq \mathrm{tr}(\rho_1) - \epsilon\end{aligned}$$

where $Y_2' = Y_2 + nI$, $Y_1' = (n+1)I - Y_1$ with sufficiently large $n \in \mathbb{R}^+$ (e.g., bigger than all singular values of Y_1 and Y_2) such that Y_2' and Y_1' are both positive. The second line is derived by using the assumption $\mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$. By condition (2) since $Y_1' \otimes I_2 - I_1 \otimes Y_2' = I - (Y_1 \otimes I_2 + I_1 \otimes Y_2) \sqsubseteq I - (I - X) = X$, we have $\mathrm{tr}(Y_2'\rho_2) - \mathrm{tr}(Y_1'\rho_1) \geq -\epsilon$, and this leads to third line.

By strong duality, we have $\langle I - X, Z_{\max}\rangle \geq \mathrm{tr}(\rho_1) - \epsilon$, or equivalently, $\mathrm{tr}(Z_{\max}) - \mathrm{tr}(XZ_{\max}) \geq \mathrm{tr}(\rho_1) - \epsilon$. Since $\mathrm{tr}(Z_{\max}) = \mathrm{tr}(\rho_1)$, we have $\mathrm{tr}(XZ_{\max}) \leq \epsilon$, which says that $Z_{\max}$ is a witness of the lifting $\rho_1 X_\epsilon^\# \rho_2$.

□

Lemma B.2 (Lemma III.4)**.** *Let* $\rho : \langle \rho_1, \rho_2\rangle$*. Then,* $\mathrm{tr}(\rho) = \mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2)$.

Proof. This is direct by noting $\mathrm{tr}(\rho) = \mathrm{tr}(\mathrm{tr}_1(\rho)) = \mathrm{tr}(\rho_1) = \mathrm{tr}(\mathrm{tr}_2(\rho)) = \mathrm{tr}(\rho_2)$. □

Before proving the relationship between $\star$-coupling and partial coupling and its variant of Strassen's theorem, i.e., Proposition B.3 and Theorem B.5, we first introduce some useful definitions:

- For any Hilbert space $\mathcal{H}$, we additionally extend it to $\mathcal{H}^\star$ with one-dimension denoted by $|\star\rangle$. Let $P_\star = |\star\rangle\langle\star|$ the projection of $\star$ space and $P_\star^\perp = I_\star - P_\star$ the projection to original space. (To avoid ambiguity, we write $I_\star$ for the identity of $\mathcal{H}^\star$.)
- For any $\rho \in \mathcal{D}(\mathcal{H})$, we define the star-extension $\rho^\star \triangleq (1 - \mathrm{tr}(\rho))|\star\rangle\langle\star| + \rho \in \mathcal{D}^1(\mathcal{H}^\star)$. Obviously, $P_\star^\perp \rho^\star P_\star^\perp = \rho$.
- For $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$, we say $\rho \in \mathcal{D}(\mathcal{H}_1^\star \otimes \mathcal{H}_2^\star)$ is a $\star$-coupling of ρ_1 and ρ_2, written $\rho : \langle \rho_1, \rho_2\rangle_\star$, if $\rho : \langle \rho_1^\star, \rho_2^\star\rangle$.
- For any $A \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, we define $A^\star \in \mathsf{Pos}(\mathcal{H}_1^\star \otimes \mathcal{H}_2^\star)$ as the embedding of A.
- For $\rho \in \mathcal{D}(\mathcal{H}_1^\star \otimes \mathcal{H}_2^\star)$, we define the projection:

$$\Pi_\star^\perp(\rho) = (P_\star^\perp \otimes P_\star^\perp)\rho(P_\star^\perp \otimes P_\star^\perp) \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

- For any $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that $\rho : \langle \rho_1, \rho_2\rangle_p$, define

$$\begin{aligned}\rho^\uparrow =& (1 + \mathrm{tr}(\rho) - \mathrm{tr}(\rho_1) - \mathrm{tr}(\rho_2))|\star\star\rangle\langle\star\star| + \\ & (\rho_1 - \mathrm{tr}_2(\rho)) \otimes |\star\rangle\langle\star| + |\star\rangle\langle\star| \otimes (\rho_2 - \mathrm{tr}_1(\rho)) + \rho.\end{aligned}$$

Proposition B.3 (Relation to $\star$-coupling)**.** *For given* $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$*,* $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ *and* $A \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$*, we claim that:*

1) *Any $\star$-coupling provide a partial-coupling, i.e.,* $\Pi_\star^\perp(\rho) : \langle \rho_1, \rho_2\rangle_p$ *if* $\rho : \langle \rho_1, \rho_2\rangle_\star$*.*
2) *We can construct $\star$-coupling from a partial-coupling, i.e.,* $\rho^\uparrow : \langle \rho_1, \rho_2\rangle_\star$ *if* $\rho : \langle \rho_1, \rho_2\rangle_p$*. In fact,* $\Pi_\star^\perp(\rho^\uparrow) = \rho$*.*
3) *If* $\rho : \langle \rho_1, \rho_2\rangle_\star$*,* $\mathrm{tr}(A^\star\rho) = \mathrm{tr}(A\Pi_\star^\perp(\rho))$*. As a consequence, if* $\rho : \langle \rho_1, \rho_2\rangle_p$*, then* $\mathrm{tr}(A^\star\rho^\uparrow) = \mathrm{tr}(A\rho)$*.*

Proof. (1). Suppose $\rho : \langle \rho_1, \rho_2\rangle_\star$. Compute

$$\begin{aligned}\mathrm{tr}_2(\Pi_\star^\perp(\rho)) &= \mathrm{tr}_2((P_\star^\perp \otimes P_\star^\perp)\rho(P_\star^\perp \otimes P_\star^\perp)) \\ &= P_\star^\perp \mathrm{tr}_2((I_\star \otimes P_\star^\perp)\rho(I_\star \otimes P_\star^\perp))P_\star^\perp \\ &\sqsubseteq P_\star^\perp \mathrm{tr}_2(\rho)P_\star^\perp \\ &= P_\star^\perp \rho_1^\star P_\star^\perp \\ &= \rho_1\end{aligned}$$

where we use the fact that $\mathrm{tr}_2(\rho) = \mathrm{tr}_2((I_\star \otimes P_\star)\rho(I_\star \otimes P_\star) + (I_\star \otimes P_\star^\perp)\rho(I_\star \otimes P_\star^\perp))$. Similarly, $\mathrm{tr}_2(\Pi_\star^\perp(\rho)) \sqsubseteq \rho_2$. Furthermore, observe that

$$\begin{aligned}\mathrm{tr}(\rho) =& \mathrm{tr}((P_\star \otimes P_\star)\rho(P_\star \otimes P_\star)) + \mathrm{tr}((I_\star \otimes P_\star^\perp)\rho(I_\star \otimes P_\star^\perp)) + \\ & \mathrm{tr}((P_\star^\perp \otimes I_\star)\rho(P_\star^\perp \otimes I_\star)) - \mathrm{tr}((P_\star^\perp \otimes P_\star^\perp)\rho(P_\star^\perp \otimes P_\star^\perp)) \\ =& \mathrm{tr}((P_\star \otimes P_\star)\rho(P_\star \otimes P_\star)) + \mathrm{tr}(\rho_2) + \mathrm{tr}(\rho_1) - \mathrm{tr}(\Pi_\star^\perp(\rho))\end{aligned}$$

Note that $\mathrm{tr}(\rho) = 1$, $0 \leq \mathrm{tr}((P_\star \otimes P_\star)\rho(P_\star \otimes P_\star))$, we have $\mathrm{tr}(\rho_1) + \mathrm{tr}(\rho_2) \leq 1 + \mathrm{tr}(\Pi_\star^\perp(\rho))$.

All above implies that $\Pi_\star^\perp(\rho) : \langle \rho_1, \rho_2\rangle_p$.

(2). Suppose $\rho : \langle \rho_1, \rho_2\rangle_p$. It is straightforward that :

$$\begin{aligned}\mathrm{tr}_2(\rho^\uparrow) =& (1 + \mathrm{tr}(\rho) - \mathrm{tr}(\rho_1) - \mathrm{tr}(\rho_2))|\star\rangle\langle\star| + \\ & (\rho_1 - \mathrm{tr}_2(\rho)) + \mathrm{tr}(\rho_2 - \mathrm{tr}_1(\rho))|\star\rangle\langle\star| + \mathrm{tr}_2(\rho) \\ =& (1 - \mathrm{tr}(\rho_1))|\star\rangle\langle\star| + \rho_1 \\ =& \rho_1^\star.\end{aligned}$$

Similarly, $\mathrm{tr}_1(\rho^\uparrow) = \rho_2^\star$. Thus, $\rho^\uparrow : \langle \rho_1^\star, \rho_2^\star \rangle$, or equivalently, $\rho^\uparrow : \langle \rho_1, \rho_2 \rangle_\star$. $\Pi_\star^\perp(\rho^\uparrow) = \rho$ is trivial by computation.
(3). Note that, $A^\star$ is preserved under the projection $P_\star^\perp \otimes P_\star^\perp$, so :

$$\begin{aligned}\mathrm{tr}(A^\star \rho) &= \mathrm{tr}(A^\star (P_\star^\perp \otimes P_\star^\perp)\rho(P_\star^\perp \otimes P_\star^\perp))) \\ &= \mathrm{tr}(A\Pi_\star^\perp(\rho)).\end{aligned}$$

□

Proposition B.4 ((Sub-)convex Combination of Partial Coupling)**.** *Let $\{\lambda_i\}_{i\in I}$ be a subdistribution over index set I (i.e., $0 \le \lambda_i \le 1$ for all i, and $\sum_i \lambda_i \le 1$), and $\rho_i \in \mathcal{D}(\mathcal{H}_1)$, $\sigma_i \in \mathcal{D}(\mathcal{H}_2)$, and partial couplings $\delta_i : \langle \rho_i, \sigma_i \rangle_p$ with indices from I. Then*

$$\sum_i \lambda_i \delta_i : \Big\langle \sum_i \lambda_i \rho_i, \sum_i \lambda_i \sigma_i \Big\rangle_p.$$

As an corollary, for any $\rho \in \mathcal{D}(\mathcal{H}_1)$, $\sigma \in \mathcal{D}(\mathcal{H}_2)$ and $0 \le c \le 1$, if $\delta : \langle \rho, \sigma \rangle_p$, then $c\delta : \langle c\rho, c\sigma \rangle_p$.

Proof. First observe:

$$\begin{aligned}\mathrm{tr}_2\Big(\sum_i \lambda_i \delta_i\Big) &= \sum_i \lambda_i \,\mathrm{tr}_2(\delta_i) \sqsubseteq \sum_i \lambda_i \rho_i; \\ \mathrm{tr}_1\Big(\sum_i \lambda_i \delta_i\Big) &= \sum_i \lambda_i \,\mathrm{tr}_1(\delta_i) \sqsubseteq \sum_i \lambda_i \sigma_i.\end{aligned}$$

Further notice that,

$$\begin{aligned}\mathrm{tr}\Big(\sum_i \lambda_i \rho_i\Big) + \mathrm{tr}\Big(\sum_i \lambda_i \sigma_i\Big) &= \sum_i \lambda_i (\mathrm{tr}(\rho_i) + \mathrm{tr}(\sigma_i)) \\ &\le \sum_i \lambda_i (1 + \mathrm{tr}(\delta_i)) = \sum_i \lambda_i + \mathrm{tr}\Big(\sum_i \lambda_i \delta_i\Big) \\ &\le 1 + \mathrm{tr}\Big(\sum_i \lambda_i \delta_i\Big)\end{aligned}$$

as $\{\lambda_i\}_{i\in I}$ is a subdistribution. This completes the proof.

□

Theorem B.5 (Quantum Strassen's Theorem for Partial Coupling)**.** *For any $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$, $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$, $A \in \mathsf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ and $\epsilon \in \mathbb{R}^{+\infty}$, the following are equivalent:*

1) *There exists partial-coupling $\rho : \langle \rho_1, \rho_2 \rangle_p$ such that $\mathrm{tr}(A\rho) \le \epsilon$;*
2) *For any $y_1, y_2 \in \mathbb{R}^+$, $Y_1 \in \mathsf{Pos}(\mathcal{H}_1), Y_2 \in \mathsf{Pos}(\mathcal{H}_2)$, such that $y_1 \le y_2$, $Y_1 \le y_2 I_1$, $y_1 I_2 \le Y_2$ and $A \sqsupseteq Y_1 \otimes I_2 - I_1 \otimes Y_2$, it holds that:*

$$y_1(1 - \mathrm{tr}(\rho_1)) + \mathrm{tr}(Y_1\rho_1) \le y_2(1 - \mathrm{tr}(\rho_2)) + \mathrm{tr}(Y_2\rho_2) + \epsilon.$$

Proof. If $\epsilon = +\infty$, then both (1) and (2) trivially hold. So we consider the case that $\epsilon \in \mathbb{R}^+$, i.e., ϵ is finite. We first introduce the following condition:

3) There exists star-coupling $\rho : \langle \rho_1, \rho_2 \rangle_\star$, i.e., $\rho : \langle \rho_1^\star, \rho_2^\star \rangle$, such that $\mathrm{tr}(A^\star \rho) \le \epsilon$.

• (1 $\Rightarrow$ 3). Let ρ be the witness of (1), then $\rho^\uparrow : \langle \rho_1, \rho_2 \rangle_\star$ by Lemma B.3(2). According to Lemma B.3(3), $\mathrm{tr}(A^\star \rho^\uparrow) = \mathrm{tr}(A\rho) \le \epsilon$.
• (3 $\Rightarrow$ 1). Let ρ be the witness of (3), then $\Pi_\star^\perp(\rho) : \langle \rho_1, \rho_2 \rangle_p$ by Lemma B.3(1). According to Lemma B.3(3), $\mathrm{tr}(A\Pi_\star^\perp(\rho)) = \mathrm{tr}(A^\star \rho) \le \epsilon$.

Thus, (1) is equivalent to (3). (3) says that, $\rho_1^\star A_\epsilon^{\star\#} \rho_2^\star$, then by Theorem III.3, it is then equivalent to:

4) For any $Z_1 \in \mathsf{Pos}(\mathcal{H}_1^\star)$ and $Z_2 \in \mathsf{Pos}(\mathcal{H}_2^\star)$ such that $A^\star \sqsupseteq Z_1 \otimes I_{2^\star} - I_{1^\star} \otimes Z_2$, it holds that

$$\mathrm{tr}(Z_1 \rho_1^\star) \le \mathrm{tr}(Z_2 \rho_2^\star) + \epsilon.$$

What remaining to be shown is (2) equivalent to (4).

• (4 ⇒ 2). Set $Z_1 = y_1|\star\rangle\langle\star| + Y_1$ and $Z_2 = y_2|\star\rangle\langle\star| + Y_2$. Obviously, $Z_1 \in \mathsf{Pos}(\mathcal{H}_1^\star)$ and $Z_2 \in \mathsf{Pos}(\mathcal{H}_2^\star)$. Observe that:

$$\begin{aligned}
&A^\star - (Z_1 \otimes I_{2^\star} - I_{1^\star} \otimes Z_2) \\
&= A - (y_1|\star\rangle\langle\star| + Y_1) \otimes (|\star\rangle\langle\star| + I_2) \\
&\quad + (|\star\rangle\langle\star| + I_1) \otimes (y_2|\star\rangle\langle\star| + Y_2) \\
&= (A - (Y_1 \otimes I_2 - I_1 \otimes Y_2)) + (y_2 - y_1)|\star\star\rangle\langle\star\star| \\
&\quad + (y_2 I_1 - Y_1) \otimes |\star\rangle\langle\star| + |\star\rangle\langle\star| \otimes (Y_2 - y_1 I_2) \\
&\sqsupseteq 0.
\end{aligned}$$

So, $\operatorname{tr}(Z_1\rho_1^\star) \leq \operatorname{tr}(Z_2\rho_2^\star) + \epsilon$, or equivalently,

$$y_1(1 - \operatorname{tr}(\rho_1)) + \operatorname{tr}(Y_1\rho_1) \leq y_2(1 - \operatorname{tr}(\rho_2)) + \operatorname{tr}(Y_2\rho_2) + \epsilon.$$

• (2 ⇒ 4). For any $Z_1 \in \mathsf{Pos}(\mathcal{H}_1^\star)$ and $Z_2 \in \mathsf{Pos}(\mathcal{H}_2^\star)$ such that $A^\star \sqsupseteq Z_1 \otimes I_{2^\star} - I_{1^\star} \otimes Z_2$, by projecting it to $P_\star \otimes P_\star$, $P_\star^\perp \otimes P_\star$, $P_\star \otimes P_\star^\perp$ and $P_\star^\perp \otimes P_\star^\perp$, the Löwner preserves, and thus:

$$\begin{gathered}
y_1 - y_2 \leq 0 \qquad y_1 I_2 - Y_2 \sqsubseteq 0 \qquad Y_1 - y_2 I_1 \sqsubseteq 0 \\
Y_1 \otimes I_2 - I_1 \otimes Y_2 \sqsubseteq A
\end{gathered}$$

where $Z_1 = \left(\begin{smallmatrix} y_1 & \vdots \\ \cdots & Y_1 \end{smallmatrix}\right)$ and $Z_2 = \left(\begin{smallmatrix} y_2 & \vdots \\ \cdots & Y_2 \end{smallmatrix}\right)$. Furthermore, observe that

$$\begin{aligned}
&\operatorname{tr}(Z_1\rho_1^\star) - \operatorname{tr}(Z_2\rho_2^\star) \\
&= y_1(1 - \operatorname{tr}(\rho_1)) + \operatorname{tr}(Y_1\rho_1) - (y_2(1 - \operatorname{tr}(\rho_2)) + \operatorname{tr}(Y_2\rho_2)) \\
&\leq \epsilon
\end{aligned}$$

by employing (2), and this completes the proof. □

APPENDIX C
DEFERRED PROOFS IN "QUANTUM OPTIMAL TRANSPORT" SECTION

Proposition C.1. *Given $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ where $\mathcal{H}_1$ and $\mathcal{H}_2$ are finite-dimensional Hilbert spaces, the set of partial couplings $S = \{\rho \mid \rho : \langle\rho_1, \rho_2\rangle_p\}$ is a non-empty, closed and convex set.*

Proof. For non-emptiness, given $\rho_1 \in \mathcal{D}(\mathcal{H})_1$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_\epsilon)$. We claim $\rho = \rho_1 \otimes \rho_2 \in S$. It is direct to see that $\operatorname{tr}_2(\rho) \sqsubseteq \rho_1$ and $\operatorname{tr}_1(\rho) \sqsubseteq \rho_2$. For the trace constraint, notice that $\operatorname{tr}(\rho) = \operatorname{tr}(\rho_1)\operatorname{tr}(\rho_2)$, $\operatorname{tr}(\rho_1) \leq 1$, and $\operatorname{tr}(\rho_2) \leq 1$, we have $(1 - \operatorname{tr}(\rho_1))(1 - \operatorname{tr}(\rho_2)) \geq$, meaning that $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \operatorname{tr}(\rho)$ as we want.

For closeness, given $\rho^i \to \rho$ with $\rho^i \in S$, we show that $\rho \in S$. By definition, we know $\operatorname{tr}_2(\rho^i) \sqsubseteq \rho_1$, or equivalently, for any $\sigma \in \mathcal{D}(\mathcal{H}_1)$, $\operatorname{tr}(\rho_i\sigma \otimes I) \leq \operatorname{tr}(\rho_1\sigma)$. Fixed σ, the function $\operatorname{tr}((\sigma \otimes I)\cdot)$ is linear and continuous. Therefore, by $\rho^i \to \rho$ we know $\operatorname{tr}(\operatorname{tr}_2(\rho)\sigma) \leq \operatorname{tr}(\rho_1\sigma)$. Since the above inequality holds for any $\sigma \in \mathcal{D}(\mathcal{H})$, we conclude that $\operatorname{tr}_2(\rho) \sqsubseteq \rho_1$. Similarly we can prove $\operatorname{tr}_1(\rho) \sqsubseteq \rho_2$. By the continuity of the trace function, we can also conclude $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \operatorname{tr}(\rho)$. Therefore we have $\rho \in S$.

For convexity, suppose $\sigma_1, \sigma_2 \in S$ and $\lambda \in (0, 1)$. Consider $\rho = \lambda\sigma_1 + (1 - \lambda)\sigma_2$. From $\operatorname{tr}_2(\sigma_1) \sqsubseteq \rho_1$ and $\operatorname{tr}_2(\sigma_2) \sqsubseteq \rho_1$, we know $\lambda \operatorname{tr}_2(\sigma_1) + (1 - \lambda)\operatorname{tr}_2(\sigma_2) \sqsubseteq \lambda\rho_1 + (1 - \lambda)\rho_1$. Simplifying above, we get $\operatorname{tr}_2(\rho) \sqsubseteq \rho_1$. Similarly we have $\operatorname{tr}_1(\rho) \sqsubseteq \rho_2$. From $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \operatorname{tr}(\sigma_1)$ and $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \operatorname{tr}(\sigma_2)$, we get $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \lambda \operatorname{tr}(\sigma_1) + (1 - \lambda)\operatorname{tr}(\sigma_2)$, meaning $\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1 + \operatorname{tr}(\rho)$ and $\rho \in S$ as we desired. □

Proposition C.2 (Jointly Convexity of QOT)**.** *Let $\{\lambda_i\}_{i\in I}$ be a subdistribution over index set I, and $\rho_i \in \mathcal{D}(\mathcal{H}_1)$, $\sigma_i \in \mathcal{D}(\mathcal{H}_2)$ with indices from I. For any cost function C, It holds that:*

$$T_C\Big(\sum_i \lambda_i\rho_i, \sum_i \lambda_i\sigma_i\Big) \leq \sum_i \lambda_i T_C(\rho_i, \sigma_i).$$

As a corollary, if $\{\lambda_i\}_{i\in I}$ is a distribution and $\sigma \in \mathcal{D}(\mathcal{H}_2)$, then $T_C\big(\sum_i \lambda_i\rho_i, \sigma\big) \leq \sum_i \lambda_i T_C(\rho_i, \sigma)$.

Proof. Select $\delta_i : \langle\rho_i, \sigma_i\rangle_p$ such that $T_C(\rho_i, \sigma_i) = \operatorname{tr}(C\delta_i)$. By Proposition B.4, $\sum_i \lambda_i\delta_i : \big\langle \sum_i \lambda_i\rho_i, \sum_i \lambda_i\sigma_i \big\rangle_p$, so

$$T_C\Big(\sum_i \lambda_i\rho_i, \sum_i \lambda_i\sigma_i\Big) \leq \operatorname{tr}\Big(C\sum_i \lambda_i\delta_i\Big) = \sum_i \lambda_i \operatorname{tr}(C\delta_i) = \sum_i \lambda_i T_C(\rho_i, \sigma).$$

□

The following lemma demonstrates that for contractivity it suffices to consider only density operators, which appears useful in the following proofs.

Lemma C.3 (Lemma IV.3)**.** *Given two quantum operations $\mathcal{E}_1 \in \mathcal{QO}(\mathcal{H}_1), \mathcal{E}_2 \in \mathcal{QO}(\mathcal{H}_2)$, input and output costs , the following statement are equivalent:*

1) *$(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o;*
2) *For all $\rho_1 \in \mathcal{D}^1(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_2)$,*

$$T_{C_o}(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq T_{C_i}(\rho_1, \rho_2).$$

Proof. (1 $\Rightarrow$ 2) is trivial. For (2 $\Rightarrow$ 1), by definition, it is sufficient to show that, for all $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$, $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ and $\rho : \langle \rho_1, \rho_2 \rangle_p$, there exists $\sigma : \langle \mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2) \rangle_p$ such that :

$$\operatorname{tr}(C_o\sigma) \leq \operatorname{tr}(C_i\sigma).$$

Since ρ is a partial coupling, then $\rho_1' \triangleq \operatorname{tr}_2(\rho) \sqsubseteq \rho_1$, $\rho_2' \triangleq \operatorname{tr}_1(\rho) \sqsubseteq \rho_2$, $1 + \operatorname{tr}(\rho) \geq \operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2)$. Set $\operatorname{tr}(\rho) = c$. If $c = 0$, then $\operatorname{tr}(\mathcal{E}_1(\rho_1)) + \operatorname{tr}(\mathcal{E}_2(\rho_2)) \leq \operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2) \leq 1$, thus $0 : \langle \mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2) \rangle_p$, and obviously $\operatorname{tr}(C_i\rho) = \operatorname{tr}(C_o 0) = 0$. If $c > 0$, by taking ρ_1'/c and ρ_2'/c in (2), there must exist a partial coupling

$$\sigma : \langle \mathcal{E}_1(\rho_1'/c), \mathcal{E}_1(\rho_2'/c) \rangle_p$$

such that $\operatorname{tr}(C_i(\rho/c)) \geq \operatorname{tr}(C_o\sigma)$. By Proposition B.4, $c\sigma : \langle \rho_1', \rho_2' \rangle_p$, and $\operatorname{tr}(C_i\rho) \geq \operatorname{tr}(C_o(c\sigma))$, so it is sufficient to show $c\sigma : \langle \mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2) \rangle_p$. First observe that,

$$\operatorname{tr}_2(c\sigma) = c \operatorname{tr}(\sigma) \sqsubseteq c\mathcal{E}_1(\rho_1'/c) = \mathcal{E}_1(\rho_1') \sqsubseteq \mathcal{E}_1(\rho_1)$$

and similarly, $\operatorname{tr}_1(c\sigma) \sqsubseteq \mathcal{E}_2(\rho_2)$. On the other hand,

$$\begin{aligned} 1 + \operatorname{tr}(c\sigma) &= 1 - c + c(1 + \operatorname{tr}(\sigma)) \\ &\geq 1 - c + c(\operatorname{tr}(\mathcal{E}_1(\rho_1'/c)) + \operatorname{tr}(\mathcal{E}_2(\rho_2'/c))) \\ &= 1 - c + (\operatorname{tr}(\mathcal{E}_1(\rho_1')) + \operatorname{tr}(\mathcal{E}_2(\rho_2'))). \end{aligned}$$

Notice that $\operatorname{tr}(\rho_1 - \rho_1') \geq \operatorname{tr}(\mathcal{E}_1(\rho_1 - \rho_1'))$ since $\rho_1' \sqsubseteq \rho_1$ and $\mathcal{E}_1$ is a quantum operation, and similarly holds for ρ_2, ρ_2', we get:

$$\begin{aligned} & \operatorname{tr}(\mathcal{E}_1(\rho_1')) + \operatorname{tr}(\mathcal{E}_2(\rho_2')) \\ \geq\ & \operatorname{tr}(\mathcal{E}_1(\rho_1)) + \operatorname{tr}(\mathcal{E}_2(\rho_2)) - (\operatorname{tr}(\rho_1) + \operatorname{tr}(\rho_2)) \\ & + \operatorname{tr}(\rho_1') + \operatorname{tr}(\rho_2') \\ \geq\ & \operatorname{tr}(\mathcal{E}_1(\rho_1)) + \operatorname{tr}(\mathcal{E}_2(\rho_2)) - (1 + \operatorname{tr}(\rho)) + 2\operatorname{tr}(\rho) \\ =\ & \operatorname{tr}(\mathcal{E}_1(\rho_1)) + \operatorname{tr}(\mathcal{E}_2(\rho_2)) - 1 + c \end{aligned}$$

Combine these two inequalities, we obtain:

$$1 + \operatorname{tr}(c\sigma) \geq \operatorname{tr}(\mathcal{E}_1(\rho_1)) + \operatorname{tr}(\mathcal{E}_2(\rho_2)),$$

which completes the proof. □

Lemma C.4 (Lemma IV.4)**.** *Suppose $\mathcal{E}_1 \in \mathcal{QC}(\mathcal{H}_1), \mathcal{E}_2 \in \mathcal{QC}(\mathcal{H}_2)$ are two quantum channels. Then $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o if and only if for every $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, there exists a coupling $\sigma : \langle \mathcal{E}_1(\operatorname{tr}_2(\rho)), \mathcal{E}_2(\operatorname{tr}_1(\rho)) \rangle$ such that*

$$\operatorname{tr}(C_i\rho) \geq \operatorname{tr}(C_o\sigma).$$

Proof. (if) part. For all $\rho_1 \in \mathcal{D}^1(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_2)$, set $\rho : \langle \rho_1, \rho_2 \rangle$ which obtains $\operatorname{tr}(C_i\rho) = T_{C_i}(\rho_1, \rho_2)$. Then by assumption, there exists a coupling $\sigma : \langle \mathcal{E}_1(\operatorname{tr}_2(\rho)), \mathcal{E}_2(\operatorname{tr}_1(\rho)) \rangle$ (i.e., $\sigma : \langle \mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2) \rangle$) such that:

$$T_{C_o}(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq \operatorname{tr}(C_o\sigma) \leq \operatorname{tr}(C_i\rho) = T_{C_i}(\rho_1, \rho_2).$$

Then by Lemma IV.3 we finish this part.

(only if) part. Since coupling is preserved under scaling, and by Lemma A.8, we only need to focus on $\rho \in \mathcal{D}^1(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Choose $\sigma : \langle \mathcal{E}_1(\operatorname{tr}_2(\rho)), \mathcal{E}_2(\operatorname{tr}_1(\rho)) \rangle$ which $\operatorname{tr}(C_o\sigma) = T_{C_o}(\mathcal{E}_1(\operatorname{tr}_2(\rho)), \mathcal{E}_2(\operatorname{tr}_1(\rho)))$. By assumption, we have:

$$\operatorname{tr}(C_o\sigma) = T_{C_o}(\mathcal{E}_1(\operatorname{tr}_2(\rho)), \mathcal{E}_2(\operatorname{tr}_1(\rho))) \leq T_{C_i}(\operatorname{tr}_2(\rho), \operatorname{tr}_1(\rho)) \leq \operatorname{tr}(C_i\rho).$$

□

Proposition C.5 (Proposition IV.5)**.** *The contractivity satisfies several desired properties for data processing:*

1) *Backward. $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. $(\mathcal{E}_1^\dagger \otimes \mathcal{E}_2^\dagger)(C)$ and C. Here, $\mathcal{E}^\dagger$ is the dual of $\mathcal{E}$, which satisfies $\operatorname{tr}(A\mathcal{E}(B)) = \operatorname{tr}(\mathcal{E}^\dagger(A)B)$ for all linear operator A, B.*

2) *Consequence. Suppose $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i' and C_o', and $C_i' \sqsubseteq C_i$, $C_o \sqsubseteq C_o'$, then $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o.*
3) *Sequential composition. Suppose $(\mathcal{E}_1, \mathcal{E}_1')$ is contractive w.r.t. C_i and C_m, and $(\mathcal{E}_2, \mathcal{E}_2')$ is contractive w.r.t. C_m and C_o, then $(\mathcal{E}_2 \circ \mathcal{E}_1, \mathcal{E}_2' \circ \mathcal{E}_1')$ is contractive w.r.t. C_i and C_o.*

For any super-operator $\mathcal{E}$, its dual $\mathcal{E}^\dagger$ is another super-operator. Whenever $\mathcal{E}$ is a quantum operation with Kraus operator $\{E_i\}$, then $\mathcal{E}^\dagger$ has Kraus representation $\{E_i^\dagger\}$. $\circ$ is the composition of two quantum operations, i.e., for all ρ, $(\mathcal{E}_1 \circ \mathcal{E}_2)(\rho) \triangleq \mathcal{E}_1(\mathcal{E}_2(\rho))$.

Proof. (1) By Lemma IV.3, for any $\rho \in \mathcal{D}^1(\mathcal{H}_1 \otimes \mathcal{H}_2)$, set $\sigma = (\mathcal{E}_1 \otimes \mathcal{E}_2)(\rho)$. By the property of dual map, we have:

$$\mathrm{tr}((\mathcal{E}_1^\dagger \otimes \mathcal{E}_2^\dagger)(C)\rho) = \mathrm{tr}(C(\mathcal{E}_1 \otimes \mathcal{E}_2)(\rho)) = \mathrm{tr}(C\sigma).$$

It is then sufficient to show that $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1(\rho))\rangle_p$, which is completed by noticing that:

$$\begin{aligned}
\mathrm{tr}_2(\sigma) &= \mathrm{tr}_2((\mathcal{E}_1 \otimes \mathcal{E}_2)(\rho)) \sqsubseteq \mathcal{E}_1(\mathrm{tr}_2(\rho)),\\
\mathrm{tr}_1(\sigma) &= \mathrm{tr}_1((\mathcal{E}_1 \otimes \mathcal{E}_2)(\rho)) \sqsubseteq \mathcal{E}_2(\mathrm{tr}_1(\rho)),\\
1 + \mathrm{tr}(\sigma) &= \mathrm{tr}(\rho) + \mathrm{tr}((I \otimes I)(\mathcal{E}_1 \otimes \mathcal{E}_2)(\rho))\\
&= \mathrm{tr}((I \otimes I + \mathcal{E}_1^\dagger(I) \otimes \mathcal{E}_2^\dagger(I))\rho)\\
&\geq \mathrm{tr}((\mathcal{E}_1^\dagger(I) \otimes I + I \otimes \mathcal{E}_2^\dagger(I))\rho)\\
&= \mathrm{tr}(\mathcal{E}_1^\dagger(I)\,\mathrm{tr}_2(\rho)) + \mathrm{tr}(\mathcal{E}_2^\dagger(I)\,\mathrm{tr}_1(\rho))\\
&= \mathrm{tr}(\mathcal{E}_1(\mathrm{tr}_2(\rho))) + \mathrm{tr}(\mathcal{E}_2(\mathrm{tr}_1(\rho))).
\end{aligned}$$

First two hold since $\mathcal{E}_1$ and $\mathcal{E}_2$ are quantum operations, and furthermore, $\mathcal{E}_1^\dagger(I) \sqsubseteq I$ and $\mathcal{E}_2^\dagger(I) \sqsubseteq I$, thus, $0 \sqsubseteq (I - \mathcal{E}_1^\dagger(I)) \otimes (I - \mathcal{E}_2^\dagger(I))$ which then leads to the inequality of fifth line.

(2) By Lemma IV.3, for any $\rho \in \mathcal{D}^1(\mathcal{H}_1 \otimes \mathcal{H}_2)$, by assumption, there exists $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1(\rho))\rangle_p$ such that $\mathrm{tr}(C_i'\rho) \geq \mathrm{tr}(C_o'\sigma)$. Thus,

$$\mathrm{tr}(C_i\rho) \geq \mathrm{tr}(C_i'\rho) \geq \mathrm{tr}(C_o'\sigma) \geq \mathrm{tr}(C_o\sigma).$$

(3) For any ρ_1 and ρ_1', and any partial coupling $\rho : \langle \rho_1, \rho_1'\rangle_p$, by the first assumption, there exists a partial coupling $\sigma : \langle \mathcal{E}_1(\rho_1), \mathcal{E}_1'(\rho_1')\rangle_p$ such that $\mathrm{tr}(C_i\rho) \geq \mathrm{tr}(C_m\sigma)$. From the second assumption there is a partial coupling $\sigma' : \langle \mathcal{E}_2(\mathcal{E}_1(\rho_1)), \mathcal{E}_2'(\mathcal{E}_1'(\rho_1'))\rangle_p$, or equivalently, $\sigma' : \langle (\mathcal{E}_1 \circ \mathcal{E}_2)(\rho_1), (\mathcal{E}_1' \circ \mathcal{E}_2')(\rho_1')\rangle_p$ such that $\mathrm{tr}(C_m\sigma) \geq \mathrm{tr}(C_o\sigma')$, which concludes the proof by noticing $\mathrm{tr}(C_i\rho) \geq \mathrm{tr}(C_o\sigma')$. □

Proposition C.6 (Split Cost)**.** *The contractivity can further be checked via splitting output cost. Formally, Suppose $\mathcal{E}_1, \mathcal{E}_2$ are quantum channels. $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C and $Q_1 \otimes I + I \otimes Q_2$ if and only if*

$$C \sqsupseteq \mathcal{E}_1^\dagger(Q_1) \otimes I + I \otimes \mathcal{E}_2^\dagger(Q_2).$$

Proof. The if part can be proved by combining Proposition IV.5 (1) and (2). For the only if part, by employing Lemma IV.4, we have for all $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, there exists $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1(\rho))\rangle$ such that

$$\begin{aligned}
\mathrm{tr}(C\rho) &\geq \mathrm{tr}((Q_1 \otimes I + I \otimes Q_2)\sigma)\\
&= \mathrm{tr}(Q_1\,\mathrm{tr}_2(\sigma)) + \mathrm{tr}(Q_2\,\mathrm{tr}_1(\sigma))\\
&= \mathrm{tr}(Q_1\mathcal{E}_1(\mathrm{tr}_2(\rho))) + \mathrm{tr}(Q_2\mathcal{E}_2(\mathrm{tr}_1(\rho))\\
&= \mathrm{tr}((\mathcal{E}_1^\dagger(Q_1) \otimes I + I \otimes \mathcal{E}_2^\dagger(Q_2))\rho).
\end{aligned}$$

Since this holds for all ρ, we must have: $C \sqsupseteq \mathcal{E}_1^\dagger(Q_1) \otimes I + I \otimes \mathcal{E}_2^\dagger(Q_2)$. □

Theorem C.7 (Theorem IV.6)**.** *Suppose $\mathcal{E}_1$ and $\mathcal{E}_2$ are quantum channels and costs $C_i \in \mathsf{Pos}^\infty$ and $C_o \in \mathsf{Pos}$ (i.e., C_o is finite). Then the following statements are equivalent:*

1) *$(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. C_i and C_o*
2) *for all $(Y_1, Y_2, n) \in \mathcal{Y}$, $(\mathcal{E}_1, \mathcal{E}_2)$ is contractive w.r.t. $C_i + nI$ and $Y_1 \otimes I + I \otimes (nI - Y_2)$, where $\mathcal{Y} \triangleq \{(Y_1, Y_2, n) \mid n \in \mathbb{N}; 0 \sqsubseteq Y_1; 0 \sqsubseteq Y_2 \sqsubseteq nI; C_o \sqsupseteq Y_1 \otimes I - I \otimes Y_2\}$.*

Proof. As $\mathcal{E}_1$ and $\mathcal{E}_2$ are quantum channels, we employ Lemma IV.4 to interpret contractivity.

(1) says that for all $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ there is a $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1)(\rho)\rangle$ such that $\mathrm{tr}(C_o\sigma) \leq \mathrm{tr}(C_i\rho)$, or equivalently,

$$\mathcal{E}_1(\mathrm{tr}_2(\rho)) C_{o\epsilon}^{\#} \mathcal{E}_2(\mathrm{tr}_1)(\rho)$$

where $\epsilon = \mathrm{tr}(C_i\rho)$.

(2) says that for all $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, positive Hermitians Y_1, Y_2 and n such that $Y_2 \sqsubseteq nI$ (where such an n always exists for any Y_2) and $Y_1 \otimes I - I \otimes Y_2 \sqsubseteq C_o$, there exists a coupling $\sigma : \langle \mathcal{E}_1(\mathrm{tr}_2(\rho)), \mathcal{E}_2(\mathrm{tr}_1)(\rho)\rangle$ such that

$$\mathrm{tr}(C_i\rho) + n\,\mathrm{tr}(\rho) \geq \mathrm{tr}((Y_1 \otimes I)\sigma) + n\,\mathrm{tr}(\sigma) - \mathrm{tr}((I \otimes Y_2)\sigma)$$

which, by noticing $\mathrm{tr}(\sigma) = \mathrm{tr}(\rho)$ since $\mathcal{E}_1$ and $\mathcal{E}_2$ are quantum channels, is equivalent to

$$\mathrm{tr}(Y_1(\mathcal{E}_1\,\mathrm{tr}_2(\rho))) \leq \mathrm{tr}(Y_2(\mathcal{E}_2\,\mathrm{tr}_1(\rho))) + \mathrm{tr}(C_i\rho).$$

The equivalence then follows from Theorem III.3. □

Symmetric space is useful for describing equivalence of states, as studied in [8]:

Lemma C.8 (State Equivalence (e.g. [2] prop 3.2)). *Let $=_{sym}$ be the projector $\frac{1}{2}(I + \mathsf{SWAP})$. Then, for any $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H})$,*

$$\rho_1 = \rho_2 \iff \rho_1(=_{sym})^{\#}\rho_2.$$

Proposition C.9 (Proposition IV.7). *Two quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ are equivalent if and only if for all density operators ρ_1, ρ_2, $T_s(\mathcal{E}_1(\rho_1), \mathcal{E}_2(\rho_2)) \leq T_s(\rho_1, \rho_2)$.*

Proof. The "only if" part holds directly by the contractivity of stable QOT under data processing [12].

For the "if" part, for any $\rho \in \mathcal{D}^1(\mathcal{H})$, from the assumption, we have $0 \leq T_s(\rho, \rho) \leq T(\rho, \rho) = 0$. Thus, $T_s(\mathcal{E}_1(\rho), \mathcal{E}_2(\rho)) = 0$, or equivalently, $T(\mathcal{E}_1(\rho) \otimes \frac{I}{2}, \mathcal{E}_2(\rho) \otimes \frac{I}{2}) = 0$, indicating $\mathcal{E}_1(\rho) \otimes \frac{I}{2} = \mathcal{E}_2(\rho) \otimes \frac{I}{2}$. Then, we know $\mathcal{E}_1(\rho) = \mathcal{E}_2(\rho)$ for all ρ, meaning that $\mathcal{E}_1 = \mathcal{E}_2$. □

Proposition C.10 (Proposition IV.8). *Given $\rho_1, \rho_2 \in \mathcal{D}^1(\mathcal{H})$ and $\epsilon \in \mathbb{R}^+$, the following are equivalent:*

1) *$T_s(\rho_1, \rho_2) \leq \epsilon$;*
2) *For all $Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2)$ such that $P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)$, it holds that:*

$$\mathrm{tr}(\mathrm{tr}_2(Y_1)\rho_1) \leq \mathrm{tr}(\mathrm{tr}_2(Y_2))\rho_2) + \epsilon.$$

Proof. By the property of T_s, we first observe:

$$T_s(\rho_1, \rho_2) = \inf_{\tau : \langle \rho_1 \otimes \frac{I}{2}, \rho_2 \otimes \frac{I}{2}\rangle} (P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2]\tau),$$

which implies that, (1) is equivalent to $(\rho_1 \otimes \frac{I}{2})\big(P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2]\big)^{\#}_{\epsilon}(\rho_2 \otimes \frac{I}{2})$. Employing Theorem III.3, (1) is further equivalent to:

3) for all $Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2)$ such that $P^{\perp}_{sym}[\mathcal{H} \otimes \mathcal{H}_2] \geq Y_1 \otimes I - I \otimes Y_2$, it holds that:

$$\mathrm{tr}\left(Y_1\big(\rho_1 \otimes \frac{I}{2}\big)\right) \leq \mathrm{tr}\left(Y_2\big(\rho_2 \otimes \frac{I}{2}\big)\right) + \epsilon.$$

Notice that, $\mathrm{tr}(Y_i(\rho_i \otimes \frac{I}{2})) = \mathrm{tr}(\mathrm{tr}_2(\frac{Y_i}{2})\rho_i)$ for $i = 1, 2$, direct substitutions of $Y_i' = \frac{Y_i}{2}$ translate (3) to (2). □

APPENDIX D
DEFERRED PROOFS IN "A QUANTUM RELATIONAL HOARE LOGIC" SECTION

Lemma D.1 (Lemma VI.2). *$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ if and only if for all $z \in Z$, $([\![S_1]\!], [\![S_2]\!])$ is contractive w.r.t. P and Q.*

Proof. We employ Lemma IV.3 to interpret contractive.

(if) part. For all $z \in Z$, and $\rho \in \mathcal{D}^1(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, by assumption we have:

$$T_Q([\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))) \leq T_P(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho)) \leq \mathrm{tr}(P\rho).$$

Set $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle_p$ such that $T_Q([\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))) = \mathrm{tr}(Q\sigma)$. Then $\mathrm{tr}(Q\sigma) \leq \mathrm{tr}(P\rho)$.

(only if) part. For all $z \in Z$, $\rho_1 \in \mathcal{D}^1(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_2)$, set $\rho : \langle \rho_1, \rho_2\rangle$ such that $T_P(\rho_1, \rho_2) = \mathrm{tr}(P\rho)$. By assumption, there exists $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle_p$ (i.e., $\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)\rangle_p$) such that:

$$T_P(\rho_1, \rho_2) = \mathrm{tr}(P\rho) \geq \mathrm{tr}(Q\sigma) \geq T_Q([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)).$$

□

Lemma D.2 (qOTL Validity Alternative). *$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ if and only if for every $z \in Z$, $\rho_1 \in \mathcal{D}(\mathcal{H}_{S_1})$, $\rho_2 \in \mathcal{D}(\mathcal{H}_{S_2})$ and partial coupling $\rho : \langle \rho_1, \rho_2\rangle_p$, there exists a partial coupling $\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)\rangle_p$ such that*

$$\mathrm{tr}(P\rho) \geq \mathrm{tr}(Q\sigma).$$

Proof. (if) part. For every $z \in Z$, $\rho_1 \in \mathcal{D}(\mathcal{H}_{S_1})$, $\rho_2 \in \mathcal{D}(\mathcal{H}_{S_2})$, select partial coupling $\rho : \langle \rho_1, \rho_2 \rangle_p$ such that $T_P(\rho_1, \rho_2) = \mathrm{tr}(P\rho)$, by assumption there exists a partial coupling $\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2) \rangle_p$ such that

$$T_Q([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \leq \mathrm{tr}(Q\sigma) \leq \mathrm{tr}(P\rho) = T_P(\rho_1, \rho_2),$$

so $([\![S_1]\!], [\![S_2]\!])$ is contractive w.r.t. P and Q, then by Lemma VI.2.

(only if) part. For every $z \in Z$, by Lemma VI.2, $([\![S_1]\!], [\![S_2]\!])$ is contractive w.r.t. P and Q. For $\rho_1 \in \mathcal{D}(\mathcal{H}_{S_1})$, $\rho_2 \in \mathcal{D}(\mathcal{H}_{S_2})$ and partial coupling $\rho : \langle \rho_1, \rho_2 \rangle_p$, select partial coupling $\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2) \rangle_p$ such that $T_Q([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) = \mathrm{tr}(Q\sigma)$, then:

$$\mathrm{tr}(Q\sigma) = T_Q([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \leq T_P(\rho_1, \rho_2) \leq \mathrm{tr}(P\rho).$$

□

Lemma D.3 (qOTL Validity for AST Programs)**.** *Suppose S_1 and S_2 are AST programs. Then $\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ if and only if for every $z \in Z$, and $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho)) \rangle$ such that*

$$\mathrm{tr}(P_z\rho) \geq \mathrm{tr}(Q_z\sigma).$$

Proof. Direct by Lemma VI.2 and Lemma IV.4. □

Theorem D.4 (Theorem VI.3)**.** *If $\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$ then $\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$.*

Proof. By induction on the structural of the program, analogously to the soundness proof in [2].

(skip), (assign-L), (apply-L): By employing Lemma VI.2 and Proposition IV.5(1) and the denotational semantics.

(seq): By employing Lemma VI.2 and Proposition IV.5(3) and the denotational semantics.

(if-L): By employing Lemma VI.2 and Lemma IV.3, it remains to be shown that for all $\rho \in \mathcal{D}^1$ and $\sigma \in \mathcal{D}^1$,

$$T_Q([\![\mathbf{if}]\!](\rho), \sigma) \leq T_{\sum_m (M_m \otimes I)^\dagger_m P_m (M_m \otimes I)}(\rho, \sigma).$$

Set $\rho_m = \mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$ and $p_m = \mathrm{tr}(\rho_m)$, so $[\![\mathbf{if}]\!](\rho) = \sum_m p_m [\![S_m]\!](\rho_m/p_m)$. By assumption and Proposition C.2, we have:

$$T_Q([\![\mathbf{if}]\!](\rho), \sigma) = T_Q(\sum_m p_m [\![S_m]\!](\rho_m/p_m), \sigma) \leq \sum_m p_m T_Q([\![S_m]\!](\rho_m/p_m), \sigma) \leq \sum_m p_m T_{P_m}(\rho_m/p_m, \sigma)$$

On the other hand, select $\delta : \langle \rho, \sigma \rangle$ such that

$$\begin{aligned} T_{\sum_m (M_m \otimes I)^\dagger_m P_m (M_m \otimes I)}(\rho, \sigma) &= \mathrm{tr}((\sum_m (M_m \otimes I)^\dagger_m P_m (M_m \otimes I))\delta) \\ &= \sum_m p_m \,\mathrm{tr}(P_m((M_m \otimes I)\delta(M_m \otimes I)^\dagger_m / p_m)). \end{aligned}$$

Notice that, $(M_m \otimes I)\delta(M_m \otimes I)^\dagger_m / p_m$ is in fact a coupling of $\langle \rho_m/p_m, \sigma \rangle$, so

$$\mathrm{tr}(P_m((M_m \otimes I)\delta(M_m \otimes I)^\dagger_m / p_m)) \geq T_{P_m}(\rho_m/p_m, \sigma),$$

and this complete the proof.

(while-L): Let $z \in Z$ and ρ be the initial joint state. Set $\sigma_0 = \rho$, and inductively define

$$\sigma'_{n+1} : \langle [\![S]\!](\mathrm{tr}_2(\mathcal{E}_1(\sigma_n)/\,\mathrm{tr}(\mathcal{E}_1(\sigma_n)))), \mathrm{tr}_1(\mathcal{E}_1(\sigma_n)/\,\mathrm{tr}(\mathcal{E}_1(\sigma_n))) \rangle_p$$

as the partial coupling obtained by applying (IH) on initial state $\mathcal{E}_1(\sigma_n)/\,\mathrm{tr}(\mathcal{E}_1(\sigma_n))$, and $\sigma_{n+1} = \mathrm{tr}(\mathcal{E}_1(\sigma_n))\sigma_{n+1}$. For simplicity, we write

$$R = ((M_0 \otimes I)^\dagger P (M_0 \otimes I) + (M_1 \otimes I)^\dagger Q (M_1 \otimes I)).$$

By (IH), we have $\mathrm{tr}(Q\mathcal{E}_1(\sigma_n)/\,\mathrm{tr}(\mathcal{E}_1(\sigma_n))) \geq \mathrm{tr}(R\sigma'_{n+1})$, or equivalently, $\mathrm{tr}(Q\mathcal{E}_1(\sigma_n)) \geq \mathrm{tr}(R\sigma_{n+1})$.

We first check $\mathrm{tr}_2(\sigma_n) = ([\![S]\!] \circ \mathcal{E}_1)^n(\mathrm{tr}_2(\rho))$ by induction on n. The base case $n = 0$ is trivial. For $n+1$, observe that:

$$\begin{aligned} \mathrm{tr}_2(\sigma_{n+1}) &= \mathrm{tr}(\mathcal{E}_1(\sigma_n))\,\mathrm{tr}_2(\sigma'_{n+1}) \\ &\sqsubseteq \mathrm{tr}(\mathcal{E}_1(\sigma_n))[\![S]\!](\mathrm{tr}_2(\mathcal{E}_1(\sigma_n)/\,\mathrm{tr}(\mathcal{E}_1(\sigma_n)))) \\ &= [\![S]\!](\mathrm{tr}_2(\mathcal{E}_1(\sigma_n))) \\ &= ([\![S]\!] \circ \mathcal{E}_1)(\mathrm{tr}_2(\sigma_n)). \end{aligned}$$

On the other hand,

$$\begin{aligned}1+\operatorname{tr}(\sigma_{n+1}) &= 1+\operatorname{tr}(\mathcal{E}_1(\sigma_n))\operatorname{tr}(\sigma'_{n+1})\\ &\geq 1+\operatorname{tr}(\mathcal{E}_1(\sigma_n))(\operatorname{tr}([\![S]\!](\operatorname{tr}_2(\mathcal{E}_1(\sigma_n)/\operatorname{tr}(\mathcal{E}_1(\sigma_n)))))\\ &\qquad + \operatorname{tr}(\operatorname{tr}_1(\mathcal{E}_1(\sigma_n)/\operatorname{tr}(\mathcal{E}_1(\sigma_n)))) - 1)\\ &= 1+\operatorname{tr}([\![S]\!](\operatorname{tr}_2(\mathcal{E}_1(\sigma_n))))\\ &= 1+\operatorname{tr}(([\![S]\!]\circ\mathcal{E}_1)(\operatorname{tr}_2(\sigma_n)))\end{aligned}$$

These two together imply $\operatorname{tr}_2(\sigma_{n+1}) = ([\![S]\!]\circ\mathcal{E}_1)(\operatorname{tr}_2(\sigma_n)) = ([\![S]\!]\circ\mathcal{E}_1)^{n+1}(\operatorname{tr}_2(\rho))$. Furthermore, $\operatorname{tr}_1(\sigma'_{n+1}) \sqsubseteq \operatorname{tr}_1(\mathcal{E}_1(\sigma_n)/\operatorname{tr}(\mathcal{E}_1(\sigma_n)))$, or equivalently, $\operatorname{tr}_1(\sigma_{n+1}) \sqsubseteq \operatorname{tr}_1(\mathcal{E}_1(\sigma_n))$.

Set $\sigma = \sum_n \mathcal{E}_0(\sigma_n)$. Its convergence is ensured by realizing that

$$\begin{aligned}\operatorname{tr}(\sigma) &= \sum_n \operatorname{tr}(\mathcal{E}_0(\operatorname{tr}_2(\sigma_n))) = \sum_n \operatorname{tr}(\mathcal{E}_0((([\![S]\!]\circ\mathcal{E}_1)^n(\operatorname{tr}_2(\rho))))\\ &= \operatorname{tr}([\![\mathbf{while}]\!](\operatorname{tr}_2(\rho))) \leq \operatorname{tr}(\rho).\end{aligned}$$

Next, we check the inequality :

$$\begin{aligned}\operatorname{tr}(R\rho) =&\ \operatorname{tr}(P\mathcal{E}_0(\sigma_0)+Q\mathcal{E}_1(\sigma_0))\\ \geq&\ \operatorname{tr}(P\mathcal{E}_0(\sigma_0))+\operatorname{tr}(R\sigma_1)\\ =&\ \operatorname{tr}(P\mathcal{E}_0(\sigma_0))+\operatorname{tr}(P\mathcal{E}_0(\sigma_1)+Q\mathcal{E}_1(\sigma_1))\\ =&\ \sum_{n=0}^{k}\operatorname{tr}(P\mathcal{E}_0(\sigma_n))+\operatorname{tr}(Q\mathcal{E}_1(\sigma_k))\\ \geq&\ \operatorname{tr}(P\sigma).\end{aligned}$$

Thus, it is sufficient to check $\sigma : \langle [\![\mathbf{while}]\!](\operatorname{tr}_2(\rho)), \operatorname{tr}_1(\rho)\rangle_p$ as follows:

$$\begin{aligned}\operatorname{tr}_2(\sigma) &= \sum_n \mathcal{E}_0(\operatorname{tr}_2(\sigma_n)) = \sum_n \mathcal{E}_0([\![S]\!]\circ\mathcal{E}_1)^n(\operatorname{tr}_2(\rho))\\ &= [\![\mathbf{while}]\!](\operatorname{tr}_2(\rho)),\\ \operatorname{tr}_1(\rho) &= \operatorname{tr}_1(\mathcal{E}_0(\sigma_0)+\mathcal{E}_1(\sigma_0))\\ &\sqsupseteq \operatorname{tr}_1(\mathcal{E}_0(\sigma_0))+\operatorname{tr}_1(\sigma_1)\\ &= \operatorname{tr}_1(\mathcal{E}_0(\sigma_0))+\operatorname{tr}_1(\mathcal{E}_0(\sigma_1)+\mathcal{E}_1(\sigma_1))\\ &\sqsupseteq \sum_{n=0}^{k}\operatorname{tr}_1(\mathcal{E}_0(\sigma_n))+\operatorname{tr}_1(\mathcal{E}_1(\sigma_n))\\ &\sqsupseteq \operatorname{tr}_1(\sigma)\\ 1+\operatorname{tr}(\sigma) &= \operatorname{tr}(\operatorname{tr}_1(\rho))+\operatorname{tr}([\![\mathbf{while}]\!](\operatorname{tr}_2(\rho))).\end{aligned}$$

(csq): By employing Lemma VI.2 and Item 2.

(Strassen): By employing Lemma VI.2 and Theorem IV.6. Note that Q should be finite which is inherited from Theorem III.3. □

Lemma D.5 (Lemma VI.4)**.** *For every AST program S, we have*

$$\vdash Z : \{([\![S]\!]^\dagger \otimes I)(Q)\}\ S \sim \mathbf{skip}\ \{Q\}.$$

Proof. By induction.

Case $\mathbf{skip}$: direct from the definition and (skip).

Case $q := |0\rangle$: direct from the definition and (assign-L).

Case $\bar{q} := U[\bar{q}]$: direct from the definition and (apply-L).

Case $S_1; S_2$: Assume that for any Q we have $\vdash Z : \{([\![S_i]\!]^\dagger \otimes I)(Q)\}\ S_i \sim \mathbf{skip}\ \{Q\}$ for $i = 1, 2$, we directly get from (seq) since $(([\![S_1; S_2]\!]^\dagger) \otimes I)(Q) = ([\![S_1]\!]^\dagger \otimes I)[([\![S_2]\!]^\dagger \otimes I)(Q)]$ by Lemma A.8:

$$\frac{\begin{array}{c}\vdash Z : \{([\![S_1]\!]^\dagger \otimes I)[([\![S_2]\!]^\dagger \otimes I)(Q)]\}\ S_1 \sim \mathbf{skip}\ \{([\![S_2]\!]^\dagger \otimes I)(Q)\}\\ \vdash Z : \{([\![S_2]\!]^\dagger \otimes I)(Q)\}\ S_2 \sim \mathbf{skip}\ \{Q\}\end{array}}{\vdash Z : \{(([\![S_1; S_2]\!]^\dagger) \otimes I)(Q)\}\ S_1; S_2 \sim \mathbf{skip}\ \{Q\}}$$

Case **if**: assume that for any Q and m we have $\vdash Z : \{[\![S_m]\!]^\dagger \otimes I(Q)\}\ S_m \sim \mathbf{skip}\ \{Q\}$. Then, it follows directly from (if-L) that

$$\vdash Z : \{\sum_m (M_m \otimes I)^\dagger[([\![S_m]\!]^\dagger \otimes I)(Q)](M_m \otimes I)\}\ \mathbf{if} \sim \mathbf{skip}\ \{Q\}.$$

By Lemma A.8, knowing that

$$\begin{aligned}
&\sum_m (M_m \otimes I)^\dagger[([\![S_m]\!]^\dagger \otimes I)(Q)](M_m \otimes I)\\
=\ &\sum_m (\mathcal{E}_m^\dagger \otimes I)[([\![S_m]\!]^\dagger \otimes I)(Q)]\\
=\ &((\sum_m \mathcal{E}_m^\dagger \circ [\![S_m]\!]^\dagger) \otimes I)(Q)\\
=\ &((\sum_m [\![S_m]\!] \circ \mathcal{E}_m)^\dagger \otimes I)(Q)\\
=\ &([\![\mathbf{if}]\!]^\dagger \otimes I)(Q)
\end{aligned}$$

then allows us to conclude that

$$\vdash Z : \{([\![\mathbf{if}]\!]^\dagger \otimes I)(Q)\}\ \mathbf{if} \sim \mathbf{skip}\ \{Q\}$$

as required.

Case **while**: assume that for any Q we have $\vdash Z : \{([\![S]\!]^\dagger \otimes I)(Q)\}\ S \sim \mathbf{skip}\ \{Q\}$. Then, we get that

$$\vdash Z : \{([\![S]\!]^\dagger \otimes I)[([\![\mathbf{while}]\!]^\dagger \otimes I)(Q)]\}\ S \sim \mathbf{skip}\ \{([\![\mathbf{while}]\!]^\dagger \otimes I)(Q)\}$$

Let $P = ([\![S]\!]^\dagger \otimes I)[([\![\mathbf{while}]\!]^\dagger \otimes I)(Q)]$. Then, by the (least) fixed point property of $[\![\mathbf{while}]\!]$, i.e., $[\![\mathbf{while}]\!] = \mathcal{E}_0 + [\![\mathbf{while}]\!] \circ ([\![S]\!] \circ \mathcal{E}_1)$, we obtain that

$$\begin{aligned}
([\![\mathbf{while}]\!]^\dagger \otimes I)(Q) &= [(\mathcal{E}_0^\dagger + (\mathcal{E}_1^\dagger \circ [\![S]\!]^\dagger) \circ [\![\mathbf{while}]\!]^\dagger) \otimes I](Q)\\
&= (\mathcal{E}_0^\dagger \otimes I)(Q) + (\mathcal{E}_1^\dagger \otimes I)(P)
\end{aligned}$$

by Lemma A.8. We thus obtain by (while-L) that

$$\frac{\vdash Z : \{P\}\ S \sim \mathbf{skip}\ \{(\mathcal{E}_0^\dagger \otimes I)(Q) + (\mathcal{E}_1^\dagger \otimes I)(P)\}}{\vdash Z : \{(\mathcal{E}_0^\dagger \otimes I)(Q) + (\mathcal{E}_1^\dagger \otimes I)(P)\}\ \mathbf{while} \sim \mathbf{skip}\ \{Q\}}$$

which is the same as

$$\vdash Z : \{([\![\mathbf{while}]\!]^\dagger \otimes I)(Q)\}\ \mathbf{while} \sim \mathbf{skip}\ \{Q\}$$

as required. □

Lemma D.6 (Lemma VI.5)**.** *For every AST programs S_1, S_2, we have*

$$\vdash Z : \{([\![S_1]\!]^\dagger \otimes [\![S_2]\!]^\dagger)(Q)\}\ S_1 \sim S_2\ \{Q\}$$

Proof. By using Lemma VI.4, its symmetric version and the rule (seq) we get:

$$\frac{\begin{array}{c}\vdash Z : \{([\![S_1]\!]^\dagger \otimes I)[(I \otimes [\![S_2]\!]^\dagger)(Q)]\}\ S_1 \sim \mathbf{skip}\ \{(I \otimes [\![S_2]\!]^\dagger)(Q)\}\\ \vdash Z : \{(I \otimes [\![S_2]\!]^\dagger)(Q)\}\ \mathbf{skip} \sim S_2\ \{Q\}\end{array}}{\vdash Z : \{([\![S_1]\!]^\dagger \otimes [\![S_2]\!]^\dagger)(Q)\}\ S_1 \sim S_2\ \{Q\}}\ \text{(seq)}$$

as required by Lemma A.8. □

Theorem D.7 (Theorem VI.6)**.** *For every AST programs S_1, S_2, we have:*

$$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q_1 \otimes I + I \otimes Q_2\}$$

implies

$$\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q_1 \otimes I + I \otimes Q_2\}$$

Proof. According to Lemma VI.2 and Proposition C.6, by assumption, it holds that

$$\begin{aligned}
P &\sqsupseteq ([\![S_1]\!]^\dagger(Q_1)) \otimes I + I \otimes ([\![S_2]\!]^\dagger(Q_2))\\
&= ([\![S_1]\!] \otimes [\![S_2]\!])^\dagger(Q_1 \otimes I + I \otimes Q_2)
\end{aligned}$$

by employing Lemma A.8, and since S_1, S_2 are AST, so $[\![S_1]\!]^\dagger$ and $[\![S_2]\!]^\dagger$ are unital maps, i.e., $[\![S_1]\!]^\dagger(I) = I$ and $[\![S_2]\!]^\dagger(I) = I$.

Then, by Lemma VI.5 and the (csq) rule, we can derive

$$\frac{\begin{array}{c} P \sqsupseteq ([\![S_1]\!] \otimes [\![S_2]\!])^\dagger(Q) \\ \vdash Z : \{([\![S_1]\!] \otimes [\![S_2]\!])^\dagger(Q)\}\ S_1 \sim S_2\ \{Q\} \end{array}}{\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}}$$

where $Q = Q_1 \otimes I + I \otimes Q_2$, as required. □

Theorem D.8 (Theorem VI.7)**.** *For every AST S_1, S_2 programs and bounded predicate $Q \in \mathsf{Pos}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, we have*

$$\vDash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$$

implies

$$\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}$$

Proof. By Lemma VI.2 and Theorem IV.6, we know that

$$\vDash Z, (Y_1, Y_2, n) \in \mathcal{Y} : \{P + nI\} S_1 \sim S_2\ \{Y_1 \otimes I + I \otimes (nI - Y_2)\}$$

where $\mathcal{Y}$ is defined as in Theorem IV.6 with $C_i = P$ and $C_o = Q$.

Follows from Theorem VI.6 the completeness for split post-conditions, we know that:

$$\vdash Z, (Y_1, Y_2, n) \in \mathcal{Y} : \{P + nI\} S_1 \sim S_2\ \{Y_1 \otimes I + I \otimes (nI - Y_2)\}.$$

Finally by applying rule (duality), we have

$$\vdash Z : \{P\}\ S_1 \sim S_2\ \{Q\}.$$

□

Proposition D.9 (Proposition X.1)**.** *Let S_1, S_2 be AST programs and $0 \sqsubseteq P, Q \sqsubseteq I$ be predicates. Then*

$$\vDash_{\mathsf{rqPD}} \{P\}\ S_1 \sim S_2\ \{Q\} \iff \vDash \{I - P\}\ S_1 \sim S_2\ \{I - Q\}.$$

Proof. From [2], we know that $\vDash_{\mathsf{rqPD}} \{P\}\ S_1 \sim S_2\ \{Q\}$ iff for all $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle$ such that

$$\mathrm{tr}(P\rho) \leq \mathrm{tr}(Q\sigma).$$

Since $S_1, S_2 \in \mathsf{AST}$, $\mathrm{tr}(\rho) = \mathrm{tr}(\sigma)$, thus it is equivalent to

$$\mathrm{tr}((I - Q)\sigma) \leq \mathrm{tr}((I - P)\rho),$$

which, according to Lemma D.3, it equivalent to $\vDash \{I - P\}\ S_1 \sim S_2\ \{I - Q\}$ in our logic. Since $P, Q \sqsubseteq I$, so it is guaranteed that $I - P, I - Q \in \mathsf{Pos}$. □

Proof of Proposition VII.2. ($\Rightarrow$) part. For any $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ such that $\mathrm{supp}(\rho) \subseteq X$, by assumption and Lemma D.3, we know that there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle$ such that

$$0 \leq \mathrm{tr}(Y^\perp \sigma) \leq \mathrm{tr}((X \mid 0)\rho) = 0,$$

the last equation is due to Lemma A.7 as $\mathrm{tr}(X^\perp \rho) = 0$. This asserts that $\mathrm{supp}(\sigma) \subseteq Y$, which conclude that $\vDash_{\mathsf{pqRHL}} \{X\}\ S_1 \sim S_2\ \{Y\}$.

($\Leftarrow$) part. By Lemma D.3, for any $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, if $\mathrm{tr}(X^\perp \rho) \neq 0$, then $\mathrm{tr}((X \mid 0)\rho) = +\infty$, by convention then it holds. Otherwise, $\mathrm{tr}(X^\perp \rho) = 0$, so $\mathrm{tr}((X \mid 0)\rho) = 0$ and $\mathrm{supp}(\rho) \subseteq X$, by assumption, there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))\rangle$ such that $\mathrm{supp}(\sigma) \subseteq Y$, which leads to

$$\mathrm{tr}(Y^\perp \sigma) = 0 \leq \mathrm{tr}((X \mid 0)\rho),$$

and this completes the proof. □

Proposition D.10. *For programs S_1, S_2, any Z, and Z-parameterised predicate P and Z-parameterised projector $X \in \mathcal{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, the following holds:*

$$\vDash Z : \{X \mid 0\}\ S_1 \sim S_2\ \{P\} \iff \vDash Z : \{X \mid 0\}\ S_1 \sim S_2\ \{\mathrm{supp}(P)\}.$$

As a corollary, if $X \in \mathcal{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, then

$$\vDash Z : \{X \mid 0\}\ S_1 \sim S_2\ \{Y \mid 0\} \iff \vDash Z : \{X \mid 0\}\ S_1 \sim S_2\ \{Y^\perp\}.$$

Proof. For any $z \in Z$, and $\rho \in \mathcal{D}^1(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, if $\mathrm{tr}(X\rho) \neq 0$, then $\mathrm{tr}((X \mid 0)\rho) = +\infty$, thus both LHS and RHS holds, i.e., exists partial coupling σ of outputs such that $\mathrm{tr}((X \mid 0)\rho) \geq \mathrm{tr}(P\sigma)$ and $\mathrm{tr}((X \mid 0)\rho) \geq \mathrm{tr}(\mathrm{supp}(P)\sigma)$. Otherwise, $\mathrm{tr}(X\rho) = 0$, then $\mathrm{tr}((X \mid 0)\rho) = 0$, then for any partial coupling σ of outputs, $\mathrm{tr}(P\sigma) \leq \mathrm{tr}((X \mid 0)\rho) = 0$ if and only if $\mathrm{tr}(\mathrm{supp}(P)\sigma) \leq \mathrm{tr}((X \mid 0)\rho) = 0$, so LHS is equivalent to RHS. □

APPENDIX E
DEFERRED PROOFS IN "TWO-SIDED RULES" SECTION

Theorem E.1 (Theorem VI.9)**.** *For AST programs S_1, S_2, and measurements $M = \{M_1, \cdots, M_k\}$ and $N = \{N_1, \cdots, N_k\}$, the following are equivalent:*

1) $\emptyset \overset{(S_1,S_2)}{\vDash} M \approx N$;
2) $\vDash (Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, n) \in \mathcal{Y}_k : \{nI\}S_1 \sim S_2\big\{(\sum_i M_i^\dagger Y_i M_i) \otimes I + I \otimes \big[nI - (\sum_i N_i^\dagger Z_i N_i)\big]\big\}$ *where* $\mathcal{Y}_k = \{(Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, n) \mid \forall\, i,\ 0 \sqsubseteq Y_i,\ 0 \sqsubseteq Z_i \sqsubseteq nI, Y_i \otimes I - I \otimes Z_i \sqsubseteq 0, \forall\, j \neq i,\ Y_i \otimes I - I \otimes Z_j \sqsubseteq I\}$.

Proof. (1 ⇒ 2). By Lemma D.3 , for any $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, set $\rho_1 = \mathrm{tr}_2(\rho)$ and $\rho_2 = \mathrm{tr}_1(\rho)$, $\sigma_1 = [\![S_1]\!](\rho_1)$ and $\sigma_2 = [\![S_2]\!](\rho_2)$. By first assumption, we know that for all i, $\mathrm{tr}(M_i\sigma_1 M_i^\dagger) = \mathrm{tr}(N_i\sigma_2 N_i^\dagger)$ and denote it by p_i. Set the state

$$\sigma_1' = \begin{pmatrix} M_1\sigma_1 M_1^\dagger & 0 & \cdots & 0 \\ 0 & M_2\sigma_1 M_2^\dagger & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_k\sigma_1 M_k^\dagger \end{pmatrix} \qquad \sigma_2' = \begin{pmatrix} N_1\sigma_2 N_1^\dagger & 0 & \cdots & 0 \\ 0 & N_2\sigma_2 N_2^\dagger & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & N_k\sigma_2 N_k^\dagger \end{pmatrix}$$

and obviously, $\sigma_1' \in \mathcal{D}(\mathcal{H}_k \otimes \mathcal{H}_{S_1})$ and $\sigma_2' \in \mathcal{D}(\mathcal{H}_k \otimes \mathcal{H}_{S_2})$ where $\mathcal{H}_k$ is the k-dimensional Hilbert space. In other words, $\sigma_1' = \sum_i |i\rangle\langle i| \otimes M_i\sigma_1 M_i^\dagger$ and $\sigma_2' = \sum_i |i\rangle\langle i| \otimes N_i\sigma_2 N_i^\dagger$. Consider the PSD $A = \sum_{i \neq j}(|i\rangle\langle i| \otimes I_{S_1}) \otimes (|j\rangle\langle j| \otimes I_{S_2}) \in \mathsf{Pos}((\mathcal{H}_k \otimes \mathcal{H}_{S_1}) \otimes (\mathcal{H}_k \otimes \mathcal{H}_{S_2}))$. We claim that $\sigma_1' A_0^{\#} \sigma_2'$, since we can construct coupling

$$\sigma' = \sum_i (|i\rangle\langle i| \otimes M_i\sigma_1 M_i^\dagger) \otimes (|i\rangle\langle i| \otimes N_i\sigma_2 N_i^\dagger)/p_i,$$

which $\sigma : \langle \sigma_1', \sigma_2' \rangle$ and $\mathrm{tr}(A\sigma') = 0$. By Theorem III.3, we know that for all $Y \in \mathsf{Pos}(\mathcal{H}_k \otimes \mathcal{H}_{S_1})$ and $Z \in \mathsf{Pos}(\mathcal{H}_k \otimes \mathcal{H}_{S_2})$ such that $A \sqsupseteq Y \otimes (I_k \otimes I_{S_2}) - (I_k \otimes I_{S_1}) \otimes Z$, it holds that: $\mathrm{tr}(Y\sigma_1') \leq \mathrm{tr}(Z\sigma_2')$. Now, back to (2) which we aim to prove, for any $(Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, n) \in \mathcal{Y}_k$, set $Y = \sum_i |i\rangle\langle i| \otimes Y_i$ and $Z = \sum_i |i\rangle\langle i| \otimes Z_i$, we check that:

$$\begin{aligned} Y \otimes (I_k \otimes I_{S_1}) - (I_k \otimes I_{S_2}) \otimes Z &= \Big(\sum_i |i\rangle\langle i| \otimes Y_i\Big) \otimes \Big(\sum_j |j\rangle\langle j| \otimes I_{S_2}\Big) - \Big(\sum_i |i\rangle\langle i| \otimes I_{S_1}\Big) \otimes \Big(\sum_j |j\rangle\langle j| \otimes Z_j\Big) \\ &= \sum_i [(|i\rangle\langle i| \otimes Y_i) \otimes (|i\rangle\langle i| \otimes I_{S_2}) - (|i\rangle\langle i| \otimes I_{S_1}) \otimes (|i\rangle\langle i| \otimes Z_i)] - \\ &\quad \sum_{i \neq j} [(|i\rangle\langle i| \otimes Y_i) \otimes (|j\rangle\langle j| \otimes I_{S_2}) - (|i\rangle\langle i| \otimes I_{S_1}) \otimes (|j\rangle\langle j| \otimes Z_j)] \\ &= \sum_i (|i\rangle\langle i| \otimes |i\rangle\langle i|) \otimes (Y_i \otimes I_{S_2} - I_{S_1} \otimes Z_i) + \sum_{i \neq j} (|i\rangle\langle i| \otimes |j\rangle\langle j|) \otimes (Y_i \otimes I_{S_2} - I_{S_1} \otimes Z_j) \\ &\sqsubseteq \sum_{i \neq j} (|i\rangle\langle i| \otimes |j\rangle\langle j|) \otimes (I_{S_1} \otimes I_{S_2}) \\ &= A \end{aligned}$$

where, in the fourth and fifth line, we change the order of Hilbert space $(\mathcal{H}_k \otimes \mathcal{H}_{S_1}) \otimes (\mathcal{H}_k \otimes \mathcal{H}_{S_2}) \to (\mathcal{H}_k \otimes \mathcal{H}_k) \otimes (\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ as they are isomorphic. Thus, it holds that $\mathrm{tr}(Y\sigma_1') \leq \mathrm{tr}(Z\sigma_2')$, or equivalently,

$$\begin{aligned} 0 \geq \mathrm{tr}(Y\sigma_1') - \mathrm{tr}(Z\sigma_2') &= \mathrm{tr}\Big(\Big(\sum_i |i\rangle\langle i| \otimes Y_i\Big)\Big(\sum_i |i\rangle\langle i| \otimes M_i\sigma_1 M_i^\dagger\Big)\Big) - \mathrm{tr}\Big(\Big(\sum_i |i\rangle\langle i| \otimes Z_i\Big)\Big(\sum_i |i\rangle\langle i| \otimes N_i\sigma_2 N_i^\dagger\Big)\Big) \\ &= \sum_i \mathrm{tr}(Y_i M_i \sigma_1 M_i^\dagger) - \sum_i \mathrm{tr}(Z_i N_i \sigma_2 N_i^\dagger) \\ &= \mathrm{tr}\big((\textstyle\sum_i M_i^\dagger Y_i M_i)\sigma_1\big) - \mathrm{tr}\big((\textstyle\sum_i N_i^\dagger Z_i N_i)\sigma_2\big). \end{aligned}$$

Note that $\mathrm{tr}(\rho) = \mathrm{tr}(\sigma_1) = \mathrm{tr}(\sigma_2)$ and set it as p. Let $\sigma \triangleq \sigma_1 \otimes \sigma_2/p$, realizing that $\sigma : \langle \sigma_1, \sigma_2 \rangle$, and observe that

$$\begin{aligned} \mathrm{tr}((nI)\rho) &\geq \mathrm{tr}((nI)\sigma) + \mathrm{tr}\big((\textstyle\sum_i M_i^\dagger Y_i M_i)\sigma_1\big) - \mathrm{tr}\big((\textstyle\sum_i N_i^\dagger Y_i N_i)\sigma_2\big) \\ &= \mathrm{tr}((nI)\sigma) + \mathrm{tr}\big(((\textstyle\sum_i M_i^\dagger Y_i M_i) \otimes I_{S_2})\sigma\big) - \mathrm{tr}\big((I_{S_1} \otimes (\textstyle\sum_i N_i^\dagger Z_i N_i))\sigma\big) \\ &= \mathrm{tr}\big(\big((\textstyle\sum_i M_i^\dagger Y_i M_i) \otimes I + I \otimes \big[nI - (\textstyle\sum_i N_i^\dagger Z_i N_i)\big]\big)\sigma\big) \end{aligned}$$

As ρ is arbitrary, so we finish the proof.

($2 \Rightarrow 1$). For any $\rho_1 \in \mathcal{D}^1(\mathcal{H}_{S_1})$ and $\rho_2 \in \mathcal{D}^1(\mathcal{H}_{S_2})$, by Lemma D.3 and Lemma IV.3, choose $\rho \triangleq \rho_1 \otimes \rho_2 \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ which is a coupling of $\langle \rho_1, \rho_2 \rangle$. For any $i = 1, \cdots k$, select $Y_i = I$, $Z_i = I$, $n = 1$, $Y_j = 0$ and $Z_j = 0$ for all $j \neq i$. It is then obvious that $(Y_1, \cdots, Y_k, Z_1, \cdots, Z_k, 1) \in \mathcal{Y}$, so by assumption, there exists a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho)) \rangle$ (or, equivalently, $\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2) \rangle$) such that

$$\begin{aligned} n\,\mathrm{tr}(\rho) \geq\ & \mathrm{tr}\left(\left(\left(\textstyle\sum_j M_j^\dagger Y_j M_j\right) \otimes I + I \otimes \left[nI - \left(\textstyle\sum_j N_j^\dagger Z_j N_j\right)\right]\right)\sigma\right) \\ =\ & \mathrm{tr}(((M_i^\dagger M_i) \otimes I + nI - I \otimes (N_i^\dagger N_i))\sigma) \\ =\ & \mathrm{tr}(M_i^\dagger M_i\, \mathrm{tr}_2(\sigma)) - \mathrm{tr}(N_i^\dagger N_i\, \mathrm{tr}_1(\sigma)) + n\,\mathrm{tr}(\sigma) \\ =\ & \mathrm{tr}(M_i([\![S_1]\!](\rho_1))M_i^\dagger) - \mathrm{tr}(N_i([\![S_2]\!](\rho_2))N_i^\dagger) + n\,\mathrm{tr}(\rho), \end{aligned}$$

since $S_1, S_2 \in \mathsf{AST}$. Thus, for all i, $\mathrm{tr}(M_i([\![S_1]\!](\rho_1))M_i^\dagger) \leq \mathrm{tr}(N_i([\![S_2]\!](\rho_2))N_i^\dagger)$. Notice that

$$\sum_i \mathrm{tr}(M_i([\![S_1]\!](\rho_1))M_i^\dagger) = \mathrm{tr}([\![S_1]\!](\rho_1)) = \mathrm{tr}(\rho_1) = \mathrm{tr}(\rho_2) = \mathrm{tr}([\![S_2]\!](\rho_2)) = \sum_i \mathrm{tr}(N_i([\![S_2]\!](\rho_2))N_i^\dagger),$$

so it must be the case that $\mathrm{tr}(M_i([\![S_1]\!](\rho_1))M_i^\dagger) = \mathrm{tr}(N_i([\![S_2]\!](\rho_2))N_i^\dagger)$ for all i, i.e., $([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \vDash M \approx N$, and this completes the proof. □

Definition E.2 (Measurement Property, c.f. [2])**.** *Define $\Gamma \vDash Z : \{P\}M \approx N\{Q_k\}$ if for all $\rho, \sigma \in \mathcal{D}^1$ such that $(\rho, \sigma) \vDash \Gamma$ and $z \in Z$, if $T_P(\rho, \sigma) < +\infty$, then there exists <u>couplings</u> $\delta_k : \langle M_k \rho M_k^\dagger, N_k \sigma N_k^\dagger \rangle$ such that:*

$$T_P(\rho, \sigma) \geq \sum_k \mathrm{tr}(Q_k \delta_k).$$

Proposition E.3. *1). $M \approx N \vDash_{\mathsf{rqPD}} A \Rightarrow \{B_m\}$ if and only if $M \approx N \vDash \{I - A\}M \approx N\{I - B_m\}$, where $0 \sqsubseteq A, B_m \sqsubseteq I$. 2). $\vDash_{\mathsf{pqRHL}} M \approx N : X \Rightarrow \{Y_m\}$ if and only if $\vDash \{X \mid 0\}M \approx N\{Y_m^\perp\}$ where $X, Y_m \in \mathcal{S}$.*

Proof. We first prove clause (1).

(if) part. By Def. 5.2 and 5.4 in [2], for any $\rho \in \mathcal{D}^1(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that $\rho \vDash_{\mathsf{rqPD}} M \approx N$ (if ρ is partial, then we just normalize it and everything still holds since coupling, trace etc are all scalable), i.e., $\forall\, i,\ \mathrm{tr}(M_i\, \mathrm{tr}_2(\rho) M_i^\dagger) = \mathrm{tr}(N_i\, \mathrm{tr}_1(\rho) N_i^\dagger)$, in other words, $(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho)) \vDash M \approx N$. By assumption, since $A \sqsubseteq I$, so $T_{I-A}(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho)) < +\infty$, there exists couplings $\delta_i : \langle M_i\, \mathrm{tr}_2(\rho) M_i^\dagger, N_i\, \mathrm{tr}_1(\rho) N_i^\dagger \rangle$ such that

$$1 - \mathrm{tr}(A\rho) = \mathrm{tr}((I - A)\rho) \geq T_{I-A}(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho)) \geq \sum_i \mathrm{tr}((I - B_i)\delta_i = 1 - \sum_i \mathrm{tr}(B_i \delta_i),$$

that is, $\mathrm{tr}(A\rho) \leq \sum_i \mathrm{tr}(B_i \delta_i)$, or equivalently, $M \approx N \vDash_{\mathsf{rqPD}} A \Rightarrow \{B_m\}$.

(only if) part. For any $\rho_1, \rho_2 \in \mathcal{D}^1$, select coupling $\rho : \langle \rho_1, \rho_2 \rangle$ such that $\mathrm{tr}((I - A)\rho) = T_{I-A}(\rho_1, \rho_2)$. Since $(\rho_1, \rho_2) \vDash M \approx N$, so $\forall\, i,\ \mathrm{tr}(M_i\, \mathrm{tr}_2(\rho) M_i^\dagger) = \mathrm{tr}(N_i\, \mathrm{tr}_1(\rho) N_i^\dagger)$ as $\mathrm{tr}_2(\rho) = \rho_1$ and $\mathrm{tr}_1(\rho) = \rho_2$, which implies $\rho \vDash_{\mathsf{rqPD}} M \approx N$, by assumption, there exists couplings $\delta_i : \langle M_i\, \mathrm{tr}_2(\rho) M_i^\dagger, N_i\, \mathrm{tr}_1(\rho) N_i^\dagger \rangle$ such that $\mathrm{tr}(A\rho) \leq \sum_i \mathrm{tr}(B_i \delta_i)$, or equivalently,

$$T_{I-A}(\rho_1, \rho_2) = \mathrm{tr}((I - A)\rho) = 1 - \mathrm{tr}(A\rho) \geq 1 - \sum_i \mathrm{tr}(B_i \delta_i) = \sum_i \mathrm{tr}((I - B_i)\delta_i)$$

as desired.

Now we prove clause (2).

(if) part. For any $\rho_1, \rho_2 \in \mathcal{D}^1$ (the case for partial state is similar just by normalize everything) such that $\rho_1 X^\# \rho_2$. Let ρ be the witness, thus $\mathrm{supp}(\rho) \subseteq X$, in other words, $\mathrm{tr}((X \mid 0)\rho) = \mathrm{tr}(0\rho) = 0$ by Definition A.6, thus $T_{X|0}(\rho_1, \rho_2) = 0$. By assumption, there exists couplings $\delta_i : \langle M_i \rho_1 M_i^\dagger, N_i \rho_2 N_i^\dagger \rangle$ such that

$$0 = T_{X|0}(\rho_1, \rho_2) \geq \sum_i \mathrm{tr}(Y_i^\perp \delta_i),$$

so $\mathrm{tr}(Y_i^\perp \delta_i) = 0$, or equivalently, $\mathrm{supp}(\delta_i) \subseteq Y_i$. So $(M_i \rho_1 M_i^\dagger) Y_i^\# (N_i \rho_2 N_i^\dagger)$ for all i, i.e., $\vDash_{\mathsf{pqRHL}} M \approx N : X \Rightarrow \{Y_m\}$.

(only if) part. For any $\rho_1, \rho_2 \in \mathcal{D}^1$, if $T_{X|0}(\rho_1, \rho_2) = +\infty$, then it trivially holds. Otherwise, there exists a coupling $\rho : \langle \rho_1, \rho_2 \rangle$ such that $\mathrm{tr}((X \mid 0)\rho) < +\infty$, so $\mathrm{supp}(\rho) \subseteq X$, thus $\rho_1 X^\# \rho_2$, by assumption, $(M_i \rho_1 M_i^\dagger) Y_i^\# (N_i \rho_2 N_i^\dagger)$, and set δ_i as the witness. Thus, $\mathrm{supp}(\delta_i) \subseteq Y_i$, or equivalently, $\mathrm{tr}(Y_i \delta_i) = 0$. Thus, $\sum_i \mathrm{tr}(Y_i^\perp \delta_i) = 0 \leq T_{X|0}(\rho_1, \rho_2)$, and this completes the proof. □

Theorem E.4 (Theorem VI.11)**.** *The extra rules for* qOTL *in Fig. 2 are sound regarding the notion of validity.*

Proof. (assign) and (apply) are the same as applying the corresponding one-side rule twice on the left and right.

(seq+) We employ Lemma VI.2 and Lemma IV.3 to interpret judgements. For any $z \in Z$, $\rho, \sigma \in \mathcal{D}^1$ such that $(\rho, \sigma) \vDash \Gamma$, by first assumption, $T_P(\rho, \sigma) \geq T_Q([\![S_1]\!](\rho), [\![S_1']\!](\sigma))$, by entailment we know that $([\![S_1]\!](\rho), [\![S_1']\!](\sigma)) \vDash \Gamma'$, then by the second assumption, it holds that

$$T_P(\rho, \sigma) \geq T_Q([\![S_1]\!](\rho), [\![S_1']\!](\sigma)) \geq T_R([\![S_2]\!]([\![S_1]\!](\rho)), [\![S_2']\!]([\![S_1']\!](\sigma))) = T_R([\![S_1; S_2]\!](\rho), [\![S_1'; S_2']\!](\sigma)).$$

(if) For any $z \in Z$ and $\rho, \sigma \in \mathcal{D}^1$ such that $(\rho, \sigma) \vDash \Gamma$, if $T_P(\rho, \sigma) = +\infty$, then obviously $T_P(\rho, \sigma) \geq T_A([\![\mathbf{if}]\!](\rho), [\![\mathbf{if}']\!](\sigma))$, and then follows by Lemma VI.2. If $T_P(\rho, \sigma)$ is finite, by the first assumption, $\operatorname{tr}(M_k \rho M_k^\dagger) = \operatorname{tr}(M_k' \sigma M_k'^\dagger)$ (follows by the existence of coupling and let it by δ_k) and denote it by p_k. By the second assumption,

$$\operatorname{tr}(R_k \delta_k) \geq p_k T_{R_k}(M_k \rho M_k^\dagger / p_k, M_k' \sigma M_k'^\dagger / p_k) \geq p_k T_Q([\![S_k]\!](M_k \rho M_k^\dagger / p_k), [\![S_k']\!](M_k' \sigma M_k'^\dagger / p_k)).$$

Sum it up over k, we have:

$$\begin{aligned} T_C(\rho, \sigma) &\geq \sum_k \operatorname{tr}(R_k \delta_k) \\ &\geq \sum_k p_k T_Q([\![S_k]\!](M_k \rho M_k^\dagger / p_k), [\![S_k']\!](M_k' \sigma M_k'^\dagger / p_k)) \\ &\geq T_Q(\sum_k p_k [\![S_k]\!](M_k \rho M_k^\dagger / p_k), \sum_k p_k [\![S_k']\!](M_k' \sigma M_k'^\dagger / p_k) \\ &= T_Q([\![\mathbf{if}]\!](\rho), [\![\mathbf{if}']\!](\sigma)). \end{aligned}$$

Where the first inequality follows from the first assumption, the third inequality is due to Proposition C.2 since $\{p_k\}$ is a (sub)distribution. This completes the proof.

(while) Let $\mathcal{E}_0(\cdot) = M_0(\cdot)M_0^\dagger$, $\mathcal{E}_1(\cdot) = M_1(\cdot)M_1^\dagger$, $\mathcal{E}_0'(\cdot) = M_0'(\cdot)M_0'^\dagger$, $\mathcal{E}_1'(\cdot) = M_1'(\cdot)M_1'^\dagger$. Fix $z \in Z$. For any $\sigma \in \mathcal{D}^1(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, let $\rho = \operatorname{tr}_2(\sigma)$ and $\rho' = \operatorname{tr}_1(\sigma)$. It is trivial if $\operatorname{tr}(P\sigma) = +\infty$. Otherwise, $\operatorname{tr}(P\sigma) < +\infty$, so $T_P(\rho, \rho') < +\infty$. Set $\rho_0 = \rho$, $\rho_0' = \rho'$, $p_0 = 1$, so $\rho_0, \rho_0' \in \mathcal{D}^1$, and $T_p(\rho_0, \rho_0') < +\infty$. We inductively construct $\rho_n, \rho_n', \sigma_n, p_n, q_n$ as follows:

- Since $\rho_n, \rho_n' \in \mathcal{D}^1$ and $T_p(\rho_n, \rho_n') < +\infty$, by the first assumption, there exists $\sigma_n : \langle \mathcal{E}_0(\rho_n), \mathcal{E}_0'(\rho_n') \rangle$ and $\sigma_n' : \langle \mathcal{E}_1(\rho_n), \mathcal{E}_1'(\rho_n') \rangle$ such that

  $$T_P(\rho_n, \rho_n') \geq \operatorname{tr}(Q_0 \sigma_n) + \operatorname{tr}(Q_1 \sigma_n').$$

  Let $q_n = p_n \operatorname{tr}(\mathcal{E}_0(\rho_n)) = p_n \operatorname{tr}(\mathcal{E}_0'(\rho_n'))$ and $q = \operatorname{tr}(\mathcal{E}_1(\rho_n)) = \operatorname{tr}(\mathcal{E}_1'(\rho_n'))$.
- By the second assumption, we know that

  $$T_{Q_1}(\mathcal{E}_1(\rho_n)/q, \mathcal{E}_1'(\rho_n')/q) \geq T_P([\![S]\!](\mathcal{E}_1(\rho_n)/q), [\![S']\!](\mathcal{E}_1'(\rho_n')/q).$$

  Select the partial coupling $\delta_n : \langle [\![S]\!](\mathcal{E}_1(\rho_n)/q), [\![S']\!](\mathcal{E}_1'(\rho_n')/q) \rangle_p$ such that $T_P([\![S]\!](\mathcal{E}_1(\rho_n)/q), [\![S']\!](\mathcal{E}_1'(\rho_n')/q) = \operatorname{tr}(P\delta_n)$. We set $\rho_{n+1} = \operatorname{tr}_2(\delta_n)/\operatorname{tr}(\delta_n)$ and $\rho_{n+1}' = \operatorname{tr}_1(\delta_n)/\operatorname{tr}(\delta_n)$, $p_{n+1} = p_n q \operatorname{tr}(\delta_n)$. Obviously,

  $$\begin{aligned} T_P(\rho_{n+1}, \rho_{n+1}') &\leq \operatorname{tr}(P\delta_n/\operatorname{tr}(\delta_n)) = T_P([\![S]\!](\mathcal{E}_1(\rho_n)/q), [\![S']\!](\mathcal{E}_1'(\rho_n')/q)/\operatorname{tr}(\delta_n) \\ &\leq T_{Q_1}(\mathcal{E}_1(\rho_n)/q, \mathcal{E}_1'(\rho_n')/q)/\operatorname{tr}(\delta_n) \\ &\leq \operatorname{tr}(Q_1 \sigma_n'/q)/tr(\delta_n) = (p_n/p_{n+1}) \operatorname{tr}(Q_1 \sigma_n') \\ &\leq (p_n/p_{n+1}) T_P(\rho_n, \rho_n') \\ &< +\infty. \end{aligned}$$

Set $\sigma = \sum_i p_i \sigma_i$, it is sufficient to show 1) $T_P(\rho, \rho') \geq \operatorname{tr}(Q_0 \sigma)$ and 2) σ is a partial coupling of the outputs of two $\mathbf{while}$s. We first show (1) is true. First, by the construction above, we know that:

$$\begin{aligned} p_n T_p(\rho_n, \rho_n') &\geq p_n(\operatorname{tr}(Q_0 \sigma_n) + \operatorname{tr}(Q_1 \sigma_n')) \\ &\geq \operatorname{tr}(Q_0(p_n \sigma_n)) + p_n(p_{n+1}/p_n) T_P(\rho_{n+1}, \rho_{n+1}') \\ &= \operatorname{tr}(Q_0(p_n \sigma_n)) + p_{n+1} T_P(\rho_{n+1}, \rho_{n+1}'). \end{aligned}$$

Thus, we have:

$$\begin{aligned}
T_P(\rho,\rho') &= p_0 T_P(\rho_0,\rho_0') \\
&\geq \operatorname{tr}(Q_0(p_0\sigma_0)) + p_1 T_P(\rho_1,\rho_1') \\
&\geq \operatorname{tr}(Q_0(p_0\sigma_0 + p_1\sigma_1)) + p_2 T_P(\rho_2,\rho_2') \\
&\cdots \\
&\geq \operatorname{tr}\Big(Q_0\Big(\sum_i p_i\sigma_i\Big)\Big) \\
&= \operatorname{tr}(Q_0\sigma)
\end{aligned}$$

To show σ is a partial coupling, we first observe that $p_n\rho_n \sqsubseteq (\llbracket S\rrbracket \circ \mathcal{E}_1)^n(\rho)$ since:

$$p_{n+1}\rho_{n+1} = p_n q \operatorname{tr}(\delta_n) \operatorname{tr}_2(\delta_n)/\operatorname{tr}(\delta_n) \sqsubseteq p_n q \llbracket S\rrbracket(\mathcal{E}_1(\rho_n)/q) = (\llbracket S\rrbracket \circ \mathcal{E}_1)(p_n\rho_n) \sqsubseteq \cdots \sqsubseteq (\llbracket S\rrbracket \circ \mathcal{E}_1)^{n+1}(p_0\rho_0).$$

Similarly, $p_n\rho_n' \sqsubseteq (\llbracket S'\rrbracket \circ \mathcal{E}_1')^n(\rho')$. Thus, we have:

$$\begin{aligned}
p_{n+1}\operatorname{tr}_2(\sigma_{n+1}) &= p_{n+1}\mathcal{E}_0(\rho_{n+1}) = p_{n+1}\mathcal{E}_0(\operatorname{tr}_2(\delta_n)/\operatorname{tr}(\delta_n)) \\
&\sqsubseteq p_{n+1}\mathcal{E}_0(\llbracket S\rrbracket(\mathcal{E}_1(\rho_n)/q)/\operatorname{tr}(\delta_n)) = \mathcal{E}_0((\llbracket S\rrbracket \circ \mathcal{E}_1)(p_n\rho_n))) \\
&\sqsubseteq \mathcal{E}_0 \circ (\llbracket S\rrbracket \circ \mathcal{E}_1)^{n+1}(\rho))
\end{aligned}$$

which leads to

$$\operatorname{tr}_2(\sigma) = \sum_n p_n \operatorname{tr}_2(\sigma_n) \sqsubseteq \sum_n \mathcal{E}_0 \circ (\llbracket S\rrbracket \circ \mathcal{E}_1)^n(\rho)) = \llbracket \mathbf{while}[M,S]\rrbracket(\rho).$$

and similarly, $\operatorname{tr}_1(\sigma) \sqsubseteq \llbracket \mathbf{while}[M,S]\rrbracket(\rho')$.

We further observe that

$$\begin{aligned}
\operatorname{tr}(\rho) - \operatorname{tr}(\llbracket \mathbf{while}[M,S](\rho)\rrbracket) &= \operatorname{tr}(\rho) - \sum_n \operatorname{tr}((\mathcal{E}_0 \circ (\llbracket S\rrbracket \circ \mathcal{E}_1)^n)(\rho)) \\
&= \operatorname{tr}(\rho) - \operatorname{tr}(\mathcal{E}_0(\rho)) - \sum_n \operatorname{tr}((\mathcal{E}_0 \circ (\llbracket S\rrbracket \circ \mathcal{E}_1)^{n+1})(\rho)) \\
&= \operatorname{tr}(\mathcal{E}_1(\rho)) - \operatorname{tr}((\llbracket S\rrbracket \circ \mathcal{E}_1)(\rho)) + \\
&\quad \operatorname{tr}((\llbracket S\rrbracket \circ \mathcal{E}_1)(\rho)) - \sum_n \operatorname{tr}((\mathcal{E}_0 \circ (\llbracket S\rrbracket \circ \mathcal{E}_1)^n)((\llbracket S\rrbracket \circ \mathcal{E}_1)(\rho))) \\
&\geq \sum_n \operatorname{tr}((\mathcal{E}_1 - \llbracket S\rrbracket \circ \mathcal{E}_1)((\llbracket S\rrbracket \circ \mathcal{E}_1)^n(\rho))) + \lim_n \operatorname{tr}((\llbracket S\rrbracket \circ \mathcal{E}_1)^n(\rho)) \\
&\geq \sum_n ((\mathcal{E}_1 - \llbracket S\rrbracket \circ \mathcal{E}_1)(p_n\rho_n)) + \lim_n p_n
\end{aligned}$$

where the last inequality comes from 1). $\operatorname{tr}((\mathcal{I} - \llbracket S\rrbracket)\alpha) \leq \operatorname{tr}((\mathcal{I} - \llbracket S\rrbracket)\beta)$ where $\mathcal{I}$ is the identity quantum channel, if $\alpha, \beta \in \mathcal{D}$ such that $\alpha \sqsubseteq \beta$; 2). $p_n\rho_n \sqsubseteq (\llbracket S\rrbracket \circ \mathcal{E}_1)^n(\rho)$ as we proved above; 3). $\operatorname{tr}(p_n\rho_n) = p_n$. Similar result holds:

$$\operatorname{tr}(\rho') - \operatorname{tr}(\llbracket \mathbf{while}[M',S'](\rho')\rrbracket) \geq \sum_n ((\mathcal{E}_1' - \llbracket S'\rrbracket \circ \mathcal{E}_1')(p_n\rho_n')) + \lim_n p_n$$

From the fact that δ_n is a partial coupling, we have the following equivalent forms:

$$\begin{aligned}
&\operatorname{tr}(\llbracket S\rrbracket(\mathcal{E}_1(\rho_n)/q)) + \operatorname{tr}(\llbracket S'\rrbracket(\mathcal{E}_1'(\rho_n')/q)) \leq 1 + \operatorname{tr}(\delta_n) \\
\iff &\operatorname{tr}((\llbracket S\rrbracket \circ \mathcal{E}_1)(\rho_n)) + \operatorname{tr}((\llbracket S'\rrbracket \circ \mathcal{E}_1')(\rho_n')) \leq \operatorname{tr}(\mathcal{E}_1(\rho_n)) + \operatorname{tr}(\mathcal{E}_1'(\rho_n')) - \operatorname{tr}(\mathcal{E}_1(\rho_n)) + \operatorname{tr}(\mathcal{E}_1(\rho_n))\operatorname{tr}(\delta_n) \\
\iff &0 \leq \operatorname{tr}((\mathcal{E}_1 - \llbracket S\rrbracket \circ \mathcal{E}_1)(\rho_n)) + \operatorname{tr}((\mathcal{E}_1' - \llbracket S'\rrbracket \circ \mathcal{E}_1')(\rho_n')) - \operatorname{tr}(\mathcal{E}_1(\rho_n)) + \operatorname{tr}(\mathcal{E}_1(\rho_n))\operatorname{tr}(\delta_n) \\
\iff &\operatorname{tr}(\mathcal{E}_1(p_n\rho_n)) - p_{n+1} \leq \operatorname{tr}((\mathcal{E}_1 - \llbracket S\rrbracket \circ \mathcal{E}_1)(p_n\rho_n)) + \operatorname{tr}((\mathcal{E}_1' - \llbracket S'\rrbracket \circ \mathcal{E}_1')(p_n\rho_n')) \\
\iff &(p_n - p_{n+1}) - \operatorname{tr}(p_n\sigma_n) \leq \operatorname{tr}((\mathcal{E}_1 - \llbracket S\rrbracket \circ \mathcal{E}_1)(p_n\rho_n)) + \operatorname{tr}((\mathcal{E}_1' - \llbracket S'\rrbracket \circ \mathcal{E}_1')(p_n\rho_n'))
\end{aligned}$$

since $\operatorname{tr}(p_n\sigma_n) = p_n \operatorname{tr}(\mathcal{E}_0(\rho_n)) = p_n(\operatorname{tr}(\rho_n) - \operatorname{tr}(\mathcal{E}_1(\rho_n)) = p_n - \operatorname{tr}(\mathcal{E}_1(p_n\rho_n))$.

Combine these fact and back to what we aim to prove:

$$\begin{aligned}
&\mathrm{tr}([\![\mathbf{while}[M,S](\rho)]\!]) + \mathrm{tr}([\![\mathbf{while}[M',S'](\rho')]\!]) \\
\leq\ & \mathrm{tr}(\rho) + \mathrm{tr}(\rho') - \sum_n ((\mathcal{E}_1 - [\![S]\!] \circ \mathcal{E}_1)(p_n\rho_n)) - \sum_n ((\mathcal{E}_1' - [\![S']\!] \circ \mathcal{E}_1')(p_n\rho_n')) - 2\lim_n p_n \\
\leq\ & 2 - \sum_n ((p_n - p_{n+1}) - \mathrm{tr}(p_n\sigma_n)) - 2\lim_n p_n \\
=\ & 2 + \mathrm{tr}(\sigma) - (p_0 - \lim_n p_n) - 2\lim_n p_n \\
=\ & 1 + \mathrm{tr}(\sigma) - \lim_n p_n \\
\leq\ & 1 + \mathrm{tr}(\sigma).
\end{aligned}$$

Take these all together, σ is a partial coupling of $\langle [\![\mathbf{while}[M,S](\rho)]\!], [\![\mathbf{while}[M',S'](\rho')]\!]\rangle$ and this complete the proof. □

APPENDIX F
DEFERRED PROOFS IN "APPLICATIONS"

Theorem F.1 (Theorem VIII.1)**.** *Let S_1, S_2 be AST programs acting on the same Hilbert spaces, $\mathcal{H}_{S_1} = \mathcal{H}_{S_2} = \mathcal{H}$. S_1 and S_2 are semantically equivalent, i.e., $[\![S_1]\!] = [\![S_2]\!]$, if and only if,*

$$\vdash (Y_1, Y_2, n) \in \mathcal{Y} : \{nI + P_{sym}^{\perp}\} S_1 \sim S_2 \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}.$$

where $\mathcal{Y} = \{(Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2), n \in \mathbb{N}) \mid 0 \sqsubseteq Y_1, 0 \sqsubseteq 2Y_2 \sqsubseteq nI, P_{sym}^{\perp}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)\}$.

Proof. The if part is relatively easy, while, the only if part requires Proposition IV.7 that conclude from stable QOP [12].
(**if** part). Suppose Eqn. (4) holds. For any $\rho \in \mathcal{D}(\mathcal{H})$, select the input coupling as the witness of $\rho(=_{sym})^{\#}\rho$ whose existence is ensured by Prop 3.2 in [2], i.e., the coupling $\rho_{in} : \langle \rho, \rho \rangle$ such that $\mathrm{tr}(P_{sym}^{\perp}\rho_{in}) = 0$. By Eqn. (4), we know for any $(Y_1, Y_2, n) \in \mathcal{Y}$, there exists coupling $\sigma : \langle [\![S_1]\!](\rho), [\![S_2]\!](\rho)\rangle$ such that:

$$\begin{aligned}
&\mathrm{tr}((\mathrm{tr}_2(Y_1) \otimes I - I \otimes \mathrm{tr}_2(Y_2))\sigma) \\
\leq\ & \mathrm{tr}(P_{sym}^{\perp}[\mathcal{H}]\rho) = 0,
\end{aligned}$$

since $\mathrm{tr}(\rho) = \mathrm{tr}(\sigma)$, or equivalently,

$$\begin{aligned}
0 \geq & \mathrm{tr}((\mathrm{tr}_2(Y_1) \otimes I - I \otimes \mathrm{tr}_2(Y_2))\sigma) \\
=\ & \mathrm{tr}(2Y_1([\![S_1]\!](\rho) \otimes \frac{I}{2})) - \mathrm{tr}(2Y_2([\![S_2]\!](\rho) \otimes \frac{I}{2}))
\end{aligned}$$

Since $Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2)$ are arbitrary (since we can always select sufficient large $n \in \mathbb{N}$) such that $P_{sym}^{\perp}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)\}$, according to Theorem III.3, we have:

$$([\![S_1]\!](\rho) \otimes \frac{I}{2})(=_{sym})^{\#}([\![S_2]\!](\rho) \otimes \frac{I}{2}),$$

which, again by Prop 3.2 in [2], leads to $[\![S_1]\!](\rho) \otimes \frac{I}{2} = [\![S_2]\!](\rho) \otimes \frac{I}{2}$, or equivalently, $[\![S_1]\!](\rho) = [\![S_2]\!](\rho)$. Since ρ is arbitrary, we must have $[\![S_1]\!] = [\![S_2]\!]$.
(**only if** part). Since two programs are equivalent, by Proposition IV.7, we know that for any $\rho_1, \rho_2 \in \mathcal{D}^1$, $T_s([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \leq T_s(\rho_1, \rho_2) \leq T(\rho_1, \rho_2)$. Next, by Proposition IV.8, we know that for all $Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2)$ such that $P_{sym}^{\perp}[\mathcal{H} \otimes \mathcal{H}_2] \geq 2(Y_1 \otimes I - I \otimes Y_2)$, it holds that:

$$\mathrm{tr}(\mathrm{tr}_2(Y_1)[\![S_1]\!](\rho_1)) \leq \mathrm{tr}(\mathrm{tr}_2(Y_2))[\![S_2]\!](\rho_2)) + T(\rho_1, \rho_2).$$

If $n \in \mathbb{N}$ such that $0 \sqsubseteq 2Y_2 \sqsubseteq nI$, then we have:

$$\begin{aligned}
T_{\mathrm{tr}_2(Y_1)\otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))}([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) &= n + \mathrm{tr}(\mathrm{tr}_2(Y_1)[\![S_1]\!](\rho_1)) - \mathrm{tr}(\mathrm{tr}_2(Y_2))[\![S_2]\!](\rho_2)) \\
&\leq n + T(\rho_1, \rho_2) = T_{nI + P_{sym}^{\perp}}(\rho_1, \rho_2)
\end{aligned}$$

where we use the fact that S_1, S_2 are AST programs. The rest is straightforward Lemma IV.3 and Lemma VI.2. □

Proposition F.2 (Encoding of Trace Distance)**.** *The following are equivalent for all AST programs S_1, S_2 such that[3] $\mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $\mathsf{TD}([\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2)) \leq \mathrm{tr}(\Phi_1\rho_1) + \mathrm{tr}(\Phi_2\rho_2)$ *for all $z \in Z$ and $\rho_1 X^{\#} \rho_2$;*
2) $\vDash 0 \sqsubseteq P \sqsubseteq I : \{X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2)\}\ S_1 \sim S_2\ \{P \otimes I + I \otimes (I - P)\}$.

[3]We could also just ask all programs to be interpreted over $\mathcal{H} = \mathcal{H}_{\text{all variables}}$, or over $\mathcal{H} = \mathcal{H}_{var(S_1) \cup var(S_2)}$.

Proof. Firstly, (2) is equivalent to saying that for all $\rho : \langle \rho_1, \rho_2 \rangle, P$ there exists a coupling σ such that

$$\begin{aligned}\mathrm{tr}((X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2))\rho) &\geq \mathrm{tr}((P \otimes I)\sigma) + \mathrm{tr}((I \otimes (I - P))\sigma) \\ &= \mathrm{tr}(P\sigma_1) + \mathrm{tr}(\sigma) - \mathrm{tr}(P\sigma_2)\end{aligned}$$

where $\sigma_1 = [\![S_1]\!](\rho_1)$ and $\sigma_2 = [\![S_2]\!](\rho_2)$. Because S_1, S_2 are AST, this is in turn equivalent to saying that for all ρ, z and P,

$$\mathrm{tr}((X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2))\rho) - \mathrm{tr}(\rho) \geq \mathrm{tr}(P(\rho_1 - \rho_2)),$$

which is equivalent to saying that

$$\mathsf{TD}(\rho_1, \rho_2) = \max_{0 \sqsubseteq P \sqsubseteq I} \mathrm{tr}(P(\rho_1 - \rho_2)) \leq \mathrm{tr}((X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2))\rho) - \mathrm{tr}(\rho).$$

Now, if $\rho_1 X^{\#} \rho_2$ does not hold, then $\mathrm{tr}(X^{\perp}\rho) > 0$ for any ρ, In this case, $\mathrm{tr}((X \mid (I + \Phi_1 \otimes I + I \otimes \Phi_2))\rho) = +\infty$ and the inequality trivially holds. Thus, we only need to consider the case when $\rho_1 X^{\#} \rho_2$. In this case, we only need to consider any coupling ρ with $\mathrm{tr}(\rho X^{\perp}) = 0$ (by our assumption, such ρ must exist). This gives

$$\mathsf{TD}(\rho_1, \rho_2) = \max_{0 \sqsubseteq P \sqsubseteq I} \mathrm{tr}(P(\rho_1 - \rho_2)) \leq \mathrm{tr}(\Phi_1 \rho_1) + \mathrm{tr}(\Phi_2 \rho_2)$$

as we desired.

□

Proposition F.3 (Proposition VIII.7)**.** *Let $\lambda > 0$. The following are equivalent for all AST programs S_1, S_2 such that $\mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $W([\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho))) \leq \lambda \cdot W(\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho))$ *for all* $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$*;*
2) $\vDash \{\lambda^2 P^{\perp}_{sym}\}\ S_1 \sim S_2\ \{P^{\perp}_{sym}\}$.

Proof. By definition, we know that the second condition is equivalent to: for every $\rho \in \mathcal{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$, there is a coupling $\sigma : \langle [\![S_1]\!](\mathrm{tr}_2(\rho)), [\![S_2]\!](\mathrm{tr}_1(\rho)) \rangle$ such that

$$\lambda^2 \,\mathrm{tr}(\rho P^{\perp}_{sym}) \geq \mathrm{tr}(\sigma P^{\perp}_{sym}).$$

Note that σ only depends on $\mathrm{tr}_2(\rho), \mathrm{tr}_1(\rho)$. Thus, for fixed ρ_1 and ρ_2 we can write the second condition equivalently as

$$\min_{\rho : \langle \rho_1, \rho_2 \rangle} \max_{\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2) \rangle} \lambda^2 \,\mathrm{tr}(\rho P^{\perp}_{sym}) - \mathrm{tr}(\sigma P^{\perp}_{sym}) \geq 0.$$

This can be simplified to

$$\lambda^2 \min_{\rho : \langle \rho_1, \rho_2 \rangle} \mathrm{tr}(\rho P^{\perp}_{sym}) \geq \min_{\sigma : \langle [\![S_1]\!](\rho_1), [\![S_2]\!](\rho_2) \rangle} \mathrm{tr}(\sigma P^{\perp}_{sym}),$$

which is equivalent to the first condition by definition. □

Proposition F.4 (Proposition VIII.12)**.** *For a quantum system $\mathbb{S} = \langle \mathcal{H}, \rho_0, A, C, do, measure \rangle$ with $\rho_0 = |0\rangle\langle 0|$, let $G_1, G_2 \subseteq A$ be two groups of agents, and $D \subseteq C$ be a set of commands. The following are equivalent:*

- $G_1, D : |G_2$.
- $\forall \alpha \in (A \times C)^*$,

$$\begin{aligned}&\vDash a \in G_2, E = \{E_\lambda | \lambda \in \Lambda_E\} \in \mathbb{M}_a, T \subseteq \Lambda_E : \\ &\{I\}\ q := |0\rangle; S_\alpha \sim q := |0\rangle; S_{\mathsf{purge}_{G_1, D}(\alpha)}\ \{M\},\end{aligned}$$

where $M = M_T \otimes I + I \otimes (I - M_T)$ with $M_T = \sum_{\lambda \in T} E_\lambda$.

Proof. By the definition of validity, the second condition can be equivalently written as the following.

$\forall \alpha \in (A \times C)^*, a \in G_2, E = \{E_\lambda | \lambda \in \Lambda_E\} \in \mathbb{M}_a$ and $T \subseteq \Lambda_E$, we have

$$\mathrm{tr}(\rho I) \geq \mathrm{tr}(\sigma(M_T \otimes I + I \otimes (I - M_T))),$$

which could be simplified to

$$\mathrm{tr}(M_T(\sigma_1 - \sigma_2)) \leq 0,$$

with $\sigma_1 = \mathrm{tr}_2(\sigma) = \mathcal{E}_\alpha(|0\rangle\langle 0|)$, and $\sigma_2 = \mathrm{tr}_1(\sigma) = \mathcal{E}_{\mathsf{purge}_{G_1, D}(\alpha)}(|0\rangle\langle 0|)$. Now, notice that $\forall T \subseteq \Lambda_E\ \mathrm{tr}(M_T(\sigma_1 - \sigma_2)) \leq 0$ is equivalent to

$$\max_T \left(p_{E, \sigma_1}(T) - p_{E, \sigma_2}(T)\right) \leq 0,$$

we can rewrite the second condition as $\forall \alpha \in (A \times C)^*, a \in G_2$,

$$d_a\left(\mathcal{E}_\alpha(|0\rangle\langle 0|), \mathcal{E}_{\mathsf{purge}_{G_1, D}(\alpha)}(|0\rangle\langle 0|)\right) \leq 0.$$

Thus, it is equivalent to $G_1, D : |G_2$ by definition. □

Proposition F.5 (Proposition VIII.15)**.** *The following are equivalent for all AST programs S on an n-qubit system:*

1) $[\![S]\!]$ *is* (ε, δ)*-differentially private;*
2) $\vDash i \in [n], 0 \sqsubseteq M \sqsubseteq I : \{P_{i,sym}|(\exp(\varepsilon) + \delta)I\}\ S \sim S\ \{M \otimes I + \exp(\varepsilon) I \otimes (I - M)\}$.

Here $P_{i,sym} = P_{sym}[\mathcal{H}_{[n]-i}] \otimes (I_{i\langle 1\rangle} \otimes I_{i\langle 2\rangle})$ *for* $i \in [n]$.

Proof. We first notice that, by definition 1) states that for all measurement M, set A, and $\forall \rho, \sigma$, if $\exists i \in [n]$ such that $\mathrm{tr}_i(\rho) = \mathrm{tr}_i(\sigma)$, then

$$\Pr[\mathcal{E}(\rho) \in_M A] \leq \exp(\varepsilon) \cdot \Pr(\mathcal{E}(\sigma) \in_M A) + \delta.$$

This is equivalent to say $\forall M, A, \rho, \sigma$ and $\forall i \in [n]$, if $\mathrm{tr}_i(\rho) = \mathrm{tr}_i(\sigma)$, then the above inequality holds.

Now consider some arbitrary fixed $i \in [n]$, and any ρ and σ with a coupling $\rho_0 : \langle \rho, \sigma \rangle$. If $\mathrm{tr}_i(\rho) \neq \mathrm{tr}_i(\sigma)$, then $\mathrm{tr}(P^{\perp}_{i,sym}\rho_0) > 0$, and thus $\mathrm{tr}(\rho_0(P_{i,sym}|(\exp(\varepsilon) + \delta)I)) = +\infty$, meaning that it is always valid in this case. Therefore, we only need to consider the case where $\mathrm{tr}_i(\rho) = \mathrm{tr}_i(\sigma)$. In this case, we consider the case $\mathrm{supp}(\rho_0) \sqsubseteq P_{i,sym}$ without loss of generality (otherwise the validity condition holds directly). The condition is for any M satisfying $0 \sqsubseteq M \sqsubseteq I$,

$$\exp(\varepsilon) + \delta \geq \mathrm{tr}([\![S]\!](\rho)M) + \exp(\varepsilon)(1 - \mathrm{tr}([\![S]\!](\sigma)M)),$$

which could be simplified to

$$\mathrm{tr}([\![S]\!](\rho)M) \leq \exp(\varepsilon)\,\mathrm{tr}([\![S_1]\!](\sigma)M) + \delta.$$

Note that when M goes over all $0 \sqsubseteq M \sqsubseteq I$, it exactly goes over all POVMs $\sum_{m \in A} M_m$, we know that the second condition is then equivalent to the first as we want. □

We need the following proposition about the projector onto the symmetric subspace.

Proposition F.6 (Adapted from Proposition 3.2 in [55])**.** $\rho_1 = \rho_2$ *if and only if* $\rho_1(=_{sym})^{\#}\rho_2$*, where* $=_{sym}$ *stands for the space of* $\mathrm{supp}(P_{sym})$.

Proposition F.7 (Proposition VIII.5)**.** *Let $c \in \mathbb{R}^+$. The following are equivalent for all AST programs S_1, S_2 such that $\mathcal{H} = \mathcal{H}_{S_1} = \mathcal{H}_{S_2}$:*

1) $\|[\![S_1]\!] - [\![S_2]\!]\|_{\diamond} \leq 2c$;
2) $\vDash 0 \sqsubseteq P \sqsubseteq I_{\mathcal{H}\otimes\mathcal{H}} : \{P_{sym}[\mathcal{H} \otimes \mathcal{H}] \mid (1 + c)I\}\ S_1 \sim S_2\ \{P \otimes I + I \otimes (I - P)\}$.

Proof. This is direct by applying Proposition VIII.3 with $X = P_{sym}[\mathcal{H} \otimes \mathcal{H}]$, $\Phi_1 = \Phi_2 = cI/2$, and the definition of diamond distance for completely positive and trace non-increasing linear maps. □

APPENDIX G
CONCRETE EXAMPLES

A. An Example of Program Equivalence (by Duality Rules)

Example G.1 (Example 1.1 in [55])**.** *Let q be a qubit quantum variable, $\mathcal{M}$ be the computational basis measurement, and $\mathcal{M}'$ be the measurement in the basis $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. Consider the following two programs:*

$$S_1 \equiv q := |0\rangle; q := H[q]; Q_1,$$

$$S_2 \equiv q := |0\rangle; Q_2; q := H[q].$$

Here

$$Q_1 \equiv \textbf{if}\ (\square 0 \cdot \mathcal{M}[q] = 0 \to q := X[q]; \square 1 \cdot \mathcal{M}[q] = 1 \to q := H[q])\ \textbf{fi},$$

and

$$Q_2 \equiv \textbf{if}\ (\square 0 \cdot \mathcal{M}'[q] = 0 \to q := Z[q]; \square 1 \cdot \mathcal{M}'[q] = 1 \to q := H[q])\ \textbf{fi}$$

In the following, we will prove S_1 and S_2 are equivalent using one-sided rules.

In simple words, we want to show that $\{P^{\perp}_{sym}\}\ S_1 \sim S_2\ \{P^{\perp}_{sym}\}$. Using the duality rule as is stated in theorem VIII.1, we need to prove the following

$$\begin{aligned} \vdash (Y_1, Y_2, n) \in \mathcal{Y} : \{nI + P^{\perp}_{sym}\} \\ S_1 \sim S_2 \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}. \end{aligned}$$

where $\mathcal{Y} = \{(Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2), n \in \mathbb{N}) \mid 0 \sqsubseteq Y_1, 0 \sqsubseteq 2Y_2 \sqsubseteq nI, P^{\perp}_{sym}(\mathcal{H} \otimes \mathcal{H}_2) \sqsupseteq 2(Y_1 \otimes I - I \otimes Y_2)\}$.

To present our proof in a compact way, using rule R to infer the judgment $\Gamma \vdash Z : \{A\}\ P_1 \sim P_2\ \{B\}$ will be written as:

$$\begin{array}{l}\{A\}\\ \bullet\ P_1 \sim P_2 \qquad (R)\\ \{B\}\end{array}$$

The proof is as follows.

$$\begin{array}{l}\left\{nI + P_{sym}^{\perp}\right\}\{A_1\} \qquad \text{(csq)}\\ \bullet\ q := |0\rangle; \sim \mathbf{skip}; \qquad \text{(assign-L)}\\ \{A_2\}\\ \bullet\ \mathbf{skip}; \sim q := |0\rangle; \qquad \text{(assign-R)}\\ \{(HB_1H) \otimes I + I \otimes B_2\}\\ \bullet\ q := H[q]; \sim \mathbf{skip}; \qquad \text{(apply-L)}\\ \{B_1 \otimes I + I \otimes B_2\}\\ \bullet\ Q_1; \sim \mathbf{skip}; \qquad \text{(if-L)}\\ \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes B_2\}\\ \bullet\ \mathbf{skip}; \sim Q_2; \qquad \text{(if-L)}\\ \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - H\,\mathrm{tr}_2(Y_2)H)\}\\ \bullet\ \mathbf{skip}; \sim q := H[q]; \qquad \text{(apply-R)}\\ \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}\end{array}$$

Fig. 3. Verification of example G.1

Here we denote $B_1 = \langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle|0\rangle\langle 0| + \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle|1\rangle\langle 1|$, $B_2 = nI - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle|-\rangle\langle -| - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle|+\rangle\langle +|$, $A_1 = (\langle 0|HB_1H|0\rangle + \langle 0|B_2|0\rangle)I$, and $A_2 = (HB_1H) \otimes I + \langle 0|B_2|0\rangle I$. The detailed proof of Q_1 and Q_2 is as follows.

In the proof, for Q_1, we have $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$.

For the branch with measurement result 0, we have:

$$\begin{array}{l}\{(X\,\mathrm{tr}_2(Y_1)X) \otimes I + I \otimes B_2\}\\ \bullet\ q := X[q]; \sim \mathbf{skip} \qquad \text{(apply-L)}\\ \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes B_2\}\end{array}$$

For the branch with measurement result 1, we have:

$$\begin{array}{l}\{(H\,\mathrm{tr}_2(Y_1)H) \otimes I + I \otimes B_2\}\\ \bullet\ q := H[q]; \sim \mathbf{skip}; \qquad \text{(apply-L)}\\ \{\mathrm{tr}_2(Y_1) \otimes I + I \otimes B_2\}\end{array}$$

Fig. 4. Verification of Q_1 in example G.1

In the proof, for Q_2, we have $M_0' = |+\rangle\langle +|$, $M_1' = |-\rangle\langle -|$.

Finally, we need to show that $nI + P_{sym}^{\perp} \sqsupseteq A_1$ and apply the csq rule. This can be directly proved as follows:

Proposition G.2. *Denote* $B_1 = \langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle|0\rangle\langle 0| + \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle|1\rangle\langle 1|$, $B_2 = nI - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle|-\rangle\langle -| - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle|+\rangle\langle +|$, $A_1 = (\langle 0|HB_1H|0\rangle + \langle 0|B_2|0\rangle)I$, *and* $A_2 = (HB_1H) \otimes I + \langle 0|B_2|0\rangle I$, *where* $(Y_1, Y_2, n) \in \mathcal{Y}$ *with* $\mathcal{Y} = \{(Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H} \otimes \mathcal{H}_2), n \in \mathbb{N}) \mid 0 \sqsubseteq Y_1, 0 \sqsubseteq 2Y_2 \sqsubseteq nI, P_{sym}^{\perp}(\mathcal{H} \otimes \mathcal{H}_2) \sqsupseteq 2(Y_1 \otimes I - I \otimes Y_2)\}$. *Then* $nI + P_{sym}^{\perp} \sqsupseteq A_1$.

Proof. Since $P_{sym}^{\perp}(\mathcal{H} \otimes \mathcal{H}_2) \sqsupseteq 2(Y_1 \otimes I - I \otimes Y_2)$, we know for any ρ,

$$\mathrm{tr}(\rho P_{sym}^{\perp}(\mathcal{H} \otimes \mathcal{H}_2)) \geq \mathrm{tr}(2\rho(Y_1 \otimes I - I \otimes Y_2)).$$

Specifically, taking ρ of the form $\rho_0 \otimes |\Phi\rangle\langle\Phi|$ where $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we get

$$\mathrm{tr}(\rho_0 P_{sym}^{\perp}(\mathcal{H})) \geq \mathrm{tr}(\rho_0(\mathrm{tr}_2(Y_1) \otimes I - I \otimes \mathrm{tr}_2(Y_2))),$$

For the branch with measurement result 0, we have:

$$\begin{aligned}&\{\mathrm{tr}_2(Y_1)\otimes I + I\otimes(nI - ZH\,\mathrm{tr}_2(Y_2)HZ)\}\\&\bullet\ \mathbf{skip}; \sim q := Z[q]; \qquad \text{(apply-R)}\\&\{\mathrm{tr}_2(Y_1)\otimes I + I\otimes(nI - H\,\mathrm{tr}_2(Y_2)H)\}\end{aligned}$$

For the branch with measurement result 1, we have:

$$\begin{aligned}&\{\mathrm{tr}_2(Y_1)\otimes I + I\otimes(nI - \mathrm{tr}_2(Y_2))\}\\&\bullet\ \mathbf{skip}; \sim q := H[q]; \qquad \text{(apply-R)}\\&\{\mathrm{tr}_2(Y_1)\otimes I + I\otimes(nI - H\,\mathrm{tr}_2(Y_2)H)\}\end{aligned}$$

Fig. 5. Verification of Q_2 in example G.1

meaning that

$$P_{sym}^{\perp}(\mathcal{H}) \sqsupseteq (\mathrm{tr}_2(Y_1)\otimes I - I\otimes \mathrm{tr}_2(Y_2)).$$

It suffices to prove that, for any density matrix ρ, we have

$$\mathrm{tr}(\rho(nI + P_{sym}^{\perp})) \geq \mathrm{tr}(\rho A_1).$$

By simplifying the above inequality, we only needs to prove

$$2\,\mathrm{tr}(\rho P_{sym}^{\perp}) \geq \langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle + \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle.$$

Note that, for $\sigma = \frac{1}{2}(|1\rangle\langle 1|\otimes|-\rangle\langle -| + |-\rangle\langle -|\otimes|1\rangle\langle 1|)$, we have

$$\langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle + \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle = 2\,\mathrm{tr}(\sigma(\mathrm{tr}_2(Y_1)\otimes I - I\otimes\mathrm{tr}_2(Y_2))).$$

Note that σ is in the symmetric subspace, we know $\mathrm{tr}(\rho P_{sym}^{\perp}) \geq \mathrm{tr}(\sigma P_{sym}^{\perp}) = 0$ for any ρ, giving that $\mathrm{tr}(\rho P_{sym}^{\perp}) \geq \mathrm{tr}(\sigma P_{sym}^{\perp}) \geq \mathrm{tr}(\sigma(\mathrm{tr}_2(Y_1)\otimes I - I\otimes\mathrm{tr}_2(Y_2)))$ as we desired. □

B. Applications of Two-sided Rules

Using theorem VIII.1, we need to prove the following

$$\begin{aligned}\vdash (Y_1,Y_2,n)\in\mathcal{Y} : \{&nI + P_{sym}^{\perp}\}\\ &S_1 \sim S_2\{\mathrm{tr}_2(Y_1)\otimes I + I\otimes(nI - \mathrm{tr}_2(Y_2))\}.\end{aligned}$$

where $\mathcal{Y} = \{(Y_1, Y_2 \in \mathsf{Pos}(\mathcal{H}\otimes\mathcal{H}_2), n\in\mathbb{N}) \mid 0\sqsubseteq Y_1, 0\sqsubseteq 2Y_2\sqsubseteq nI, P_{sym}^{\perp}(\mathcal{H}\otimes\mathcal{H}_2)\sqsupseteq 2(Y_1\otimes I - I\otimes Y_2)\}$.

For simplicity, using rule R to infer the judgment $\Gamma \vdash Z : \{A\}\ P_1 \sim P_2\ \{B\}$ with measurement conditions or side conditions Γ will be written as

$$\begin{aligned}&\{A\}\{SC:\Gamma\}\\&\bullet\ P_1 \sim P_2 \qquad (R)\\&\{B\}\end{aligned}$$

The proof can be found in fig. 6, For simplicity, we write

$$\begin{aligned}B = nI &+ \langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle|0\rangle\langle 0|\otimes I - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle I\otimes|+\rangle\langle +|\\&+ \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle|1\rangle\langle 1|\otimes I - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle I\otimes|-\rangle\langle -|,\end{aligned}$$

and $c = \frac{1}{2}(\langle 1|\,\mathrm{tr}_2(Y_1)|1\rangle + \langle -|\,\mathrm{tr}_2(Y_1)|-\rangle - \langle -|\,\mathrm{tr}_2(Y_2)|-\rangle - \langle 1|\,\mathrm{tr}_2(Y_2)|1\rangle)$. We also use proposition G.2 for applying the csq rule in the first line.

To apply the rule (if), we need to first verify the measurement condition $\mathcal{M}\approx\mathcal{M}'$ and the measurement property $\mathcal{M}\approx\mathcal{M}'\vDash\{B\}\mathcal{M}\approx\mathcal{M}'\{A_{00},A_{11}\}$ before applying the (if) and (seq+) rule at $Q_1;\sim Q_2;$. For the measurement condition, it can be proved by using theorem VI.9 as follows. As the theorem states, we only need to prove

$$\{nI\}\ q := |0\rangle; q := H[q]; \sim q := |0\rangle; \left\{(\textstyle\sum_i M_i^{\dagger}Y_iM_i)\otimes I + I\otimes\left[nI - (\sum_i M_i'^{\dagger}Z_iM_i')\right]\right\}$$

where $\mathcal{Y}_2 = \{(Y_0,Y_1,Z_0,Z_1,n) \mid \forall i,\ 0\sqsubseteq Y_i,\ 0\sqsubseteq Z_i\sqsubseteq nI, Y_i\otimes I - I\otimes Z_i\sqsubseteq 0, \forall j\neq i,\ Y_i\otimes I - I\otimes Z_j\sqsubseteq I\}$. By applying the rules (apply) and (assign), we only need to prove

$$\langle +|Z_0|+\rangle + \langle -|Z_1|-\rangle \geq \langle 0|Y_0|0\rangle + \langle 1|Y_1|1\rangle,$$

$\{nI + P_{sym}^{\perp}\}\ \{cI\}$(csq)
$\bullet\ q := |0\rangle; \sim q := |0\rangle;$ (assign)
$\{(H \otimes I)B(H \otimes I)\}$
$\bullet\ q := H[q]; \sim \mathbf{skip};$ (apply-L)
$\{B\}\ \{SC : \mathcal{M} \approx \mathcal{M}'\}$
$\bullet\ Q_1; \sim Q_2;$ (if)
$\{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - H\,\mathrm{tr}_2(Y_2)H)\}$
$\bullet\ \mathbf{skip}; \sim q := H[q];$ (apply-R)
$\{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}$

Fig. 6. Verification of example G.1 using two-sided rules

For the if branch with measurement result being 0, we have

$\{A_{00} \equiv X\,\mathrm{tr}_2(Y_1)X \otimes I + I \otimes (nI - ZH\,\mathrm{tr}_2(Y_2)HZ)\}$
$\bullet\ q := X[q]; \sim q := Z[q];$ (apply)
$\{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - H\,\mathrm{tr}_2(Y_2)H)\}$

For the if branch with measurement result being 1, we have

$\{A_{11} \equiv H\,\mathrm{tr}_2(Y_1)H \otimes I + I \otimes (nI - \mathrm{tr}_2(Y_2))\}$
$\bullet\ q := H[q]; \sim q := H[q];$ (apply)
$\{\mathrm{tr}_2(Y_1) \otimes I + I \otimes (nI - H\,\mathrm{tr}_2(Y_2)H)\}$

Fig. 7. Verification of the if in example G.1 using two-sided rules

which is a direct result by using $Y_i \otimes I - I \otimes Z_i \sqsubseteq 0$ on the states $|0\rangle|+\rangle$ for $i = 0$ and $|1\rangle|-\rangle$ for $i = 1$, respectively. With the measurement condtion, we verify the measurement property as follows. By definition, we need to prove for all ρ, σ such that $(\rho, \sigma) \vDash \mathcal{M} \approx \mathcal{M}'$, if $T_B(\rho, \sigma) < +\infty$, then there exist couplings $\delta_0 : \langle M_0^\dagger \rho M_0, M_0'^\dagger \sigma M_0' \rangle$ and $\delta_1 : \langle M_1^\dagger \rho M_1, M_1'^\dagger \sigma M_1' \rangle$, such that

$$T_B(\rho, \sigma) \geq \mathrm{tr}(A_{00}\delta_0) + \mathrm{tr}(A_{11}\delta_1).$$

As B, A_{00} and A_{11} are split, the above inequality can be simplified to

$$\mathrm{tr}(B(\rho \otimes \sigma)) \geq \langle 0|\rho|0\rangle\,\mathrm{tr}(A_{00}|0\rangle\langle 0| \otimes |+\rangle\langle +|) + \langle 1|\rho|1\rangle\,\mathrm{tr}(A_{11}|1\rangle\langle 1| \otimes |-\rangle\langle -|),$$

with $\langle 0|\rho|0\rangle = \langle +|\sigma|+\rangle$ and $\langle 1|\rho|1\rangle = \langle -|\sigma|-\rangle$, as implied by $(\rho, \sigma) \vDash \mathcal{M} \approx \mathcal{M}'$. Thus, the inequality further simplifies to $0 \geq 0$ as all terms are cancelled.

APPENDIX H
STABILIZED QUANTUM OPTIMAL TRANSPORT COST

In this section, we briefly review the proof of

$$T_s(\rho, \sigma) = T(\rho \otimes \frac{I}{2}, \sigma \otimes \frac{I}{2})$$

in [12] for completeness.

We begin with a decomposition of the projector onto the asymmetric subspace.

Lemma H.1 (Identity (1) in [12])**.** *We have*

$$\mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2) = \mathrm{P}_{\mathrm{asym}}(d_1) \otimes \mathrm{P}_{\mathrm{sym}}(d_2) + \mathrm{P}_{\mathrm{sym}}(d_1) \otimes \mathrm{P}_{\mathrm{asym}}(d_2).$$

The following lemma is a special case of the Schur-Weyl duality. Suppose $X \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$, and let Σ_d be the following UU-twirling channel

$$\Sigma_d(X) = \int_{\mathcal{U}_d} (U \otimes U)X(U^\dagger \otimes U^\dagger)\mathrm{d}U,$$

where the integral is with respect to the Haar measure on group $\mathcal{U}_d$ of $d \times d$ unitary matrices. Then, we have:

Lemma H.2 (Theorem 10 in [56])**.**

$$\Sigma_d(X) = \mathrm{Tr}[XP_{\mathrm{sym}}(d)]\frac{P_{\mathrm{sym}}(d)}{\mathrm{Tr}[P_{\mathrm{sym}}(d)]} + \mathrm{Tr}[XP_{\mathrm{asym}}(d)]\frac{P_{\mathrm{asym}}(d)}{\mathrm{Tr}[P_{\mathrm{asym}}(d)]},$$

where $P_{\mathrm{sym}}(d) = (I - F_d)/2$ is the projector onto the symmetric subspace, and $P_{\mathrm{asym}}(d) = I - P_{\mathrm{sym}}(d)$.

Proposition H.3. *The channel Σ_d is self-dual with respect to the Hilbert-Schmidt inner product.*

Proof. For any A and B, we have

$$\begin{aligned}
\mathrm{tr}[A^\dagger \Sigma_d(B)] &= \mathrm{tr}[A^\dagger \int_{\mathcal{U}_d} (U \otimes U)B(U^\dagger \otimes U^\dagger)\mathrm{d}U] \\
&= \int_{\mathcal{U}_d} \mathrm{tr}[A^\dagger (U \otimes U)B(U^\dagger \otimes U^\dagger)]\mathrm{d}U \\
&= \int_{\mathcal{U}_d} \mathrm{tr}[(U^\dagger \otimes U^\dagger)A^\dagger (U \otimes U)B]\mathrm{d}U \\
&= \int_{\mathcal{U}_d} \mathrm{tr}[(U \otimes U)A^\dagger (U^\dagger \otimes U^\dagger)B]\mathrm{d}U \\
&= \mathrm{tr}[\Sigma_d(A^\dagger)B].
\end{aligned}$$

□

Proposition H.4. *Using the above notations, we have*

$$(id_{d_1} \otimes id_{d_1} \otimes \Sigma_{d_2})(\mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)) = \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2).$$

Proof. This can be verified directly by using lemma H.1 and lemma H.2. □

Theorem H.5 (Theorem 3.3 in [12])**.** *For d_1-dimensional quantum density matrices ρ_1 and σ_1, and d_2-dimensional quantum matrices ρ_2 and σ_2, we have*

$$T(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) \geq T\left(\rho_1 \otimes \frac{I_2}{2}, \sigma_1 \otimes \frac{I_2}{2}\right).$$

Proof. Let $\tau_{A_1A_2B_1B_2}$ be an optimal coupling state that gives the value $T(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2)$. Equivalently speaking, we have

$$T\left(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2\right) = \mathrm{Tr}\left[\tau_{A_1B_1A_2B_2}\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)\right],$$

with $\tau_{A_1A_2} = \rho_1 \otimes \rho_2$, and $\tau_{B_1B_2} = \sigma_1 \otimes \sigma_2$. By proposition H.4 and proposition H.3, we have

$$T\left(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2\right) = \mathrm{Tr}\left[\tau_{A_1B_1A_2B_2}\Phi(\mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2))\right] = \mathrm{Tr}\left[\Phi(\tau_{A_1B_1A_2B_2})\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)\right]$$

where Φ is the $id_{d_1} \otimes id_{d_1} \otimes \Sigma_{d_2}$ channel. Using lemma H.1, we have

$$\begin{aligned}
\Phi(\tau_{A_1B_1A_2B_2}) = &\mathrm{tr}_{A_2B_2}[\tau_{A_1B_1A_2B_2}(I \otimes \mathrm{P}_{\mathrm{sym}}(d_2))] \otimes \frac{P_{\mathrm{sym}}(d_2)}{\mathrm{Tr}[P_{\mathrm{sym}}(d_2)]} \\
&+ \mathrm{tr}_{A_2B_2}[\tau_{A_1B_1A_2B_2}(I \otimes \mathrm{P}_{\mathrm{asym}}(d_2))] \otimes \frac{P_{\mathrm{asym}}(d_2)}{\mathrm{Tr}[P_{\mathrm{asym}}(d_2)]}.
\end{aligned}$$

Therefore, we could write

$$X_{A_1B_1} = \mathrm{tr}_{A_2B_2}[\tau_{A_1B_1A_2B_2}(I \otimes \mathrm{P}_{\mathrm{asym}}(d_2))]$$

and

$$Y_{A_1B_1} = \mathrm{tr}_{A_2B_2}[\tau_{A_1B_1A_2B_2}(I \otimes \mathrm{P}_{\mathrm{sym}}(d_2))],$$

with

$$X_{A_1B_1} + Y_{A_1B_1} = \mathrm{tr}_{A_2B_2}[\tau_{A_1B_1A_2B_2}].$$

Then, we have

$$\begin{aligned}
\mathrm{Tr}\left[\Phi(\tau_{A_1B_1A_2B_2})\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)\right] &= \mathrm{Tr}\left[\left(X_{A_1B_1} \otimes \frac{P_{\mathrm{sym}}(d_2)}{\mathrm{Tr}[P_{\mathrm{sym}}(d_2)]}\right) \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)\right] \\
&+ \mathrm{Tr}\left[\left(Y_{A_1B_1} \otimes \frac{P_{\mathrm{asym}}(d_2)}{\mathrm{Tr}[P_{\mathrm{asym}}(d_2)]}\right) \mathrm{P}_{\mathrm{asym}}(d_1 \otimes d_2)\right] \\
&= \mathrm{Tr}\left[X_{A_1B_1}\, \mathrm{P}_{\mathrm{asym}}(d_1)\right] + \mathrm{Tr}\left[Y_{A_1B_1}\, \mathrm{P}_{\mathrm{sym}}(d_1)\right].
\end{aligned}$$

The last step is by using lemma H.1 and the orthogonality of $\mathrm{P}_{\mathrm{asym}}$ and $\mathrm{P}_{\mathrm{sym}}$.

Now, define the state

$$\widetilde{\tau}_{A_1B_1A_2B_2} = X_{A_1B_1} \otimes \frac{P_{\mathrm{sym}}(2)}{\mathrm{Tr}[P_{\mathrm{sym}}(d_2)]} + Y_{A_1B_1} \otimes \frac{P_{\mathrm{asym}}(2)}{\mathrm{Tr}[P_{\mathrm{asym}}(2)]}.$$

Note that $\widetilde{\tau}_{A_1B_1A_2B_2}$ is a density operator of dimension $d_1 \times d_2 \times 2 \times 2$. We claim it is a coupling state of $\rho_1 \otimes I/2$ and $\sigma_1 \otimes I/2$, this is because

$$\tau_{A_1A_2} = X_{A_1} \otimes I/2 + Y_{A_1} \otimes I/2 = \rho_1 \otimes I/2,$$

and

$$\tau_{B_1B_2} = X_{B_1} \otimes I/2 + Y_{B_1} \otimes I/2 = \sigma_1 \otimes I/2.$$

From a similar argument as above, we know

$$\mathrm{Tr}\left[\widetilde{\tau}_{A_1B_1A_2B_2}\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes 2)\right] = \mathrm{Tr}\left[X_{A_1B_1}\, \mathrm{P}_{\mathrm{asym}}(d_1)\right] + \mathrm{Tr}\left[Y_{A_1B_1}\, \mathrm{P}_{\mathrm{sym}}(d_1)\right]$$

Therefore, we know

$$T\left(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2\right) = \mathrm{Tr}\left[\widetilde{\tau}_{A_1B_1A_2B_2}\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes 2)\right] \geq T\left(\rho_1 \otimes I/2, \sigma_1 \otimes I/2\right),$$

as $T\left(\rho_1 \otimes I/2, \sigma_1 \otimes I/2\right)$ is the minimum value of $\mathrm{Tr}\left[\tau'_{A_1B_1A_2B_2}\, \mathrm{P}_{\mathrm{asym}}(d_1 \otimes 2)\right]$ over all coupling states $\tau'_{A_1B_1A_2B_2}$. □

From theorem H.5, we could immediately get $T_s(\rho, \sigma) = T(\rho \otimes \frac{I_2}{2}, \sigma \otimes \frac{I_2}{2})$. This is because

$$T(\rho \otimes \frac{I_2}{2}, \sigma \otimes \frac{I_2}{2}) \geq \inf_{\gamma} T(\rho \otimes \gamma, \sigma \otimes \gamma) \geq T(\rho \otimes \frac{I_2}{2}, \sigma \otimes \frac{I_2}{2}).$$

The first inequality is by the definition of $\inf$, and the second is by applying theorem H.5.

APPENDIX I
KANTOROVICH-RUBINSTEIN DUALITY

We first review the Kantorovich duality theorem in the theory of optimal transport.

Theorem I.1 (Kantorovich Duality, Theorem 5.10 in [57])**.** *Suppose$(\mathcal{X}, \mu)$ and $(\mathcal{Y}, \nu)$ are two Polish spaces. Let $c : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}^{+\infty}$ be a lower semi-continuous function such that there exists some real-valued upper semi-continuous functions $a \in L^1(\mu)$ and $b \in L^1(\nu)$, with*

$$c(x, y) \geq a(x) + b(y), \forall (x, y) \in \mathcal{X} \times \mathcal{Y}.$$

Then, we have

$$\min_{\pi \in \Gamma(\mu,\nu)} \int_{\mathcal{X}\times\mathcal{Y}} c(x, y) \mathrm{d}\pi(x, y) = \sup_{\substack{\psi \in \mathcal{C}_b(\mathcal{X}),\\ \phi \in \mathcal{C}_b(\mathcal{X});\\ \psi - \phi \leq c}} \left(\int_{\mathcal{Y}} \phi(y) \mathrm{d}\nu(y) - \int_{\mathcal{X}} \psi(x) \mathrm{d}\mu(x)\right),$$

where $\mathcal{C}_b$ denotes the set of continuous bounded functions, and L^1 is the Lesbegue space of exponent 1.

Here, a Polish space refers to a topological space that is separable and completely metrizable. With the above theorem, we have:

Theorem I.2 (Kantorovich-Rubinstein Duality)**.** *Let μ, ν be discrete probability distributions over X and Y respectively, and let $c : X \times Y \to [0, +\infty)$ be a bounded function. Then*

$$\inf_{\theta \in \Gamma(\mu,\nu)} \mathbb{E}_\theta[c] = \sup_{(n, c_1, c_2) \in \mathcal{W}} (\mathbb{E}_\mu[c_1] + \mathbb{E}_\nu[c_2] - n)$$

where $\Gamma(\mu, \nu)$ denotes the set of probabilistic couplings of μ and ν and $(n, c_1, c_2) \in \mathcal{W}$ iff for every $x \in X$ and $y \in Y$, we have $0 \leq c_1(x), c_2(y)$ and $c_1(x) + c_2(y) \leq c(x, y) + n$.

Proof. We first note that a countable set with the discrete topology is always a Polish space, and bounded functions on the discrete space is always continuous. Now, by applying theorem I.1 with $\psi = -b_1$ and $\phi = b_2$, we have

$$\inf_{\theta \in \Gamma(\mu,\nu)} \mathbb{E}_\theta[c] = \sup_{(b_1, b_2) \in \mathcal{B}} (\mathbb{E}_\mu[b_1] + \mathbb{E}_\nu[b_2]),$$

where $(b_1, b_2) \in \mathcal{B}$ iff b_1 and b_2 are bounded functions, and for every $x \in X$ and $y \in Y$, we have $b_1(x) + b_2(y) \leq c(x, y)$.

We now show

$$\sup_{(b_1, b_2) \in \mathcal{B}} (\mathbb{E}_\mu[b_1] + \mathbb{E}_\nu[b_2]) = \sup_{(n, c_1, c_2) \in \mathcal{W}} (\mathbb{E}_\mu[c_1] + \mathbb{E}_\nu[c_2] - n).$$

Since b_1 and b_2 are bounded, there exists some integer m satisfying $|b_1(x)| \leq m$ and $|b_2(y)| \leq m$. We can then write $c_1(x) = b_1(x) + m$ and $c_2(y) = b_2(y) + m$ with $n = 2m$, getting $0 \leq c_1(x)$ and $0 \leq c_2(y)$. This gives

$$\sup_{(b_1,b_2)\in\mathcal{B}} (\mathbb{E}_\mu[b_1] + \mathbb{E}_\nu[b_2]) \leq \sup_{(n,c_1,c_2)\in\mathcal{W}} (\mathbb{E}_\mu[c_1] + \mathbb{E}_\nu[c_2] - n).$$

For the other direction, observe that for fixed n, c is bounded and $c_1(x) + c_2(y) \leq c(x, y) + n$, we can know c_1 and c_2 is bounded. Therefore, write $b_1 = c_1$ and $b_2 = c_2 - n$ gives the desired result.

□

APPENDIX J
POSTPONED TECHNICAL PROOFS

In this section, we give proofs of the lemmas that are omitted in the previous part of the appendix.

Lemma J.1 (Lemma A.7)**.** *We have the following properties for $A, A_1, A_2 \in \mathsf{Pos}^\infty(\mathcal{H})$:*

- *Scalar product cA for $c \in \mathbb{R}^{+\infty}$ is defined such that for all $|\psi\rangle$, $\langle\psi|cA|\psi\rangle = c\langle\psi|A|\psi\rangle$.*
- *Addition $A_1 + A_2$ such that for all $|\psi\rangle \in \mathcal{H}$, $\langle\psi|(A_1 + A_2)|\psi\rangle = \langle\psi|A_1|\psi\rangle + \langle\psi|A_2|\psi\rangle$.*
- *Tensor product $A_1 \otimes A_2$ such that for all $|\psi_1\rangle, |\psi_2\rangle$, $(\langle\psi_1| \otimes \langle\psi_2|)(A_1 \otimes A_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (\langle\psi_1|A_1|\psi_1\rangle) \cdot (\langle\psi_2|A_2|\psi_2\rangle)$.*
- *Let M be a linear operator with $\mathcal{H}$ as its domain, $M^\dagger AM$ can be defined such that for all $|\psi\rangle$, $\langle\psi|(M^\dagger AM)|\psi\rangle = \langle\phi|A|\phi\rangle$ where $|\phi\rangle = M|\psi\rangle$.*
- *For $P \in \mathsf{Pos}$ with decomposition $P = \sum_i a_i|\psi_i\rangle\langle\psi_i|$ ($0 \leq a_i$), the trace is $\mathrm{tr}(AP) = \sum_i a_i\langle\psi_i|A|\psi_i\rangle$. Note that the value is unique for any decomposition.*
- *For $\mathcal{E} \in \mathcal{QO}$ (more generally, CP maps) with Kraus operators $\{E_i\}$, $\mathcal{E}^\dagger(A) = \sum_i E_i^\dagger A E_i$. Note that it is unique for arbitrary Kraus operators.*
- *$A_1 = A_2$ if for all $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle = \langle\psi|A_2|\psi\rangle$.*
- *$A_1 \sqsubseteq A_2$ if for all $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle \leq \langle\psi|A_2|\psi\rangle$.*

Proof. In the following, let $A = \sum_i \lambda_i X_i$, where X_i is the projection onto the corresponding eigenspace. We will also write A as $A = P_A + \infty X_A$, where $P_A = \sum_{\lambda_i<+\infty} \lambda_i X_i$ is the "finite" component of A, and $X_A = \sum_{\lambda_i=+\infty} X_i$ is the "infinite" space of A. Similarly, we write $A_1 = \sum_i \lambda_i^{(1)} X_i^{(1)} = P_{A_1} + \infty \cdot X_{A_1}$ and $A_2 = \sum_i \lambda_i^{(2)} X_i^{(2)} = P_{A_2} + \infty \cdot X_{A_2}$.

- For the scalar product cA, we define it as $cA = \sum_i c\lambda_i X_i$. By the definition of inner product, it is direct that $\langle\psi|cA|\psi\rangle = c\langle\psi|A|\psi\rangle$.
- For the addition operation, we define it as $A_1 + A_2 = X^\perp(P_{A_1} + P_{A_2})X^\perp + \infty \cdot X$, where $X = X_{A_1} \vee X_{A_2}$. We now verify that $\langle\psi|A_1 + A_2|\psi\rangle = \langle\psi|A_1|\psi\rangle + \langle\psi|A_2|\psi\rangle$. If $\langle\psi|A_1 + A_2|\psi\rangle < +\infty$, then we know $|\psi\rangle \in X^\perp$, meaning that $X^\perp|\psi\rangle = |\psi\rangle$. Then, by the definition of X, we know $\langle\psi|A_1|\psi\rangle < +\infty$ and $\langle\psi|A_2|\psi\rangle < +\infty$. Thus, in this case the condition holds. Now, consider the case when $\langle\psi|A_1 + A_2|\psi\rangle = +\infty$. Then, we know $\langle\psi|X|\psi\rangle > 0$. We claim either $\langle\psi|X_1|\psi\rangle > 0$ or $\langle\psi|X_2|\psi\rangle > 0$, because otherwise $|\psi\rangle \in X_1^\perp \cap X_2^\perp$, contradicting $\langle\psi|X|\psi\rangle > 0$.
- For the tensor product, we define it as $P_{A_1} \otimes P_{A_2} + \infty \cdot X$, where $X = (\mathrm{supp}\,(P_{A_1}) \otimes X_{A_2}) \vee (X_{A_1} \otimes \mathrm{supp}\,(P_{A_2})) \vee (X_{A_1} \otimes X_{A_2})$. We now verify that it satisfies the property. For any $|\psi_1\rangle$ and $|\psi_2\rangle$, first suppose that $\langle\psi_1|\langle\psi_2|A_1 \otimes A_2|\psi_1\rangle|\psi_2\rangle = 0$. We know that $X|\psi_1\rangle|\psi_2\rangle = 0$ and $\langle\psi_1|\langle\psi_2|P_{A_1} \otimes P_{A_2}|\psi_1\rangle|\psi_2\rangle = 0$. Therefore, without loss of generality we can assume $\langle\psi_1|P_{A_1}|\psi_1\rangle = 0$. From $X|\psi_1\rangle|\psi_2\rangle = 0$, we know $X_{A_1}|\psi_1\rangle = 0$, meaning that $\langle\psi_1|A_1|\psi_1\rangle = 0$ as we want.
  Now, consider the case $0 < \langle\psi_1|\langle\psi_2|A_1 \otimes A_2|\psi_1\rangle|\psi_2\rangle < +\infty$. By definition, we know $X|\psi_1\rangle|\psi_2\rangle = 0$, $\langle\psi_1|P_{A_1}|\psi_1\rangle \neq 0$, $\langle\psi_2|P_{A_2}|\psi_2\rangle \neq 0$, We first claim $\langle\psi_1|A_1|\psi_1\rangle \neq 0$, and $\langle\psi_2|A_2|\psi_2\rangle \neq 0$. If not, without loss of generality, we assume $\langle\psi_1|A_1|\psi_1\rangle = 0$. It gives $|\psi_1\rangle \in (\mathrm{supp}(P_{A_1}) \vee X_{A_1})$, meaning that $X|\psi_1\rangle|\psi_2\rangle = 0$. We then know $\langle\psi_1|\langle\psi_2|A_1 \otimes A_2|\psi_1\rangle|\psi_2\rangle = 0$, a contradiction. We then claim $\langle\psi_1|A_1|\psi_1\rangle < +\infty$, and $\langle\psi_2|A_2|\psi_2\rangle < +\infty$. Suppose for simplicity that $\langle\psi_1|A_1|\psi_1\rangle = +\infty$, we know $X_{A_1}|\psi_1\rangle \neq 0$. Combined with $\langle\psi_2|A_2|\psi_2\rangle \neq 0$. we conclude that projecting $|\psi_1\rangle|\psi_2\rangle$ onto the space $X_{A_1} \otimes \mathrm{supp}\,(P_{A_2}) \vee X_{A_1} \otimes X_{A_2}$ is non-zero, meaning $\langle\psi_1|\langle\psi_2|A_1 \otimes A_2|\psi_1\rangle|\psi_2\rangle = +\infty$, a contradiction. Since both $\langle\psi_1|A_1|\psi_1\rangle$ and $\langle\psi_2|A_2|\psi_2\rangle$ are non-zero and finite, a direct computation will give the equation we want.
  For the case when $\langle\psi_1|\langle\psi_2|A_1 \otimes A_2|\psi_1\rangle|\psi_2\rangle = +\infty$, we know $X|\psi_1\rangle|\psi_2\rangle \neq 0$. Suppose $\langle\psi_1|A_1|\psi_1\rangle < +\infty$, and $\langle\psi_2|A_2|\psi_2\rangle < +\infty$. we could conclude $X_{A_1}|\psi_1\rangle = X_{A_2}|\psi_2\rangle = 0$, giving $X|\psi_1\rangle|\psi_2\rangle = 0$, a contradiction. Thus, without loss of generality, we can assume $\langle\psi_1|A_1|\psi_1\rangle = +\infty$. We then claim $\langle\psi_2|A_2|\psi_2\rangle \neq 0$. Otherwise we will get $X|\psi_1\rangle|\psi_2\rangle = 0$. We then conclude $\langle\psi_1|A_1|\psi_1\rangle\langle\psi_2|A_2|\psi_2\rangle = +\infty$ as we want.
- $MAM^\dagger$ can be defined as $MP_AM^\dagger + \infty \cdot \mathrm{supp}(MXM^\dagger)$. For any $|\phi\rangle = M|\psi\rangle$, if $\langle\phi|A|\phi\rangle < +\infty$, we know that $X|\phi\rangle = 0$, meaning that $\langle\psi|MXM^\dagger|\psi\rangle = 0$ Thus, $\langle\psi|MAM^\dagger|\psi\rangle = \langle\psi|MP_AM^\dagger|\psi\rangle < +\infty$, and by definition $\langle\psi|MAM^\dagger|\psi\rangle = \langle\psi|MP_AM^\dagger|\psi\rangle = \langle\phi|A|\phi\rangle$ as we want. If $\langle\phi|A|\phi\rangle = +\infty$, we know that $X|\phi\rangle \neq 0$, or equivalently, $XM^\dagger|\psi\rangle \neq 0$, meaning $\langle\psi|MAM^\dagger|\psi\rangle = +\infty$ as we want.

- For $P \in \mathsf{Pos}$, define $\mathrm{tr}(AP) = \mathrm{tr}(P_A P)$ if $X_A P = 0$, and $+\infty$ otherwise. If $P = \sum_i a_i |\psi_i\rangle\langle\psi_i|$ with $a_i \geq 0$. We first notice that it suffices to consider the set of j with $a_j > 0$ as $0 \cdot +\infty = 0$. We then notice that $\mathrm{supp}(P) = \mathrm{span}_i \{|\psi_i\rangle\}$. Thus, if $\mathrm{tr}(AP) < +\infty$, then $X_A|\psi_i\rangle = 0$ for any i, with $\mathrm{tr}(AP) = \mathrm{tr}(P_A P) = \sum_i a_i \langle\psi_i|P_A|\psi_i\rangle$ as we want. If $\mathrm{tr}(AP) = +\infty$, then $X_A \cap \mathrm{span}_i \{|\psi_i\rangle\} \neq 0$, meaning that there must be some i with $\langle\psi_i|A|\psi_i\rangle = +\infty$. Then, we know $\sum_i a_i \langle\psi_i|A|\psi_i\rangle = +\infty$ as we want.
- For a CP map $\mathcal{E}^\dagger$ and $A = P_A + \infty X_A$, define $\mathcal{E}^\dagger(A) = X^\perp \mathcal{E}(P_A) X^\perp + \infty X$, where $X = \mathrm{supp}(\mathcal{E}(X_A))$. For $\mathcal{E}$ with Kraus operators E_i, we know X can be written as $X = \mathrm{supp}(\sum_i E_i^\dagger X_A E_i) = \vee_i \mathrm{supp}(E_i^\dagger X_A E_i)$. By definition, we know in this case $\mathcal{E}^\dagger(A)$ can be written as $\sum_i E_i^\dagger A E_i$ as we desired.
- We first prove that $X_{A_1} = X_{A_2}$. If not, let $|\psi\rangle$ be a normalized state in $X_{A_1} \cap X_{A_2}^\perp$. We know $X_{A_2}|\psi\rangle = 0$ but $X_{A_1}|\psi\rangle = |\psi\rangle$. This means $\langle\psi|A_1|\psi\rangle = +\infty$ but $\langle\psi|A_2|\psi\rangle < +\infty$, a contradiction. Now, given that $X_{A_1} = X_{A_2}$, we know that for any $|\psi\rangle \in X_{A_1}^\perp \supseteq (\mathrm{supp}(P_{A_1}) \vee \mathrm{supp}(P_{A_2}))$, $\langle\psi|P_{A_1}|\psi\rangle = \langle\psi|P_{A_2}|\psi\rangle$, meaning that $P_{A_1} = P_{A_2}$ as we desired.
- We extend the Löwner order of positive semi-definite operators to infinite-valued positive semi-definite operators as follows: for $A, B \in \mathsf{Pos}^\infty(\mathcal{H})$, we say $A \sqsubseteq B$ if for any $|\psi\rangle$, $\langle\psi|A|\psi\rangle \leq \langle\psi|B|\psi\rangle$. By the definition of trace, it is clear that $A \sqsubseteq B$ if for any ρ, $\mathrm{tr}(A\rho) \leq \mathrm{tr}(B\rho)$. It is clear that it satisfies reflexivity and transitivity. For antisymmetry, it follows from the previous property. Thus it is a partial order.

□

Lemma J.2 (Lemma A.8)**.** *In the following, let $a, b, c \in \mathbb{R}^{+\infty}$, $A, A_1, A_2 \in \mathsf{Pos}^\infty$, $M, M_1, M_2, \cdots \in \mathcal{L}$, and $P, P_1, P_2 \cdots \in \mathsf{Pos}$. We have the following properties:*

- $0A = 0$, $1A = A$, $a(bA) = (ab)A$;
- $0 + A = A + 0 = A$, $A_1 + A_2 = A_2 + A_1$, $A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$;
- $0 \otimes A = A \otimes 0 = 0$, $A_1 \otimes (A_2 \otimes A_3) = (A_1 \otimes A_2) \otimes A_3$;
- $A \otimes (cA_1 + A_2) = c(A \otimes A_1) + (A \otimes A_2)$; $(cA_1 + A_2) \otimes A = c(A_1 \otimes A) + (A_2 \otimes A)$;
- $0^\dagger A 0 = 0$, $M_2^\dagger (M_1^\dagger A M_1) M_2 = (M_1 M_2)^\dagger A (M_1 M_2)$; $M^\dagger (cA_1 + A_2) M = c(M^\dagger A_1 M) + M^\dagger A_2 M$;
- $(M_1 \otimes M_2)^\dagger (A_1 \otimes A_2)(M_1 \otimes M_2) = (M_1^\dagger A_1 M_1) \otimes (M_2^\dagger A_2 M_2)$;
- $\mathrm{tr}(A(cP_1 + P_2)) = c\,\mathrm{tr}(AP_1) + \mathrm{tr}(AP_2)$; $\mathrm{tr}((cA_1 + A_2)P) = c\,\mathrm{tr}(A_1 P) + \mathrm{tr}(A_2 P)$;
- $\mathrm{tr}((A_1 \otimes A_2)(P_1 \otimes P_2)) = \mathrm{tr}(A_1 P_1)\,\mathrm{tr}(A_2 P_2)$; $\mathrm{tr}((M^\dagger A M)P) = \mathrm{tr}(A(MPM^\dagger))$.
- $\mathrm{tr}((A \otimes I)P) = \mathrm{tr}(A\,\mathrm{tr}_2(P))$; $\mathrm{tr}((I \otimes A)P) = \mathrm{tr}(A\,\mathrm{tr}_1(P))$;
- $\mathrm{tr}(A|\phi\rangle\langle\phi|) = \langle\phi|A|\phi\rangle$.
- $A_1 = A_2$ *iff for all* $P \in \mathsf{Pos}$ *(or* $P \in \mathcal{D}$*) such that* $\mathrm{tr}(A_1 P) = \mathrm{tr}(A_2 P)$;
- $A_1 \sqsubseteq A_2$ *iff for all* $P \in \mathsf{Pos}$ *(or* $P \in \mathcal{D}$*) such that* $\mathrm{tr}(A_1 P) \leq \mathrm{tr}(A_2 P)$;
- $A_1 \sqsubseteq A_2$ *implies* $M^\dagger A_1 M \sqsubseteq M^\dagger A_2 M$; $A_1 \sqsubseteq A_2$ *and* $A_3 \sqsubseteq A_4$ *implies* $cA_1 + A_3 \sqsubseteq cA_2 + A_4$.

As direct corollaries, for CP map $\mathcal{E}, \mathcal{E}_1, \mathcal{E}_2$,

- $\mathrm{tr}(A\mathcal{E}(P)) = \mathrm{tr}(\mathcal{E}^\dagger(A)P)$; $A_1 \sqsubseteq A_2$ *implies* $\mathcal{E}(A_1) \sqsubseteq \mathcal{E}(A_2)$;
- $(c\mathcal{E}_1 + \mathcal{E}_2)(A) = c\mathcal{E}_1(A) + \mathcal{E}_2(A)$; $\mathcal{E}(cA_1 + A_2) = c\mathcal{E}(A_1) + \mathcal{E}(A_2)$;
- $\mathcal{E}_2(\mathcal{E}_1(A)) = (\mathcal{E}_2 \circ \mathcal{E}_1)(A)$; $(\mathcal{E}_1 \otimes \mathcal{E}_2)(A_1 \otimes A_2) = \mathcal{E}_1(A_1) \otimes \mathcal{E}_2(A_2)$.

Proof. We prove the above properties as follows:

- For $0A = 0$, $1A = A$, $a(bA) = (ab)A$, it follows directly from the definition.
- For $0 + A = A + 0 = A$, $A_1 + A_2 = A_2 + A_1$, $A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$, it follows from the definition of addition of infinite-valued predicates. For instance, to prove $A + 0 = A$, we have, for any $|\psi\rangle$, $\langle\psi|A+0|\psi\rangle = \langle\psi|A|\psi\rangle + \langle\psi|0|\psi\rangle = \langle\psi|A|\psi\rangle$. Then the claim follows directly by noting that $A_1 = A_2$ if for any $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle = \langle\psi|A_2|\psi\rangle$.
- For $0 \otimes A = A \otimes 0 = 0$, $A_1 \otimes (A_2 \otimes A_3) = (A_1 \otimes A_2) \otimes A_3$, it follows from the definition.
- For $A \otimes (cA_1 + A_2) = c(A \otimes A_1) + (A \otimes A_2)$; $(cA_1 + A_2) \otimes A = c(A_1 \otimes A) + (A_2 \otimes A)$, it follows from the definition.
- To prove $0^\dagger A 0 = 0$, we notice that for any $|\psi\rangle$, $\langle\psi|0^\dagger A 0|\psi\rangle = \langle\phi|A|\phi\rangle = 0 = \langle\psi|0|\psi\rangle$ for $|\phi\rangle = 0|\psi\rangle = 0$. Then we know $0^\dagger A 0 = 0$ as we want. The propositions $M_2^\dagger (M_1^\dagger A M_1) M_2 = (M_1 M_2)^\dagger A (M_1 M_2)$ and $M^\dagger (cA_1 + A_2) M = c(M^\dagger A_1 M) + M^\dagger A_2 M$ can be proved similarly.
- To prove $(M_1 \otimes M_2)^\dagger (A_1 \otimes A_2)(M_1 \otimes M_2) = (M_1^\dagger A_1 M_1) \otimes (M_2^\dagger A_2 M_2)$, it follows from the definition and the fact that $X_{M_1^\dagger A_1 M_1} = \mathrm{supp}(M_1^\dagger X_{A_1} M_1)$. Actually, $(M_1 \otimes M_2)^\dagger (A_1 \otimes A_2)(M_1 \otimes M_2) = (M_1^\dagger P_{A_1} M_1) \otimes (M_2^\dagger P_{A_2} M_2) + \mathrm{supp}((M_1 \otimes M_2)^\dagger) X (M_1 \otimes M_2))$, where $X = (\mathrm{supp}\,(P_{A_1}) \otimes X_{A_2}) \vee (X_{A_1} \otimes \mathrm{supp}\,(P_{A_2})) \vee (X_{A_1} \otimes X_{A_2})$. $(M_1^\dagger A_1 M_1) \otimes (M_2^\dagger A_2 M_2) = (M_1^\dagger P_{A_1} M_1) \otimes (M_2^\dagger P_{A_2} M_2) + \infty Y$, where $Y = \left(\mathrm{supp}\left(M_1^\dagger P_{A_1} M_1\right) \otimes \mathrm{supp}(M_2^\dagger X_{A_2} M_2)\right) \vee \left(\mathrm{supp}(M_1^\dagger X_{A_1} M_1) \otimes \mathrm{supp}\left(M_2^\dagger P_{A_2} M_2\right)\right) \vee \left(\mathrm{supp}(M_1^\dagger X_{A_1} M_1) \otimes \mathrm{supp}(M_2^\dagger X_{A_2} M_2)\right)$. It can be shown that $X = Y$ by using the properties $\mathcal{E}(X_1 \vee X_2) = \mathcal{E}(X_1) \vee \mathcal{E}(X_2)$ and $\mathcal{E}(\mathrm{supp}(\rho)) = \mathrm{supp}(\mathcal{E}(\rho))$.

- For $\mathrm{tr}(A(cP_1+P_2)) = c\,\mathrm{tr}(AP_1)+\mathrm{tr}(AP_2)$, if $c=0$ then it is direct. In the following, we assume $c>0$. if $X_AP_1 = X_AP_2 = 0$, then the equation is direct by definition. Suppose $X_AP_1 \neq 0$, which means $\mathrm{tr}(AP_1) = +\infty$. In this case, we have $X_A(cP_1+P_2) \neq 0$, meaning the left hand side is also $+\infty$. The case $X_AP_2 \neq 0$ and $\mathrm{tr}((cA_1+A_2)P) = c\,\mathrm{tr}(A_1P)+\mathrm{tr}(A_2P)$ can be proved similarly.
- For $\mathrm{tr}((A_1\otimes A_2)(P_1\otimes P_2)) = \mathrm{tr}(A_1P_1)\,\mathrm{tr}(A_2P_2)$, if $X_{A_1}P_1 = X_{A_2}P_2 = 0$, then it is direct by computation. Now, by symmetry consider the case $X_{A_1}P_1 \neq 0$, which means $\mathrm{tr}(A_1P_1) = +\infty$ (the case $X_{A_2}P_2 \neq 0$ can be proved similarly). If $\mathrm{tr}(A_2P_2) = 0$, then $P_2 \in (\mathrm{supp}(P_{A_2}) \vee X_{A_2})^\perp$. In this case, $X_{A_1\otimes A_2}P_1\otimes P_2 = 0$, and $\mathrm{tr}((A_1\otimes A_2)(P_1\otimes P_2)) = \mathrm{tr}((P_{A_1}\otimes P_{A_2})(P_1\otimes P_2)) = 0$. If $\mathrm{tr}(A_2P_2)\neq 0$, then $X_{A_1\otimes A_2}P_1\otimes P_2 \neq 0$, and both left and right hand sides takes $+\infty$ as we desired.
  For $\mathrm{tr}((M^\dagger AM)P) = \mathrm{tr}(A(MPM^\dagger))$, we note that $\mathrm{supp}(M^\dagger X_AM)P = 0$ is equivalent to $M^\dagger\,\mathrm{supp}(X_A)MP = 0$, and the latter can be written as $\mathrm{supp}(X_A)MPM^\dagger = 0$. Then, the property follows directly from definition.
- For $\mathrm{tr}((A\otimes I)P) = \mathrm{tr}(A\,\mathrm{tr}_2(P))$, we note that $A\otimes I = P_A\otimes I + X_A\otimes I$. Thus, $X_A\,\mathrm{tr}_2(P) = 0$ if and only if $X_{A\otimes I}P = 0$. Then, the equation follows directly from the definition. $\mathrm{tr}((I\otimes A)P) = \mathrm{tr}(A\,\mathrm{tr}_1(P))$ can be proved in a similar way.
- For $\mathrm{tr}(A|\phi\rangle\langle\phi|) = \langle\phi|A|\phi\rangle$, it is direct by definition.
- For $A_1 = A_2$ iff for all $P\in\mathsf{Pos}$ (or $P\in\mathcal{D}$) such that $\mathrm{tr}(A_1P) = \mathrm{tr}(A_2P)$, the "if" part can be proved using the previous property and the proposition that $A_1 = A_2$ if for all $|\psi\rangle$, $\langle\psi|A_1|\psi\rangle = \langle\psi|A_2|\psi\rangle$. The "only if" part is direct by definition.
- For $A_1\sqsubseteq A_2$ iff for all $P\in\mathsf{Pos}$ (or $P\in\mathcal{D}$) such that $\mathrm{tr}(A_1P)\leq\mathrm{tr}(A_2P)$, the "if" part can be proved by limiting P to be rank-1 projectors $|\psi\rangle\langle\psi|$. For the "only if" part, consider the spectral decomposition of $P = \sum_i a_i|\psi_i\rangle\langle\psi_i|$. We have $\mathrm{tr}(A_1P) = \mathrm{tr}(A_1\sum_i a_i|\psi_i\rangle\langle\psi_i|) = \sum_i a_i\langle\psi_i|A_1|\psi_i\rangle$, and $\mathrm{tr}(A_2P) = \mathrm{tr}(A_2\sum_i a_i|\psi_i\rangle\langle\psi_i|) = \sum_i a_i\langle\psi_i|A_2|\psi_i\rangle$. Since $A_1\sqsubseteq A_2$, we have $\langle\psi_i|A_1|\psi_i\rangle\leq\langle\psi_i|A_2|\psi_i\rangle$ for every i. The result then follows directly.
- For $A_1\sqsubseteq A_2$ implies $M^\dagger A_1M\sqsubseteq M^\dagger A_2M$, let $|\psi\rangle$ be any state. Then, a direct computation gives $\langle\psi|M^\dagger A_1M|\psi\rangle = \langle\phi|A_1|\phi\rangle \leq \langle\phi|A_2|\phi\rangle = \langle\psi|M^\dagger A_2M|\psi\rangle$, where $|\phi\rangle = M|\psi\rangle$. Thus, $M^\dagger A_1M\sqsubseteq M^\dagger A_2M$ follows by definition. For $A_1\sqsubseteq A_2$ and $A_3\sqsubseteq A_4$ implies $cA_1+A_3\sqsubseteq cA_2+A_4$, consider any $|\psi\rangle$, $A_1\sqsubseteq A_2$ implies $\langle\psi|A_1|\psi\rangle\leq\langle\psi|A_2|\psi\rangle$. Similarly we have $\langle\psi|A_3|\psi\rangle\leq\langle\psi|A_4|\psi\rangle$. Therefore we know $\langle\psi|cA_1+A_3|\psi\rangle = c\langle\psi|A_1|\psi\rangle+\langle\psi|A_3|\psi\rangle \leq c\langle\psi|A_2|\psi\rangle+\langle\psi|A_4|\psi\rangle = \langle\psi|cA_2+A_4|\psi\rangle$, and the result follows by definition.
- For $\mathrm{tr}(A\mathcal{E}(P)) = \mathrm{tr}(\mathcal{E}^\dagger(A)P)$, we write $\mathcal{E}(P) = \sum_j E_jPE_j^\dagger$. Then, we have $\mathrm{tr}(A\mathcal{E}(P)) = \mathrm{tr}(A\sum_j E_jPE_j^\dagger) = \sum_j\mathrm{tr}(AE_jPE_j^\dagger) = \sum_j\mathrm{tr}(E_j^\dagger AE_jP) = \mathrm{tr}(\mathcal{E}^\dagger(A)P)$. For $A_1\sqsubseteq A_2$ implies $\mathcal{E}(A_1)\sqsubseteq\mathcal{E}(A_2)$, write $\mathcal{E}(A) = \sum_j E_j^\dagger AE_j$. We now for any j, $E_j^\dagger A_1E_j\sqsubseteq E_j^\dagger A_2E_j$, thus $\sum_j E_j^\dagger A_1E_j\sqsubseteq\sum_j E_j^\dagger A_2E_j$ as we want.
- For $(c\mathcal{E}_1+\mathcal{E}_2)(A) = c\mathcal{E}_1(A)+\mathcal{E}_2(A)$ take any $P\in\mathsf{Pos}$, we have $\mathrm{tr}(P(c\mathcal{E}_1+\mathcal{E}_2)(A)) = \mathrm{tr}((c\mathcal{E}_1+\mathcal{E}_2)^\dagger(P)(A))c\,\mathrm{tr}(\mathcal{E}_1^\dagger(P)A)+\mathrm{tr}(\mathcal{E}_2^\dagger(P)A) = \mathrm{tr}(Pc\mathcal{E}_1(A))+\mathrm{tr}(P\mathcal{E}_2(A)) = \mathrm{tr}(P(c\mathcal{E}_1+\mathcal{E}_2)(A))$. Then the result follows. For $\mathcal{E}(cA_1+A_2) = c\mathcal{E}(A_1)+\mathcal{E}(A_2)$, write $\mathcal{E}(A) = \sum_j E_jAE_j^\dagger$. We then have $\mathcal{E}(cA_1+A_2) = \sum_j E_j(cA_1+A_2)E_j^\dagger = c\sum_j E_jA_1E_j^\dagger+\sum_j E_jA_2E_j^\dagger = c\mathcal{E}(A_1)+\mathcal{E}(A_2)$ as we want.
- $\mathcal{E}_2(\mathcal{E}_1(A)) = (\mathcal{E}_2\circ\mathcal{E}_1)(A)$ is by definition. For $(\mathcal{E}_1\otimes\mathcal{E}_2)(A_1\otimes A_2) = \mathcal{E}_1(A_1)\otimes\mathcal{E}_2(A_2)$, let $A_1 = P_{A_1}+\infty X_{A_1}$, $A_2 = P_{A_2}+\infty X_{A_2}$, and $A_1\otimes A_2 = P_{A_1}\otimes P_{A_2}+\infty X$, where $X = (\mathrm{supp}\,(P_{A_1})\otimes X_{A_2})\vee(X_{A_1}\otimes\mathrm{supp}\,(P_{A_2}))\vee(X_{A_1}\otimes X_{A_2})$. Then, $(\mathcal{E}_1\otimes\mathcal{E}_2)(A_1\otimes A_2) = (\mathcal{E}_1\otimes\mathcal{E}_2)(P_{A_1}\otimes P_{A_2})+\infty Y$, where $Y = \mathrm{supp}((\mathcal{E}_1\otimes\mathcal{E}_2)(X))$ and $\mathcal{E}_1(A_1)\otimes\mathcal{E}_2(A_2) = (\mathcal{E}_1\otimes\mathcal{E}_2)(P_{A_1}\otimes P_{A_2})+\infty Z$, where $Z = (\mathrm{supp}\,(\mathcal{E}_1(P_{A_1}))\otimes\mathcal{E}_2(X_{A_2}))\vee(\mathcal{E}_1(X_{A_1})\otimes\mathrm{supp}\,(\mathcal{E}_2(P_{A_2})))\vee(\mathcal{E}_1(X_{A_1})\otimes\mathcal{E}_2(X_{A_2}))$. It is clear that $Y = Z$ by using the properties $\mathcal{E}(X_1\vee X_2) = \mathcal{E}(X_1)\vee\mathcal{E}(X_2)$ and $\mathcal{E}(\mathrm{supp}(\rho)) = \mathrm{supp}(\mathcal{E}(\rho))$.

□