Abstract interpretation, Hoare logic, and incorrectness logic for quantum programs

YUAN FENG, University of Technology Sydney, Australia
SANJIANG LI, University of Technology Sydney, Australia

Abstract interpretation, Hoare logic, and incorrectness (or reverse Hoare) logic are powerful techniques for static analysis of computer programs. All of them have been successfully extended to the quantum setting, but largely developed in parallel. In this paper, we examine the relationship between these techniques in the context of verifying quantum while-programs, where the abstract domain and the set of assertions for quantum states are well-structured. In particular, we show that any complete quantum abstract interpretation induces a quantum Hoare logic and a quantum incorrectness logic, both of which are sound and relatively complete. Unlike the logics proposed in the literature, the induced logic systems are in a forward manner, making them more useful in certain applications. Conversely, any sound and relatively complete quantum Hoare logic or quantum incorrectness logic induces a complete quantum abstract interpretation. As an application, we are able to show the non-existence of any sound and relatively complete quantum Hoare logic or incorrectness logic if tuples of local subspaces are taken as assertions.

CCS Concepts: • **Theory of computation** → **Denotational semantics**; **Axiomatic semantics**; **Hoare logic**; **Program verification**; **Assertions**.

Additional Key Words and Phrases: Quantum programming, abstract interpretation, incorrectness logic

ACM Reference Format:
Yuan Feng and Sanjiang Li. . Abstract interpretation, Hoare logic, and incorrectness logic for quantum programs. 1, , Article 1 (January), 26 pages.

1 INTRODUCTION

Abstract interpretation, originated by Cousot and Cousot [Cousot and Cousot 1977], is a powerful technique for static analysis of program correctness. The key idea of abstract interpretation is to provide an over-approximation (abstraction) of the concrete program semantics. Consequently, analysis of programs can be done at the abstract level, which is usually much simpler, and correctness in the abstract domain implies correctness in the concrete domain. Over the past few decades, abstract interpretation has become increasingly popular in describing and analysing computational models in many different areas of computer science, such as model checking [Clarke et al. 2003, 1994; Cousot and Cousot 2000; Dams et al. 1997], process calculi [Cleaveland and Riely 1994; Venet 1996], type inference [Comini et al. 2008; Cousot 1997], and theorem proving [Plaisted 1981]. More recently, analysis of quantum programs using abstract interpretation was proposed in [Yu and Palsberg 2021], where tuples of local subspaces of the state Hilbert space are regarded as abstraction of quantum states.

Hoare logic [Hoare 1969] is one of the most popular syntax-oriented approaches for verifying the correctness of computer programs. The core notion of Hoare logic is the program correctness expressed in the form of Hoare triples $\{p\}\ S\ \{q\}$ where S is a program, and p and q are *assertions* that describe the pre- and post-conditions of S, respectively. For non-probabilistic programs, assertions are typically first-order logic formulas. Intuitively, the triple $\{p\}\ S\ \{q\}$ states that if S is executed

Authors' addresses: Yuan Feng, Centre for Quantum Software and Information, University of Technology Sydney, NSW, Australia, Yuan.Feng@uts.edu.au; Sanjiang Li, Centre for Quantum Software and Information, University of Technology Sydney, NSW, Australia, Sanjiang.Li@uts.edu.au.

. XXXX-XXXX//1-ART1 $15.00
https://doi.org/

at a *state* (evaluation of program variables) satisfying p and it terminates, then q must hold in the final state. This is called *partial correctness*. If termination is further guaranteed in all states that satisfy p, then partial correctness becomes a *total* one. Hoare logic provides a proof system which can systematically deduce the correctness of a program represented by such a triple. After decades of development, Hoare logic has been successfully applied to the analysis of programs with nondeterminism, recursion, parallel execution, probabilistic features, etc. For a detailed survey, please refer to [Apt et al. 2010; Apt and Olderog 2019].

In recent years, Hoare-type logics for quantum programs have been developed. Unlike the classical case, a logic system for assertions of quantum states was proposed only very recently [Ying 2022]; most quantum Hoare logics developed so far simply take a certain semantic set as possible assertions. [D'Hondt and Panangaden 2006] proposes to regard positive operators not greater than (w.r.t. Löwner order) the identity operator as (quantitative) assertions of quantum states. Then the *degree* of a quantum state ρ satisfying an assertion M is denoted $\mathrm{Tr}(M\rho)$, the expected value of outcomes if ρ is measured according to the projective measurement determined by M. A Hoare triple for quantum programs then has the form $\{M\}\ S\ \{N\}$ where S is a quantum program, and M and N are quantum assertions, and it is partially (resp. totally) correct if

$$\mathrm{Tr}(M\rho) \leq \mathrm{Tr}(N \cdot [\![S]\!](\rho)) + \mathrm{Tr}(\rho) - \mathrm{Tr}([\![S]\!](\rho))$$

(resp. $\mathrm{Tr}(M\rho) \leq \mathrm{Tr}(N \cdot [\![S]\!](\rho))$) for any quantum state ρ [Feng et al. 2022; Feng and Ying 2021; Ying 2012, 2016; Ying et al. 2022]. Note that the term $\mathrm{Tr}(\rho) - \mathrm{Tr}([\![S]\!](\rho))$ appearing in partial correctness but not in total correctness denotes the probability for S to diverge (not terminate) at ρ. Another line of research, which is conceptually and computationally simpler, is to regard subspaces (or equivalently, orthogonal projectors) of the associated Hilbert space as (qualitative) assertions, and a quantum state ρ satisfies a subspace assertion P iff the support (the image space of linear operators) of ρ is included in P [Unruh 2019; Zhou et al. 2019]. Partial correctness of $\{P\}\ S\ \{Q\}$ means that $[\![S]\!](\rho)$ satisfies Q as long as ρ satisfies P, similar to the classical case. Total correctness further requires that $\mathrm{Tr}([\![S]\!](\rho)) = \mathrm{Tr}(\rho)$ for all ρ satisfying P. Obviously, subspace based Hoare logics are special cases of positive operator based ones, by noting that projectors are positive operators with eigenvalues being either 0 or 1. For comparison with abstract interpretation, we will consider this simplified form of quantum Hoare logic in this paper.

Incorrectness logic [O'Hearn 2019], or reverse Hoare logic [Vries and Koutavas 2011], is a complementary method to reason about the *incorrectness* of programs. Similar to Hoare logic, the key notion of incorrectness logic is a triple $[p]\ S\ [q]$ which asserts that any state satisfying q is reachable from a state satisfying p by executing the program S. Note that the postcondition q in the Hoare triple $\{p\}\ S\ \{q\}$ provides an *over-approximation* of the set of final states when starting with states in p, while q in the incorrectness triple $[p]\ S\ [q]$ provides an *under-approximation* of the same set. Again, incorrectness logic has recently been extended to analyse quantum programs where quantum assertions are taken as subspaces of the associated Hilbert space [Yan et al. 2022].

So far, the aforementioned approaches for analysis of quantum programs, namely abstract interpretation, Hoare logic, and incorrectness logic, have been developed largely in parallel. In this paper we analyse the relationship between them. Our discovery is twofold:

(1) Given a quantum abstract interpretation in which the abstract domain for quantum states is well-structured, a quantum Hoare logic is naturally induced which is sound (resp. sound and relatively complete) if the abstract operator is sound (resp. complete) for each basic command of the quantum language under consideration. Similar results apply to quantum incorrectness logic as well. Compared to the applied Hoare logic [Zhou et al. 2019] and incorrectness logic [Yan et al. 2022] for quantum programs, our induced logic systems are in a forward fashion, making them more useful in certain applications.

(2) Conversely, for any quantum Hoare logic in which the set of assertions for quantum states is well-structured, a quantum abstract interpretation is naturally induced which is sound (resp. complete) if the Hoare logic is sound (resp. sound and relatively complete). Again, similar results apply to quantum incorrectness logic as well. As an application, these results imply the non-existence of any sound and relatively complete Hoare or incorrectness logic for quantum programs if tuples of local subspaces are taken as assertions.

The rest of this paper is organised as follows. We review in Sec. 2 some basic notions from abstract interpretation and quantum computing that will be used throughout this paper. In Sec. 3, a simple quantum while-language is introduced, which serves as the target language of our analysis, and its concrete denotational semantics is defined. We examine the relationship between well-structured abstract domains and sets of assertions for quantum states in Sec. 4, which sets the stage for the discussion that follows. Sec. 5 is the main part of this paper, where we elaborate on how a sound (resp. sound and relatively complete) Hoare logic and a sound (resp. complete) abstract interpretation of quantum programs can be derived from each other. Similar results are also discussed for incorrectness logic. Finally, Sec. 6 concludes the paper and points out some directions for future study.

2 PRELIMINARIES

This section is devoted to fixing some notations from abstract interpretation and quantum computing that will be used in this paper. For a thorough introduction to the relevant backgrounds, please refer to [Miné 2017] (abstract interpretation) and [Nielsen and Chuang 2002] (quantum computing).

2.1 Abstract Interpretation

Let the concrete domain for program states be a partially ordered set, a.k.a poset, $(C, \leq_C)$. Typically, elements in C are subsets of program states, and $\leq_C$ is just the set inclusion. Let the abstract domain be another poset $(A, \leq_A)$. The concrete and abstract domains are related by a pair of monotonic functions $\alpha : C \to A$ and $\gamma : A \to C$. The pair (α, γ) is said to form a *Galois connection*, denoted $(C, \leq_C) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \leq_A)$, if for all $c \in C$ and $a \in A$, $c \leq_C \gamma(a)$ iff $\alpha(c) \leq_A a$. Furthermore, if $\alpha \circ \gamma = \mathrm{id}_A$ then (α, γ) forms a *Galois embedding*, where id_A is the identity relation over A. Note that a Galois connection $(C, \leq_C) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \leq_A)$ is a Galois embedding iff any of the following holds: (1) α is surjective, that is, for all $a \in A$, there exists $c \in C$ such that $\alpha(c) = a$; (2) γ is injective, that is, for all $a, a' \in A$, $\gamma(a) = \gamma(a')$ implies $a = a'$.

Given an operator $f : C \to C$ in the concrete domain, an abstract operator $f^\# : A \to A$ is called a *sound abstraction* of f if $\alpha \circ f \leq_A f^\# \circ \alpha$, and it is *complete* if $\alpha \circ f = f^\# \circ \alpha$. It is easy to check that complete abstractions are closed under composition; that is, if $f^\#$ and $g^\#$ are complete abstractions of f and g respectively, then $f^\# \circ g^\#$ is a complete abstraction of $f \circ g$. Note that a complete abstraction does not necessarily exist. However, the *best abstraction* of f, defined as $\alpha \circ f \circ \gamma$, always exists. It is the smallest one among all sound abstractions.

Remark 1. *In the literature, there are alternative definitions of sound and complete abstraction using the concretisation function γ instead of the abstraction function α. Specifically, an abstract operator $f^\#$ of f is sound if $f \circ \gamma \leq_C \gamma \circ f^\#$, and it is complete if $f \circ \gamma = \gamma \circ f^\#$. It can be easily checked that when (α, γ) forms a Galois connection, these two notions of soundness are equivalent; that is, $\alpha \circ f \leq_A f^\# \circ \alpha$ iff $f \circ \gamma \leq_C \gamma \circ f^\#$. However, the two notions of completeness are in general incomparable. Nevertheless, in either case the complete abstraction, if exists, must be the best abstraction.*

2.2 Basic quantum computing

Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and $\dim(\mathcal{H})$ denote its dimension. Following the tradition of quantum computing, vectors in $\mathcal{H}$ are denoted in the Dirac form $|\psi\rangle$. The inner and outer products of two vectors $|\psi\rangle$ and $|\phi\rangle$ are written as $\langle\psi|\phi\rangle$ and $|\psi\rangle\langle\phi|$ respectively. Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$ and $A \in \mathcal{L}(\mathcal{H})$. Denote by $\mathrm{Tr}(A) = \sum_{i\in I}\langle\psi_i|A|\psi_i\rangle$ the *trace* of A where $\{|\psi_i\rangle : i \in I\}$ is an orthonormal basis of $\mathcal{H}$. The *adjoint* of A, denoted $A^\dagger$, is the unique linear operator in $\mathcal{L}(\mathcal{H})$ such that $\langle\psi|A|\phi\rangle = \langle\phi|A^\dagger|\psi\rangle^*$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. Here, for a complex number z, z^* denotes its conjugate. An operator $A \in \mathcal{L}(\mathcal{H})$ is said to be (1) *hermitian* if $A^\dagger = A$; (2) *unitary* if $A^\dagger A = I_\mathcal{H}$, the identity operator on $\mathcal{H}$; (3) *positive* if for all $|\psi\rangle \in \mathcal{H}$, $\langle\psi|A|\psi\rangle \geq 0$. Every hermitian operator A has a *spectral decomposition* form $A = \sum_{i\in I}\lambda_i|\psi_i\rangle\langle\psi_i|$ where $\{|\psi_i\rangle : i \in I\}$ constitute an orthonormal basis of $\mathcal{H}$. The Löwner (partial) order $\sqsubseteq$ on $\mathcal{L}(\mathcal{H})$ is defined by letting $A \sqsubseteq B$ iff $B - A$ is positive.

A linear operator $\mathcal{E}$ from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$ is called a *super-operator*. It is said to be (1) *positive* if it maps positive operators on $\mathcal{H}_1$ to positive operators on $\mathcal{H}_2$; (2) *completely positive* if $\mathcal{I}_\mathcal{H} \otimes \mathcal{E}$ is positive for all finite dimensional Hilbert space $\mathcal{H}$, where $\mathcal{I}_\mathcal{H}$ is the identity super-operator on $\mathcal{L}(\mathcal{H})$; (3) *trace-preserving* (resp. *trace-nonincreasing*) if $\mathrm{Tr}(\mathcal{E}(A)) = \mathrm{Tr}(A)$ (resp. $\mathrm{Tr}(\mathcal{E}(A)) \leq \mathrm{Tr}(A)$ for any positive operator $A \in \mathcal{L}(\mathcal{H}_1)$. Given the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$, the *partial trace* with respect to $\mathcal{H}_2$, denoted $\mathrm{Tr}_{\mathcal{H}_2}$, is a linear mapping from $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ to $\mathcal{L}(\mathcal{H}_1)$ such that for any $|\psi_i\rangle, |\phi_i\rangle \in \mathcal{H}_i$,

$$\mathrm{Tr}_{\mathcal{H}_2}(|\psi_1\rangle\langle\phi_1| \otimes |\phi_1\rangle\langle\phi_2|) = \langle\phi_2|\phi_1\rangle|\psi_1\rangle\langle\phi_1|.$$

The definition extends linearly to $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

According to von Neumann's formalism of quantum mechanics [Von Neumann 1955], any quantum system with finite degrees of freedom is associated with a finite-dimensional Hilbert space $\mathcal{H}$ called its *state space*. When $\dim(\mathcal{H}) = 2$, such a system is called a *qubit*, the analogy of bit in classical computing. A *pure state* of the system is described by a normalised vector in $\mathcal{H}$. When the system is in state $|\psi_i\rangle$ with probability p_i, $i \in I$, it is in a *mixed* state, represented by the *density operator* $\sum_{i\in I} p_i|\psi_i\rangle\langle\psi_i|$ on $\mathcal{H}$. Obviously, a density operator is positive and has trace 1. In this paper, we follow Selinger's convention [Selinger 2004] to regard *partial density operators*, i.e. positive operators with traces not greater than 1 as (unnormalised) quantum states. Intuitively, a partial density operator ρ denotes a legitimate quantum state $\rho/\mathrm{Tr}(\rho)$ which is obtained with probability $\mathrm{Tr}(\rho)$. Denote by $\mathcal{D}(\mathcal{H})$ the set of partial density operators on $\mathcal{H}$. The state space of a composite system (e.g., a quantum system consisting of multiple qubits) is the tensor product of the state spaces of its components. For any ρ in $\mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, the partial traces $\mathrm{Tr}_{\mathcal{H}_1}(\rho)$ and $\mathrm{Tr}_{\mathcal{H}_2}(\rho)$ are the reduced quantum states of ρ on $\mathcal{H}_2$ and $\mathcal{H}_1$, respectively.

The *evolution* of a closed quantum system is described by a unitary operator on its state space: if the states of the system at t_1 and t_2 are ρ_1 and ρ_2, respectively, then $\rho_2 = U\rho_1U^\dagger$ for some unitary U. The general dynamics that can occur in a physical system is described by a completely positive and trace-preserving super-operator. Note that the unitary transformation $\mathcal{E}_U(\rho) \triangleq U\rho U^\dagger$ is such a super-operator. A (projective) quantum *measurement* $\mathcal{M}$ is described by a collection $\{P_i : i \in O\}$ of projectors (hermitian operators with eigenvalues being either 0 or 1) in the state space $\mathcal{H}$, where O is the set of measurement outcomes. It is required that the measurement operators P_i's satisfy the completeness equation $\sum_{i\in I} P_i = I_\mathcal{H}$. If the system was in state ρ before measurement, then the probability of observing outcome i is given by $p_i = \mathrm{Tr}(P_i\rho)$, and the state of the post-measurement system becomes $\rho_i = P_i\rho P_i/p_i$ whenever $p_i > 0$. Sometime we use a hermitian operator M in $\mathcal{L}(\mathcal{H})$

called *observable* to represent a projective measurement. To be specific, let

$$M = \sum_{m \in spec(M)} m P_m$$

where $spec(M)$ is the set of eigenvalues of M, and P_m the projection onto the eigenspace associated with m. Then the projective measurement determined by M is $\{P_m : m \in spec(M)\}$.

3 A SIMPLE QUANTUM WHILE-LANGUAGE

The target quantum language of our analysis is an extension of the purely quantum while-language defined in [Feng et al. 2007; Ying 2012] with assertions. Let V, ranged over by $q, r, \cdots$, be a finite set of (qubit-type) quantum variables. For any subset W of V, let

$$\mathcal{H}_W \triangleq \bigotimes_{q \in W} \mathcal{H}_q,$$

where $\mathcal{H}_q$ is the 2-dimensional Hilbert space associated with q. As we use subscripts to distinguish Hilbert spaces with different quantum variables, their order in the tensor product is irrelevant.

The syntax of our language is given as follows:

$$\begin{array}{rcll} S & ::= & \textbf{skip} & \textit{(no-op)} \\ & | & \bar{q} := |0\rangle & \textit{(initialisation)} \\ & | & \bar{q} *= U & \textit{(unitary operation)} \\ & | & \textbf{assert } P[\bar{q}] & \textit{(assertion)} \\ & | & S_0; S_1 & \textit{(sequence)} \\ & | & \textbf{if } P[\bar{q}] \textbf{ then } S_1 \textbf{ else } S_0 \textbf{ end} & \textit{(conditional)} \\ & | & \textbf{while } P[\bar{q}] \textbf{ do } S \textbf{ end} & \textit{(loop)} \end{array}$$

where S, S_0 and S_1 are quantum programs, $\bar{q} \triangleq q_1, \ldots, q_t$ a (ordered) tuple of distinct quantum variables from V, U a unitary operator on $\mathcal{H}_{\bar{q}}$, and P a subspace of $\mathcal{H}_{\bar{q}}$. Sometimes we also use $\bar{q}$ to denote the (unordered) set $\{q_1, q_2, \ldots, q_t\}$.

For clarification, we often use subscripts to emphasise the quantum system on which an operator is performed. For example, P_W means P acting on system W. To simplify notations, we do not distinguish P_W with its cylindrical extension $P_W \otimes I_{V \setminus W}$ to $\mathcal{H}_V$. Furthermore, we use the same symbol, say P, to denote both a subspace and its corresponding projector. The correct meaning of theses notations should be clear from the context. Consequently, a quantum state $|\psi\rangle \in P$ iff $P|\psi\rangle = |\psi\rangle$. Here, the former P denotes a subspace, while the latter one denotes the corresponding projector.

Definition 3.1 (Denotational semantics). Let S be a quantum program. The *denotational semantics* of S is a mapping $[\![S]\!] : \mathcal{D}(\mathcal{H}_V) \to \mathcal{D}(\mathcal{H}_V)$ defined inductively in Fig. 1, where $P_{\bar{q}}^{\perp} = I_{\mathcal{H}_V} - P_{\bar{q}}$ is the projector onto the orthocomplement of $P_{\bar{q}}$ in $\mathcal{H}_V$.

Intuitively, the **skip** statement does not change the input state, while $\bar{q} := |0\rangle$ sets the system $\bar{q}$ to state $|0\rangle$ where $|\bar{q}| = t$. Note that $|i\rangle_{\bar{q}}\langle j|$ denotes the operator $|i\rangle\langle j|$ acting on $\bar{q}$, and $\{|0\rangle, \cdots, |2^t - 1\rangle\}$ constitute the computational basis of $\mathcal{H}_{\bar{q}}$. The statement $\bar{q} *= U$ applies the unitary operator U on $\bar{q}$, while **assert** $P[\bar{q}]$ measures system $\bar{q}$ according to the projective measurement $\{P, P^{\perp}\}$ and post-selects the outcome for P; that is, if $P^{\perp}$ is observed, then the program aborts without outputting anything (or equivalently, it outputs the zero operator). Note also that here we adopt the convenience of using a partial density operator ρ to encode both the (normalised) quantum state $\rho/\mathrm{Tr}(\rho)$ and the probability $\mathrm{Tr}(\rho)$ of reaching it [Selinger 2004]. Similarly, the branching statement **if** $P[\bar{q}]$ **then** S_1 **else** S_0 **end** also measures system $\bar{q}$ according to the projective measurement $\{P, P^{\perp}\}$

$$
\begin{aligned}
[\![\mathbf{skip}]\!](\rho) &= \rho \\
[\![\bar{q} := |0\rangle]\!](\rho) &= \sum_{i=0}^{2^t-1} |0\rangle_{\bar{q}}\langle i|\rho|i\rangle_{\bar{q}}\langle 0| \\
[\![\bar{q} *= U]\!](\rho) &= U_{\bar{q}}\rho U_{\bar{q}}^{\dagger} \\
[\![\mathbf{assert}\ P[\bar{q}]]\!](\rho) &= P_{\bar{q}}\rho P_{\bar{q}} \\
[\![S_0; S_1]\!](\rho) &= [\![S_1]\!] \circ [\![S_0]\!](\rho) \\
[\![\mathbf{if}\ P[\bar{q}]\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0\ \mathbf{end}]\!](\rho) &= [\![\mathbf{assert}\ P[\bar{q}]; S_1]\!](\rho) + [\![\mathbf{assert}\ P^{\perp}[\bar{q}]; S_0]\!](\rho) \\
[\![\mathbf{while}\ P[\bar{q}]\ \mathbf{do}\ S\ \mathbf{end}]\!](\rho) &= \sum_{i=0}^{\infty} [\![(\mathbf{assert}\ P[\bar{q}]; S)^i; \mathbf{assert}\ P^{\perp}[\bar{q}]]\!](\rho)
\end{aligned}
$$

Fig. 1. Denotational semantics for quantum programs.

and then executes S_1 or S_0 depending on the measurement outcome. The output of this statement is defined as the combination of the two branches. Again, thanks to the convention of partial density operators, this combination is simply the summation of the output states from both branches. Finally, the while loop **while** $P[\bar{q}]$ **do** S **end** takes into account the output states from different iterations. The well-definedness of the semantics of while loops comes from the fact that the set $\mathcal{D}(\mathcal{H}_V)$ of partial density operators on $\mathcal{H}_V$ is a complete partial order set [Selinger 2004; Ying 2016].

For the purpose of abstract interpretation for quantum programs, we take, and fix throughout this paper,

$$(\mathcal{Q} \triangleq 2^{\mathcal{D}(\mathcal{H}_V)}, \subseteq, \cup, \cap, \emptyset, \mathcal{D}(\mathcal{H}_V))$$

to be the concrete domain for their (collecting) semantics, where $\cup$ and $\cap$ are respectively the normal union and intersection over sets of quantum states. Thus $\mathcal{Q}$ is a complete lattice. The denotational semantics defined in Definition 3.1 is then extended to the concrete domain by letting $[\![S]\!](R) = \{[\![S]\!](\rho) : \rho \in R\}$ for any $R \in \mathcal{Q}$. Obviously, such defined $[\![S]\!]$ is monotonic with respect to $\subseteq$; that is, $[\![S]\!](R) \subseteq [\![S]\!](R')$ whenever $R \subseteq R'$.

4 ABSTRACT QUANTUM DOMAINS V.S. QUANTUM ASSERTIONS

The main contribution of this paper is a close relationship between abstract interpretation and Hoare/incorrectness logic for quantum programs. To this end, we first examine the relationship between abstract domains and assertions for quantum states. For the sake of simplicity, we assume that both the abstract quantum domain and the quantum assertion set are taken as a complete lattice. Furthermore, note that the concrete domain $\mathcal{Q}$ of quantum states defined in Sec. 3 enjoys a linear structure: for any $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H}_V)$ and $x_1, x_2 > 0$, it holds that $x_1\rho_1 + x_2\rho_2 \in \mathcal{D}(\mathcal{H}_V)$ whenever $\mathrm{Tr}(x_1\rho_1 + x_2\rho_2) \leq 1$. To respect this structure, we put some natural restrictions on both the abstract domain and the assertion set.

4.1 Well-structured abstract quantum domain

Let $(\mathcal{A}, \leq_{\mathcal{A}}, \vee, \wedge, \perp, \top)$ be a complete lattice. For $\mathcal{A}$ to be an abstract domain for the set of quantum state, we assume a pair of monotonic functions $\alpha : \mathcal{Q} \to \mathcal{A}$ (abstraction) and $\gamma : \mathcal{A} \to \mathcal{Q}$ (concretisation).

Definition 4.1. The complete lattice $\mathcal{A}$ as an abstract domain of $\mathcal{Q}$ is said to be *well-structured*, if

(1) (α, γ) forms a Galois embedding between $\mathcal{Q}$ and $\mathcal{A}$; and
(2) for any $\rho_i \in \mathcal{D}(\mathcal{H}_V)$ and $x_i > 0$, $i = 1, 2, \ldots$, with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,

$$\alpha\left(\sum_i x_i \rho_i\right) = \bigvee_i \alpha(\rho_i). \tag{1}$$

Here and in the following, we abbreviate $\alpha(\{\rho\})$ into $\alpha(\rho)$ for simplicity.

Note that if (α, γ) forms a Galois connection, then $\alpha\left(\bigcup_i \{\rho_i\}\right) = \bigvee_i \alpha(\rho_i)$. Thus the second condition in the above definition can be regarded as an analogy of this property for linear combination of quantum states.

The following lemma gives equivalent characterisations of the second condition in Definition 4.1 in terms of the concretisation function.

Lemma 4.2. *Let $(\mathcal{A}, \leq_{\mathcal{A}}, \vee, \wedge, \bot, \top)$ be a complete lattice, with $\alpha : \mathcal{Q} \to \mathcal{A}$ and $\gamma : \mathcal{A} \to \mathcal{Q}$ forming a Galois embedding. Then the following three statements are equivalent:*

(1) *$\mathcal{A}$ is well-structured;*
(2) *for any $a \in \mathcal{A}$, $\rho_i \in \mathcal{D}(\mathcal{H}_V)$, and $x_i > 0$ with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,*

$$\sum_i x_i \rho_i \in \gamma(a) \quad \Leftrightarrow \quad \forall i, \rho_i \in \gamma(a); \tag{2}$$

(3) *for any $a \in \mathcal{A}$, $\gamma(a)$ as a subset of $\mathcal{D}(\mathcal{H}_V)$ is*
- *convex;*
- *ω-cpo: if for each $i \geq 1$, $\rho_i \in \gamma(a)$ and $\rho_i \sqsubseteq \rho_{i+1}$, then $\bigsqcup_i \rho_i \in \gamma(a)$;*
- *down-closed: if $\rho \sqsubseteq \sigma$ and $\sigma \in \gamma(a)$, then $\rho \in \gamma(a)$ as well; and*
- *closed under positive scalar multiplication: if $\rho \in \gamma(a)$ and $x\rho \in \mathcal{D}(\mathcal{H}_V)$ with $x > 0$, then $x\rho \in \gamma(a)$ as well.*

Proof. (1) $\Leftrightarrow$ (2): Direct from the observation that

$$\sum_i x_i \rho_i \in \gamma(a) \quad \Leftrightarrow \quad \alpha\left(\sum_i x_i \rho_i\right) \leq_{\mathcal{A}} a$$

while

$$\forall i, \rho_i \in \gamma(a) \quad \Leftrightarrow \quad \forall i,\ \alpha(\rho_i) \leq_{\mathcal{A}} a \quad \Leftrightarrow \quad \bigvee_i \alpha(\rho_i) \leq_{\mathcal{A}} a$$

(2) $\Rightarrow$ (3): For any $a \in \mathcal{A}$, it is easy to see from the sufficiency part of Eq.(2) that $\gamma(a)$ is convex and closed under positive scalar multiplication. Now if $\rho \sqsubseteq \sigma$ and $\sigma \in \gamma(a)$, then $\sigma - \rho \in \mathcal{D}(\mathcal{H}_V)$ as well. From the fact that $\rho + (\sigma - \rho) = \sigma$, we know $\rho \in \gamma(a)$ from the necessity part of Eq.(2). Thus $\gamma(a)$ is down-closed.

Finally, if for each $i \geq 1$, $\rho_i \in \gamma(a)$ and $\rho_i \sqsubseteq \rho_{i+1}$, then $\rho_{i+1} - \rho_i \in \gamma(a)$ as well. From the fact that

$$\bigsqcup_i \rho_i = \rho_1 + \sum_{i \geq 1} (\rho_{i+1} - \rho_i),$$

we know $\bigsqcup_i \rho_i \in \gamma(a)$ from the sufficiency part of Eq.(2). Thus $\gamma(a)$ is an ω-cpo.

(3) $\Rightarrow$ (2): The proof consists of two parts:

$$\begin{aligned} \sum_i x_i \rho_i \in \gamma(a) \quad &\Rightarrow \quad \forall i, x_i \rho_i \in \gamma(a) && \text{(down-closed)} \\ &\Rightarrow \quad \forall i, \rho_i \in \gamma(a) && \text{(scaling)} \end{aligned}$$

and

$$\begin{aligned}
\forall i, \rho_i \in \gamma(a) \quad &\Rightarrow \quad \forall n > 0, \ \sum_{i=1}^{n} \frac{x_i}{\sum_{i=1}^{n} x_i} \rho_i \in \gamma(a) && \text{(convexity)} \\
&\Rightarrow \quad \forall n > 0, \ \sum_{i=1}^{n} x_i \rho_i \in \gamma(a) && \text{(scaling)} \\
&\Rightarrow \quad \sum_{i} x_i \rho_i \in \gamma(a) && (\omega\text{-cpo)}
\end{aligned}$$ □

Example 4.3 (Subspace abstract domain). The simplest example of well-structured abstract domain for quantum states is the subspace domain

$$(\mathcal{S}(\mathcal{H}_V), \subseteq, \vee, \cap, \{0\}, \mathcal{H}_V)$$

where $\mathcal{S}(\mathcal{H}_V)$ is the set of all subspaces (or equivalently, all projectors) of $\mathcal{H}_V$, $\subseteq$ is the ordinary subset relation between subspaces (or equivalently, the Löwner order between the corresponding projectors), and the join $P \vee Q = \text{span}(P \cup Q)$ is defined as the subspace spanned by elements from P or Q. Then this domain is a complete lattice. Let the concretisation and abstraction functions $\gamma_s : \mathcal{S}(\mathcal{H}_V) \to \mathcal{Q}$ and $\alpha_s : \mathcal{Q} \to \mathcal{S}(\mathcal{H}_V)$ be defined as follows: for any $P \in \mathcal{S}(\mathcal{H}_V)$ and $R \in \mathcal{Q}$,

$$\begin{aligned}
\gamma_s(P) &\triangleq \{\rho \in \mathcal{D}(\mathcal{H}_V) : \lceil \rho \rceil \subseteq P\}, \\
\alpha_s(R) &\triangleq \bigvee \{\lceil \rho \rceil : \rho \in R\}.
\end{aligned}$$

Here $\lceil \rho \rceil$ denotes the support subspace of ρ. We now show that such defined α_s and γ_s form a Galois embedding between the concrete domain $\mathcal{Q}$ and the abstract domain $\mathcal{S}(\mathcal{H}_V)$:

$$\begin{aligned}
R \subseteq \gamma_s(P) \quad &\Leftrightarrow \quad R \subseteq \{\rho \in \mathcal{D}(\mathcal{H}_V) : \lceil \rho \rceil \subseteq P\} \\
&\Leftrightarrow \quad \forall \rho \in R, \lceil \rho \rceil \subseteq P \\
&\Leftrightarrow \quad \alpha_s(R) \subseteq P
\end{aligned}$$

where the necessity part of the last equivalence is from the fact that P is a subspace. Furthermore, it is easy to check that α_s is surjective: for any $P \in \mathcal{S}(\mathcal{H}_V)$, $\alpha_s(\gamma_s(P)) = P$.

Finally, for any $\rho_i \in \mathcal{D}(\mathcal{H}_V)$ and $x_i > 0$, $i = 1, 2, \ldots$, with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,

$$\alpha_s\left(\sum_i x_i \rho_i\right) = \left\lceil \sum_i x_i \rho_i \right\rceil = \bigvee_i \lceil \rho_i \rceil = \bigvee_i \alpha_s(\rho_i).$$

Thus $\mathcal{S}(\mathcal{H}_V)$ is a well-structured abstract domain for quantum states in $\mathcal{D}(\mathcal{H}_V)$.

We now show that the subspace abstract domain $\mathcal{S}(\mathcal{H}_V)$ presented in Example 4.3 is actually the *most concrete* well-structured abstract quantum domain, in the sense that any other well-structured abstract domain can be regarded as an abstraction of $\mathcal{S}(\mathcal{H}_V)$ in terms of a Galois embedding. For this purpose we first prove

Lemma 4.4. *Let $\mathcal{A}$ be a well-structured abstract domain for quantum states, with $\alpha : \mathcal{Q} \to \mathcal{A}$ being the abstraction function. For any $R_1, R_2 \subseteq \mathcal{D}(\mathcal{H}_V)$,*

$$\alpha_s(R_1) = \alpha_s(R_2) \quad \Rightarrow \quad \alpha(R_1) = \alpha(R_2).$$

Consequently, we have $\alpha = \alpha \circ \gamma_s \circ \alpha_s$.

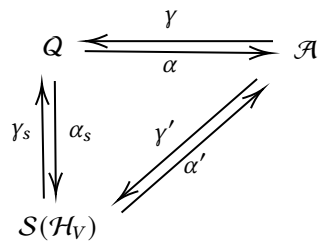
Proof. Suppose $\alpha_s(R_1) = \alpha_s(R_2)$. For any $\rho \in R_1$, as $\mathcal{H}_V$ is finite dimensional, we can always find a set of states $\rho_1, \ldots, \rho_n$ in R_2, $\mathrm{Tr}(\rho_i) = 1$, and $x > 0$ such that $x\rho \sqsubseteq \sum_{i=1} \rho_i/n$. Thus from the assumption that $\mathcal{A}$ is a well-structured, we have

$$\alpha(\rho) = \alpha(x\rho) \leq_{\mathcal{A}} \bigvee_{i=1}^{n} \alpha(\rho_i) \leq_{\mathcal{A}} \alpha(R_2).$$

Thus $\alpha(R_1) = \bigvee\{\alpha(\rho) : \rho \in R_1\} \leq_{\mathcal{A}} \alpha(R_2)$. The other direction can be similarly proved.

The last part of the lemma follows from the observation that for any $R \subseteq \mathcal{D}(\mathcal{H}_V)$, $\alpha_s(R) = \alpha_s \circ \gamma_s \circ \alpha_s(R)$. □

Theorem 4.5. *Let $\mathcal{A}$ be a well-structured abstract domain for quantum states, with $\alpha : \mathcal{Q} \to \mathcal{A}$ and $\gamma : \mathcal{A} \to \mathcal{Q}$ being the abstraction and concretisation functions respectively. Then there exists a Galois embedding (α', γ') with $\alpha' : \mathcal{S}(\mathcal{H}_V) \to \mathcal{A}$ and $\gamma' : \mathcal{A} \to \mathcal{S}(\mathcal{H}_V)$ such that $\alpha = \alpha' \circ \alpha_s$ and $\gamma = \gamma_s \circ \gamma'$. That is, the following diagram commutes for α's and γ's respectively:*



Proof. Let $\alpha' \triangleq \alpha \circ \gamma_s$ and $\gamma' \triangleq \alpha_s \circ \gamma$. From the fact that $\gamma \circ \alpha \geq_{\mathcal{Q}} \mathrm{id}_{\mathcal{Q}}$ we have

$$\gamma' \circ \alpha' = \alpha_s \circ \gamma \circ \alpha \circ \gamma_s \geq_{\mathcal{S}(\mathcal{H}_V)} \alpha_s \circ \gamma_s = \mathrm{id}_{\mathcal{S}(\mathcal{H}_V)}.$$

Furthermore, from Lemma 4.4, we have $\alpha' \circ \alpha_s = \alpha \circ \gamma_s \circ \alpha_s = \alpha$ and so

$$\alpha' \circ \gamma' = \alpha' \circ \alpha_s \circ \gamma = \alpha \circ \gamma = \mathrm{id}_{\mathcal{A}}.$$

Thus $\mathcal{S}(\mathcal{H}_V) \underset{\alpha'}{\overset{\gamma'}{\leftrightarrows}} \mathcal{A}$ is indeed a Galois embedding. Finally, from $\gamma_s \circ \alpha_s \geq_{\mathcal{Q}} \mathrm{id}_{\mathcal{Q}}$ we have

$$\gamma_s \circ \alpha_s \circ \gamma \geq_{\mathcal{A}} \gamma.$$

On the other hand,

$$\gamma = \gamma \circ \alpha \circ \gamma = \gamma \circ \alpha \circ \gamma_s \circ \alpha_s \circ \gamma \geq_{\mathcal{A}} \gamma_s \circ \alpha_s \circ \gamma.$$

Thus $\gamma_s \circ \gamma' = \gamma_s \circ \alpha_s \circ \gamma = \gamma$. □

The following lemma is useful in the analysis of conditional and loop constructs in our quantum while language.

Lemma 4.6. *Suppose $\mathcal{A}$ as an abstract domain of quantum states is well-structured. Then for any $R \subseteq \mathcal{D}(\mathcal{H}_V)$,*

$$\alpha([\![\textbf{if } P[\bar{q}] \textbf{ then } S_1 \textbf{ else } S_0 \textbf{ end}]\!](R)) = \alpha([\![\textbf{assert } P[\bar{q}]; S_1]\!](R)) \vee \alpha([\![\textbf{assert } P^{\perp}[\bar{q}]; S_0]\!](R))$$

$$\alpha([\![\textbf{while } P[\bar{q}] \textbf{ do } S \textbf{ end}]\!](R)) = \bigvee_{i \geq 0} \alpha\left([\![(\textbf{assert } P[\bar{q}]; S)^i; \textbf{assert } P^{\perp}[\bar{q}]]\!](R)\right)$$

Proof. We only prove for the conditional case; the loop one is similar. Let $T_1 = \textbf{assert}\ P[\bar{q}]; S_1$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]; S_0$. Then

$$\begin{aligned}\alpha([\![\textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}]\!](R)) &= \alpha(\{[\![T_1]\!](\rho) + [\![T_0]\!](\rho) : \rho \in R\}) \\ &= \bigvee \{\alpha([\![T_1]\!](\rho) + [\![T_0]\!](\rho)) : \rho \in R\} \\ &= \bigvee \{\alpha([\![T_1]\!](\rho)) \vee \alpha([\![T_0]\!](\rho)) : \rho \in R\} \\ &= \bigvee \{\alpha([\![T_1]\!](\rho)) : \rho \in R\} \vee \bigvee \{\alpha([\![T_0]\!](\rho)) : \rho \in R\} \\ &= \alpha([\![T_1]\!](R)) \vee \alpha([\![T_0]\!](R))\end{aligned}$$

where the second and the last equalities follow from the fact that (α, γ) forms a Galois embedding, and the third one from Eq. (1). □

For well-structured abstract domain $\mathcal{A}$, if we are given a proper definition for the abstract operator $[\![e]\!]$, which is assumed to be monotonic, of each basic command $e \in \{\textbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} *= U,\ \textbf{assert}\ P[\bar{q}]\}$, then the abstract operator $[\![S]\!]^\# : \mathcal{A} \to \mathcal{A}$ for any composite quantum program S can be defined inductively as follows: for any $a \in \mathcal{A}$,

(1) $[\![S_0; S_1]\!]^\#(a) \triangleq [\![S_1]\!]^\# \circ [\![S_0]\!]^\#(a)$;
(2) $[\![\textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}]\!]^\#(a) \triangleq [\![\textbf{assert}\ P[\bar{q}]; S_1]\!]^\#(a) \vee [\![\textbf{assert}\ P^\perp[\bar{q}]; S_0]\!]^\#(a)$;
(3) $[\![\textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}]\!]^\#(a) \triangleq \bigvee_{i\geq 0} [\![(\textbf{assert}\ P[\bar{q}]; S_1)^i; \textbf{assert}\ P^\perp[\bar{q}]]\!]^\#(a)$.

It is easy to check that the induced abstract operator $[\![S]\!]^\#$ is monotonic for any S as well. The following theorem shows that such defined abstract operators are sound (resp. complete) if they are sound (resp. complete) for basic commands.

Theorem 4.7. *Let $\mathcal{A}$ be a well-structured abstract domain of quantum states.*

(1) *If $[\![e]\!]^\#$ is sound for all basic commands e, then $[\![S]\!]^\#$ is sound for any program S.*
(2) *If $[\![e]\!]^\#$ is complete for all basic commands e, then $[\![S]\!]^\#$ is complete for any program S.*

Proof. For clause (1), it suffices to prove by induction on the structure of S that $\alpha \circ [\![S]\!] \leq_{\mathcal{A}} [\![S]\!]^\# \circ \alpha$ for any program S. Note that here we lift the order $\leq_{\mathcal{A}}$ between elements of $\mathcal{A}$ to functions from $\mathcal{Q}$ to $\mathcal{A}$ in an entry-wise way. The basis case is directly from the assumption.

(1) Let $S \equiv S_0; S_1$. By induction we have $\alpha \circ [\![S_i]\!] \leq_{\mathcal{A}} [\![S_i]\!]^\# \circ \alpha$ for $i = 0, 1$. Then from the monotonicity of $[\![S_0]\!]$ and $[\![S_1]\!]^\#$,

$$\alpha \circ [\![S]\!] = \alpha \circ [\![S_1]\!] \circ [\![S_0]\!] \leq_{\mathcal{A}} [\![S_1]\!]^\# \circ \alpha \circ [\![S_0]\!] \leq_{\mathcal{A}} [\![S_1]\!]^\# \circ [\![S_0]\!]^\# \circ \alpha = [\![S]\!]^\# \circ \alpha.$$

(2) Let $S \equiv \textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}$. Let $T_1 = \textbf{assert}\ P[\bar{q}]; S_1$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]; S_0$. Then by induction, we have $\alpha \circ [\![T_i]\!] \leq_{\mathcal{A}} [\![T_i]\!]^\# \circ \alpha$ for $i = 0, 1$. Then from Lemma 4.6, for any $R \subseteq \mathcal{D}(\mathcal{H}_V)$,

$$\begin{aligned}\alpha \circ [\![S]\!](R) &= \alpha \circ [\![T_1]\!](R) \vee \alpha \circ [\![T_0]\!](R) \\ &\leq_{\mathcal{A}} [\![T_1]\!]^\# \circ \alpha(R) \vee [\![T_0]\!]^\# \circ \alpha(R) = [\![S]\!]^\# \circ \alpha(R).\end{aligned}$$

(3) Let $S \equiv \textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}$. Let $T = \textbf{assert}\ P[\bar{q}]; S$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]$. Then by induction, we have $\alpha \circ [\![T]\!] \leq_{\mathcal{A}} [\![T]\!]^\# \circ \alpha$ and $\alpha \circ [\![T_0]\!] \leq_{\mathcal{A}} [\![T_0]\!]^\# \circ \alpha$. From Lemma 4.6, for any $R \subseteq \mathcal{D}(\mathcal{H}_V)$,

$$\begin{aligned}\alpha \circ [\![S]\!](R) &= \bigvee_{i\geq 0} \alpha \circ [\![T_0]\!] \circ [\![T]\!]^i(R) \\ &\leq_{\mathcal{A}} \bigvee_{i\geq 0} [\![T_0]\!]^\# \circ ([\![T]\!]^\#)^i \circ \alpha(R) = [\![S]\!]^\# \circ \alpha(R).\end{aligned}$$

This completes the proof of clause (1). Clause (2) can be similarly proved. □

The following example shows that the abstract domain $\mathcal{S}(\mathcal{H}_V)$ allows every quantum program to have a complete abstraction.

Example 4.8. Consider the well-structured abstract domain $\mathcal{S}(\mathcal{H}_V)$ of quantum states presented in Example 4.3. Let us define for each basic command the corresponding abstract operator as follows: for any $Q \in \mathcal{S}(\mathcal{H}_V)$,

$$\begin{aligned} [\![\mathbf{skip}]\!]^\#(Q) &\triangleq Q \\ [\![\bar{q} := |0\rangle]\!]^\#(Q) &\triangleq \left\{|0\rangle_{\bar{q}} \otimes |\psi\rangle : |\psi\rangle \in \lceil \mathrm{Tr}_{\bar{q}}(Q) \rceil\right\} \\ [\![\bar{q} *= U]\!]^\#(Q) &\triangleq \left\{U_{\bar{q}}|\psi\rangle : |\psi\rangle \in Q\right\} \\ [\![\mathbf{assert}\ P[\bar{q}]]\!]^\#(Q) &\triangleq \mathrm{span}\left\{P_{\bar{q}}|\psi\rangle : |\psi\rangle \in Q\right\}. \end{aligned} \tag{3}$$

We would like to prove that these abstract operators are all complete. First, it is easy to check that al the sets on the right-hand side of Eq. (3) are valid subspaces of $\mathcal{H}_V$. Let us take $\mathbf{assert}\ P[\bar{q}]$ as an example. For any $R \in \mathcal{Q}$,

$$\begin{aligned} \alpha_s \circ [\![\mathbf{assert}\ P[\bar{q}]]\!](R) &= \left\lceil \bigcup \left\{P_{\bar{q}} \rho P_{\bar{q}} : \rho \in R\right\}\right\rceil \\ &= \mathrm{span}\left\{P_{\bar{q}}|\psi\rangle : |\psi\rangle \in \lceil \rho \rceil, \rho \in R\right\}. \end{aligned}$$

On the other hand, let $Q' \triangleq \bigvee \{\lceil \rho \rceil : \rho \in R\}$. Then

$$\begin{aligned} [\![\mathbf{assert}\ P[\bar{q}]]\!]^\# \circ \alpha_s(R) &= [\![\mathbf{assert}\ P[\bar{q}]]\!]^\#(Q') \\ &= \mathrm{span}\left\{P_{\bar{q}}|\phi\rangle : |\phi\rangle \in Q'\right\}. \end{aligned}$$

Note that any $|\phi\rangle$ in Q' can be written as a linear combination $|\phi\rangle = \sum_i \beta_i |\psi_i\rangle$ where each $|\psi_i\rangle$ is taken from the support subspace of some state in R; that is, $|\psi_i\rangle \in \lceil \rho_i \rceil$ while $\rho_i \in R$. Thus

$$P_{\bar{q}}|\phi\rangle \in \mathrm{span}\left\{P_{\bar{q}}|\psi\rangle : |\psi\rangle \in \lceil \rho \rceil, \rho \in R\right\},$$

and consequently, $[\![\mathbf{assert}\ P[\bar{q}]]\!]^\# \circ \alpha_s(R) \subseteq \alpha_s \circ [\![\mathbf{assert}\ P[\bar{q}]]\!](R)$. The other direction of inclusion is obvious.

From Theorem 4.7, such defined abstract operators can be extended to any composite quantum programs, and the extended ones are also complete. In the following, we show a more direct way to define these complete abstract operators. Note that for any quantum program S, the denotational semantics $[\![S]\!]$ can be regarded as a completely positive and trace non-increasing super-operator over the set $\mathcal{D}(\mathcal{H}_V)$ of partial density operators. Thus by Kraus representation theorem [Kraus et al. 1983], there exist a finite set of Kraus operators $E_k, k \in K$, such that for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, $[\![S]\!](\rho) = \sum_k E_k \rho E_k^\dagger$. The abstract operator corresponding to S can then be defined as follows:

$$[\![S]\!]^\#(Q) \triangleq \mathrm{span}\{E_k|\psi\rangle : k \in K, |\psi\rangle \in Q\}.$$

Furthermore, this definition coincides with the abstract operators defined in Eq. (3). Note that

$$\left\lceil [\![S]\!](\rho) \right\rceil = \left\lceil \sum_k E_k \rho E_k^\dagger \right\rceil = \mathrm{span}\left\{E_k|\psi\rangle : k \in K, |\psi\rangle \in \lceil \rho \rceil\right\}.$$

Following similar lines of the proof for completeness of $[\![\mathbf{assert}\ P[\bar{q}]]\!]^\#$ above, we can show that

$$\alpha_s \circ [\![S]\!](R) = [\![S]\!]^\# \circ \alpha_s(R)$$

for any program S and set of states R. In other words, $[\![S]\!]^\#$ is indeed the complete abstraction of $[\![S]\!]$.

To conclude this subsection, we show a useful property of complete abstraction of functions on quantum states.

Lemma 4.9. *Let $\mathcal{A}$ be a well-structured abstract domain for quantum states. Let $a_i \in \mathcal{A}$ for each i, and $f^\# : \mathcal{A} \to \mathcal{A}$ be the complete abstraction of operator $f : \mathcal{D}(\mathcal{H}_V) \to \mathcal{D}(\mathcal{H}_V)$. Then*

$$f^\#(\bigvee_i a_i) = \bigvee_i f^\#(a_i).$$

Proof. Let $R_i = \gamma(a_i)$. Then from the assumption that (α, γ) forms a Galois embedding between $\mathcal{Q}$ and $\mathcal{A}$, we have $a_i = \alpha(R_i)$. Note that $\alpha(\bigcup_i R_i) = \bigvee_i \alpha(R_i)$. Thus

$$\begin{aligned} f^\#(\bigvee_i \alpha(R_i)) &= f^\#(\alpha(\bigcup_i R_i)) = \alpha(f(\bigcup_i R_i)) \\ &= \alpha(\bigcup_i f(R_i)) = \bigvee_i \alpha(f(R_i)) \\ &= \bigvee_i f^\#(\alpha(R_i)). \end{aligned}$$

□

4.2 Well-structured quantum assertions

Following the common practice of quantum Hoare logics in the literature, for the purpose of verification we only assume a semantic set of assertions $\mathcal{A}$ for quantum states and a *satisfaction* relation $\models$ on $\mathcal{D}(\mathcal{H}_V) \times \mathcal{A}$. However, we do assume some structure of $\mathcal{A}$. Firstly, let a partial order $\leq_{\mathcal{A}}$ on $\mathcal{A}$ be defined as follows: $a \leq_{\mathcal{A}} a'$ iff for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, $\rho \models a$ implies $\rho \models a'$. Furthermore, to describe conjunction and disjunction of assertions, we assume that $\mathcal{A}$ constitutes a complete lattice and let the meet and join be denoted by $\wedge$ and $\vee$, respectively. Finally, we make some assumptions on $\models$ to reflect the linear structure of $\mathcal{D}(\mathcal{H}_V)$.

Definition 4.10. The complete lattice $\mathcal{A}$ as a set of quantum assertions for $\mathcal{D}(\mathcal{H}_V)$ is said to be *well-structured*, whenever

(1) if $\rho \models a$ for all $a \in A$ where $A \subseteq \mathcal{A}$, then $\rho \models \bigwedge A$; and
(2) for any $a \in \mathcal{A}$, $\rho_i \in \mathcal{D}(\mathcal{H}_V)$, and $x_i > 0$ with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,

$$\sum_i x_i \rho_i \models a \quad \text{iff} \quad \forall i, \rho_i \models a.$$

Example 4.11. Recall the complete lattice

$$(\mathcal{S}(\mathcal{H}_V), \subseteq, \vee, \cap, \{0\}, \mathcal{H}_V)$$

of all subspaces of $\mathcal{H}_V$ defined in Example 4.3. We have shown that it is a well-structured abstract domain for quantum states in $\mathcal{D}(\mathcal{H}_V)$. Now we show that it can also serve as a well-structured set of quantum assertions by naturally defining the satisfaction relation $\models$ as follows: for any $\rho \in \mathcal{D}(\mathcal{H}_V)$ and $P \in \mathcal{S}(\mathcal{H}_V)$,

$$\rho \models P \quad \text{iff} \quad \lceil \rho \rceil \subseteq P.$$

Firstly, for any subspaces P and Q, $P \subseteq Q$ iff for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, $\lceil \rho \rceil \subseteq P$ implies $\lceil \rho \rceil \subseteq Q$. Secondly, if $\lceil \rho \rceil \subseteq P$ for all $P \in A$ where A is a set of subspaces in $\mathcal{S}(\mathcal{H}_V)$, then obviously $\lceil \rho \rceil \subseteq \bigwedge A$ as well. Finally, for any $P \in \mathcal{S}(\mathcal{H}_V)$, $\rho_i \in \mathcal{D}(\mathcal{H}_V)$, and $x_i > 0$ with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,

$$\left\lceil \sum_i x_i \rho_i \right\rceil \subseteq P \quad \text{iff} \quad \forall i, \lceil \rho_i \rceil \subseteq P.$$

Thus $\mathcal{S}(\mathcal{H}_V)$ as a set of quantum assertions is indeed well-structured.

4.3 Well-structured abstract domains v.s. well-structured assertions

Now we examine the relationship between well-structured abstract domains and assertion sets for quantum states. Firstly, we show how to transform a well-structured abstract quantum domain into a well-structured assertion set for quantum states.

Lemma 4.12. *Let $(\mathcal{A}, \leq_{\mathcal{A}}, \vee, \wedge, \bot, \top)$ be a well-structured abstract domain for quantum states, with $\alpha : \mathcal{Q} \to \mathcal{A}$ and $\gamma : \mathcal{A} \to \mathcal{Q}$ being the abstraction and concretisation functions respectively. Then the satisfaction relation $\models$ on $\mathcal{D}(\mathcal{H}_V) \times \mathcal{A}$, defined as for any $a \in \mathcal{A}$ and $\rho \in \mathcal{D}(\mathcal{H}_V)$,*

$$\rho \models a \quad \textit{iff} \quad \rho \in \gamma(a),$$

turns $\mathcal{A}$ into a well-structured set of assertions for quantum states.

Proof. First, from the fact that (α, γ) forms a Galois embedding between $\mathcal{Q}$ and $\mathcal{A}$, for any $a, a' \in \mathcal{A}$,

$$a \leq_{\mathcal{A}} a' \quad \Leftrightarrow \quad \gamma(a) \subseteq \gamma(a') \quad \Leftrightarrow \quad \forall \rho, \rho \models a \text{ implies } \rho \models a'.$$

We now prove that the two conditions in Definition 4.10 are satisfied. To show (1), we note that for any $A \subseteq \mathcal{A}$ and $\rho \in \mathcal{D}(\mathcal{H}_V)$,

$$\begin{aligned}
\forall a \in A, \rho \models a \quad &\Rightarrow \quad \forall a \in A, \rho \in \gamma(a) \\
&\Rightarrow \quad \forall a \in A, \alpha(\rho) \leq_{\mathcal{A}} a \qquad \text{(Galois connection)} \\
&\Rightarrow \quad \alpha(\rho) \leq_{\mathcal{A}} \bigwedge A \\
&\Rightarrow \quad \rho \in \gamma\left(\bigwedge A\right) \qquad \text{(Galois connection)} \\
&\Rightarrow \quad \rho \models \bigwedge A.
\end{aligned}$$

Furthermore, (2) is directly from Lemma 4.2(2). □

Conversely, a well-structured set of quantum assertions can be easily transformed into a well-structured abstract domain for quantum states as well.

Lemma 4.13. *Let $(\mathcal{A}, \leq_{\mathcal{A}}, \vee, \wedge, \bot, \top)$ be a well-structured set of quantum assertions, with $\models$ on $\mathcal{D}(\mathcal{H}_V) \times \mathcal{A}$ being the satisfaction relation. Then the pair of functions $\alpha : \mathcal{Q} \to \mathcal{A}$ and $\gamma : \mathcal{A} \to \mathcal{Q}$, defined as for any $a \in \mathcal{A}$ and $R \subseteq \mathcal{D}(\mathcal{H}_V)$,*

$$\begin{aligned}
\gamma(a) &\triangleq \{\rho \in \mathcal{D}(\mathcal{H}_V) : \rho \models a\} \\
\alpha(R) &\triangleq \bigwedge \{b \in \mathcal{A} : R \subseteq \gamma(b)\}.
\end{aligned}$$

turn $\mathcal{A}$ into a well-structured abstract domain for quantum states.

Proof. We have to prove that the two conditions in Definition 4.1 are satisfied. First, from the assumption that $\models$ is consistent with $\leq_{\mathcal{A}}$, it is easy to prove that both γ and α are monotonic functions. Second, to show (α, γ) forms a Galois connection between $\mathcal{Q}$ and $\mathcal{A}$, it suffices to prove that for any $a \in \mathcal{A}$ and $R \subseteq \mathcal{D}(\mathcal{H}_V)$, $R \subseteq \gamma(a)$ iff $\alpha(R) \leq_{\mathcal{A}} a$. Let $A_R = \{b \in \mathcal{A} : R \subseteq \gamma(b)\}$. Then

$$\begin{aligned}
R \subseteq \gamma(a) \quad &\Rightarrow \quad a \in A_R \\
&\Rightarrow \quad \alpha(R) = \bigwedge A_R \leq_{\mathcal{A}} a.
\end{aligned}$$

Conversely, suppose $\alpha(R) \leq_{\mathcal{A}} a$. For any $\rho \in R$ and $b \in A_R$, we have $\rho \in \gamma(b)$, so $\rho \models b$. Thus from the fact that $\mathcal{A}$ as an assertion set is well-structured, $\rho \models \bigwedge A_R = \alpha(R)$ as well. By the assumption $\alpha(R) \leq_{\mathcal{A}} a$, we have $\rho \models a$, and so $\rho \in \gamma(a)$ as desired. Finally, for any a, we can show that $\alpha(\gamma(a)) = a$ from the fact that the satisfaction relation $\models$ is consistent with the partial order $\leq_{\mathcal{A}}$.

From the fact that (α, γ) forms a Galois embedding between $\mathcal{Q}$ and $\mathcal{A}$, the remaining part of the proof is then directly from Lemma 4.2. □

$$\text{(Exp)}\quad \{a\}\ e\ \{[\![e]\!]^{\#}(a)\} \qquad \text{where } e \in \{\textbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} \mathrel{*}= U,\ \textbf{assert}\ P[\bar{q}]\}$$

$$\text{(Seq)}\quad \frac{\{a\}\ S_0\ \{a'\},\ \{a'\}\ S_1\ \{b\}}{\{a\}\ S_0; S_1\ \{b\}} \qquad \text{(Meas)}\quad \frac{\{a\}\ \textbf{assert}\ P[\bar{q}]; S_1\ \{b_1\},\ \{a\}\ \textbf{assert}\ P^{\perp}[\bar{q}]; S_0\ \{b_0\}}{\{a\}\ \textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}\ \{b_0 \vee b_1\}}$$

$$\text{(Imp)}\quad \frac{a \leq_{\mathcal{A}} a',\ \{a'\}\ S\ \{b'\},\ b' \leq_{\mathcal{A}} b}{\{a\}\ S\ \{b\}} \qquad \text{(While)}\quad \frac{\{a\}\ \textbf{assert}\ P[\bar{q}]; S\ \{a\},\ \{a\}\ \textbf{assert}\ P^{\perp}[\bar{q}]\ \{b\}}{\{a\}\ \textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}\ \{b\}}$$

Table 1. Proof system for partial correctness induced by abstraction domain $(\mathcal{A}, \leq_{\mathcal{A}})$.

Example 4.14. We have already shown in Examples 4.3 and 4.11 that the complete lattice

$$(\mathcal{S}(\mathcal{H}_V), \subseteq, \vee, \cap, \{0\}, \mathcal{H}_V)$$

can be both a well-structured abstract domain and a well-structured set of assertions for quantum states. Actually, it can be easily seen that the Galois embedding (α_s, γ_s) defined in Example 4.3 and the satisfaction relation $\models$ defined in Example 4.11 satisfy the transformations stated in Lemmas 4.12 and 4.13.

5 QUANTUM HOARE LOGIC V.S. ABSTRACT INTERPRETATION

This section is devoted to the relationship between Hoare/incorrectness logic and abstract interpretation for quantum programs written in the while-language presented in Sec. 3.

5.1 Hoare logic induced by abstract interpretation

Let $\mathcal{A}$ be a well-structured abstract domain of program states, and an abstract monotonic operator $[\![e]\!]^{\#}$ be defined for each basic command $e \in \{\textbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} \mathrel{*}= U,\ \textbf{assert}\ P[\bar{q}]\}$. Then a Hoare-type proof system is naturally induced as follows:

(1) Take $\mathcal{A}$ to be the set of assertions. Furthermore, for any $\rho \in \mathcal{D}(\mathcal{H}_V)$ and $a \in \mathcal{A}$, $\rho \models a$ iff $\rho \in \gamma(a)$. From Lemma 4.12, $\mathcal{A}$ as a set of assertions is also well-structured.
(2) A correctness formula $\{a\}\ S\ \{b\}$ is valid, denoted $\models \{a\}\ S\ \{b\}$, if $[\![S]\!](\gamma(a)) \subseteq \gamma(b)$; that is, $\gamma(b)$ is an over-approximation of $[\![S]\!](\gamma(a))$. From the assumption that (α, γ) forms a Galois embedding, this is equivalent to $[\![S]\!]^b(a) \leq_{\mathcal{A}} b$ where $[\![S]\!]^b = \alpha \circ [\![S]\!] \circ \gamma$ is the best abstraction of $[\![S]\!]$ in $\mathcal{A}$.
(3) The proof system (for partial correctness) is presented as in Table 1. A correctness formula $\{a\}\ S\ \{b\}$ is said to be derivable, denoted $\vdash \{a\}\ S\ \{b\}$, if it has a proof sequence in the logic system.

Recall that such a proof system is said to be *sound* if $\vdash \{a\}\ S\ \{b\}$ implies $\models \{a\}\ S\ \{b\}$ for any correctness formula $\{a\}\ S\ \{b\}$; while it is *relatively complete* if the other direction of implication holds. The following theorem gives a close relationship between an abstract interpretation and the Hoare-type logic system induced by it.

Theorem 5.1. *Let $\mathcal{A}$ be a well-structured abstract domain of quantum states.*

(1) *If the abstract operator $[\![e]\!]^{\#}$ is sound for each basic command e, then the induced proof system presented in Table 1 is sound.*
(2) *If the abstract operator $[\![e]\!]^{\#}$ is complete for each basic command e, then the induced proof system is both sound and relatively complete.*

Proof. For the first part, we have to prove that whenever $\vdash \{a\}\ S\ \{b\}$, then $[\![S]\!](\gamma(a)) \subseteq \gamma(b)$ or equivalently, $[\![S]\!]^b(a) \leq_{\mathcal{A}} b$. This can be done by induction on the proof length of $\vdash \{a\}\ S\ \{b\}$. For the last step of the proof, we have the following cases:

(1) Rule (Exp) is used. In this case, $S \equiv e$ for some basic command e, and $b \equiv [\![e]\!]^\#(a)$. The result then follows from the assumption that $[\![e]\!]^\#$ is sound; that is, $[\![e]\!](\gamma(a)) \subseteq \gamma([\![e]\!]^\#(a))$.

(2) Rule (Seq) is used. By induction, $[\![S_0]\!](\gamma(a)) \subseteq \gamma(a')$ and $[\![S_1]\!](\gamma(a')) \subseteq \gamma(b)$. Thus

$$[\![S_0; S_1]\!](\gamma(a)) = [\![S_1]\!]([\![S_0]\!](\gamma(a))) \subseteq \gamma(b).$$

(3) Rule (Imp) is used. Then the result follows from the monotonicity of $[\![S]\!]^b$ for all program S.

(4) Rule (Meas) is used. Let $T_1 = \textbf{assert}\ P[\bar{q}]; S_1$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]; S_0$. By induction, we have $[\![T_i]\!]^b(a) \leq_{\mathcal{A}} b_i$ for $i = 0, 1$. Thus from Lemma 4.6,

$$[\![\textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}]\!]^b(a) = [\![T_0]\!]^b(a) \vee [\![T_1]\!]^b(a) \leq_{\mathcal{A}} b_0 \vee b_1.$$

(5) Rule (While) is used. From induction hypothesis, we have

$$[\![\textbf{assert}\ P[\bar{q}]; S]\!]^b(a) \leq_{\mathcal{A}} a, \quad [\![\textbf{assert}\ P^\perp[\bar{q}]]\!]^b(a) \leq_{\mathcal{A}} b.$$

Let $T_i = (\textbf{assert}\ P[\bar{q}]; S)^i; \textbf{assert}\ P^\perp[\bar{q}]$ where $i = 0, 1, \ldots$. By induction on i we can show $[\![T_i]\!]^b(a) \leq_{\mathcal{A}} b$ for all $i \geq 0$. Thus from Lemma 4.6,

$$[\![\textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}]\!]^b(a) = \bigvee_{i \geq 0} [\![T_i]\!]^b(a) \leq_{\mathcal{A}} b.$$

For the second part, suppose $[\![e]\!]^\#$ is complete for any basic command e. Then from Theorem 4.7, the induced abstract operator $[\![S]\!]^\#$ is complete for any quantum program S. Thus it must be the best abstraction; that is $[\![S]\!]^\# = [\![S]\!]^b$. Now we have to show that whenever $[\![S]\!]^b(a) \leq_{\mathcal{A}} b$, then $\vdash \{a\}\ S\ \{b\}$. From Rule (Imp), it suffices to show

$$\vdash \{a\}\ S\ \{[\![S]\!]^b(a)\}$$

by induction on the structure of S. The basis case where $S \equiv e$ for some $e \in \{\textbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} *= U,\ \textbf{assert}\ P[\bar{q}]\}$ is directly from Rule (Exp). For other cases,

(1) $S \equiv S_0; S_1$. This follows from the fact that complete abstractions are closed under operator composition; that is, $[\![S_0; S_1]\!]^b = [\![S_1]\!]^b \circ [\![S_0]\!]^b$.

(2) $S \equiv \textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}$. Let $T_1 = \textbf{assert}\ P[\bar{q}]; S_1$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]; S_0$. Then by induction, we have

$$\vdash \{a\}\ T_1\ \{[\![T_1]\!]^b(a)\}, \qquad \vdash \{a\}\ T_0\ \{[\![T_0]\!]^b(a)\}.$$

Furthermore, from Lemma 4.6,

$$[\![S]\!]^b(a) = \alpha \circ [\![T_1]\!] \circ \gamma(a) \vee \alpha \circ [\![T_0]\!] \circ \gamma(a) = [\![T_1]\!]^b(a) \vee [\![T_0]\!]^b(a).$$

Thus the result follows from Rule (Meas).

(3) $S \equiv \textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}$. Let $T = \textbf{assert}\ P[\bar{q}]; S, T_0 = \textbf{assert}\ P^\perp[\bar{q}]$, and $a^* = \bigvee_{i \geq 0} ([\![T]\!]^b)^i(a)$. Then by induction,

$$\vdash \{a^*\}\ T\ \{[\![T]\!]^b(a^*)\}, \qquad \vdash \{a^*\}\ T_0\ \{[\![T_0]\!]^b(a^*)\}.$$

From Lemma 4.9, we have $[\![T]\!]^b(a^*) = \bigvee_{i \geq 0} ([\![T]\!]^b)^{i+1}(a) \leq_{\mathcal{A}} a^*$ and

$$[\![T_0]\!]^b(a^*) = \bigvee_{i \geq 0} [\![T_0]\!]^b \circ ([\![T]\!]^b)^i(a) = [\![S]\!]^b(a)$$

where the second equality is from Lemma 4.6. The result then follows from Rules (Imp), (While), and the fact that $a \leq_{\mathcal{A}} a^*$. □

Example 5.2 (Hoare logic induced by subspace abstract interpretation). Recall from Examples 4.3 and 4.8 that the subspace abstract domain $\mathcal{S}(\mathcal{H}_V)$ for quantum states is well-structured, and the abstract operators for basic commands defined in Eq. (3) are complete. Thus by Theorems 5.1 the induced Hoare-type proof system presented in Table 1 is both sound and relatively complete when assertions are taken from $\mathcal{S}(\mathcal{H}_V)$.

Note that the applied quantum Hoare logic proposed in [Zhou et al. 2019] also uses elements of $\mathcal{S}(\mathcal{H}_V)$ as assertions. A correctness formulas $\{P\}\ S\ \{Q\}$ is correct (with respect to partial correctness), denoted $\models_{\text{ap}} \{P\}\ S\ \{Q\}$, if for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, whenever $\lceil \rho \rceil \subseteq P$, $\lceil [\![S]\!](\rho) \rceil \subseteq Q$. Using the concretisation function γ_s from $\mathcal{S}(\mathcal{H}_V)$ to $\mathcal{Q}$ defined in Example 4.3, this is equivalent to $[\![S]\!](\gamma_s(P)) \subseteq \gamma_s(Q)$, coinciding with our correctness definition.

We now compare our proof system with the applied quantum Hoare logic. First, let us examine the inference rules for initialisation $\bar{q} := |0\rangle$:

$$\text{(Init)} \quad \{P\}\ \bar{q} := |0\rangle\ \{|0\rangle_{\bar{q}}\langle 0| \otimes \lceil \text{Tr}_{\bar{q}}(P) \rceil\} \qquad\qquad \text{(Init-ap)} \quad \{I_{\bar{q}} \otimes f(Q)\}\ \bar{q} := |0\rangle\ \{Q\}.$$

The left one is from our system, while the right one is taken from [Zhou et al. 2019] where

$$f(Q) \triangleq \bigvee \{T \in \mathcal{S}(\mathcal{H}_V) : |0\rangle_{\bar{q}}\langle 0| \otimes T \subseteq Q\}.$$

We now prove that with the help of Rule (Imp), these two rules are indeed equivalent:

(1) (Init) $\Rightarrow$ (Init-ap). Suppose Q is given. Let $P \triangleq I_{\bar{q}} \otimes f(Q)$. Then $\lceil \text{Tr}_{\bar{q}}(P) \rceil = f(Q)$. Thus from (Init) we have $\{P\}\ \bar{q} := |0\rangle\ \{|0\rangle_{\bar{q}}\langle 0| \otimes f(Q)\}$, and so (Init-ap) follows from (Imp) by noting that $|0\rangle_{\bar{q}}\langle 0| \otimes f(Q) \subseteq Q$.

(2) (Init-ap) $\Rightarrow$ (Init). Suppose P is given. Let $Q \triangleq |0\rangle_{\bar{q}}\langle 0| \otimes \lceil \text{Tr}_{\bar{q}}(P) \rceil$. Then $f(Q) = \lceil \text{Tr}_{\bar{q}}(P) \rceil$. Thus from (Init-ap) we have $\{I_{\bar{q}} \otimes \lceil \text{Tr}_{\bar{q}}(P) \rceil\}\ \bar{q} := |0\rangle\ \{Q\}$, and so (Init) follows from (Imp) by noting that $P \subseteq I_{\bar{q}} \otimes \lceil \text{Tr}_{\bar{q}}(P) \rceil$.

It is evident that the proof system of [Zhou et al. 2019] works in a backward manner; that is, it tries to give *the weakest precondition* of a postcondition. In contrast, our logic system in Table 1 works in a forward manner by trying to give *the strongest postcondition* of a precondition. Due to this complementary nature, we believe that these two systems will be useful in different applications.

Next, let us examine the abstract interpretation for quantum circuits proposed in [Yu and Palsberg 2021] where tuples of subspaces of some subsystems, instead of subspaces of the whole system, are regarded as abstract elements for quantum states.

Example 5.3 (Local-subspace abstract domain). Let a signature σ be a tuple of proper subsets of V; formally, $\sigma \triangleq (s_1, \cdots, s_m)$ where $m \geq 1$ and for each i, $s_i \subset V$. Then the abstract subspace domain with signature σ is given by

$$(\mathcal{S}(\mathcal{H}_V)_\sigma, \sqsubseteq_\sigma, \sqcup_\sigma, \sqcap_\sigma, \bot_\sigma, \top_\sigma)$$

where

$$\mathcal{S}(\mathcal{H}_V)_\sigma \triangleq \left\{(P_1, \cdots, P_m) : \forall i, P_i \text{ is a subspace of } \mathcal{H}_{s_i}\right\},$$

the partial order $\sqsubseteq_\sigma$ and the lattice operators $\sqcup_\sigma$ and $\sqcap_\sigma$ are all defined in the entry-wise way, $\bot_\sigma \triangleq (0_{s_1}, \cdots, 0_{s_m})$, and $\top_\sigma \triangleq (I_{s_1}, \cdots, I_{s_m})$. Again, this domain is a complete lattice. When each s_i contains exactly two quantum variables, this is similar to the octagon domain for classical programs.

The abstraction and concretisation functions are defined naturally as follows. For any $\widetilde{P} \triangleq (P_1, \cdots, P_m) \in \mathcal{S}(\mathcal{H}_V)_\sigma$ and $R \in \mathcal{Q}$,

$$\alpha_\sigma(R) \triangleq (Q_1, \cdots, Q_m), \text{ where } Q_i \triangleq \bigvee \{\lceil \rho_i \rceil : \rho \in R\} \text{ and}$$
$$\rho_i \triangleq \mathrm{Tr}_{V \setminus s_i}(\rho) \text{ is the reduced state of } \rho \text{ in the subsystem } s_i;$$
$$\gamma_\sigma(\widetilde{P}) \triangleq \bigcap_{i=1}^{m} \gamma_s(P_i) = \bigcap_{i=1}^{m} \left\{\rho \in \mathcal{D}(\mathcal{H}_V) : \lceil \rho \rceil \subseteq P_i \otimes I_{V \setminus s_i}\right\}.$$

Intuitively, $\alpha_\sigma(R)$ is the tuple of subspaces in which each component subspace is spanned by all the quantum states in R restricted on the corresponding subsystems, while $\gamma_\sigma(\widetilde{P})$ is collectively determined by all the local subspaces P_i in $\widetilde{P}$ when P_i is regarded as a subspace of the whole quantum system V. In other words, $\mathcal{S}(\mathcal{H}_V)_\sigma$ is essentially the direct product of the individual abstract domains $\mathcal{S}(\mathcal{H}_{s_i})$.

We now show that for each signature σ, $\mathcal{S}(\mathcal{H}_V)_\sigma$ is well-structured. First, for any $\widetilde{P} \in \mathcal{S}(\mathcal{H}_V)_\sigma$ and $R \in \mathcal{Q}$,

$$\begin{aligned}
\alpha_\sigma(R) \sqsubseteq_\sigma \widetilde{P} \quad &\Leftrightarrow \quad \forall i, \bigvee \{\lceil \rho_i \rceil : \rho \in R\} \subseteq P_i \\
&\Leftrightarrow \quad \forall i, \forall \rho \in R, \left\lceil \mathrm{Tr}_{V \setminus s_i}(\rho) \right\rceil \subseteq P_i \\
&\Leftrightarrow \quad \forall \rho \in R, \forall i, \lceil \rho \rceil \subseteq P_i \otimes I_{V \setminus s_i} \\
&\Leftrightarrow \quad R \subseteq \gamma_\sigma(\widetilde{P})
\end{aligned}$$

where the third equivalence follows from the fact that $\lceil \rho \rceil \subseteq \left\lceil \mathrm{Tr}_{V \setminus s_i}(\rho) \right\rceil \otimes I_{V \setminus s_i}$ and $\left\lceil \mathrm{Tr}_{V \setminus s_i}(\lceil \rho \rceil) \right\rceil = \left\lceil \mathrm{Tr}_{V \setminus s_i}(\rho) \right\rceil$ for all $\rho \in \mathcal{D}(\mathcal{H}_V)$. Furthermore, α_σ is surjective. Thus the pair $(\alpha_\sigma, \gamma_\sigma)$ forms a Galois embedding between $\mathcal{Q}$ and $\mathcal{S}(\mathcal{H}_V)_\sigma$. Second, for any $k = 1, \cdots, m$, $\rho_i \in \mathcal{D}(\mathcal{H}_V)$, and $x_i > 0$ with $\sum_i x_i \rho_i \in \mathcal{D}(\mathcal{H}_V)$,

$$\left(\alpha_\sigma\left(\sum_i x_i \rho_i\right)\right)_k = \left\lceil \mathrm{Tr}_{V \setminus s_k}\left(\sum_i x_i \rho_i\right)\right\rceil = \bigvee_i \left\lceil \mathrm{Tr}_{V \setminus s_k}(\rho_i)\right\rceil = \left(\bigvee_i \alpha_\sigma(\rho_i)\right)_k.$$

It is obvious that the best abstraction $[\![S]\!]^b_\sigma = \alpha_\sigma \circ [\![S]\!] \circ \gamma_\sigma$ is sound for any quantum program S. Thus from Theorem 5.1, the proof system presented in Table 1, when $[\![e]\!]^\#$ in Rule (Exp) is replaced by $[\![e]\!]^b_\sigma$, is sound for quantum assertions taken from $\mathcal{S}(\mathcal{H}_V)_\sigma$. However, as the following counter-example shows, $[\![S]\!]^b_\sigma$ is in general not a complete abstraction for $[\![S]\!]$. For simplicity, we consider the case where $V = \{q_1, q_2, q_3\}$ and $\sigma = (\{q_1, q_2\}, \{q_2, q_3\})$. Let $|\Phi^\pm\rangle \triangleq \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$, U be a unitary operator on $\mathcal{D}(\mathcal{H}_V)$ which maps $|\Phi^+\rangle$ to $|000\rangle$ and $|\Phi^-\rangle$ to $|111\rangle$, and $S \triangleq q_1, q_2, q_3 *= U$. Let $\Phi^+ = |\Phi^+\rangle\langle\Psi^+|$. Note that Φ^+ can be regarded as either the density operator corresponding to the pure state $|\Phi^+\rangle$ or the projector onto the one dimensional subspace spanned by $|\Phi^+\rangle$. Then

$$\alpha_\sigma \circ [\![S]\!](\Phi^+) = (P^{00}_{q_1,q_2}, P^{00}_{q_2,q_3}) \quad \text{and} \quad \alpha_\sigma(\Phi^+) = (P^{=}_{q_1,q_2}, P^{=}_{q_2,q_3})$$

where $P^{ii} = \mathrm{span}\{|ii\rangle\}$, $i = 0, 1$, and $P^{=} = \mathrm{span}\{|00\rangle, |11\rangle\}$. However, since $\Phi^- \in \gamma_\sigma(\alpha_\sigma(\Phi^+))$, we have

$$|111\rangle\langle 111| \in [\![S]\!] \circ \gamma_\sigma \circ \alpha_\sigma(\Phi^+).$$

Thus if $[\![S]\!]^b_\sigma \circ \alpha_\sigma(\Phi^+) = (Q_1, Q_2)$ then it must hold that $|11\rangle \in Q_1$ and $|11\rangle \in Q_2$. Consequently, $\alpha_\sigma \circ [\![S]\!](\Phi^+) \neq [\![S]\!]^b_\sigma \circ \alpha_\sigma(\Phi^+)$ as desired.

As $[\![S]\!]^b_\sigma$ is not a complete, Theorem 5.1 tells us nothing about the completeness of the induced Hoare system. Actually, we are going to show in Sec. 5.3 that there does not exist a relatively complete Hoare system which takes $\mathcal{S}(\mathcal{H}_V)_\sigma$ as the set of assertions.

$$\text{(Exp-In)}\quad [a]\ e\ [[[e]]^{\#}(a)] \qquad \text{where } e \in \{\mathbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} *= U,\ \mathbf{assert}\ P[\bar{q}]\}$$

$$\text{(Seq-In)}\quad \frac{[a]\ S_0\ [a'],\ [a']\ S_1\ [b]}{[a]\ S_0; S_1\ [b]} \qquad \text{(Meas-In)}\quad \frac{[a]\ \mathbf{assert}\ P[\bar{q}]; S_1\ [b_1],\ [a]\ \mathbf{assert}\ P^{\perp}[\bar{q}]; S_0\ [b_0]}{[a]\ \mathbf{if}\ P[\bar{q}]\ \mathbf{then}\ S_1\ \mathbf{else}\ S_0\ \mathbf{end}\ [b_0 \vee b_1]}$$

$$\text{(Imp-In)}\quad \frac{a' \leq_{\mathcal{A}} a,\ [a']\ S\ [b'],\ b \leq_{\mathcal{A}} b'}{[a]\ S\ [b]} \qquad \text{(While-In)}\quad \frac{\forall i, [a_i]\ \mathbf{assert}\ P[\bar{q}]; S\ [a_{i+1}],\ [a_i]\ \mathbf{assert}\ P^{\perp}[\bar{q}]\ [b_i]}{[a_0]\ \mathbf{while}\ P[\bar{q}]\ \mathbf{do}\ S\ \mathbf{end}\ [\bigvee_{i\geq 0} b_i]}$$

Table 2. Proof system for incorrectness logic induced by abstract domain $(\mathcal{A}, \leq_{\mathcal{A}})$.

5.2 Incorrectness logic induced by abstract interpretation

In the previous section, we show how an abstract interpretation of quantum programs is closely related to a quantum Hoare logic induced by it. Interestingly, a quantum incorrectness logic system can also be induced by a quantum abstract interpretation.

Let $\mathcal{A}$ be a well-structured abstract domain of program states, and an abstract monotonic operator $[[e]]^{\#}$ be defined for each basic command $e \in \{\mathbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} *= U,\ \mathbf{assert}\ P[\bar{q}]\}$. Then an incorrectness proof system is naturally induced as follows:

(1) Take $\mathcal{A}$ to be the set of assertions, and the satisfaction relation is similarly defined as for the Hoare logic case in the previous section. Again, $\mathcal{A}$ as a set of assertions is also well-structured.
(2) A specification formula $[a]\ S\ [b]$ holds, denoted $\models_{\text{in}} [a]\ S\ [b]$, if $b \leq_{\mathcal{A}} [[S]]^b(a)$. That is, b is an under-approximation of $\alpha([[S]] \circ \gamma(a))$, the abstraction for the set of reachable states of S starting in $\gamma(a)$.
(3) The proof system is presented as in Table 2. Denote by $\vdash_{\text{in}} [a]\ S\ [b]$ if the formula $[a]\ S\ [b]$ can be deduced from it.

Compared with the Hoare logic system in Table 1, the main difference lies in the consequence rule. In Rule (Imp), we strengthen preconditions and weaken postconditions, while in Rule (Imp-In) we weaken preconditions and strengthen postconditions. This is due to the fact that Hoare logic reasons about over-approximation while incorrectness logic reasons about under-approximation of program semantics.

As abstract interpretation usually provides an over-approximation for program analysis, a sound abstraction does not necessarily guarantee the soundness of the induced incorrectness logic. However, as the following theorem states, a complete abstract interpretation indeed guarantees that the induced incorrectness logic is both sound and relatively complete.

Theorem 5.4. *Let $\mathcal{A}$ be a well-structured abstract domain of quantum programs. If the abstract operator $[[e]]^{\#}$ is complete for each basic command e, then the induced incorrectness logic system presented in Table 2 is both sound and relatively complete; that is,*

$$\vdash_{\text{in}} [a]\ S\ [b] \qquad \textit{iff} \qquad \models_{\text{in}} [a]\ S\ [b]$$

for any specification formula $[a]\ S\ [b]$.

Proof. First, from Theorem 4.7, if $[[e]]^{\#}$ is complete for each basic command e, then $[[S]]^{\#}$ is complete for any program S. Thus $[[S]]^{\#} = [[S]]^b$.

To prove the soundness, we have to show that whenever $\vdash_{\text{in}} [a]\ S\ [b]$, then $b \leq_{\mathcal{A}} [[S]]^b(a)$. This can be proved by induction on the proof length of $\vdash_{\text{in}} [a]\ S\ [b]$. For the last step of the proof, we have the following cases:

(1) Rule (Exp-In) is used. In this case, $S \equiv e$ for some $e \in \{\textbf{skip},\ \bar{q} := |0\rangle,\ \bar{q} *= U,\ \textbf{assert}\ P[\bar{q}]\}$, and $b \equiv [\![e]\!]^b(a)$. The result then trivially follows.
(2) Rule (Seq-In) is used. This follows from the fact that complete abstractions are closed under operator composition; that is, $[\![S_0; S_1]\!]^b = [\![S_1]\!]^b \circ [\![S_0]\!]^b$.
(3) Rule (Imp-In) is used. Then the result follows from the monotonicity of $[\![S]\!]^b$ for all program S.
(4) Rule (Meas-In) is used. Let $T_1 = \textbf{assert}\ P[\bar{q}]; S_1$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]; S_0$. By induction, we have $b_i \leq_{\mathcal{A}} [\![T_i]\!]^b(a)$ for $i = 0, 1$. Thus from Lemma 4.6,

$$b_0 \vee b_1 \leq_{\mathcal{A}} [\![T_0]\!]^b(a) \vee [\![T_1]\!]^b(a) = [\![\textbf{if}\ P[\bar{q}]\ \textbf{then}\ S_1\ \textbf{else}\ S_0\ \textbf{end}]\!]^b(a).$$

(5) Rule (While-In) is used. Let $T = \textbf{assert}\ P[\bar{q}]; S$ and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]$. From induction hypothesis, we have for any $i \geq 0$, $a_{i+1} \leq_{\mathcal{A}} [\![T]\!]^b(a_i)$ and $b_i \leq_{\mathcal{A}} [\![T_0]\!]^b(a_i)$. By induction on i we can show $a_i \leq_{\mathcal{A}} ([\![T]\!]^b)^i(a_0)$ for all $i \geq 0$. Thus from Lemma 4.6,

$$\bigvee_{i\geq 0} b_i \leq_{\mathcal{A}} \bigvee_{i\geq 0} [\![T_0]\!]^b(a_i) \leq_{\mathcal{A}} \bigvee_{i\geq 0} [\![T_0]\!]^b \circ ([\![T]\!]^b)^i(a_0) = [\![\textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}]\!]^b(a_0).$$

For the completeness part, we have to show that whenever $b \leq_{\mathcal{A}} [\![S]\!]^b(a)$, then $\vdash_{\text{in}} [a]\ S\ [b]$. First, from Rule (Imp-In), it suffices to show

$$\vdash_{\text{in}} [a]\ S\ [[\![S]\!]^b(a)]$$

by induction on the structure of S. The proof is similar to the corresponding part of Theorem 5.1 for Hoare logic, except for the while loop which we prove as follows.

Let $S \equiv \textbf{while}\ P[\bar{q}]\ \textbf{do}\ S\ \textbf{end}$, $T = \textbf{assert}\ P[\bar{q}]; S$, and $T_0 = \textbf{assert}\ P^\perp[\bar{q}]$. By induction, for any $i \geq 0$,

$$\vdash_{\text{in}} [([\![T]\!]^b)^i(a)]\ T\ [([\![T]\!]^b)^{i+1}(a)], \quad \vdash_{\text{in}} [([\![T]\!]^b)^i(a)]\ T_0\ [[\![T_0]\!]^b \circ ([\![T]\!]^b)^i(a)].$$

Thus from (While-In),

$$\vdash_{\text{in}} [a]\ S\ [\bigvee_{i\geq 0} [\![T_0]\!]^b \circ ([\![T]\!]^b)^i(a)],$$

and the result follows from Lemma 4.6 and the fact that complete abstractions are closed under operator composition. □

Example 5.5 (Quantum incorrectness logic induced by subspace abstract interpretation). Again, as the subspace abstract interpretation defined Example 4.8 is complete, from Theorems 5.4 we know that the induced incorrectness logic system presented in Table 2 is both sound and complete when assertions are taken from $\mathcal{S}(\mathcal{H}_V)$.

The incorrectness logic proposed in [Yan et al. 2022] also uses elements of $\mathcal{S}(\mathcal{H}_V)$ as assertions. A specification formula $[P]\ S\ [Q]$ is valid if for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, whenever $P \subseteq \lceil \rho \rceil$, $Q \subseteq \lceil [\![S]\!](\rho) \rceil$. It is easy to see that this is equivalent to $Q \leq_{\mathcal{A}} [\![S]\!]^b(P)$ where the best abstraction $[\![S]\!]^b$ is defined using the abstraction and concretisation functions presented in Example 4.3, coinciding with our correctness definition. Again, the difference between our proof system and the one proposed in [Yan et al. 2022] is that the former works in a forward manner while the latter in a backward manner.

5.3 Abstract interpretation induced by Hoare logic

Now we consider the reverse problems of deriving a quantum abstract interpretation from a quantum Hoare/incorrectness logic. Let $\mathcal{A}$ be a well-structured set of quantum assertions, and PS be a Hoare-type proof system (of partial correctness) for quantum programs, where the assertions are taken from $\mathcal{A}$. Without loss of generality, we assume that PS consists of an axiom (schema) for

each basic command and a proof rule for each program construct such as sequential composition, conditional branching, and while loop. Furthermore, it provides a consequence rule of the form

$$\frac{a \leq_{\mathcal{A}} a',\ \{a'\}\ S\ \{b'\},\ b' \leq_{\mathcal{A}} b}{\{a\}\ S\ \{b\}}$$

for precondition strengthening and postcondition weakening. A correctness formula $\{a\}\ S\ \{a'\}$ in PS is semantically valid, written $\models_{\mathrm{PS}} \{a\}\ S\ \{a'\}$, if for any $\rho \in \mathcal{D}(\mathcal{H}_V)$, $\rho \models a$ implies $[\![S]\!](\rho) \models a'$. It is derivable, written $\vdash_{\mathrm{PS}} \{a\}\ S\ \{a'\}$, if it has a proof sequence in PS. Then an abstract interpretation for quantum programs is naturally induced by PS as follows:

- Take $\mathcal{A}$ to be the abstract domain of quantum states, and define the pair of abstraction-concretisation functions (α, γ) as in Lemma 4.13. Then $\mathcal{A}$ as an abstract domain is also well-structured.
- For any quantum program S, let $[\![S]\!]^{\#} : \mathcal{A} \to \mathcal{A}$ with

$$[\![S]\!]^{\#}(a) = \bigwedge \{a' \in \mathcal{A} : \vdash_{\mathrm{PS}} \{a\}\ S\ \{a'\}\} \tag{4}$$

  for any $a \in \mathcal{A}$ be the abstract operator of $[\![S]\!]$.

Thanks to the complete lattice structure of the assertion set $\mathcal{A}$, the strongest postconditions always exist in PS. For any quantum program S and $a \in \mathcal{A}$, let

$$spc(S, a) \triangleq \bigwedge \{a' \in \mathcal{A} : \models_{\mathrm{PS}} \{a\}\ S\ \{a'\}\}. \tag{5}$$

We now prove that $spc(S, a)$ is the strongest postcondition of a with respect to S. Furthermore, it coincides with the best abstraction of S.

Lemma 5.6. *For any quantum program S and $a \in \mathcal{A}$,*

(1) $\models_{\mathrm{PS}} \{a\}\ S\ \{spc(S, a)\}$;
(2) *for any $a' \in \mathcal{A}$, if $\models_{\mathrm{PS}} \{a\}\ S\ \{a'\}$ then $spc(S, a) \leq_{\mathcal{A}} a'$;*
(3) $spc(S, a) = [\![S]\!]^b(a)$ *where* $[\![S]\!]^b = \alpha \circ [\![S]\!] \circ \gamma$ *is the best abstraction of* $[\![S]\!]$.

Proof. Firstly, clause (2) is easy from Eq. (5). To prove (1), take any ρ with $\rho \models a$ and $a' \in \mathcal{A}$. If $\models_{\mathrm{PS}} \{a\}\ S\ \{a'\}$, then $[\![S]\!](\rho) \models a'$. Thus $[\![S]\!](\rho) \models spc(S, a)$ from the first condition of Definition 4.10.

To prove (3), we first observe that $\models_{\mathrm{PS}} \{a\}\ S\ \{[\![S]\!]^b(a)\}$. Thus $spc(S, a) \leq_{\mathcal{A}} [\![S]\!]^b(a)$ from (2). For the converse part, take any $a' \in \mathcal{A}$ with $\models_{\mathrm{PS}} \{a\}\ S\ \{a'\}$. Then $[\![S]\!] \circ \gamma(a) \subseteq \gamma(a')$, which implies that $[\![S]\!]^b(a) \leq_{\mathcal{A}} a'$. Thus $[\![S]\!]^b(a) \leq_{\mathcal{A}} spc(S, a)$ from the arbitrariness of a'. □

The following theorem gives a close relationship between a Hoare-type logic system and the abstract interpretation induced by it.

Theorem 5.7. *Let $\mathcal{A}$ be a well-structured set of quantum assertions, and* PS *a Hoare-type logic system for quantum programs with assertions taken from $\mathcal{A}$.*

(1) *If* PS *is sound, then the induced abstract interpretation is sound.*
(2) *If* PS *is sound and relatively complete, then the induced abstract interpretation is complete.*

Proof. For any $a \in \mathcal{A}$ and quantum program S, let

$$F_{\vdash}(S, a) \triangleq \{a' \in \mathcal{A} : \vdash_{\mathrm{PS}} \{a\}\ S\ \{a'\}\} \quad \text{and} \quad F_{\models}(S, a) \triangleq \{a' \in \mathcal{A} : \models_{\mathrm{PS}} \{a\}\ S\ \{a'\}\}.$$

Now to prove (1), note that if PS is sound then $F_{\vdash}(S, a) \subseteq F_{\models}(S, a)$. Thus $[\![S]\!]^b(a) \leq_{\mathcal{A}} [\![S]\!]^{\#}(a)$ by Lemma 5.6(3), which implies that the abstraction $[\![S]\!]^{\#}$ is sound.

To prove (2), note that if PS is relatively complete then $F_{\models}(S, a) \subseteq F_{\vdash}(S, a)$. Thus $[\![S]\!]^{\#}(a) \leq_{\mathcal{A}} [\![S]\!]^b(a)$, which, together with (1), implies that $[\![S]\!]^{\#}$ is the best abstraction of S. The rest of the proof consists of four steps.

(i) As the first step, we prove that for any S_2 and S_1,

$$[\![S_1; S_2]\!]^\# = [\![S_2]\!]^\# \circ [\![S_1]\!]^\#.$$

For any $a \in \mathcal{A}$, we know from the completeness of PS that $\vdash_{\mathrm{PS}} \{a\}\ S_1; S_2\ \{[\![S_1; S_2]\!]^\#(a)\}$. Furthermore, as there is only one proof rule for sequential composition, there must exist $a_1, b \in \mathcal{A}$ such that

$$a \leq_{\mathcal{A}} a_1, \quad \vdash_{\mathrm{PS}} \{a_1\}\ S_1\ \{b\}, \quad \vdash_{\mathrm{PS}} \{b\}\ S_2\ \{a'\}, \quad a' \leq_{\mathcal{A}} [\![S_1; S_2]\!]^\#(a).$$

Then

$$\begin{aligned} [\![S_2]\!]^\# \circ [\![S_1]\!]^\#(a) &\leq_{\mathcal{A}} [\![S_2]\!]^\# \circ [\![S_1]\!]^\#(a_1) \\ &\leq_{\mathcal{A}} [\![S_2]\!]^\#(b) \\ &\leq_{\mathcal{A}} a' \leq_{\mathcal{A}} [\![S_1; S_2]\!]^\#(a). \end{aligned}$$

The other direction that $[\![S_1; S_2]\!]^\#(a) \leq_{\mathcal{A}} [\![S_2]\!]^\# \circ [\![S_1]\!]^\#(a)$ is easy from the fact $\gamma \circ \alpha \geq_Q \mathrm{id}_Q$.

(ii) The next step is to show that for any set R of quantum states, we can always find a single state (not necessarily in R) which shares the same abstraction with R. Specifically, we have

Claim 5.1. *For any $R \subseteq \mathcal{D}(\mathcal{H}_V)$, there exists a single state $\rho_R \in \mathcal{D}(\mathcal{H}_V)$ with $\mathrm{Tr}(\rho_R) = 1$ such that*

$$\alpha([\![S]\!](\rho_R)) = \alpha([\![S]\!](R))$$

for all quantum program S. In particular, $\alpha(\rho_R) = \alpha(R)$.

Proof of Claim 5.1. As $\mathcal{H}_V$ is finite dimensional, we can always find a set of states $\rho_1, \ldots, \rho_n$ in R, $\mathrm{Tr}(\rho_i) = 1$, such that

$$\alpha_s(R) = \bigvee \{\lceil \rho \rceil : \rho \in R\} = \bigvee_{i=1}^{n} \lceil \rho_i \rceil .$$

Let $\rho_R = \sum_{i=1}^n \rho_i/n$. Then for any S,

$$\alpha_s([\![S]\!](\rho_R)) = \alpha_s\left(\sum_{i=1}^n \frac{1}{n}[\![S]\!](\rho_i)\right) = \bigvee_{i=1}^n \alpha_s([\![S]\!](\rho_i)) = \alpha_s([\![S]\!](R)).$$

Then $\alpha([\![S]\!](\rho_R)) = \alpha([\![S]\!](R))$ from Lemma 4.4. □

(iii) The third step is to show that our while-language is powerful enough to prepare an arbitrarily given state. Specifically, we have

Claim 5.2. *For any $\rho \in \mathcal{D}(\mathcal{H}_V)$ with $\mathrm{Tr}(\rho) = 1$, there exists a quantum program S^ρ which turns any quantum state into state ρ; that is, for all $\sigma \in \mathcal{D}(\mathcal{H}_V)$,*

$$[\![S^\rho]\!](\sigma) = \mathrm{Tr}(\sigma) \cdot \rho.$$

Consequently, for all $R \subseteq \mathcal{D}(\mathcal{H}_V)$ and program S,

$$\alpha([\![S^\rho; S]\!](R)) = \alpha([\![S]\!](\rho))$$

whenever $R \neq \{0\}$.

Proof of Claim 5.2. Let $\rho = \sum_{i=0}^{d-1} \lambda_i |\psi_i\rangle\langle\psi_i|$, $d = 2^{|V|}$, be the spectral decomposition of ρ where $\{|\psi_i\rangle : i = 0, \ldots, d-1\}$ constitute some orthonormal basis of $\mathcal{H}_V$. Let $|\psi\rangle =$

$\sum_{i=0}^{d-1} \sqrt{\lambda_i}|\psi_i\rangle$. From the assumption that $\mathrm{Tr}(\rho) = 1$ we know that $|\psi\rangle$ is a valid quantum (pure) state. Thus we can find a unitary operator U on $\mathcal{H}_V$ such that $U|0\rangle = |\psi\rangle$. Let

$$
\begin{array}{l}
S^\rho \triangleq \\
\quad \bar{q} := |0\rangle;\ \bar{q} *= U; \\
\quad \textbf{if } P_0[\bar{q}] \textbf{ then} \\
\qquad \textbf{skip}; \\
\quad \textbf{else if } P_1[\bar{q}] \textbf{ then} \\
\qquad\quad \textbf{skip}; \\
\qquad \textbf{else} \\
\qquad\quad \cdots \\
\qquad \textbf{end} \\
\quad \textbf{end}
\end{array}
$$

where $\bar{q} = V$, and for any $i = 0, \ldots, d-1$, $P_i = |\psi_i\rangle\langle\psi_i|$. Note that for any $\sigma \in \mathcal{D}(\mathcal{H}_V)$,

$$[\![\bar{q} := |0\rangle]\!](\sigma) = \mathrm{Tr}(\sigma) \cdot |0\rangle\langle 0|.$$

Then it is easy to show that $[\![S^\rho]\!](\sigma) = \mathrm{Tr}(\sigma) \cdot \rho$. The last part of the claim follows from the linearity of $[\![S]\!]$. □

(iv) Now for any quantum program S, $R \subseteq \mathcal{D}(\mathcal{H}_V)$, and $a \in \mathcal{A}$ with $\gamma(a) \neq \{0\}$,

$$
\begin{aligned}
\alpha \circ [\![S]\!](R) &= \alpha([\![S]\!](\rho_R)) && \text{Claim 5.1} \\
&= \alpha \circ [\![S^{\rho_R}; S]\!] \circ \gamma(a) && \text{Claim 5.2} \\
&= [\![S^{\rho_R}; S]\!]^\#(a) && [\![\cdot]\!]^\# \text{ is the best abstraction} \\
&= [\![S]\!]^\# \circ [\![S^{\rho_R}]\!]^\#(a) && \text{Step (i)} \\
&= [\![S]\!]^\# \circ \alpha \circ [\![S^{\rho_R}]\!] \circ \gamma(a) \\
&= [\![S]\!]^\# \circ \alpha(\rho_R) && \text{Claim 5.2} \\
&= [\![S]\!]^\# \circ \alpha(R). && \text{Claim 5.1}
\end{aligned}
$$

Thus $\alpha \circ [\![S]\!] = [\![S]\!]^\# \circ \alpha$ as desired. □

Example 5.8 (Abstract interpretation induced by applied quantum Hoare logic). Recall from Example 5.2 that the applied quantum Hoare logic [Zhou et al. 2019], which is both sound and relatively complete, uses elements of $\mathcal{S}(\mathcal{H}_V)$ as assertions. Thus by Theorems 5.7, the induced abstract interpretation on subspace domain is complete, where the abstraction and concretisation functions are defined in Lemma 4.13 and the abstract operators defined in Eq.(4). It is easy to check that this induced abstract interpretation for quantum programs is exactly the one defined in Example 4.8.

Example 5.9. Let us revisit Example 5.3. We have already shown that although the local-subspace abstract domain $\mathcal{S}(\mathcal{H}_V)_\sigma$ is well-structured for any signature σ, the best abstraction $[\![S]\!]^b_\sigma$ is in general not complete for $[\![S]\!]$. Thus from Theorem 5.7, it is impossible to have a sound and relatively complete Hoare-type logic system with elements in $\mathcal{S}(\mathcal{H}_V)_\sigma$ being taken as assertions.

5.4 Abstract interpretation induced by incorrectness logic

Let $\mathcal{A}$ be a well-structured set of quantum assertions, and IN an incorrectness logic system for quantum programs, where the assertions are taken from $\mathcal{A}$. Similar to the case of Hoare logic in the last subsection, we assume that IN consists of an axiom (schema) for each basic command and a proof rule for each program construct, except that the consequence rule is now of the form

$$\frac{a \leq_{\mathcal{A}} a',\ [a]\ S\ [b],\ b' \leq_{\mathcal{A}} b}{[a']\ S\ [b']}$$

for precondition weakening and postcondition strengthening. A correctness formula $[a]\ S\ [a']$ in IN is semantically valid, written $\models_{\text{IN}} [a]\ S\ [a']$, if

$$a' \leq_{\mathcal{A}} \bigwedge \{b \in \mathcal{A} : \forall \rho \models a, [\![S]\!](\rho) \models b\}. \tag{6}$$

Note that the right-hand side of Eq.(6) denotes the strongest assertion which is satisfied by all reachable states starting from some state satisfying a, and a' provides an under-approximation for it. The formula $[a]\ S\ [a']$ is derivable, written $\vdash_{\text{IN}} [a]\ S\ [a']$, if it has a proof sequence in IN.

An abstract interpretation for quantum programs is then naturally induced by IN as follows:

- Take $\mathcal{A}$ to be the abstract domain of quantum states, and define the pair of abstraction-concretisation functions (α, γ) as in Lemma 4.13. Then $\mathcal{A}$ as an abstract domain is also well-structured.
- For any quantum program S, let $[\![S]\!]^{\#} : \mathcal{A} \to \mathcal{A}$ with

$$[\![S]\!]^{\#}(a) = \bigvee \{a' \in \mathcal{A} : \vdash_{\text{IN}} [a]\ S\ [a']\} \tag{7}$$

  for any $a \in \mathcal{A}$ be the abstract operator of $[\![S]\!]$.

For any quantum program S and $a \in \mathcal{A}$, let

$$wpc(S, a) \triangleq \bigvee \{a' \in \mathcal{A} : \models_{\text{IN}} [a]\ S\ [a']\}. \tag{8}$$

We now prove that $wpc(S, a)$ is the weakest postcondition of a with respect to S, and it is exactly the best abstraction of S.

Lemma 5.10. *For any quantum program S and $a \in \mathcal{A}$,*

(1) $\models_{\text{IN}} [a]\ S\ [wpc(S, a)]$;
(2) *for any $a' \in \mathcal{A}$, if* $\models_{\text{IN}} [a]\ S\ [a']$ *then* $a' \leq_{\mathcal{A}} wpc(S, a)$;
(3) $wpc(S, a) = [\![S]\!]^b(a)$.

Proof. Note that from the definitions of α and γ in Lemma 4.13, we have

$$\begin{aligned}
[\![S]\!]^b(a) &= \alpha \circ [\![S]\!] \circ \gamma(a) \\
&= \bigwedge \left\{ b \in \mathcal{A} : [\![S]\!] \circ \gamma(a) \subseteq \gamma(b) \right\} \\
&= \bigwedge \left\{ b \in \mathcal{A} : \forall \rho \in \gamma(a), [\![S]\!](\rho) \in \gamma(b) \right\} \\
&= \bigwedge \left\{ b \in \mathcal{A} : \forall \rho \models a, [\![S]\!](\rho) \models b \right\}.
\end{aligned}$$

Thus $\models_{\text{IN}} [a]\ S\ [a']$ iff $a' \leq_{\mathcal{A}} [\![S]\!]^b(a)$, and so $wpc(S, a) = [\![S]\!]^b(a)$ from Eq. (8). Finally, (1) and (2) follow from (3) directly. □

The following theorem gives a close relationship between a quantum incorrectness logic system and the abstract interpretation induced by it.

Theorem 5.11. *Let $\mathcal{A}$ be a well-structured set of quantum assertions, and* IN *an incorrectness logic system for quantum programs with assertions taken from $\mathcal{A}$. If* IN *is sound and relatively complete, then the induced abstract interpretation is complete.*

Proof. For any $a \in \mathcal{A}$ and quantum program S, let

$$G_{\vdash}(S,a) \triangleq \{a' \in \mathcal{A} : \vdash_{\text{IN}} [a]\ S\ [a']\} \quad \text{and} \quad G_{\models}(S,a) \triangleq \{a' \in \mathcal{A} : \models_{\text{IN}} [a]\ S\ [a']\}.$$

As IN is sound and relatively complete, we have $G_{\vdash}(S,a) = G_{\models}(S,a)$. Thus $[\![S]\!]^{\#}(a) = [\![S]\!]^{b}(a)$ from Lemma 5.10(3), and so $[\![S]\!]^{\#}$ is the best abstraction of S.

Let S_1 and S_2 be two quantum programs. From Lemma 5.10 and completeness of IN, we have for all $a \in \mathcal{A}$,

$$\vdash_{\text{IN}} [a]\ S_1\ [[\![S_1]\!]^{\#}(a)] \quad \text{and} \quad \vdash_{\text{IN}} [[\![S_1]\!]^{\#}(a)]\ S_2\ [[\![S_2]\!]^{\#} \circ [\![S_1]\!]^{\#}(a)],$$

and so $\vdash_{\text{IN}} [a]\ S_1; S_2\ [[\![S_2]\!]^{\#} \circ [\![S_1]\!]^{\#}(a)]$ from the rule for sequential composition. Thus $[\![S_2]\!]^{\#} \circ [\![S_1]\!]^{\#}(a) \leq_{\mathcal{A}} [\![S_1; S_2]\!]^{\#}(a)$ from Eq. (7). However, from the fact that $\gamma \circ \alpha \geq_{Q} \mathrm{id}_{Q}$, we know that $[\![S_1; S_2]\!]^{\#}(a) \leq_{\mathcal{A}} [\![S_2]\!]^{\#} \circ [\![S_1]\!]^{\#}(a)$. Thus

$$[\![S_1; S_2]\!]^{\#} = [\![S_2]\!]^{\#} \circ [\![S_1]\!]^{\#}.$$

The rest of the proof is the same as in Theorem 5.7 (starting from the second step). □

Example 5.12 (Abstract interpretation induced by quantum incorrectness logic). Recall from Example 5.5 that the quantum incorrectness logic presented in [Yan et al. 2022] is both sound and relatively complete. Thus by Theorems 5.11, the induced abstract interpretation on subspace domain is complete, where the abstraction and concretisation functions are defined in Lemma 4.13 and the abstract operators defined in Eq.(7). It is easy to check that this induced abstract interpretation for quantum programs is also the one defined in Example 4.8.

Similar to Example 5.9, Theorem 5.11 also implies that it is impossible to have a sound and relatively complete incorrectness logic system with elements in $\mathcal{S}(\mathcal{H}_V)_{\sigma}$ being taken as assertions.

To conclude this section, we note the following corollary, which can be directly shown from Theorems 5.1, 5.4, 5.7, and 5.11.

Corollary 5.13. *Let $\mathcal{A}$ be a well-structured set of assertions for quantum states. The following two statements are equivalent:*

(1) *there exists a sound and relatively complete quantum Hoare logic system;*
(2) *there exists a sound and relatively complete quantum incorrectness logic system.*

6 CONCLUSION

We have shown a close relationship between abstract interpretation and Hoare/incorrectness logic for quantum programs, when the abstract domain and the set of assertions for quantum states are well-structured. With this relationship, we obtain sound and relatively complete Hoare logic and incorrectness logic for quantum programs. The induced logic systems are in a forward manner, complementing the (backward) applied quantum Hoare logic and incorrectness logic proposed in the literature. Conversely, our result also implies the non-existence of any sound and relatively complete Hoare or incorrectness logic for quantum programs if tuples of local subspaces are taken as assertions for quantum states.

For future work, we plan to consider quantitative assertions where a quantum state satisfies a property with some degree (a number in $[0,1]$). Natural candidates for such assertions are hermitian operators between 0 and the identity, as widely used in the expectation-based quantum Hoare logics. To this end, we have to first establish a theory of abstract interpretation when such hermitian-operator assertions are regarded as abstraction of quantum states.

REFERENCES

Krzysztof Apt, Frank S De Boer, and Ernst-Rüdiger Olderog. 2010. *Verification of sequential and concurrent programs*. Springer Science & Business Media.

Krzysztof R Apt and Ernst-Rüdiger Olderog. 2019. Fifty years of Hoare's logic. *Formal Aspects of Computing* 31, 6 (2019), 751–807.

Edmund Clarke, Orna Grumberg, Somesh Jha, Yuan Lu, and Helmut Veith. 2003. Counterexample-guided abstraction refinement for symbolic model checking. *Journal of the ACM (JACM)* 50, 5 (2003), 752–794.

Edmund M Clarke, Orna Grumberg, and David E Long. 1994. Model checking and abstraction. *ACM transactions on Programming Languages and Systems (TOPLAS)* 16, 5 (1994), 1512–1542.

Rance Cleaveland and James Riely. 1994. Testing-based abstractions for value-passing systems. In *CONCUR'94: Concurrency Theory*. Springer, 417–432.

Marco Comini, Ferruccio Damiani, and Samuel Vrech. 2008. On polymorphic recursion, type systems, and abstract interpretation. In *International Static Analysis Symposium*. Springer, 144–158.

Patrick Cousot. 1997. Types as abstract interpretations. In *Proceedings of the 24th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. 316–331.

Patrick Cousot and Radhia Cousot. 1977. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of the 4th ACM SIGACT-SIGPLAN symposium on Principles of programming languages*. 238–252.

Patrick Cousot and Radhia Cousot. 2000. Temporal abstract interpretation. In *Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. 12–25.

Dennis Dams, Rob Gerth, and Orna Grumberg. 1997. Abstract interpretation of reactive systems. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 19, 2 (1997), 253–291.

Ellie D'Hondt and Prakash Panangaden. 2006. Quantum weakest preconditions. *Mathematical Structures in Computer Science* 16, 3 (2006), 429–451.

Yuan Feng, Runyao Duan, Zhengfeng Ji, and Mingsheng Ying. 2007. Proof rules for the correctness of quantum programs. *Theoretical Computer Science* 386, 1-2 (2007), 151–166.

Yuan Feng, Sanjiang Li, and Mingsheng Ying. 2022. Verification of Distributed Quantum Programs. *ACM Transactions on Computational Logic (TOCL)* 23, 3 (2022), 1–40.

Yuan Feng and Mingsheng Ying. 2021. Quantum Hoare logic with classical variables. *ACM Transactions on Quantum Computing* 2, 4 (2021), 1–43.

Charles Antony Richard Hoare. 1969. An axiomatic basis for computer programming. *Commun. ACM* 12, 10 (1969), 576–580.

Karl Kraus, Arno Böhm, John D Dollard, and WH Wootters. 1983. States, effects, and operations: fundamental notions of quantum theory. *Lecture notes in physics* 190 (1983).

Antoine Miné. 2017. Tutorial on static inference of numeric invariants by abstract interpretation. *Foundations and Trends in Programming Languages* 4, 3-4 (2017), 120–372.

Michael A Nielsen and Isaac Chuang. 2002. Quantum computation and quantum information.

Peter W O'Hearn. 2019. Incorrectness logic. *Proceedings of the ACM on Programming Languages* 4, POPL (2019), 1–32.

David A Plaisted. 1981. Theorem proving with abstraction. *Artificial Intelligence* 16, 1 (1981), 47–108.

Peter Selinger. 2004. Towards a quantum programming language. *Mathematical Structures in Computer Science* 14, 4 (2004), 527–586.

Dominique Unruh. 2019. Quantum hoare logic with ghost variables. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 1–13.

Arnaud Venet. 1996. Abstract interpretation of the π-calculus. In *LOMAPS Workshop on Analysis and Verification of Multiple-Agent Languages*. Springer, 51–75.

John Von Neumann. 1955. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ.

Edsko de Vries and Vasileios Koutavas. 2011. Reverse hoare logic. In *International Conference on Software Engineering and Formal Methods*. Springer, 155–171.

Peng Yan, Hanru Jiang, and Nengkun Yu. 2022. On incorrectness logic for Quantum programs. *Proceedings of the ACM on Programming Languages* 6, OOPSLA (2022), 1–28.

Mingsheng Ying. 2012. Floyd–Hoare logic for quantum programs. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 33, 6 (2012), 1–49.

Mingsheng Ying. 2016. *Foundations of Quantum Programming*. Morgan Kaufmann.

Mingsheng Ying. 2022. Birkhoff-von Neumann Quantum Logic as an Assertion Language for Quantum Programs. *arXiv preprint arXiv:2205.01959* (2022).

Mingsheng Ying, Li Zhou, Yangjia Li, and Yuan Feng. 2022. A proof system for disjoint parallel quantum programs. *Theoretical Computer Science* 897 (2022), 164–184.

Nengkun Yu and Jens Palsberg. 2021. Quantum Abstract Interpretation. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation (PLDI 2021)*. 542–558.

Li Zhou, Nengkun Yu, and Mingsheng Ying. 2019. An applied quantum Hoare logic. In *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*. 1149–1162.