UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Galina Pass

Quantum Relational Hoare Logic Judgements

Master's Thesis (30 ECTS)

Supervisor: Dominique Peer Ghislain Dr Unruh, PhD

Tartu 2021

Quantum Relational Hoare Logic Judgements

Abstract:
With the development of quantum and post-quantum cryptography, it becomes necessary to verify security proofs of protocols. For this, quantum Relational Hoare Logic was developed. The main object of this logic is judgments that demonstrate the various connections between two quantum programs. Their are for possible ways to define judgements: with quantum predicates or operators, with separability requirement or without it. The subject of study in this thesis is the question of whether it is possible for such a judgment to answer the question whether it holds or not. The chosen approach is to use the linear and convex conical structure of the studied objects to apply semidefinite and cone programming. This allowed to apply results related to the optimization of linear functions over a set of separable operators. This provide an efficient algorithm for the two definitions without the separability constraint. For the other two types of judgements this approach gives a reformulation of the problem in terms of cone programming and polynomials non-negativity. This allows to algorithmically check connections between quantum programs and continue the studies with a new point of view on the judgements solvability.

Keywords:
Quantum cryptography, quantum information, semidefinite programming, cone programming, convex optimization relational Hoare logic

CERCS:
$P170$ Computer science, numerical analysis, systems, control

Kvant-relatsioonilised hoare-loogikaotsused

Lühikokkuvõte:
Kvant- ja postkvantkrüptograafia väljatöötamisel on vajalik protokollide turbetõendite kontrollimine. Selleks töötati välja kvant-Relatsiooniline Hoare Logic. Selle loogika peamine objekt on hinnangud, mis demonstreerivad kahe kvantprogrammi erinevaid seoseid. Nende abil saab otsuseid määratleda võimalike viiside abil: kvantpredikaatide või operaatoritega, eraldatavuse nõudega või ilma selleta. Selle lõputöö uurimisobjektiks on küsimus, kas sellisel kohtuotsusel on võimalik vastata küsimusele, kas see kehtib või mitte. Valitud lähenemisviis on uuritud objektide lineaarse ja kumera koonusstruktuuri kasutamine pooleldi lõpliku ja koonuse programmeerimiseks. See võimaldas rakendada lineaarsete funktsioonide optimeerimisega seotud tulemusi eraldatavate operaatorite komplekti kohal. See pakub mõlema definitsiooni jaoks tõhusat algoritmi ilma eraldatavuse piiranguta. Kahe ülejäänud kohtuotsuse tüübi puhul annab see lähenemisviis probleemi ümbersõnastamise koonuse programmeerimise ja polünoomide mitte-negatiivsuse osas. See võimaldab algoritmiliselt kontrollida seoseid kvantprogrammide vahel ja jätkata uuringuid uue vaatenurgaga lahendite lahendatavuse kohta.

Võtmesõnad:
Kvantkrüptograafia, kvantteave, semifinite programmeerimine, koonuse programmeerimine, kumera optimeerimise suhteline Hoare loogika

CERCS:
P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Contents

1 Introduction

Quantum Realtional Hoare Logic (RHL) is a logic for verification of connections between two quantum programs. Such logics are needed as a method of automated verification of the security proofs of protocols. Handwritten proofs can be very complex and errors may occur. Not only quantum but also post-quantum cryptography uses the concepts of quantum information theory. Therefore, any classical logic is not suitable for the purposes of quantum cryptography. Quantum RHL is a quntum generalization of the probabilistic RHL to the quantum case.

Judgments are the main object of the quantum RHL. This a way to describe various connections between two quantum programs. The question considered in this work is whether it is possible for a fixed judgment to determine whether it holds or not. The chosen approach is to use the conical structure of objects of judgment for the application of semidefinite and conic programming.

We have looked at four different definitions of judgment. First, we simplified the problem by reducing it to a simpler one. In the simplified problem, we wrote down semidefinite and cone programs for each variant of the definition. In the cases where we managed to reduce the problem to a semidefinite program, we showed that this is enough to consider the judgment solvable. The case of conical programs is more complicated. We have applied optimization techniques for an approximate solution and this has led to reformulations of the problem that may be useful in the future.

In the section 2, we introduce all the necessary concepts concerning quantum RHL to define the judgements. We also prove some necessary facts about operators and quantum predicates.

In the section 3, We define semidefinite programming and explain why it can be efficiently solved. We also introduce the concept of convex cones and cone programming and state the strong duality theorem for cone programs.

In the section 4, we state the results about reducing linear optimization over the set of separable mixed states to checking whether a polynomial is a sum of squares. We also show that the latter is a semidefinite feasibility problem.

In the section 5, we show the conic structure of the sets of initial operators and reduce deciding whether a judgement holds to the case of a fixed initial operator. We also write down semidefinite and cone programs for every definition of judgements and show when it helps to decide whether a judgement holds.

2 Quantum Relational Hoare Logic

In this section we explain the concepts of quantum Relational Hoare logic (RHL), We cover the necessary preliminaries and facts based on the paper [1]. In this section we consider the infinite dimensional case for the sake of generality. In the following sections we reduce ourselves to the finite dimensional case.

The main definition related to quantum RHL that we want to give is the definition of judgements of the form $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$, where **c** and **d** are quantum programs and the meaning of A and B can vary. Judgements describe a connection between two quantum programs. The high level idea is that if a pre-condition A is satisfied before the execution of **c** and **d** then a post-condition B is satisfied after the execution of the programs. We consider multiple formal definitions to make sense of this concept.

The first step towards getting an intuition of judgements can be done by looking at the case of the classical deterministic Relational Hoare Logic.

Let $\mathbf{c}, \mathbf{d}$ be deterministic programs. Let A, B be Boolean predicates that contain variables of **c** and **d**. If m_1, m_2 is a pair of variable assignments (equivalently *memories*) for **c** and **d** correspondingly, then we write $[\![A]\!]_{m_1,m_2}$, $[\![B]\!]_{m_1,m_2}$ for evaluations of A and B on these memories and $[\![\mathbf{c}]\!](m_1), [\![\mathbf{d}]\!](m_2)$ for the results of running programs on these memories. The corresponding judgement $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ is defined as follows.

Definition 2.1 (deterministic RHL, informal)**.** $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ holds if and only if for any pair of memories m_1, m_2 such that $[\![A]\!]_{m_1,m_2} = 1$ we have $[\![B]\!]_{m_1',m_2'} = 1$, where $m_1' = [\![\,\mathbf{c}]\!]\,(m_1), m_2' = [\![\,\mathbf{d}]\!]\,(m_2)$.

Example. Let's consider $\{A\} = \{x_1 = x_2\}, \{B\} = \{x_1 < x_2\}$ and $\mathbf{c} = x \leftarrow x - 2$, $\mathbf{d} = x \leftarrow x - 1$. We can see that the judgement

$$\{x_1 = x_2\}x \leftarrow x - 2 \sim x \leftarrow x - 1\{x_1 < x_2\}$$

holds by definition.

2.1 Basic Concepts

To start formalizing the definition of quantum RHL judgement analogous to the classical deterministic example above, we need to step by step define all the necessary concepts.

Definition 2.2. A *program variable* x is defined by a set Type_x and a flag "classical" or "quantum".

The meaning of the set from the above definition is different for classical and quantum variables. If x is a classical variable, then Type_x is a set of all values that x can store. If q is a quantum variable, then q can store superpositions of the elements from Type_q.

Definition 2.3. Let $V = V^{\text{cl}} \cup V^{\text{qu}}$ be a set of variables (classical and quantum). We associate a set $\text{Type}_V^{\text{Set}}$ with V defined as follows.

$$\text{Type}_V^{\text{Set}} = \{f \mid \forall x \in V \quad f(x) \in \text{Type}_x\}$$

$\text{Type}_V^{\text{Set}}$ is the set of all classical memories that can be assigned to the variables of V. Analogously this set can be viewed as

$$\text{Type}_V^{\text{Set}} = \prod_{x \in V} \text{Type}_x.$$

Definition 2.4. Let $V = (x_1, \ldots, x_n)$ be a list of variables (classical and quantum).

$$\text{Type}_V^{\text{List}} = \text{Type}_{x_1} \times \ldots \times \text{Type}_{x_n}$$

Although $\text{Type}_V^{\text{Set}}$ and $\text{Type}_V^{\text{List}}$ are isomorphic as sets for a fixed list V, the difference lies in the fact that the components of the first one are numbered by elements of V and of the second one are numbered by natural numbers.

The next definition describes the probability distributions and clarify the necessary notation for quantum RHL.

Definition 2.5. For a set X define

- $D(X) = \{\mu : X \to \mathbb{R}_+\}$, the set of all *distributions* on X;
- $D^{\leq 1}(X) = \{\mu : X \to \mathbb{R}_+ \mid \sum_{x \in X} \mu(x) \leq 1\}$, the set of all *subprobability distributions* on X;
- A distribution $\mu \in D(X)$ is called *total* if and only if $\sum_{x \in X} \mu(x) = 1$.

For a set of variables V we use the following notations

- $D[V] = D(\text{Type}_V^{\text{Set}})$;
- $D^{\leq 1}[V] = D^{\leq 1}(\text{Type}_V^{\text{Set}})$

Intuitively, $D[V]$ is a set of all probability distributions on the classical values that can be assigned to the elements of V.

Next, we introduce a Hilbert space which should be understood as the set of pure quantum states that we will be dealing with.

Definition 2.6. Let X be a set. Define a Hilbert space

$$\ell^2(X) = \{\psi : X \to \mathbb{C} \mid \|\psi\|^2 = \sum_{x \in X} |\psi(x)|^2 \text{ exists}\}$$

with inner product

$$\langle \psi, \phi \rangle = \sum_{x \in X} \psi(x)^* \phi(x),$$

where $\psi(x)^*$ denotes complex conjugate.

For $x \in X$ consider $|x\rangle : X \to \mathbb{C}$ defined as

$$|x\rangle\,(y) = \begin{cases} 1, & \text{if } y = x \\ 0, & \text{otherwise} \end{cases}$$

The set $\{|x\rangle \mid x \in X\}$ forms computational basis of $\ell^2(X)$. It is straightforward from the definition that these functions indeed form an orthonormal basis with respect to the inner product that is used in the definition of $\ell^2(X)$.

For a set of variables V we use the notation $\ell^2[V] = \ell^2(\text{Type}_V^{\text{Set}})$, i.e. $\ell^2[V]$ is the set of superpositions of the possible assignments of values to the variables from V (equivalently, superpositions of possible memories). Therefore, we also use Dirac's notations for the elements of $\ell^2[V]$.

Let V, W be sets of variables such that $V \cap W = \varnothing$. We define tensor product of the corresponding Hilbert spaces as

$$\ell^2[V] \otimes \ell^2[W] = \ell^2[V \cup W]$$
$$(\psi \otimes \phi)(m_1, m_2) = \psi(m_1)\phi(m_2)$$

Further we use a shorter notation $\ell^2[VW]$ for this tensor product.

Now we can give the necessary notations and the definitions for the operators on a Hilbert space.

Definition 2.7. Let X, Y be sets and $L : \ell^2(X) \to \ell^2(Y)$ be a linear operator. L is called *bounded* if and only if there exists a constatnt $c \geq 0$ such that for any $\psi \in \ell^2(X)$ holds

$$\|L\psi\|_{\ell^2(Y)} \leq c\|\psi\|_{\ell^2(X)}$$

The set of all bounded operators $L : \ell^2(X) \to \ell^2(Y)$ is denoted by $B(X, Y)$. The set of all bounded operators $L : \ell^2(X) \to \ell^2(X)$ is denoted by $B(X, X)$.

Let V, W be two sets of variables. We use the notation $B[V, W]$ for $B(\text{Type}_V^{\text{Set}}, \text{Type}_W^{\text{Set}})$. That is $B[V, W]$ is the set of bounded operators that map pure quantum states $\ell^2[V]$ to pure quantum states $\ell^2[W]$. Let V_1, V_2, W_1, W_2 be sets of variables. We define

$$B[V_1, W_1] \otimes B[V_2, W_2] = B[V_1 V_2, W_1 W_2]$$

(the $\cup$ sign is omitted as above). This definition corresponds to the defined above tensor product because we can rewrite it as follows

$$B[V_1, W_1] \otimes B[V_2, W_2] = \{L : \ell^2[V_1] \otimes \ell^2[V_2] \to \ell^2[W_1] \otimes \ell^2[W_2] \mid L \text{ is bounded}\}$$

Definition 2.8. Let X, Y be sets and $L : \ell^2(X) \to \ell^2(Y)$ be a bounded linear operator. An operator $L^* : \ell^2(Y) \to \ell^2(X)$ is called *adjoint* to L if and only if for any $\psi \in \ell^2(X), \phi \in \ell^2(Y)$ holds

$$\langle L\psi, \phi \rangle_{\ell^2(Y)} = \langle \psi, L^* \phi \rangle_{\ell^2(X)}$$

If $L = L^*$ (in particular $X = Y$) then L is called *self-adjoint* or *Hermitian*.

The set of all Hermitian operators $L : \ell^2(X) \to \ell^2(X)$ is denoted by $\text{Herm}(X) \subset B(X)$.

Remark. We look at the set $\text{Herm}(X)$ as a real Hilbert space of dimension $|X|^2$ (see e.g. [5]) with the inner product

$$\langle L_1, L_2 \rangle = \text{Tr}(L_1 L_2)$$

Lemma 1. *Let X be a set and $L \in$ Herm(X) be a self-adjoint operator, then $\langle L\psi, \psi \rangle \in \mathbb{R}$ for any $\psi \in \ell^2(X)$.*

Proof. From the conjugate symmetry of inner product we can conclude

$$\langle L\psi, \psi \rangle = \langle \psi, L\psi \rangle^*$$

On the other hand, L is self-adjoint and

$$\langle L\psi, \psi \rangle = \langle \psi, L\psi \rangle$$

Therefore,

$$\langle L\psi, \psi \rangle = \langle \psi, L\psi \rangle^* = \langle \psi, L\psi \rangle \in \mathbb{R}$$

□

Remark. In the finite-dimensional case, L^* is just a conjugate transposed matrix which is often denoted by $L^\dagger$. Therefore, the next definitions are very simple in the finite-dimensional case and impose some conditions simply on complex matrices.

Definition 2.9. Let X, Y be sets and $L \in B(X, Y)$ be a bounded linear operator. L is an *isometry* if and only if $L^* L = I_{\ell^2(Y)}$.

The set of all isometries $L : \ell^2(X) \to \ell^2(Y)$ is denoted by $\mathrm{Iso}(X, Y) \subset B(X, Y)$.

Definition 2.10. Let X, Y be sets and $U \in B(X, Y)$ be a bounded linear operator. U is an *unitary* if and only if $U^*U = I_{\ell^2(Y)}$ and $UU^* = I_{\ell^2(X)}$.

The set of all unitaries $U : \ell^2(X) \to \ell^2(Y)$ is denoted by $\mathrm{U}(X, Y) \subset \mathrm{Iso}(X, Y)$.
Next, we give definitions to introduce trace-class operators.

Definition 2.11. Let X be a set and $L \in \mathrm{Herm}(X)$ be a self-adjoint operator. L is *positive* if and only if $\langle\psi| L |\psi\rangle \geq 0$ for every $|\psi\rangle \in \ell^2(X)$.

Definition 2.12. Let X be a set and $L \in B(X, Y)$ be a bounded operator. We define $|L|$ as the unique positive operator such that $|L|^2 = L^*L$.

Definition 2.13. Let X be a set and $L \in B(X)$ be a bounded operator. L is a *trace-class* operator if and only if

$$\sum_{e \in E} \langle |L| e, e \rangle < \infty$$

for an orthonormal basis E of $\ell^2(X)$.

The set of all trace-class operators $L : \ell^2(X) \to \ell^2(X)$ is denoted by $\mathrm{T}(X) \subset B(X)$.

Definition 2.14. Let X be a set and $L \in \mathrm{T}(X)$. We define *trace* of L as

$$\mathrm{Tr}(L) = \sum_{e \in E} \langle Le, e \rangle$$

for an orthonormal basis E of $\ell^2(X)$.

Remark. The sums in the definitions above are independent on the basis, we refer to [2] for the proof. Note that in the finite-dimensional case this corresponds to the usual definition of trace.

The set of all positive Hermitian trace-class operators $L : \ell^2(X) \to \ell^2(X)$ is denoted by $\mathrm{T}^+(X) \subset \mathrm{T}(X)$.

For a set of variables V, we use a notation $\mathrm{T}^+[V] = \mathrm{T}^+(\mathrm{Type}^{\mathrm{Set}}_V)$. This set represents the set of *m*ixed states from $\ell^2[V]$ (mixed states are also called *density operators* and *state mixtures*).

Definition 2.15. Let $V = V^{\mathrm{cl}} \cup V^{\mathrm{qu}}$ be a set of variables (classical and quantum), $\rho \in \mathrm{T}[V]$ is a *cq-operator* if it can be written as

$$\rho = \sum_m \mathrm{proj}(|m\rangle_{V^{\mathrm{cl}}}) \otimes \rho_m$$

where m is taken over $\mathrm{Type}^{\mathrm{Set}}_{V^{\mathrm{cl}}}$, $\mathrm{proj}(|m\rangle_{V^{\mathrm{cl}}})$ denotes the projector onto $\mathrm{Span}(m)$ in $\ell^2[V^{\mathrm{cl}}]$,$\rho_m \in \mathrm{T}[V^{\mathrm{qu}}]$.

This definition means that the classical part is in state m with probability $\mathrm{Tr}(\rho_m)$ and the quantum state is ρ_m up to a normalization.

The set of all cq-operators is denoted by $\mathrm{T}_{cq}[V] \subseteq \mathrm{T}[V]$.

The next definition of a separable operator is crucial in this work. It is a necessary part of the formalization of quantum RHL judgements. Therefore, this concept will constantly appear on the following pages.

Definition 2.16. Let V_1, V_2 be sets of variables, $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *separable* is there exists $\rho_i^1 \in \mathrm{T}^+[V_1]$, $\rho_i^2 \in \mathrm{T}^+[V_2]$ such that

$$\rho = \sum_i \rho_i^1 \otimes \rho_i^2$$

Definition 2.17. Let V, W be sets of variables, $\mathcal{E} : \mathrm{T}[V] \to \mathrm{T}[W]$ is a is a *completely positive* linear map if and only if for any $k \in \mathbb{N}$ the operator

$$\mathbb{I} \otimes \mathcal{E} : \mathbb{C}^{k\times k} \otimes \mathrm{T}[V] \to \mathbb{C}^{k\times k} \otimes \mathrm{T}[W]$$

$$\begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \dots & a_{kk} \end{pmatrix} \otimes \rho \mapsto \begin{pmatrix} \rho(a_{11}) & \dots & \rho(a_{1k}) \\ \vdots & & \vdots \\ \rho(a_{k1}) & \dots & \rho(a_{kk}) \end{pmatrix}$$

maps positive elements to positive elements.

Definition 2.18. Let V, W be sets of variables, $\mathcal{E} : \mathrm{T}[V] \to \mathrm{T}[W]$ is a *superoperator* if the following two conditions hold:

- $\mathcal{E}$ is a completely positive linear map;
- For any $\rho \in \mathrm{T}[V]$ holds $\mathrm{Tr}(\mathcal{E}\rho) \leq \mathrm{Tr}(\rho)$ ($\mathcal{E}$ is *trace decreasing*).

An operator $\mathcal{E} : T_{cq}[V] \to T_{cq}[W]$ satisfying two properties above is called a *cq-superoperator*.

Remark. For a set of variables V, trace can be viewed as a superoperator $\mathrm{Tr} : \mathrm{T}[V] \to \mathbb{C}$. We can think analogously about partial trace.

Definition 2.19. Let V, W be sets of variables, $\sigma \otimes \tau \in \mathrm{T}[VW]$. *Partial trace* is defined as

$$\mathrm{Tr}_{[V]} : \mathrm{T}[VW] \to \mathrm{T}[W]$$
$$\sigma \otimes \tau \mapsto \mathrm{Tr}(\sigma) \cdot \tau$$

Remark. Since $B[VW] = B[V] \otimes B[W]$, it is sufficient to define partial trace only on the operators of the form $\sigma \otimes \tau$ because the rest is uniquely defined by linearity.

This superoperator is needed to define mixed states of parts of the system given a mixed state of the whole system.

One more quantum mechanical concept that we need to formalize is the concept of projective measurements. For a set of variables V we denote the set of all projective measurements on $\ell^2[V]$ with possible outcomes in a set D by $\text{Meas}(D, V)$. In more detail, we have

$$\text{Meas}(D, V) = \{M : D \to B[V] \mid \forall z \in D : M(z) \text{ is a projector}, \sum_z M(z) \leq \mathbb{I}_{\ell^2[V]}\}$$

where $\sum_z M(z) \leq \mathbb{I}_{\ell^2[V]}$ means that $\mathbb{I}_{\ell^2[V]} - \sum_z M(z)$ is self-adjoint and positive. A measurement $M : D \to B[V]$ is called *total* if and only if $\sum_z M(z) = \mathbb{I}_{\ell^2[V]}$.

Finally, the last thing that we need before defining quantum programs is expressions.

Definition 2.20. Let V be a set of variables. An *expression* e is a pair $(\text{fv}(e) \subseteq V^{\text{cl}}, [\![e]\!] : \text{Type}_V^{\text{Set}} \to \text{Type}_e^{\text{exp}})$, where

- $\text{fv}(e)$ is the set of free variables of e
- $[\![e]\!] : \text{Type}_V^{\text{Set}} \to \text{Type}_e^{\text{exp}}, m \mapsto [\![e]\!]_m$ is the evaluation function of e

such that for any $m, m' \in \text{Type}_V^{\text{Set}}$ holds

$$m\big|_{\text{fv}(e)} = m'\big|_{\text{fv}(e)} \implies [\![e]\!]_m = [\![e]\!]_{m'}$$

2.2 Quantum Programs

Quantum programs are constructed according to the following syntax (grammar) [1]. Let $\mathbf{c}, \mathbf{d}$ be programs, x be a classical variable, $q_1 \dots q_n$ be quantum variables, e be an expression.

$\mathbf{c}, \mathbf{d} :=$ skip	(no operation)
$x \leftarrow e$	(classical assignment)
$x \overset{\$}{\leftarrow} e$	(classical sampling)
if e then $\mathbf{c}$ else $\mathbf{d}$	(conditional)

while e do $\mathbf{c}$	(loop)
$\mathbf{c}; \mathbf{d}$	(sequential composition)
$q_1 \dots q_n \overset{\text{q}}{\leftarrow} e$	(initialization of quantum registers)
apply e to $q_1 \dots q_n$	(quantum application)
$x \leftarrow$ measure $q_1 \dots q_n$ with e	(measurement)

The set of free variables of a program $\mathbf{c}$ is then

$$\text{fv}(\mathbf{c}) = \cup_{e \in \mathbf{c}} \text{fv}(e) \cup \{x \mid x \leftarrow e, x \overset{\$}{\leftarrow} e, x \leftarrow \text{ measure } q_1 \dots q_n \in \mathbf{c}\} \cup$$

$$\{q_1 \dots q_n \mid q_1 \dots q_n \overset{\text{q}}{\leftarrow} e, \text{apply } e \text{ to } q_1 \dots q_n, x \leftarrow \text{ measure } q_1 \dots q_n \in \mathbf{c}\}$$

Let $\mathbb{B} = \{\text{True}, \text{False}\}$ denote Boolean. We assume that the following properties are satisfied.

$x \leftarrow e$	$\text{Type}_e^{\text{exp}} \subseteq \text{Type}_x$
$x \overset{\$}{\leftarrow} e$	$\text{Type}_e^{\text{exp}} \subseteq D^{\leq 1}(\text{Type}_x)$
if e then $\mathbf{c}$ else $\mathbf{d}$	$\text{Type}_e^{\text{exp}} \subseteq \mathbb{B}$
while e do $\mathbf{c}$	$\text{Type}_e^{\text{exp}} \subseteq \mathbb{B}$
$q_1 \dots q_n \overset{\text{q}}{\leftarrow} e$	$\text{Type}_e^{\text{exp}} \subseteq \ell^2(\text{Type}_{q_1 \dots q_n}^{\text{list}}), \forall \psi \in \text{Type}_e^{\text{exp}} : \|\psi\| = 1$
apply e to $q_1 \dots q_n$	$\text{Type}_e^{\text{exp}} \subseteq \text{Iso}(\text{Type}_{q_1 \dots q_n}^{\text{list}})$
$x \leftarrow$ measure $q_1 \dots q_n$ with e	$\text{Type}_e^{\text{exp}} \subseteq \text{Meas}(\text{Type}_x, \ell^2(\text{Type}_{q_1 \dots q_n}^{\text{list}}))$

These rules are necessary for a program to be meaningful. In classical assignment, expression e evaluates to a value that can be taken by variable x, in classical sampling to a distribution, etc.

If $\mathbf{c}$ is a quantum program then its *semantics* is a cq-superoperator $[\![\mathbf{c}]\!] : T_{cq}[V] \to T_{cq}[V]$ that satisfies specific rules. We do not list the rules here because we will not refer to it in the subject of this work. See [1].

2.3 Quantum Predicates

Quantum predicates are a part of one of the ways to give meaning to A and B in the notion of quantum RHL judgement $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$. For a set of variables V, linear subspaces of $\ell^2[V]$ are used to define quantum predicates on the variables of V.

Definition 2.21. Let V be a set of variables, $\rho \in \mathrm{T}^+[V]$ be a density operator. Let P be a projector with the smallest image such that $P\rho P = \rho$. We define support of ρ as $\mathrm{supp}\rho = \mathrm{Im}(P)$.

Definition 2.22. Let V be a set of variables, A be a linear subspace of $\ell^2[V]$, $\rho \in \mathrm{T}^+[V]$ be a density operator. We say that ρ *satisfies* A if and only if $\mathrm{supp}\rho \subseteq A$.

In the next lemma we give several useful equivalent definitions for the satisfiability of quantum predicates.

Lemma 2. *Let V be a set of variables, A be a quantum predicate, $P_A \in \boldsymbol{T}^+[V]$ be the orthogonal projector onto A, $\rho \in \boldsymbol{T}^+[V]$ be a density operator. The following conditions are equivalent.*

1. *ρ satisfies A*
2. $P_A \rho P_A = \rho$
3. $\mathrm{Tr}(P_A\rho) = \mathrm{Tr}(\rho)$
4. $\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho\big) = 0$
5. *ρ is a mixture of states in A, i.e. $\rho = \sum_i \boldsymbol{proj}(\psi_i) = \sum_i |\psi_i\rangle\langle\psi_i|$ for some $\psi_i \in A$*

Proof. $\mathbf{1}. \implies \mathbf{2}.$ By definition, ρ satisfies A implies that $\mathrm{supp}\rho \subseteq A$, i.e. for the projector P with the smallest image such that $P\rho P = \rho$ holds

$$\mathrm{Im}P \subseteq A$$

This implies

$$PP_A = P_A P = P$$

Therefore,

$$P_A\rho P_A = P_A P\rho P P_A = P\rho P = \rho$$

$\mathbf{2}. \implies \mathbf{3}.$ Using the properties of trace and projectors we can write the following chain of equalities.

$$\mathrm{Tr}(P_A\rho) = \mathrm{Tr}\big(P_A^2\rho\big) = \mathrm{Tr}(P_A\rho P_A) = \mathrm{Tr}(\rho)$$

$\mathbf{3}. \implies \mathbf{4}.$

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(P_A\rho) + \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho\big) = \mathrm{Tr}(\rho) + \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho\big)$$

Hence,

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho\big) = 0$$

$\mathbf{4.} \implies \mathbf{5}$. Since ρ is a density operator, it can be written as a mixture of orthogonal states from $\ell^2[V]$.

$$\rho = \sum_i |\psi_i\rangle \langle\psi_i|$$

Since

$$0 = \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho\big) = \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho(\mathbb{I}_{\ell^2[V]} - P_A)\big)$$

and $(\mathbb{I}_{\ell^2[V]} - P_A)\rho(\mathbb{I}_{\ell^2[V]} - P_A)$ is a positive operator, we can conclude that $(\mathbb{I}_{\ell^2[V]} - P_A)\rho(\mathbb{I}_{\ell^2[V]} - P_A) = 0$. Therefore,

$$0 = \sum_i (\mathbb{I}_{\ell^2[V]} - P_A) |\psi_i\rangle \langle\psi_i| (\mathbb{I}_{\ell^2[V]} - P_A)$$

States $|\psi_i\rangle$ are linearly independent, which allows us to get rid of the sum.

$$0 = (\mathbb{I}_{\ell^2[V]} - P_A) |\psi_i\rangle \langle\psi_i| (\mathbb{I}_{\ell^2[V]} - P_A) = (|\psi_i\rangle - P_A |\psi_i\rangle)(|\psi_i\rangle - P_A |\psi_i\rangle)^*$$

Finally, we get

$$P_A |\psi_i\rangle = |\psi_i\rangle$$

i.e. $\psi_i \in A$.

$\mathbf{5.} \implies \mathbf{1}$. Assume that $\rho = \sum_i |\psi_i\rangle \langle\psi_i|$, where $|\psi_i\rangle \in A$. Let P' be a projector onto $\mathrm{Span}(\{|\psi_i\rangle\}_i)$. Clearly, $P'\rho P' = \rho$ and $\mathrm{Im}(P') \subseteq A$. Therefore, for the projector P with the smallest image such that $P\rho P = \rho$ also holds $\mathrm{Im}P \subseteq A$. □

Quantum predicates defined this way satisfy the linearity properties, which easily follow from the equivalent reformulations from the lemma above.

Lemma 3. *Let $\rho_1, \rho_2 \in T^+[V]$ be density operators, $p_1, p_2 > 0$, A be a quantum predicate.*

1. *ρ_1, ρ_2 satisfy A $\implies$ $p_1\rho_1 + p_2\rho_2$ satisfies A*
2. *$p_1\rho_1 + p_2\rho_2$ satisfies A $\implies$ ρ_1, ρ_2 satisfy A*

Proof. $\mathbf{1}$. By lemma 2, ρ_1, ρ_2 satisfy A is equivalent to

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_1\big) = \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_2\big) = 0$$

Using the linearity of trace, we obtain

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)(p_1\rho_1 + p_2\rho_2)\big) = p_1 \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_1\big) + p_2 \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_2\big) = 0$$

2. Analogously,

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)(p_1\rho_1 + p_2\rho_2)\big) = 0$$

and

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)(p_1\rho_1 + p_2\rho_2)\big) = p_1\,\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_1\big) + p_2\,\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_2\big) = 0$$

Note that the traces are non-negative

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_i\big) = \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_i(\mathbb{I}_{\ell^2[V]} - P_A)\big) > 0$$

since $(\mathbb{I}_{\ell^2[V]} - P_A)\rho_i(\mathbb{I}_{\ell^2[V]} - P_A)$ are positive operators.

Taking into account $p_1, p_2 > 0$, we conclude that

$$\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_1\big) = \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V]} - P_A)\rho_2\big) = 0$$

□

2.3.1 quantum RHL judgements

In this subsection we give three different definitions of judgements. Namely, we list several ways to formalize the intuition "if a state satisfies a pre-condition on the variables of two programs then the state after execution of these two programs satisfies a post-condition". For us, each variant of the definition of judgements is of interest, since they are the subject of study in this work, regardless of the context of the logic itself and the frame rules.

In the following definitions, let $\mathbf{c}, \mathbf{d}$ be quantum programs with $\mathrm{fv}(\mathbf{c}) = \mathrm{fv}(\mathbf{d}) = V$. Let V_1, V_2 be two copies of V. We will say that V_1 is the set of free variables of $\mathbf{c}$ and V_2 is the set of free variables of $\mathbf{d}$. We also use the notation Tr_i for the partil trace operators Tr_{V_i}.

We start with so-called non-separable judgements where we do not require separability in the initial and final mixed states.

Definition 2.23. Let A, B be quantum predicates of $\ell^2[V_1V_2]$. $\{A\}\mathbf{c} \sim_{\text{nonsep}} \mathbf{d}\{B\}$ holds if and only if for any $\rho \in \mathrm{T}^+[V_1V_2]$ that satisfies A there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ that satisfies B such that

- $\mathrm{Tr}_2(\rho') = [\![\,\mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\,\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$

However, the main definition is the following one. It differs from the one above in only one place: separability is required for both initial and final states. This definition turned out to be the correct definition for the quantum RHL in terms of proving frame rules.

Definition 2.24. Let A, B be quantum predicates of $\ell^2[V_1V_2]$. $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ holds if and only if for any $\rho \in \mathrm{Sep}[V_1V_2]$ that satisfies A there exists $\rho' \in \mathrm{Sep}[V_1V_2]$ that satisfies B such that

- $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

The next lemma holds for both separable and non-separable cases.

Lemma 4. *$\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ holds if and only if for any $|\psi\rangle \in A$ holds $\{Span(|\psi\rangle)\}\mathbf{c} \sim \mathbf{d}\{B\}$.*

Proof. See [1]. □

The next definition is different from the other ones because it has operators instead of quantum predicates. The idea of using operators lies in the fact that "predicates" are not Boolean anymore but are satisfied to some amount that is represented by trace. The intuition is that the final state satisfies the post-condition at least as much as the initial state satisfies the pre-condition.

Definition 2.25. Let $\mathcal{A}, \mathcal{B} \in \mathrm{T}^+[V_1V_2]$ be operators. $\{\mathcal{A}\}\mathbf{c} \sim^{\mathrm{op}}_{\mathrm{nonsep}} \mathbf{d}\{\mathcal{B}\}$ holds if and only if for any $\rho \in \mathrm{T}^+[V_1V_2]$ there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

- $\mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$
- $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

And, analogously, a separable version.

Definition 2.26. Let $\mathcal{A}, \mathcal{B} \in \mathrm{T}^+[V_1V_2]$ be operators. $\{\mathcal{A}\}\mathbf{c} \sim^{\mathrm{op}} \mathbf{d}\{\mathcal{B}\}$ holds if and only if for any $\rho \in \mathrm{Sep}[V_1V_2]$ there exists $\rho' \in \mathrm{Sep}[V_1V_2]$ such that

- $\mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$
- $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

The question of this work is whether any of these judgements is decidable. The approach chosen to answer this question is to use the linearity in the definitions and the cone structure of the set $\mathrm{Sep}[V_1V_2]$ to apply semidefinite programming and cone programming. The basics are described in the sections below.

3 Semidefinite Programming, Cones and Cone Programming

In this section we introduce the necessary concepts and facts about semidefinite programming, cones and cone Programming based on the book [3]. All the concepts are defined for a finite dimensional real vector space. We consider the space Herm$[V_1V_2]$, where V_1, V_2 are two copies of a finite set of variables. We use the notations that were introduced above for this particular case.

3.1 Semidefinite Programming

We start with semidefinite programming. This is a concept that naturally arises in quantum information theory, since its main objects are positive operators.

Definition 3.1. Let $c, a_i \in \text{Herm}[V_1V_2]$, $b_i \in \mathbb{R}$, $i = 1, \ldots, m$. These parameters define a *semidefinite program in standard form*.

$$\begin{aligned} \text{minimize} \quad & \text{Tr}(cx) \\ \text{subject to} \quad & \text{Tr}(a_i x) = b, \\ & x \in \mathbf{T}^+[V_1V_2] \end{aligned}$$

Remark. We can switch minimization to maximization by taking $-c$.

A semidefinite program in standard form is also called *primal*. Next, we define the *dual* program.

Definition 3.2. Let $c, A_i \in \text{Herm}[V_1V_2]$, $b_i \in \mathbb{R}$, $i = 1, \ldots, m$. A *dual* semidefinite program with this parameters is defined as follows.

$$\begin{aligned} \text{maximize} \quad & \text{Tr}(by) \\ \text{subject to} \quad & c - \sum_{i=1}^{m} y_i a_i \in \mathbf{T}^+[V_1V_2] \end{aligned}$$

where $b = (b_1, \ldots, b_m) \in \mathbb{R}^m$

Next, we introduce the weak duality of semidefinite programming, which is very easy to prove.

Lemma 5. *Let $c, A_i \in$ Herm$[V_1V_2]$, $b_i \in \mathbb{R}$, $i = 1, \ldots, m$. Let p, d be optimal values of the primal and dual problems defined by these parameters correspondingly. Then $p \geq d$.*

Proof. Denote $a(x) = (\mathrm{Tr}(a_1 x), \ldots, \mathrm{Tr}(a_m x))$. Then $a^*(y) = \sum_{i=1}^m y_i a_i$.

The following calculation shows that the difference of the objective functions $\mathrm{Tr}(cx) - \mathrm{Tr}(by)$ is non-negative.

$$\mathrm{Tr}(cx) - \mathrm{Tr}(by) = \mathrm{Tr}(cx) - \mathrm{Tr}(a(x)y) = \mathrm{Tr}(cx) - \mathrm{Tr}(xa^*(y)) = \mathrm{Tr}((c - a^*(y))x) \geq 0$$

The final inequality holds since $(c - a^*(y))$ and x are positive operators.

□

Using the weak duality we can write a system of linear equations on the optimal points. To solve a system of linear equations, we can use, for example, Newton's method (see e.g. [4]). Therefore, the plan we followed for solving the problems in this work is to reduce these problems to semidefinite programs.

3.2 Cones and Cone Programming

In this subsection we first define convex cones and dual cones and show the necessary properties. Then we introduce cone programming and its duality.

Definition 3.3. Let $K \subseteq \mathrm{Herm}[V_1 V_2]$. The set K is a *convex cone* if it satisfies the following two properties.

1. For any $x \in K$, $\lambda \geq 0$ holds $\lambda x \in K$
2. For any $x_1, x_2 \in K$ holds $x_1 + x_2 \in K$

Remark. Since in this work there are no cones other than convex ones, we identify the concepts of a cone and a convex cone.

As examples of convex cones we consider $\mathrm{T}^+[V_1 V_2]$ and $\mathrm{Sep}[V_1 V_2]$ because we use it strongly in the following sections.

Lemma 6. *$T^+[V_1 V_2]$ is a convex cone.*

Proof. Let $\rho, \rho_1, \rho_2 \in \mathrm{T}^+[V_1 V_2], \lambda \geq 0$. We check the two cone properties for these points.

1. $\rho \in \mathrm{T}^+[V_1 V_2]$ is equivalent to $\langle\psi| \rho |\psi\rangle \geq 0$ for any $|\psi\rangle \in \ell^2[V_1 V_2]$. Then

$$\langle\psi| \lambda\rho |\psi\rangle = \lambda \langle\psi| \rho |\psi\rangle \geq 0$$

2. $\rho_1, \rho_2 \in \mathrm{T}^+[V_1 V_2]$ is equivalent to $\langle\psi| \rho_1 |\psi\rangle, \langle\psi| \rho_2 |\psi\rangle \geq 0$ for any $|\psi\rangle \in \ell^2[V_1 V_2]$. Then

$$\langle\psi| (\rho_1 + \rho_2) |\psi\rangle = \langle\psi| \rho_1 |\psi\rangle + \langle\psi| \rho_2 |\psi\rangle \geq 0$$

□

Lemma 7. *Sep$[V_1V_2]$ is a convex cone.*

Proof. Let $\rho, \sigma, \tau \in \text{Sep}[V_1V_2], \lambda \geq 0$.

1. $\rho \in \text{Sep}[V_1V_2]$ implies that $\rho = \sum_i \rho_i^1 \otimes \rho_i^2$ for some $\rho_i^1 \in \text{T}^+[V_1], \rho_i^2 \in \text{T}^+[V_2]$. Then

$$\lambda\rho = \lambda \sum_i \rho_i^1 \otimes \rho_i^2 = \sum_i \lambda\rho_i^1 \otimes \rho_i^2$$

As we have checked in lemma 6, $\lambda\rho_i^1 \in \text{T}^+[V_1]$.

2. Analogously, $\sigma = \sum_i \sigma_i^1 \otimes \sigma_i^2, \tau = \sum_i \tau_i^1 \otimes \tau_i^2$ for some $\sigma_i^1, \tau_i^1 \in \text{T}^+[V_1], \sigma_i^2, \tau_i^2 \in \text{T}^+[V_2]$. If we consider $\sigma + \tau$ we get a sum of the same form again.

□

Remark. $\text{T}^+[V_1V_2]$ and $\text{Sep}[V_1V_2]$ are also closed as sets, see e.g. [5].

Next we introduce the concept of a dual cone and show some of its properties.

Definition 3.4. Let $K \subseteq \text{Herm}[V_1V_2]$ be a convex cone. Then its *dual* K^* is defined as follows.

$$K^* = \{y \in \text{Herm}[V_1V_2] \mid \text{Tr}(yx) \geq 0 \quad \forall x \in K\}$$

Claim 1. *K^* defined above is a convex cone.*

Proof. We check the two properties of a convex cone.

1. Let $y \in K^*$, $\lambda \geq 0$. Then $\text{Tr}(yx) \geq 0$ for every $x \in K$. Then

$$\text{Tr}((\lambda y)x) = \lambda \,\text{Tr}(yx) \geq 0$$

2. Let $y_1, y_2 \in K^*$. Then $\text{Tr}(y_1x), \text{Tr}(y_2x) \geq 0$ for every $x \in K$. Then

$$\text{Tr}((y_1 + y_2)x) = \text{Tr}(y_1x) + \text{Tr}(y_2x) \geq 0$$

□

Lemma 8. *Let K_1, K_2 be two convex cones. Then $(K_1 \cap K_2)^* = \{y_1 + y_2 \mid y_1 \in K_1^*, y_2 \in K_2^*\}$.*

Proof. See, e.g. [6]. □

Finally, we introduce cone programs and its strong duality theorem.

Definition 3.5. Let V, W be finite dimensional real vector spaces. Let $K \subseteq V, K \subseteq W$ be closed convex cones, $\mathcal{L} : V \to W$ be a linear operator, $b \in W, c \in V$. A *cone program* defined by these parameters is

$$\begin{aligned} &\text{maximize} && \langle c, x \rangle \\ &\text{subject to} && b - \mathcal{L}(x) \in L, \\ & && x \in K \end{aligned}$$

Remark. A cone program in the form defined above is also called *primal*.

Definition 3.6. Let V, W be finite dimensional real Hilbert spaces. Let $K \subseteq V, K \subseteq W$ be closed convex cones, $\mathcal{L} : V \to W$ be a linear operator, $b \in W, c \in V$. A *dual cone program* defined by these parameters is

$$\begin{aligned} &\text{minimize} && \langle b, y \rangle \\ &\text{subject to} && \mathcal{L}^*(x) - c \in K^*, \\ & && y \in L^* \end{aligned}$$

Definition 3.7. Let V, W be finite dimensional real Hilbert spaces. Let $K \subseteq V, K \subseteq W$ be closed convex cones, $\mathcal{L} : V \to W$ be a linear operator, $b \in W, c \in V$. A point $x \in V$ is called an *interior point* of a cone program defined by these parameters if and only if $x \in K$, $b - \mathcal{L}(x) \in L$ and the following holds.

- If $L = \{0\}$ then $x \in \text{Int}(K)$
- If $L \neq \{0\}$ then $b - \mathcal{L}(x) \in \text{Int}(L)$

Theorem 1. *Let $\mathfrak{P}, \mathfrak{D}$ be a primal cone program and its dual. If $\mathfrak{P}$ is such that*

1. *$\mathfrak{P}$ is feasible*
2. *the value of $\mathfrak{P}$ is finite*
3. *$\mathfrak{P}$ has an interior point*

then $\mathfrak{D}$ is also feasible and has the same value.

Proof. See [3].

□

4 Linear Optimization over the Set of Separable States

In this section we introduce some of the results from the paper [7] that are used in the following sections. We use the notations that are defined in the sections above.

Let $|\psi\rangle \in \ell^2[V_1], |\phi\rangle \in \ell^2[V_2], |V_1 \models |V_2 \models n$. Then $|\psi\rangle, |\phi\rangle$ can be viewed as complex vectors (e.g. in the computational basis). Consider $|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|, \sigma \in \text{Herm}[V_1V_2]$. We can explicitly write down the inner product of this two operators.

$$\text{Tr}(\sigma(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|)) = \sum_{ijkl} \sigma_{ijkl}\psi_i\psi_k^*\phi_j\phi_l^*$$

where $*$ denotes complex conjugate. What we obtain is a polynomial of degree 4 of entries of ψ and ϕ and their complex conjugates. We use the following notation.

$$\mathcal{P}_\sigma(|\psi\rangle, |\phi\rangle) = \sum_{ijkl} \sigma_{ijkl}\psi_i\psi_k^*\phi_j\phi_l^*$$

The set of separable operators can be represented as follows.

$$\text{Sep}[V_1V_2] = \text{Conv}(\{|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| \mid |\psi\rangle \in \ell^2[V_1], |\phi\rangle \in \ell^2[V_2]\})$$

where Conv denotes convex hull. Consider the dual cone of $\text{Sep}[V_1V_2]$. By definition it is

$$\text{Sep}[V_1V_2]^* = \{\sigma \in \text{Herm}[V_1V_2] \mid \text{Tr}(\sigma x) \geq 0 \quad \forall x \in \text{Sep}[V_1V_2]\}$$

The condition $\text{Tr}(\sigma x) \geq 0$ is then a non-negativity condition for the polynomial $\mathcal{P}_\sigma$. This leads us to a characterization of the $\text{Sep}[V_1V_2]^*$.

Theorem 2. *$\text{Sep}[V_1V_2]^* = \{\sigma \in \text{Herm}[V_1V_2] \mid \mathcal{P}_\sigma$ is non-negative$\}$*

Proof. Above. □

Next, we introduce the DPS (Doherty-Parrilo-Spedalier) hierarchy. We do it by defining the duals.

$$\text{DPS}_l^* = \{\sigma \in \text{Herm}[V_1V_2] \mid |y|^{2(l-1)}\mathcal{P}_\sigma \text{ is a sum of squares of polynomials}\}$$

Remark. Further we write sum of squares instead of sum of squares of polynomials.

Lemma 9. *The following chain of inclusions holds.*

$$\text{Sep}[V_1V_2] \subseteq \ldots \subseteq \text{DPS}_l \subseteq \ldots \subseteq \text{DPS}_1$$

Proof. See [7]. □

Denote by $h_{Sep}(\sigma)$ the optimal value of the following optimization problem.

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}(\sigma x) \\ \text{subject to} \quad & 1 - \mathrm{Tr}(x) \in \{0\}, \\ & x \in \mathrm{Sep}[V_1 V_2] \end{aligned}$$

Analogously define $h_{\mathrm{DPS}_l}(\sigma)$.

Theorem 3. *Let $\sigma \in Herm[V_1 V_2]$ be a positive operator. Then*

$$h_{Sep}(\sigma) \leq h_{DPS_l}(\sigma) \leq (1 + c\frac{n^2}{l^2}) h_{Sep}(\sigma)$$

for any $l > c'n$, where $c, c' > 0$ are constants.

Proof. See [7]. □

Remark. In our case the trace condition is not important, since we can always rescale the trace.

Theorems 2 and 3 imply that instead of deciding the membership problem for $\mathrm{Sep}[V_1 V_2]^*$, it is possible to decide whether a polynomial is a sum of squares. Finally, we introduce the proof that deciding whether a polynomial is a sum of squares is a semidefinite feasibility problem [8].

Lemma 10. *Let $p(x)$ be a polynomial. Then deciding whether $p(x)$ is a sum of squares is a semidefinite feasibility problem.*

Proof. Assume that $p(x) = \sum_i q(x)^2$ for some polynomials $q_i(x)$ such that $\deg(q_1) \leq d$ for some d. Then

$$q_i(x) = c_i^{\mathsf{T}} [x]_d$$

where c_i is a vector of coefficients of q_i, $[x]_d$ is a vector of all monomials of degree not greater than d. Then $p(x)$ can be rewritten as follows.

$$p(x) = \sum_i q(x)^2 = \sum_i (c_i^{\mathsf{T}} [x]_d)^2 = \sum_i [x]_d^{\mathsf{T}} c_i c_i^{\mathsf{T}} [x]_d$$

Denote by $Q = \sum_i c_i c_i^{\mathsf{T}}$. This is a positive operator. Then the equality

$$p(x) = \sum_i [x]_d^{\mathsf{T}} Q [x]_d$$

is a linear condition on the entries of Q. □

5 Analysis of Quantum RHL Judgements

In this section we analyze quantum RHL judgements. First, we reduce the satisfiability problem to the case of a fixed initial operator. Then we reformulate the satisfiability of different types of judgements in terms of semidefinite and cone programs and argue about its solvability.

We fix quantum programs$[\![\mathbf{c}]\!], [\![\mathbf{d}]\!]$ and their sets of free variables V_1, V_2 that are two copies of the same set, quantum predicates A, B, operators$\mathcal{A}, \mathcal{B} \in \mathrm{T}^+[V_1V_2]$. We assume that $|V_1| = |V_2| = n$, that is, we consider finite dimensional spaces.

5.1 Conic structure of initial states sets

In this section we define several types of sets of initial states and show that all of them have conic structure. We will give the definitions corresponding to the judgements $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ and $\{\mathcal{A}\}\mathbf{c} \sim^{\mathrm{op}} \mathbf{d}\{\mathcal{B}\}$. The definitions for non-separable cases are the same, just without the separability conditions.

Definition 5.1. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *relevant* if and only if there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

1. ρ' satisfies B
2. $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!](\mathrm{Tr}_2(\rho))$
3. $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!](\mathrm{Tr}_1(\rho))$
4. $\rho' \in \mathrm{Sep}[V_1V_2]$

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by $\mathcal{R}$.

Definition 5.2. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *A-relevant* if and only if is relevant and ρ satisfies A.

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by A-$\mathcal{R}$.

Definition 5.3. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *Sep-relevant* if and only if is relevant and $\rho \in \mathrm{Sep}[V_1V_2]$.

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by Sep-$\mathcal{R}$.

Definition 5.4. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *A, Sep-relevant* if and only if is *A-relevant* and *Sep-relevant*.

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by A, Sep-$\mathcal{R}$.

Definition 5.5. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *relevant*^{op} if and only if there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

1. $\mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$
2. $\mathrm{Tr}_2(\rho') = [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))$
3. $\mathrm{Tr}_1(\rho') = [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$
4. $\rho' \in \mathrm{Sep}[V_1V_2]$

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by $\mathcal{R}^{\mathrm{op}}$.

Definition 5.6. Let $\rho \in \mathrm{T}^+[V_1V_2]$. We say that ρ is *Sep-relevant*^{op} if and only if is relevant and $\rho \in \mathrm{Sep}[V_1V_2]$.

The set of all relevant operators in $\mathrm{T}^+[V_1V_2]$ is denoted by Sep-$\mathcal{R}^{\mathrm{op}}$.

Lemma 11. *Let $\rho_1, \rho_2 \in T^+[V_1V_2]$ be relevant. Then $\rho = \rho_1 + \rho_2$ is relevant.*

Proof. Let $\rho_1', \rho_2' \in \mathrm{T}^+[V_1V_2]$ be the corresponding operators from the definition of a relevant operator.
Let $\rho' = \rho_1' + \rho_2'$. Next, we show that ρ' is the necessary operator for the desired properties to hold.

1. By lemma 3, if ρ_1' and ρ_2' satisfy B then so does $\rho_1' + \rho_2'$.

2. By the linearity of the partial trace and quantum programs,

$$\mathrm{Tr}_2(\rho_1' + \rho_2') = \mathrm{Tr}_2(\rho_1') + \mathrm{Tr}_2(\rho_2') =$$

$$[\![\mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho_1)) + [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho_2)) = [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho_1 + \rho_2))$$

3. Analogously to **2**.

$$\mathrm{Tr}_1(\rho_1' + \rho_2') = \mathrm{Tr}_1(\rho_1') + \mathrm{Tr}_2(\rho_2') =$$
$$[\![\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho_1)) + [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho_2)) = [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho_1 + \rho_2))$$

4. Follows from the conic structure of the set $\mathrm{Sep}[V_1V_2]$ (lemma 7). □

Lemma 12. *Let $\rho \in T^+[V_1V_1]$ be relevant, $\lambda > 0$. Then $\lambda\rho$ is relevant.*

Proof. Let $\rho' \in \mathrm{T}^+[V_1V_1]$ be the corresponding operator from the definition of a relevant operator. Next, we show that $\lambda\rho'$ is the necessary operator for the desired properties to hold.

$\mathbf{1}$. By lemma 3, if ρ' satisfies B then so does $\lambda\rho'$.

$\mathbf{2}. - \mathbf{3}$. By the linearity of the partial trace and quantum programs,

$$\mathrm{Tr}_2(\lambda\rho') = \lambda\,\mathrm{Tr}_2(\rho') = \lambda\,[\![\,\mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho)) = [\![\,\mathbf{c}]\!]\,(\mathrm{Tr}_2(\lambda\rho))$$

$$\mathrm{Tr}_1(\lambda\rho') = \lambda\,\mathrm{Tr}_1(\rho') = \lambda\,[\![\,\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho)) = [\![\,\mathbf{d}]\!]\,(\mathrm{Tr}_1(\lambda\rho))$$

$\mathbf{4}$. Follows from the conic structure of the set $\mathrm{Sep}[V_1V_2]$ (lemma 7). □

Corollary 1. *The set $\mathcal{R}$ is a convex cone.*

Corollary 2. *The set A-$\mathcal{R}$ is a convex cone.*

Proof. Let $\rho, \rho_1, \rho_2 \in \mathrm{T}^+[V_1V_2]$ be A-relevant, $\lambda > 0$. The only thing that we need to show is that $\lambda\rho, \rho_1 + \rho_2$ satisfy A, which follows from lemma 3. The rest was shown in the proofs of the lemmas 11 and 12. □

Corollary 3. *The set Sep-$\mathcal{R}$ is a convex cone.*

Proof. The separability condition is closed under convex combinations and the rest was shown in the proofs of the lemmas 11 and 12. □

Corollary 4. *The set A, Sep-$\mathcal{R}$ is a convex cone.*

Lemma 13. *The set $\mathcal{R}^{op}$ is a convex cone.*

Proof. Let $\rho, \rho_1, \rho_2 \in \mathrm{T}^+[V_1V_2]$ be relevant$^{\mathrm{op}}$, $\lambda > 0$. Let $\rho', \rho_1', \rho_2' \in \mathrm{T}^+[V_1V_2]$ be the corresponding operators from the definition. Using the linearity of trace and operators, we write the following.

$$\mathrm{Tr}(\mathcal{B}(\rho_1' + \rho_2')) = \mathrm{Tr}(\mathcal{B}\rho_1' + \mathcal{B}\rho_2') = \mathrm{Tr}(\mathcal{B}\rho_1') + \mathrm{Tr}(\mathcal{B}\rho_2') \geq$$

$$\mathrm{Tr}(\mathcal{A}\rho_1) + \mathrm{Tr}(\mathcal{A}\rho_2) = \mathrm{Tr}(\mathcal{A}\rho_1 + \mathcal{A}\rho_2) = \mathrm{Tr}(\mathcal{A}(\rho_1 + \rho_2))$$

$$\mathrm{Tr}(\mathcal{B}\lambda\rho') = \lambda\,\mathrm{Tr}(\mathcal{B}\rho') \geq \lambda\,\mathrm{Tr}(\mathcal{A}\rho) = \mathrm{Tr}(\mathcal{A}\lambda\rho)$$

The rest of the conditions was checked in the proofs of the lemmas 11 and 12. □

Corollary 5. *The set Sep-$\mathcal{R}^{op}$ is a convex cone.*

We have shown that all of the defined initial states sets have the structure of convex cones. This could lead to the assumption that we can choose a finite system of generators and reduce the verification of a judgement to a finite number of checks whether it holds with fixed initial states. However, this is not the case since both cones $\mathrm{T}^+[V_1V_2]$ and $\mathrm{Sep}[V_1V_2]$ are infinitely generated. Even though we do not have this straightforward simplification, conic structure allows us to look from the geometrical point of view.

We look at one more set

$$\mathrm{supp}_A = \{\rho \in \mathrm{T}^+[V_1V_2] \mid \rho \text{ satisfies } A\}$$

It can be rewritten as

$$\mathrm{supp}_A = \{\rho \in \mathrm{T}^+[V_1V_2] \mid \mathrm{Tr}\big((\mathbb{I}_{\ell^2[V_1V_2]} - P_A)\rho\big) = 0\}$$

Therefore, this set is an intersection of a linear subspace and $\mathrm{T}^+[V_1V_1]$. Now we can state the following lemma that is an alternative geometric formulation of judgements satisfiability.

Lemma 14. *The definitions of quantum RHL judgements can be restated as follows.*

1. $\{A\}\mathbf{c} \sim_{nonsep} \mathbf{d}\{B\}$ *holds if and only if* $\mathit{supp}_A \subseteq \mathcal{R}$
2. $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ *holds if and only if* $\mathit{supp}_A \cap \mathit{Sep}[V_1V_2] \subseteq \mathit{Sep}\text{-}\mathcal{R}$
3. $\{\mathcal{A}\}\mathbf{c} \sim^{op}_{nonsep} \mathbf{d}\{\mathcal{B}\}$ *holds if and only if* $\mathcal{R}^{op} = \mathit{T}^+[V_1V_2]$
4. $\{\mathcal{A}\}\mathbf{c} \sim^{op} \mathbf{d}\{\mathcal{B}\}$ *holds if and only if* $\mathit{Sep}\text{-}\mathcal{R}^{op} = \mathit{Sep}$

Proof. A judgement $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ holds if and only if every $\rho \in \mathrm{Sep}[V_1V_1]$ that satisfies A is relevant, that is, $\mathrm{supp}_A \cap \mathrm{Sep}[V_1V_2] \subseteq \mathrm{Sep}\text{-}\mathcal{R}$. The rest of the claims is analogous and also straightforward. □

One possible approach the reduce the problem to checking whether a judgement holds on a fixed initial operator is pick this operator randomly. We show this on the separable case defined with predicates.

Lemma 15. *Assume that we sample a uniformly random operator from* $\mathit{supp}_A \cap \mathit{Sep}[V_1V_2]$ *and that all the described initial operators sets are closed. If*

$$\mathit{supp}_A \cap \mathit{Sep}[V_1V_2] \nsubseteq \mathit{Sep}\text{-}\mathcal{R}$$

then the probability η *of sampling an operator from* $(\mathit{supp}_A \cap \mathit{Sep}[V_1V_2]) \setminus \mathit{Sep}\text{-}\mathcal{R}$ *is positive.*

Proof. If $\text{supp}_A \cap \text{Sep}[V_1V_2] \not\subseteq \text{Sep-}\mathcal{R}$ then

$$\dim((\text{supp}_A \cap \text{Sep}[V_1V_2]) \setminus \text{Sep-}\mathcal{R}) = \dim(\text{supp}_A \cap \text{Sep}[V_1V_2])$$

since $(\text{supp}_A \cap \text{Sep}[V_1V_2]) \setminus \text{Sep-}\mathcal{R}$ is open in $\text{supp}_A \cap \text{Sep}[V_1V_2]$. Then

$$\dim(\text{supp}_A \cap \text{Sep}[V_1V_2]) \geq \dim(\text{supp}_A \cap \text{Sep}[V_1V_2] \cap \text{Sep-}\mathcal{R})$$

Therefore,

$$\dim((\text{supp}_A \cap \text{Sep}[V_1V_2]) \setminus \text{Sep-}\mathcal{R}) \geq dim(\text{supp}_A \cap \text{Sep}[V_1V_2] \cap \text{Sep-}\mathcal{R})$$

Hence, the set $(\text{supp}_A \cap \text{Sep}[V_1V_2]) \setminus \text{Sep-}\mathcal{R}$ has nonzero measure in the set we want to sample from.

□

Corollary 6. *Let $\delta \in (0,1)$. In the setting of lemma 15, if we sample $\log_{\frac{1}{\eta}} \frac{1}{\delta}$ times we get an operator from $(supp_A \cap Sep[V_1V_2]) \setminus Sep\text{-}\mathcal{R}$ with probability $1-\delta$.*

5.2 Applying conic and semidefinite programming techniques to quantum RHL judgements decidability problem

In this section, we assume that the initial operator is fixed and we want to check whether this operator is relevant. This assumption allows us to apply the techniques of conic and semidefinite programming.

5.2.1 Quantum RHL judgements with predicates, non-separable case

In this subsection we reduce the question whether a judgement $\{A\}\mathbf{c} \sim_{nonsep} \mathbf{d}\{B\}$ holds to a question of feasibility of a semidefinite program.

By lemma 14, $\{A\}\mathbf{c} \sim_{nonsep} \mathbf{d}\{B\}$ holds if and only if $\text{supp}_A \subseteq \mathcal{R}$.

If we fix an initial operator $\rho \in \text{supp}_A$ then checking whether this operator is relevant is checking whether there there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ that satisfies B such that

- $\mathrm{Tr}_2(\rho') = [\![\, \mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\, \mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

We can rewrite this as three linear constraints on $\rho' \in \mathrm{T}^+[V_1V_2]$.

1. $\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V_1V_2]} - P_B)\rho'\big) = 0$

2. $\mathrm{Tr}_2(\rho') = [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))$

3. $\mathrm{Tr}_1(\rho') = [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$

Since ρ is fixed, we assume that $[\![\mathbf{c}]\!]\,(\mathrm{Tr}_1(\rho))$ and $[\![\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$ are computable, i.e. we look at the right hand sides as constants. Therefore, the above constarints together with the condition $\rho' \in \mathrm{T}^+[V_1V_2]$ define a semidefinite program. We are interested whether this program is feasible.

5.2.2 Quantum RHL judgements with predicates, separable case

In these section we approach the judgements $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ from the cone programming point of view. We start similarly as in the non-separable case and immediately see that what we get is not a semidefinite program but a cone program.

By lemma 14, $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$ holds if and only if $\mathrm{supp}_A \cap \mathrm{Sep}[V_1V_2] \subseteq \text{Sep-}\mathcal{R}$.

If we fix an initial operator $\rho \in \mathrm{supp}_A \cap \mathrm{Sep}[V_1V_2]$ then checking whether this operator is relevant is checking whether there there exists $\rho' \in \mathrm{Sep}[V_1V_2]$ that satisfies B such that

- $\mathrm{Tr}_2(\rho') = [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))$
- $\mathrm{Tr}_1(\rho') = [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$

We can write it as a cone program and ask whether this program is feasible. Here

- $K = \mathrm{Sep}[V_1V_2]$
- $L = \{0\}$
- $-\mathcal{L}(\rho') = (\mathrm{Tr}\big((\mathbb{I}_{\ell^2[V_1V_2]} - P_B)\rho'\big), \mathrm{Tr}_2(\rho'), \mathrm{Tr}_1(\rho'))$
- $b = (0, [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho)), [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho)))$

To solve the feasibility of such a program, we have to come up with tricks because the cone of separable operators is very complex.

Since $L = \{0\}$, we can use more convinient notations. Denote

$$\mathfrak{A} = \{\rho' \in \mathrm{Herm}[V_1V_2] \mid \mathcal{L}(\rho') - b \in \{0\}\}$$

The set $\mathfrak{A}$ is an affine subspace of $\mathrm{Herm}[V_1V_2]$. The question of feasibility of the conic program above is equivalent to asking whether $\mathfrak{A} \cap \mathrm{Sep}[V_1V_2] = \varnothing$. We assume that $0 \notin \mathfrak{A}$. Otherwise, the intersection $\mathfrak{A} \cap \mathrm{Sep}[V_1V_2]$ is never empty and the initial state ρ is zero, i.e. this is a trivial case. We will try to answer this question writing other cone programs with objective functions and trying to exploit the duality of cone programming.

Affine subspace of co-dimension 1**.** We start with the case where we assume that $\operatorname{codim}\mathfrak{A} = 1$, that is we assume that $\mathfrak{A}$ is a hyperplane in Herm$[V_1V_2]$.

Remark. In the case of the judgements $\{A\}\mathbf{c} \sim \mathbf{d}\{B\}$, $\operatorname{codim}\mathfrak{A}$ is never 1. This can be easily seen from the fact that $\mathfrak{A}$ is an intersection of the following affine subspaces.

$$\mathfrak{A} = \{\rho' \mid \mathrm{Tr}_2(\rho') = [\![\,\mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))\} \cap \{\rho' \mid \mathrm{Tr}_1(\rho') = [\![\,\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))\} \cap \{\rho' \mid \mathrm{supp}\rho' \subseteq B\}$$

Therefore, $\dim\mathfrak{A}$ is upper bounded by the dimensions of each of these subspaces. Computing the rank of partial trace or direct calculation of the kernel show that

$$\dim(\{\rho' \mid \mathrm{Tr}_1(\rho') = [\![\,\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))\}) = n^4 - n^2$$

where $|V_1 \models |V_2 \models n$. However, we still show this case because it was solved completely and the solution illustrates the intuition behind the approach in the more general case.

So, we consider the question whether $\mathrm{Sep}[V_1V_2] \cap \mathfrak{A} = \varnothing$, where $\mathfrak{A}$ is a hyperplane defined by an equation $\mathcal{L}(x) = b$ (we switch the variable from ρ to x here to be more consistent with the notations used in cone programs). That is, we assume that $b \in \mathbb{R}_{\geq 0}$ and $\mathcal{L}$ is a linear functional. Therefore, we will represent this hyperplane using inner product. We additionally assume that $\mathrm{Sep}[V_1V_2] \cap \mathfrak{A} \subseteq \{x \mid \mathrm{Tr}(x) \leq 1\}$. This is a legal assumption because we can always rescale the trace.

Denote by $a \in \mathrm{Herm}[V_1V_2]$ a normalized operator orthogonal to $\mathfrak{A}$ such that for every $x \in \mathfrak{A}$ we have $\mathrm{Tr}(ax) = b$. Consider the following cone program $\mathfrak{P}_1$.

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}(ax) \\ \text{subject to} \quad & 1 - \mathrm{Tr}(x) \in \mathbb{R}_{\geq 0}, \\ & x \in \mathrm{Sep}[V_1V_2] \end{aligned}$$

We start with showing that the value of the program $\mathfrak{P}_1$ leads to an answer to the original question whether $\mathrm{Sep}[V_1V_2] \cap \mathfrak{A} = \varnothing$.

Lemma 16. *In the notations of the program $\mathfrak{P}_1$, the following holds.*

1. *If* $\max \mathrm{Tr}(ax) \geq b$*, then Sep*$[V_1V_2] \cap \mathfrak{A} \neq \varnothing$
2. *If* $\max \mathrm{Tr}(ax) < b$*, then Sep*$[V_1V_2] \cap \mathfrak{A} = \varnothing$

Proof. We analyze the two cases separately.

1. First, note that $0 \in \mathrm{Sep}[V_1V_2]$ and $\mathrm{Tr}(a \cdot 0) = 0$.

Assume that there exists $x \in \text{Sep}[V_1V_2]$ such that $\text{Tr}(ax) \geq b$. Then, due to the convexity of the cone $\text{Sep}[V_1V_2]$, the whole segment connecting 0 and x lies in $\text{Sep}[V_1V_2]$. Hence, there exists $x' \in \text{Sep}[V_1V_2]$ such that $\text{Tr}(ax') = b$. Since

$$\mathfrak{A} = \{z \mid \text{Tr}(az) = b\}$$

we conclude that $x' \in \mathfrak{A}$. Therefore, $x' \in \text{Sep}[V_1V_2] \cap \mathfrak{A}$ and this intersection is not empty.

2. Assume that $\max \text{Tr}(ax) < b$. Then

$$\text{Sep}[V_1V_2] \cap \{x \mid \text{Tr}(x) \leq 1\} \cap \mathfrak{A} = \varnothing$$

This holds because $\text{Sep}[V_1V_2] \cap \{x \mid \text{Tr}(x) \leq 1\}$ is the set of feasible points for the program $\mathfrak{P}_1$ and for any point x in this intersection $\text{Tr}(ax) < b$.

Since $\text{Sep}[V_1V_2] \cap \mathfrak{A} \subseteq \{x \mid \text{Tr}(x) \leq 1\}$, we obtain the following.

$$\text{Sep}[V_1V_2] \cap \{x \mid \text{Tr}(x) \leq 1\} \cap \mathfrak{A} = \text{Sep}[V_1V_2] \cap \mathfrak{A} = \varnothing$$

This completes the proof. □

Next, we how that $\mathfrak{P}_1$ satisfies the necessary properties to apply the strong duality theorem.

Lemma 17. *The program $\mathfrak{P}_1$ satisfies the following properties*

1. *$\mathfrak{P}_1$ is feasible*
2. *the value of $\mathfrak{P}_1$ is finite*
3. *$\mathfrak{P}_1$ has an interior point*

Proof. We show that properties are satisfied one by one.

1. Take the 0 operator. It lies both in $\text{Sep}[V_1V_2]$ and $\{x \mid \text{Tr}(x) \leq 1\}$. Therefore,

$$\text{Sep}[V_1V_2] \cap \{x \mid \text{Tr}(x) \leq 1\} \neq \varnothing$$

and the program $\mathfrak{P}_1$ is feasible.

2. We need to check that there exists $x \in \text{Sep}[V_1V_2]$ such that $1 - \text{Tr}(x) > 0$. Again, if we take the 0 operator as such x, we see that the desired property holds.

3. To show that the value $\max \text{Tr}(ax)$ is finite we upper bound the trace with the norm (see e.g. [9]).

$$|\text{Tr}(ax)| \leq \|a\| \cdot |\text{Tr}(x)| \leq \|a\|$$

□

Corollary 7. *Let $\mathfrak{D}_1$ be the dual program of the program $\mathfrak{P}_1$. Then $\mathfrak{D}_1$ is feasible and its value is equal to the value of $\mathfrak{P}_1$.*

Proof. Be lemma 17, $\mathfrak{P}_1$ satisfies the conditons of the strong duality of cone programming theorem 1.

□

Now we can switch to the dual program $\mathfrak{D}_1$. We start with writing it down by the definition.

$$\begin{aligned} \text{minimize} \quad & \operatorname{Tr}(1 \cdot y) \\ \text{subject to} \quad & \operatorname{Tr}^*(y) - a \in \text{Sep}[V_1V_2]^*, \\ & y \in \mathbb{R}^*_{\geq 0} \end{aligned}$$

Here the $*$ denotes adjoint for operators and dual for cones.

Claim 2. *The dual operator of the trace acts as $\operatorname{Tr}^*(y) = y \cdot \mathbb{I}_{\ell^2[V_1V_2]}$ on every $y \in \mathbb{R}$.*

Proof. The dual operator is defined by the equality

$$\operatorname{Tr}(\operatorname{Tr}(x)y) = \operatorname{Tr}(x \operatorname{Tr}^*(y))$$

for every $x \in \text{Herm}[V_1V_2], y \in \mathbb{R}$. Using the linearity of the trace, we write the following chain of equalities.

$$\operatorname{Tr}(\operatorname{Tr}(x)y) = \operatorname{Tr}(\operatorname{Tr}\big(x\mathbb{I}_{\ell^2[V_1V_2]}\big)y) = \operatorname{Tr}\big(x(y \cdot \mathbb{I}_{\ell^2[V_1V_2]})\big) = \operatorname{Tr}(x \operatorname{Tr}^*(y))$$

Therefore,

$$\operatorname{Tr}^*(y) = y \cdot \mathbb{I}_{\ell^2[V_1V_2]}$$

□

Using the claim above and the theorem 2, we can rewrite the program $\mathfrak{D}_1$.

$$\begin{aligned} \text{minimize} \quad & y \\ \text{subject to} \quad & \mathcal{P}_{(y \cdot \mathbb{I}_{\ell^2[V_1V_2]} - a)} \text{ is non-negative}, \\ & y \in \mathbb{R}_{\geq 0} \end{aligned}$$

Since $\mathcal{P}_{(y \cdot \mathbb{I}_{\ell^2[V_1V_2]} - a)}$ is defined through the trace and it is a linear operator, we have

$$\mathcal{P}_{(y \cdot \mathbb{I}_{\ell^2[V_1V_2]} - a)} = y\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_a$$

This allows us to rewrite $\mathfrak{D}_1$ in the final form.

$$\begin{aligned} &\text{minimize} && y \\ &\text{subject to} && y\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_a \text{ is non-negative}, \\ & && y \in \mathbb{R}_{\geq 0} \end{aligned}$$

There are two possible cases.

- If $y = b$ is feasible, i.e. $b\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_a$ is non-negative, then $\min y \leq b$.
- If $y = b$ is not feasible, i.e. $b\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_a$ is not non-negative, then $\min y > b$.

Therefore, we only need to analyze whether the polynomial $b\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_a$ is non-negative. This is a problem that can be solved approximately by theorem 3.

The only problem that we face here is that there is one case for which this approach does not work. When we decide whether $y = b$ is a feasible point we get two possibilities

- $\max \mathrm{Tr}(ax) \leq b$
- $\max \mathrm{Tr}(ax) > b$

If $\max \mathrm{Tr}(ax) > b$ then we can conclude that $\mathrm{Sep}[V_1V_2] \cap \mathfrak{A} \neq \varnothing$. However, if $\max \mathrm{Tr}(ax) \leq b$ then we can only conclude that either $\mathrm{Sep}[V_1V_2] \cap \mathfrak{A} = \varnothing$ or $\max \mathrm{Tr}(ax) = b$. Therefore, in this particular case when $\max \mathrm{Tr}(ax) = b$ we cannot solve the problem with this approach.

Affine subspace of co-dimension at least 2**.** Here we assume that $\mathrm{codim}(\mathfrak{A}) \geq 2$. The initial idea for this case was to reduce it to the previous one. That is, to represent $\mathfrak{A}$ as a hyperplane. This could be done by looking at $\mathfrak{A}$ as at a hyperplane in some linear subspace in $\mathrm{Herm}[V_1V_2]$. It naturally led to the idea to consider $\mathrm{Span}(\mathfrak{A})$, since $\mathfrak{A}$ has co-dimension 1 in this subspace.

Considering $\mathrm{Span}(\mathfrak{A})$ helps to overcome yet another difficulty. We can only write cone programs for which we know feasibility in advance. Otherwise, we cannot use the duality. Since $\mathrm{Span}(\mathfrak{A})$ is a linear subspace, it contains 0. Therefore,

$$\mathrm{Sep}[V_1V_2] \cap \mathrm{Span}(\mathfrak{A}) \neq \varnothing$$

One more important thing is that $\mathrm{Sep}[V_1V_2] \cap \mathrm{Span}(\mathfrak{A})$ is a convex cone as it is an intersection of a convex cone and a linear space.

We start with a lemma that gives one more motivation to consider $\mathrm{Span}(\mathfrak{A})$.

Lemma 18.

1. *If Sep*$[V_1V_2] \cap$ *Span*$(\mathfrak{A}) = \{0\}$*, then Sep*$[V_1V_2] \cap \mathfrak{A} = \varnothing$
2. *If Int*$($*Sep*$[V_1V_2]) \cap$ *Span*$(\mathfrak{A}) \neq \{0\}$*, then Sep*$[V_1V_2] \cap \mathfrak{A} \neq \varnothing$ *or* $-$*Sep*$[V_1V_2] \cap \mathfrak{A} \neq \varnothing$

Proof. See [10]. □

Since we have this connection between the intersections, we consider the following cone program $\mathfrak{P}_2$.

$$\begin{aligned} \text{maximize} \quad & \operatorname{Tr}\left(x\mathbb{I}_{\ell^2[V_1V_2]}\right) \\ \text{subject to} \quad & 1 - \operatorname{Tr}(x) \in \mathbb{R}_{\geq 0}, \\ & x \in \text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}) \end{aligned}$$

Remark. $\operatorname{Tr}\left(x\mathbb{I}_{\ell^2[V_1V_2]}\right) = \operatorname{Tr}(x)$. We only write it in this form to match the form of a cone program.

First, we show the value of this program helps us to verify whether $\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}) = \{0\}$.

Lemma 19. *In the notations of the program* $\mathfrak{P}_2$ *the following holds.*

1. *If Sep*$[V_1V_2] \cap$ *Span*$(\mathfrak{A}) = \{0\}$*, then* $\max \operatorname{Tr}(x) = 0$
2. *If Sep*$[V_1V_2] \cap$ *Span*$(\mathfrak{A}) \neq \{0\}$*, then* $\max \operatorname{Tr}(x) \neq 0$

Proof. We consider the cases separately.

1. Assume that $\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}) = \{0\}$. Then $\max \operatorname{Tr}(x) = \operatorname{Tr}(0) = 0$.

2. Assume that $\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}) \neq \{0\}$. Then there exists a non-zero $x \in \text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A})$. Since $x \in \text{Sep}[V_1V_2]$, it is a positive non-zero operator. Therefore, $\operatorname{Tr}(x) > 0$.

□

Next, we show that the duality is applicable to the program $\mathfrak{P}_2$.

Lemma 20. *The program* $\mathfrak{P}_2$ *satisfies the following properties*

1. $\mathfrak{P}_2$ *is feasible*
2. *the value of* $\mathfrak{P}_2$ *is finite*

3. $\mathfrak{P}_2$ *has an interior point*

Proof. The properties $\mathbf{1}$. and $\mathbf{2}$. can be proven exactly the same way as it was done in lemma 17.

$\mathbf{3}$. This property is straightforward: $\mathrm{Tr}(x) \leq 1$.

□

Corollary 8. *Let* $\mathfrak{D}_2$ *be the dual program of the program* $\mathfrak{P}_2$*. Then* $\mathfrak{D}_2$ *is feasible and its value is equal to the value of* $\mathfrak{P}_2$*.*

Now we are ready to write down the dual program $\mathfrak{D}_2$. We omit the steps that were explained in the previous paragraph.

$$\begin{aligned} &\text{minimize} && y \\ &\text{subject to} && y \cdot \mathbb{I}_{\ell^2[V_1V_2]} - \mathbb{I}_{\ell^2[V_1V_2]} \in (\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}))^*, \\ &&& y \in \mathbb{R}_{\geq 0} \end{aligned}$$

The next step is to figure out what $(\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}))^*$ is. By lemma 8,

$$(\text{Sep}[V_1V_2] \cap \text{Span}(\mathfrak{A}))^* = \text{Sep}[V_1V_2]^* + \text{Span}(\mathfrak{A})^*$$

By lemma the theorem 2, we know what $\text{Sep}[V_1V_2]^*$ is. Next, we analyze $\text{Span}(\mathfrak{A})^*$.

Claim 3. *Span*$(\mathfrak{A})^* =$ *Span*$(\mathfrak{A})^\perp$.

Proof. We show the two inclusions.

$\subseteq$: Let $y \in \text{Span}(\mathfrak{A})^*$, then

$$\mathrm{Tr}(yx) \geq 0 \quad \forall x \in \text{Span}(\mathfrak{A})$$

Since $\text{Span}(\mathfrak{A})$ is a linear space, for every $x \in \text{Span}(\mathfrak{A})$ holds $-x \in \text{Span}(\mathfrak{A})$. Therefore,

$$\mathrm{Tr}(y(-x)) = -\mathrm{Tr}(yx) \geq 0 \quad \forall x \in \text{Span}(\mathfrak{A})$$

Hence,

$$\mathrm{Tr}(yx) = 0 \quad \forall x \in \text{Span}(\mathfrak{A})$$

$\supseteq$: This inclusion is straightforward. Let $y \in \text{Span}(\mathfrak{A})^\perp$. Then

$$\mathrm{Tr}(yx) = 0 \geq 0 \quad \forall x \in \text{Span}(\mathfrak{A})$$

□

Corollary 9. $(\mathit{Sep}[V_1V_2] \cap \mathit{Span}(\mathfrak{A}))^* = \mathit{Sep}[V_1V_2]^* + \mathit{Span}(\mathfrak{A}))^\perp$.

We rewrite the dual program $\mathfrak{D}_2$.

$$\begin{aligned} \text{minimize} \quad & y \\ \text{subject to} \quad & (y-1)\mathbb{I}_{\ell^2[V_1V_2]} \in \mathrm{Sep}[V_1V_2]^* + \mathrm{Span}(\mathfrak{A})^\perp, \\ & y \in \mathbb{R}_{\geq 0} \end{aligned}$$

Checking whether $y = 0$ is a feasible point is the same as checking whether $-\mathbb{I}_{\ell^2[V_1V_2]} \in \mathrm{Sep}[V_1V_2]^* + \mathrm{Span}(\mathfrak{A})^\perp$. This leads us to the following reformulation of the problem.

Corollary 10.

1. *If there exists $z \in \mathfrak{A}^\perp$ such that $-\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_z$ is a non-negative polynomial, then $\mathit{Sep}[V_1V_2] \cap \mathit{Span}(\mathfrak{A}) \neq \varnothing$.*
2. *If for any $z \in \mathfrak{A}^\perp$ the polynomial $-\mathcal{P}_{\mathbb{I}_{\ell^2[V_1V_2]}} - \mathcal{P}_z$ is not non-negative, then $\mathit{Sep}[V_1V_2] \cap \mathit{Span}(\mathfrak{A}) = \varnothing$ and $\mathit{Sep}[V_1V_2] \cap \mathfrak{A} = \varnothing$.*

Remark. $\mathrm{Span}(\mathfrak{A})^\perp$ is replaced by $\mathfrak{A}^\perp$ because these two sets are equal.

5.2.3 Quantum RHL judgements with operators, non-separable case

In this subsection we reduce the question whether an operator $\rho \in \mathrm{T}^+[V_1V_2]$ is $\mathrm{relevant}^{\mathrm{op}}_{\mathrm{nonsep}}$ to a semidefinite program.

By definition, we need to check that there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

1. $\mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$
2. $\mathrm{Tr}_2(\rho') = [\![\, \mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho))$
3. $\mathrm{Tr}_1(\rho') = [\![\, \mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho))$

All the right hand side parts of these conditions are viewed as constants, since ρ is fixed. Therefore, we can reformulate it in the form of a semidefinite program. Consider the following semidefinite program $\mathfrak{P}_3$.

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}(\mathcal{B}\rho') \\ \text{subject to} \quad & \mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!]\,(\mathrm{Tr}_2(\rho)), \\ & \mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!]\,(\mathrm{Tr}_1(\rho)), \\ & \rho' \in \mathrm{T}^+[V_1V_2] \end{aligned}$$

Next, we show that the value of the $\mathfrak{P}_3$ program allows us to verify whether ρ is relevant$^{\text{op}}_{\text{nonsep}}$.

Lemma 21. *In the notations of the program $\mathfrak{P}_3$, the following holds.*

1. *If $\max \mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$, then ρ is relevant$^{op}_{nonsep}$*
2. *If $\max \mathrm{Tr}(\mathcal{B}\rho') < \mathrm{Tr}(\mathcal{A}\rho)$, then ρ is not relevant$^{op}_{nonsep}$*

Proof. We consider the cases separately.

1. Assume that $\max \mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$. Then there exists $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

1. $\mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$
2. $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
3. $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

This is exactly the definition of ρ being relevant$^{\text{op}}_{\text{nonsep}}$.

2. Assume that $\max \mathrm{Tr}(\mathcal{B}\rho') < \mathrm{Tr}(\mathcal{A}\rho)$. Then for every $\rho' \in \mathrm{T}^+[V_1V_2]$ such that

1. $\mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho))$
2. $\mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho))$

holds $\mathrm{Tr}(\mathcal{B}\rho') < \mathrm{Tr}(\mathcal{A}\rho)$. That is, the desired ρ' does not exist.

□

5.2.4 Quantum RHL judgements with operators, separable case

In this section, we present a cone program whose value makes it possible to distinguish whether a fixed $\rho \in \mathrm{Sep}[V_1V_2]$ is relevant$^{\text{op}}$. However, unlike the previous case, this is not a solution to the problem, but a reformulation. This happens because of the same problems as in the case of quantum RHL judgements with predicates. Namely, the optimization is over a set that has a very difficult structure.

Let $\mathfrak{P}_4$ be the following cone program.

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}(\mathcal{B}\rho') \\ \text{subject to} \quad & \mathrm{Tr}_2(\rho') = [\![\mathbf{c}]\!] (\mathrm{Tr}_2(\rho)), \\ & \mathrm{Tr}_1(\rho') = [\![\mathbf{d}]\!] (\mathrm{Tr}_1(\rho)), \\ & \rho' \in \mathrm{Sep}[V_1V_2] \end{aligned}$$

Analogously to the previous case, we state that the program $\mathfrak{P}_4$ is reasonable. That is, the value of $\mathfrak{P}_4$ indicates whether $\rho \in \mathrm{Sep}[V_1 V_2]$ is relevant$^{\mathrm{op}}$.

Lemma 22. *In the notations of the program $\mathfrak{P}_4$, the following holds.*

1. *If* $\max \mathrm{Tr}(\mathcal{B}\rho') \geq \mathrm{Tr}(\mathcal{A}\rho)$*, then ρ is relevant^{op}*
2. *If* $\max \mathrm{Tr}(\mathcal{B}\rho') < \mathrm{Tr}(\mathcal{A}\rho)$*, then ρ is not relevant^{op}*

Proof. The proof is the same as the proof of lemma 21. □

6 Conclusion

We analyzed quantum RHL judgments. We considered four different versions of their definition and tried to establish for each whether it is possible to determine whether it holds or not for a fixed judgment.
We have showed that

- The sets of initial operators of a judgement have structure of convex cones and that deciding whether a judgement holds can be done with a fixed initial operator.
- For the judgements defined with quantum predicates and without the separability requirement it is possible to decide whether it holds with a fixed initial operator. This is done by restating the problem as a semidefinite feasibility problem.
- For the judgements defined with quantum predicates and with the separability requirement it is possible to write down a cone program that describes the same problem. This lead to a reformulation of the problem in terms of polynomials. We also showed how to solved such a cone program with a special assumption on the dimension of an affine subspace using the sum of squares relaxation.
- For the judgements defined with operators and without the separability requirement it is possible to reformulate the problem as a semidefinite optimization program. Therefore, for this type of judgements we can decide whether it holds or not.
- For the judgements defined with operators and with the separability requirement it is possible to write down a cone program that describes whether such a judgement holds.

To completely answer the question about the decidability of judgments, it is necessary to continue the analysis of cone programs and develop an algorithm, possibly approximate, which would give the final answer whether a judgment holds or not in the cases with separability as well.

References

[1] Dominique Unruh. *Quantum Relational Hoare Logic*. Proc. ACM Programming Languages (2019).

[2] Christopher Hawthorne. *A brief introduction to trace class operators*. (2015). https://cdchawthorne.com/writings/trace_class_operators.pdf

[3] Bernd Gärtner and Jiří Matoušek. *Approximation Algorithms and Semidefinite Programming*. Springer-Verlag Berlin Heidelberg (2012).

[4] Weisstein, Eric W. "Newton's Method." From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/NewtonsMethod.html

[5] Lin Chen, Dragomir Z. Djokovic. *Boundary of the set of separable states*. Proc. Roy. A 471: 20150102 (2015).

[6] Jeyakumar, V., Wolkowicz, H. *Generalizations of Slater's constraint qualification for infinite convex programs*. Mathematical Programming 57, 85–101 (1992). https://doi.org/10.1007/BF01581074

[7] Kun Fang, Hamza Fawzi. *The sum-of-squares hierarchy on the sphere, and applications in quantum information theory*. arXiv:1908.05155 (2019).

[8] G. Blekherman, P. Parrilo, R. Thomas. *Semidefinite optimization and convex algebraic geometry*. MOS-SIAM Series on Optimization, Volume 13 (2012).

[9] Rajnikant Pate1, Mitsuhiko Toda *Trace Inequalities Involving Hermitian Matrices*. Linear Algebra and its Applications 23:13-2 (1979).

[10] Simone Naldi, Rainer Sinn *Conic programming: infeasibility certificates and projective geometry*. arXiv:1810.11792 (2018).

Appendix

Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Galina Pass**,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Quantum Relational Hoare Logic Judgements,
   *(*title of thesis)

   supervised by Dominique Peer Ghislain Dr Unruh.
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Galina Pass
14/05/2021