Quantum Prerequisites

1 Quantum/Linear Algebra Prerequisites

Throughout this and the following chapters, all Hilbert spaces are *finite-dimensional* complex Hilbert spaces. This has two practical consequences that we will use repeatedly: (i) every linear operator is bounded and everywhere-defined, and (ii) spectral decompositions and matrix representations in an orthonormal basis are always available.

Notations and conventions. $\mathcal{H}$ denotes a (finite-dimensional) Hilbert space. $\mathcal{L}(\mathcal{H})$ denotes the space of linear operators (linear maps) $\mathcal{H} \to \mathcal{H}$. $\mathbf{1}$ denotes the identity operator; when needed we write $\mathbf{1}_{\mathcal{H}}$ to indicate the underlying space. $\otimes$ denotes the tensor product of spaces, vectors, and operators (which we will define precisely later on). tr denotes the trace of a linear operator. $A^\dagger$ denotes the adjoint of an operator A.

We will freely identify operators with their matrix representations in a chosen orthonormal basis when convenient, but all definitions and statements are basis-independent.

Dirac and labelled Dirac notations We use Dirac notation for vectors and linear functionals. A *ket* $|\psi\rangle \in \mathcal{H}$ denotes a vector, and its associated *bra* $\langle\psi|$ denotes the linear functional defined by $\langle\psi|\,(|\phi\rangle) := \langle\psi|\phi\rangle$, where $\langle\cdot|\cdot\rangle$ is the inner product on $\mathcal{H}$. The rank-one (outer-product) operator $|\psi\rangle\langle\phi| \in \mathcal{L}(\mathcal{H})$ acts by

$$(|\psi\rangle\langle\phi|)\,|\xi\rangle \;=\; |\psi\rangle\,\langle\phi|\xi\rangle.$$

When $\|\psi\| = 1$, the operator $|\psi\rangle\langle\psi|$ is the projection onto the one-dimensional subspace spanned by $|\psi\rangle$.

In program-logic presentations, it is often helpful to make subsystem structure explicit by labelling registers (or "locations") and writing *local* expressions that act nontrivially only on a specified subsystem.

Informally, suppose a global state space factors as

$$\mathcal{H}_{\text{global}} \;\cong\; \bigotimes_{x\in\mathsf{Reg}} \mathcal{H}_x,$$

where Reg is a finite set of register labels. A *local* operator on register x is an operator $A \in \mathcal{L}(\mathcal{H}_x)$, lifted to the global space as

$$A^{(x)} \;:=\; \mathbf{1} \otimes \cdots \otimes A \otimes \cdots \otimes \mathbf{1},$$

i.e. A placed at position x and identities elsewhere (with the understanding that the tensor-product bracketing/order is fixed by a chosen convention). Likewise, a local state on x can be embedded as $\rho^{(x)} := \rho \otimes \sigma$ where σ is some reference state on the complement system, or used via partial trace when only the reduced state on x matters. The main purpose of this notation is conceptual: it lets us write "the program updates register x" as a transformation acting on $\mathcal{H}_x$ while keeping the rest of the system implicit. When we later discuss program semantics as superoperators, this "local" viewpoint becomes central.

1.1 Hilbert spaces and tensor products

A (complex) Hilbert space $\mathcal{H}$ is a complex vector space equipped with an inner product $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ that is linear in the second argument, conjugate-linear in the first, and positive definite. The associated norm is $\|\psi\| := \sqrt{\langle\psi|\psi\rangle}$.

A family $\{|e_i\rangle\}_{i=1}^d$ is an *orthonormal basis* (ONB) of $\mathcal{H}$ if $\langle e_i|e_j\rangle = \delta_{ij}$ and every vector $|\psi\rangle \in \mathcal{H}$ can be written uniquely as $|\psi\rangle = \sum_{i=1}^d \alpha_i |e_i\rangle$.

Composite quantum systems are modelled by tensor products. Given Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, their tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ is the Hilbert space spanned by formal symbols $|\psi\rangle \otimes |\phi\rangle$, subject to bilinearity, and equipped with the inner product determined by

$$\langle \psi_1 \otimes \phi_1|\psi_2 \otimes \phi_2\rangle \;:=\; \langle \psi_1|\psi_2\rangle \langle \phi_1|\phi_2\rangle, \quad \text{extended by linearity.}$$

If $\{|e_i\rangle\}$ is an ONB of $\mathcal{H}_A$ and $\{|f_j\rangle\}$ is an ONB of $\mathcal{H}_B$, then $\{|e_i\rangle \otimes |f_j\rangle\}_{i,j}$ is an ONB of $\mathcal{H}_A \otimes \mathcal{H}_B$.

The tensor product is the mathematical mechanism behind "placing systems side-by-side". It is also the source of entanglement: not every unit vector in $\mathcal{H}_A \otimes \mathcal{H}_B$ can be written as $|\psi\rangle \otimes |\phi\rangle$. For our purposes here, the key point is that $\otimes$ is the default connective for composing both states and operations.

Lemma 1.1. *Tensor products satisfy the expected algebraic laws up to canonical unitary isomorphism:*

$$(\mathcal{H}_A \otimes \mathcal{H}_B) \otimes \mathcal{H}_C \;\cong\; \mathcal{H}_A \otimes (\mathcal{H}_B \otimes \mathcal{H}_C), \qquad \mathbb{C} \otimes \mathcal{H} \;\cong\; \mathcal{H}, \qquad \mathcal{H}_A \otimes \mathcal{H}_B \;\cong\; \mathcal{H}_B \otimes \mathcal{H}_A.$$

These identifications are implemented by explicit unitary "rebracketing" and "swap" maps.

In practice we often suppress these isomorphisms and treat $\otimes$ as associative. When subsystem bookkeeping matters ,it is best to fix a register order and keep it consistent throughout.

1.2 Linear operators and Löwner order

An *operator* on $\mathcal{H}$ is a linear map $A : \mathcal{H} \to \mathcal{H}$. The *adjoint* $A^\dagger$ is the unique operator satisfying

$$\langle \psi|A\phi\rangle \;=\; \langle A^\dagger\psi|\phi\rangle \quad \text{for all } |\psi\rangle, |\phi\rangle \in \mathcal{H}.$$

In an orthonormal basis, $A^\dagger$ corresponds to the conjugate-transpose matrix of A.

The *trace* of $A \in \mathcal{L}(\mathcal{H})$ is defined by

$$\operatorname{tr}(A) \;:=\; \sum_{i=1}^{d} \langle e_i| A |e_i\rangle,$$

where $\{|e_i\rangle\}_{i=1}^d$ is any orthonormal basis of $\mathcal{H}$. This definition is independent of the chosen orthonormal basis.

It is often convenient to equip $\mathcal{L}(\mathcal{H})$ with the Hilbert–Schmidt inner product

$$\langle A, B\rangle_{\mathrm{HS}} \;:=\; \operatorname{tr}(A^\dagger B).$$

This makes $\mathcal{L}(\mathcal{H})$ itself into a finite-dimensional Hilbert space.

Lemma 1.2. *For all $A, B \in \mathcal{L}(\mathcal{H})$ and $\alpha \in \mathbb{C}$:*

$$(A^\dagger)^\dagger = A, \qquad (AB)^\dagger = B^\dagger A^\dagger, \qquad (\alpha A + B)^\dagger = \overline{\alpha}\, A^\dagger + B^\dagger.$$

Lemma 1.3. *For all $A, B \in \mathcal{L}(\mathcal{H})$:*

$$\operatorname{tr}(A^\dagger) = \overline{\operatorname{tr}(A)}, \qquad \operatorname{tr}(AB) = \operatorname{tr}(BA).$$

More generally, for any finite product of compatible operators,

$$\operatorname{tr}(A_1 A_2 \cdots A_n) \;=\; \operatorname{tr}(A_k A_{k+1} \cdots A_n A_1 \cdots A_{k-1}) \quad \textit{(cyclicity).}$$

Lemma 1.4. *Let $\mathcal{H}_A, \mathcal{H}_B$ be Hilbert spaces. For all $A \in \mathcal{L}(\mathcal{H}_A)$ and $B \in \mathcal{L}(\mathcal{H}_B)$,*

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger, \qquad \operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B).$$

We record the operator classes that appear constantly in quantum reasoning.

Hermitian / self-adjoint An operator $H \in \mathcal{L}(\mathcal{H})$ is *Hermitian* if $H^\dagger = H$.

Positive semidefinite A Hermitian operator $A \in \mathcal{L}(\mathcal{H})$ is *positive semidefinite* (PSD), written $A \sqsupseteq 0$, if $\langle\psi| A |\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$.

Unitary An operator $U \in \mathcal{L}(\mathcal{H})$ is *unitary* if $U^\dagger U = UU^\dagger = \mathbf{1}$.

Projection An operator $P \in \mathcal{L}(\mathcal{H})$ is a *projection* if $P = P^\dagger$ and $P^2 = P$. Equivalently, P is the orthogonal projector onto its range $\mathrm{Ran}(P)$.

Theorem 1.5 (Spectral theorem)**.** *Every Hermitian operator $H \in \mathcal{L}(\mathcal{H})$ admits an orthonormal eigenbasis and a real spectral decomposition*

$$H \;=\; \sum_{i=1}^{d} \lambda_i \, |v_i\rangle \langle v_i| \, ,$$

where $\{|v_i\rangle\}$ is an orthonormal basis and $\lambda_i \in \mathbb{R}$. Moreover, $H \sqsupseteq 0$ iff all eigenvalues λ_i are ≥ 0.

Lemma 1.6. *If $A \sqsupseteq 0$ and $X \in \mathcal{L}(\mathcal{H})$, then $XAX^\dagger \sqsupseteq 0$. In particular, unitary conjugation preserves positivity: if U is unitary and $A \sqsupseteq 0$, then $UAU^\dagger \sqsupseteq 0$.*

Lemma 1.7. *If P is a projection, then $P \sqsupseteq 0$ and $P \sqsubseteq \mathbf{1}$.*

The Löwner (semidefinite) order is the standard partial order on Hermitian operators.

Definition 1.8 (Löwner order)**.** For Hermitian operators $A, B \in \mathcal{L}(\mathcal{H})$, define

$$A \sqsubseteq B \quad \Longleftrightarrow \quad B - A \sqsupseteq 0.$$

Intuitively, $A \sqsubseteq B$ means that B is "at least as large" as A in every direction of Hilbert space: it is the operator analogue of pointwise order for real-valued functions.

Theorem 1.9. *On the real vector space of Hermitian operators $\{H \in \mathcal{L}(\mathcal{H}) : H^\dagger = H\}$, the relation $\sqsubseteq$ is reflexive, antisymmetric, and transitive.*

Lemma 1.10. *If $A \sqsubseteq B$ and $C \sqsupseteq 0$, then*

$$\mathrm{tr}(CA) \leq \mathrm{tr}(CB).$$

In particular, if $\rho \sqsupseteq 0$ is any PSD operator, then $\mathrm{tr}(A\rho) \leq \mathrm{tr}(B\rho)$ *whenever $A \sqsubseteq B$.*

1.3 Quantum states as operators

We represent quantum states by density operators, i.e. positive semidefinite operators with unit trace. This representation is both mathematically convenient, and operationally meaningful since it directly encodes probabilities of measurement outcomes.

Definition 1.11. Let $\mathcal{H}$ be a finite-dimensional Hilbert space.

A *(mixed) quantum state* on $\mathcal{H}$ is a *density operator* $\rho \in \mathcal{L}(\mathcal{H})$ such that $\rho \sqsupseteq 0$ and $\mathrm{tr}(\rho) = 1$.

A *partial* (or *subnormalized*) *state* on $\mathcal{H}$ is an operator $\rho \in \mathcal{L}(\mathcal{H})$ such that $\rho \sqsupseteq 0$ and $\mathrm{tr}(\rho) \leq 1$.

Definition 1.12. A *pure state* is a density operator of the form $\rho \;=\; |\psi\rangle \langle\psi| \quad$ for some unit vector $|\psi\rangle \in \mathcal{H}, \; \|\psi\| = 1$.

Pure states are "maximally informative" descriptions of a system, while mixed states represent classical uncertainty about which pure state is present, or arise as *reduced states* of subsystems of entangled larger systems. Mathematically, the mixed states form a convex set; pure states are its extreme points.

Lemma 1.13. *Let ρ be a density operator on $\mathcal{H}$. The following are equivalent:*

(i) ρ *is pure, i.e.* $\rho = |\psi\rangle\langle\psi|$ *for some unit* $|\psi\rangle$*.*

(ii) ρ *is a rank-one projection (equivalently,* $\rho^2 = \rho$ *and* $\operatorname{tr}(\rho) = 1$*).*

(iii) $\operatorname{tr}(\rho^2) = 1$.

Lemma 1.14. *If* ρ_1, ρ_2 *are density operators and* $0 \leq \lambda \leq 1$*, then* $\lambda\rho_1 + (1-\lambda)\rho_2$ *is a density operator. The same holds for partial density operators (with* $\operatorname{tr} \leq 1$*).*

1.4 Support and support calculus

Support is the key bridge between operator-based descriptions and the projection/subspace viewpoint used in sharp-predicate (projection) logics. It is also the main tool for under-approximation reasoning in QIL.

Definition 1.15 (Support)**.** Let $A \sqsupseteq 0$ be positive semidefinite. Its *support* is the subspace

$$\operatorname{supp}(A) \ := \ \operatorname{span}\{|v\rangle : A\,|v\rangle = \lambda\,|v\rangle \ \text{ for some } \lambda > 0\}.$$

Equivalently, $\operatorname{supp}(A) = \operatorname{Ran}(A)$, the range (image) of A. We write Π_A for the orthogonal projection onto $\operatorname{supp}(A)$ (the *support projector* of A).

If A is a state (or partial state), then $\operatorname{supp}(A)$ is the subspace in which the state "actually has weight". Outside $\operatorname{supp}(A)$ the state has no component at all (zero probability for any outcome supported entirely there). This makes support a natural *boolean* satisfaction notion for projection predicates: a projection P is satisfied exactly when $\operatorname{supp}(\rho)$ lies inside the range of P.

Lemma 1.16. *For* $A \sqsupseteq 0$, $\operatorname{supp}(A) \ = \ (\ker A)^{\perp}, \qquad \Pi_A A = A\Pi_A = A, \qquad A = \Pi_A A \Pi_A.$

Lemma 1.17. *Let* $\rho \sqsupseteq 0$ *and let* P *be a projection. The following are equivalent:*

(i) $\operatorname{supp}(\rho) \subseteq \operatorname{Ran}(P)$*.*

(ii) $P\rho P = \rho$*.*

(iii) $P\rho = \rho$ *(equivalently* $\rho P = \rho$*).*

Lemma 1.18 (Support under unitary conjugation)**.** *If* U *is unitary and* $\rho \sqsupseteq 0$*, then*

$$\operatorname{supp}(U\rho U^\dagger) \ = \ U\big(\operatorname{supp}(\rho)\big), \qquad \Pi_{U\rho U^\dagger} \ = \ U\Pi_\rho U^\dagger.$$

Lemma 1.19 (Support of sums)**.** *If* $\rho_1, \rho_2 \sqsupseteq 0$*, then*

$$\operatorname{supp}(\rho_1 + \rho_2) \ = \ \operatorname{span}\big(\operatorname{supp}(\rho_1) \cup \operatorname{supp}(\rho_2)\big) \ = \ \operatorname{supp}(\rho_1) + \operatorname{supp}(\rho_2),$$

where + denotes the sum of subspaces.

1.5 Composite systems and partial trace

Let $\mathcal{H}_A, \mathcal{H}_B$ be Hilbert spaces. A joint system has state space $\mathcal{H}_A \otimes \mathcal{H}_B$. Product (uncorrelated) states are represented by tensor products $\rho_A \otimes \rho_B$.

Definition 1.20. The *partial trace over $\mathcal{H}_B$* is the unique linear map

$$\mathrm{tr}_B : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$$

such that for all $X \in \mathcal{L}(\mathcal{H}_A)$ and $M \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$,

$$\mathrm{tr}\big((X \otimes \mathbf{1}_{\mathcal{H}_B})\, M\big) \;=\; \mathrm{tr}\big(X\, \mathrm{tr}_B(M)\big).$$

Similarly, tr_A is defined by the corresponding identity with $\mathbf{1}_{\mathcal{H}_A} \otimes Y$ testers.

Operationally, tr_B means "discard/ignore subsystem B". If ρ_{AB} is the joint state, then $\rho_A := \mathrm{tr}_B(\rho_{AB})$ is exactly the state that reproduces all measurement statistics of observables acting only on A. This is the formal meaning of *local* reasoning: local predictions depend only on the reduced state.

Lemma 1.21. *The partial trace is linear and satisfies:*

(i) (Tensor rule) $\mathrm{tr}_B(A \otimes B) = \mathrm{tr}(B)\, A$ *for all* $A \in \mathcal{L}(\mathcal{H}_A)$, $B \in \mathcal{L}(\mathcal{H}_B)$.

(ii) (Trace preservation) $\mathrm{tr}(\mathrm{tr}_B(M)) = \mathrm{tr}(M)$ *for all* $M \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

(iii) (Positivity) If $M \sqsupseteq 0$*, then* $\mathrm{tr}_B(M) \sqsupseteq 0$.

Lemma 1.22. *If* ρ_{AB} *is a density operator on* $\mathcal{H}_A \otimes \mathcal{H}_B$*, then* $\rho_A := \mathrm{tr}_B(\rho_{AB})$ *and* $\rho_B := \mathrm{tr}_A(\rho_{AB})$ *are density operators on* $\mathcal{H}_A$ *and* $\mathcal{H}_B$*, respectively. If* ρ_{AB} *is a partial density operator, then so are* ρ_A *and* ρ_B.

Entanglement A joint state ρ_{AB} is a *product state* if it equals $\rho_A \otimes \rho_B$. Many joint states are not of this form; they exhibit correlations that cannot be reduced to independent local descriptions. In particular, a *pure* joint state can have *mixed* reduced states. This is the basic structural reason why local program reasoning is subtle: even if an operation acts only on subsystem A, its effect on global assertions may depend on correlations with B, and conversely, local assertions about A may require reasoning through tr_B. For more details on entanglement, one can refer to any standard quantum computing textbook.

1.6 Quantum evolution

Definition 1.23 (Unitary channel)**.** Closed-system evolution is modelled by unitary conjugation. Let U be unitary on $\mathcal{H}$. The associated state transformation is $\rho \longmapsto U\rho U^\dagger$.

Lemma 1.24. *If* $\rho \sqsupseteq 0$*, then* $U\rho U^\dagger \sqsupseteq 0$*. Moreover,* $\mathrm{tr}(U\rho U^\dagger) = \mathrm{tr}(\rho)$*, so unitary evolution maps density operators to density operators, and partial density operators to partial density operators with the same trace.*

1.7 Superoperators / quantum operations

Definition 1.25. Programs and open-system dynamics are modelled by *superoperators*, i.e. linear maps on operators. A *superoperator* (or *quantum transformation*) on $\mathcal{H}$ is a linear map

$$\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}).$$

Definition 1.26. A superoperator $\mathcal{E}$ is:

positive if $\rho \sqsupseteq 0 \Rightarrow \mathcal{E}(\rho) \sqsupseteq 0$.

completely positive (CP) if for every auxiliary Hilbert space $\mathcal{K}$, the extension $\mathbf{1}_{\mathcal{L}(\mathcal{K})} \otimes \mathcal{E}$ is positive on $\mathcal{L}(\mathcal{K} \otimes \mathcal{H})$.

Complete positivity is the mathematically correct notion of "physical" positivity: it guarantees that applying $\mathcal{E}$ to a subsystem of a larger (possibly entangled) system still yields a valid (PSD) global operator.

Definition 1.27. A superoperator $\mathcal{E}$ is:

trace-preserving (TP) if $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\rho)$ for all $\rho \sqsupseteq 0$.

trace-nonincreasing (TNI) if $\mathrm{tr}(\mathcal{E}(\rho)) \leq \mathrm{tr}(\rho)$ for all $\rho \sqsupseteq 0$.

A *quantum operation* is a superoperator that is CP and TNI. We write $\mathrm{QO}(\mathcal{H})$ for the set of quantum operations on $\mathcal{H}$.

Lemma 1.28. *Quantum operations are closed under composition and tensoring with identities:*

(i) If $\mathcal{E}, \mathcal{F} \in \mathrm{QO}(\mathcal{H})$, then $\mathcal{F} \circ \mathcal{E} \in \mathrm{QO}(\mathcal{H})$.

(ii) If $\mathcal{E} \in \mathrm{QO}(\mathcal{H})$ and $\mathcal{K}$ is any Hilbert space, then $\mathbf{1}_{\mathcal{L}(\mathcal{K})} \otimes \mathcal{E} \in \mathrm{QO}(\mathcal{K} \otimes \mathcal{H})$.

Theorem 1.29 (Kraus representation)**.** *A superoperator $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is completely positive iff there exist operators $E_1, \ldots, E_m \in \mathcal{L}(\mathcal{H})$ such that for all $\rho \in \mathcal{L}(\mathcal{H})$,*

$$\mathcal{E}(\rho) \;=\; \sum_{k=1}^{m} E_k \rho E_k^{\dagger}.$$

Any such family $\{E_k\}$ is called a Kraus family *for $\mathcal{E}$.*

Lemma 1.30. *Suppose $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^{\dagger}$. Then:*

(i) $\mathcal{E}$ is TP iff $\sum_k E_k^{\dagger} E_k = \mathbf{1}$.

(ii) $\mathcal{E}$ is TNI iff $\sum_k E_k^{\dagger} E_k \sqsubseteq \mathbf{1}$.

Definition 1.31 (Heisenberg dual (adjoint) superoperator)**.** For a superoperator $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, its *dual* (or *adjoint*) $\mathcal{E}^* : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is defined by

$$\mathrm{tr}\big(A\,\mathcal{E}(\rho)\big) \;=\; \mathrm{tr}\big(\mathcal{E}^*(A)\,\rho\big) \quad \text{for all } A, \rho \in \mathcal{L}(\mathcal{H}).$$

Lemma 1.32. *If $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^{\dagger}$, then*

$$\mathcal{E}^*(A) \;=\; \sum_k E_k^{\dagger} A E_k.$$

Moreover, $\mathcal{E}$ is TP iff $\mathcal{E}^*(\mathbf{1}) = \mathbf{1}$, and $\mathcal{E}$ is TNI iff $\mathcal{E}^*(\mathbf{1}) \sqsubseteq \mathbf{1}$.

1.8 Measurements

Measurements are inherently probabilistic and, in general, disturb the state. In the operator formalism, the most common presentation uses a family of *measurement operators* (Kraus operators indexed by outcomes), which simultaneously encode both outcome probabilities and post-measurement states.

Definition 1.33. A (finite-outcome) *measurement* on $\mathcal{H}$ is given by operators $\{M_m\}_{m\in\mathcal{M}} \subseteq \mathcal{L}(\mathcal{H})$ satisfying the completeness relation

$$\sum_{m\in\mathcal{M}} M_m^\dagger M_m \;=\; \mathbf{1}.$$

Given an input (partial) state $\rho \sqsupseteq 0$, define:

the (subnormalized) *post-measurement state for outcome* m as $\rho_m \;:=\; M_m \rho M_m^\dagger$,

the *probability of outcome* m (if $\mathrm{tr}(\rho) = 1$) as $p(m) \;:=\; \mathrm{tr}(\rho_m) \;=\; \mathrm{tr}(M_m^\dagger M_m\, \rho)$,

the *normalized conditional state* (when $p(m) > 0$) as $\rho \mid m \;:=\; \frac{\rho_m}{\mathrm{tr}(\rho_m)}$.

The family of maps $\mathcal{I}_m(\rho) := M_m \rho M_m^\dagger$ is called a (quantum) *instrument.*

Lemma 1.34. *For each outcome m, the map $\mathcal{I}_m(\rho) = M_m \rho M_m^\dagger$ is completely positive and trace-nonincreasing. Moreover, the nonselective map*

$$\mathcal{I}(\rho) \;:=\; \sum_{m\in\mathcal{M}} \mathcal{I}_m(\rho) \;=\; \sum_m M_m \rho M_m^\dagger$$

is completely positive and trace-preserving. Hence, each branch of a measurement is a quantum operation, and the overall measurement process is a quantum channel.

Definition 1.35. Given measurement operators $\{M_m\}$, define the associated *effects* (POVM elements) $E_m \;:=\; M_m^\dagger M_m$. Then $E_m \sqsupseteq 0$ and $\sum_m E_m = \mathbf{1}$.

Definition 1.36. A *projective measurement* is given by a family of projections $\{P_m\}_{m\in\mathcal{M}}$ such that

$$P_m P_{m'} = \delta_{mm'} P_m, \qquad \sum_{m\in\mathcal{M}} P_m = \mathbf{1}.$$

Projective measurements correspond to yes/no tests or sharp multi-outcome decompositions into orthogonal subspaces. It is the special case of Definition 1.33 with $M_m := P_m$.

Lemma 1.37. *Let $\{P_m\}$ be a projective measurement and $\rho \sqsupseteq 0$. Then the branch state is $\rho_m = P_m \rho P_m$, with probability $p(m) = \mathrm{tr}(P_m \rho)$, and the normalized conditional state is $\rho \mid m = \rho_m / \mathrm{tr}(\rho_m)$ when $p(m) > 0$.*

1.9 Quantum predicates / assertions

One common notion of quantum predicate is an *effect*, i.e. a positive operator bounded by the identity. This is the D'Hondt–Panangaden style widely used in expectation-based quantum Hoare logic and in the CoqQ tradition.

Definition 1.38. An *effect predicate* on $\mathcal{H}$ is an operator $P \in \mathcal{L}(\mathcal{H})$ such that $0 \sqsubseteq P \sqsubseteq \mathbf{1}$.

Definition 1.39. Given an effect predicate P and a (partial) state $\rho \sqsupseteq 0$, define its *degree of satisfaction* as

$$[\![P]\!](\rho) \;:=\; \mathrm{tr}(P\rho).$$

When ρ is normalized, $\mathrm{tr}(P\rho) \in [0, 1]$.

The quantity $\mathrm{tr}(P\rho)$ is the probability of obtaining the "yes" outcome when performing the two-outcome POVM $\{P, \mathbf{1} - P\}$ on ρ (or equivalently, the expected value of the observable P when $0 \sqsubseteq P \sqsubseteq \mathbf{1}$). Thus effects provide a *graded* notion of truth: predicates hold to a certain extent rather than as a strict yes/no.

Definition 1.40. For effects P, Q, define *entailment* by Löwner order:

$$P \models Q \iff P \sqsubseteq Q.$$

Lemma 1.41. *For Hermitian P, Q, the following are equivalent:*

(i) $P \sqsubseteq Q$.

(ii) $\mathrm{tr}(P\rho) \leq \mathrm{tr}(Q\rho)$ *for all density operators* ρ.

In particular, if P, Q are effects, then $P \sqsubseteq Q$ means Q is at least as satisfied as P in every state.

Some presentations (including CoqQ-style developments) allow *general* linear operators as assertions for algebraic convenience, and then interpret the physically meaningful cases by restricting to Hermitian operators or effects. The expectation-based satisfaction $\mathrm{tr}(P\rho)$ is physically interpretable exactly when P is Hermitian, and bounded in $[0, 1]$ exactly when P is an effect.

A second notion of predicate is a *projection*, equivalently a subspace. This yields a *boolean* satisfaction relation based on support inclusion.

Definition 1.42. A *sharp predicate* on $\mathcal{H}$ is a projection $P \in \mathcal{L}(\mathcal{H})$ (i.e. $P = P^\dagger = P^2$). We identify such a predicate with its range subspace $\mathrm{Ran}(P) \subseteq \mathcal{H}$.

Definition 1.43. Let $\rho \sqsupseteq 0$ and let P be a projection. Define

$$\rho \models P \iff \mathrm{supp}(\rho) \subseteq \mathrm{Ran}(P).$$

This satisfaction relation is *qualitative*: either the state is entirely supported inside the predicate subspace, or not. Operationally, $\rho \models P$ means that a projective test of P succeeds with certainty: indeed $\rho \models P$ iff $P\rho P = \rho$ (Lemma 1.17). Thus projection predicates capture "hard" guarantees and are well suited for reasoning about assertions that should never fail.

Definition 1.44 (Logical operations in the projection lattice)**.** Let P, Q be projections (identified with their range subspaces). Define:

Negation: $\neg P := P^\perp := \mathbf{1} - P$ (projection onto the orthogonal complement).

Conjunction: $P \wedge Q$ is the projection onto $\mathrm{Ran}(P) \cap \mathrm{Ran}(Q)$.

Disjunction: $P \vee Q$ is the projection onto $\mathrm{span}\big(\mathrm{Ran}(P) \cup \mathrm{Ran}(Q)\big)$.

Theorem 1.45 (Projection predicates form an orthomodular lattice)**.** *The set of projections on $\mathcal{H}$, ordered by range inclusion (equivalently $P \leq Q$ iff $PQ = P$), forms an orthomodular lattice with operations $\neg, \wedge, \vee$ as in Definition 1.44.*

The benefit of projection predicates is their close alignment with implementable yes/no tests and with support calculus. In particular, projection connectives mirror the support identities from Section 1.4: support of a sum corresponds to "or" (span), and support inclusion corresponds to certainty of a projective test.

Lemma 1.46. *If P is a projection, then P is an effect: $0 \sqsubseteq P \sqsubseteq \mathbf{1}$. Moreover, projections are exactly the* idempotent *effects: if $0 \sqsubseteq E \sqsubseteq \mathbf{1}$ and $E^2 = E$, then E is a projection.*

Lemma 1.47 (Certainty equivalences for projections)**.** *Let P be a projection and ρ a density operator. Then the following are equivalent:*

$$\rho \models P \iff P\rho P = \rho \iff \mathrm{tr}(P\rho) = 1.$$

This gives a clean translation rule: projection-based satisfaction can be phrased in expectation language as "satisfied with probability one", but it is often algebraically easier to reason via support, especially for under-approximation and disjunction reasoning.

1.10 Under-approximation and reachability

Classical Incorrectness Logic (IL) is designed to reason about *reachability* of bad outcomes: an incorrectness triple under-approximates what the program *can* do. In the quantum setting, one might try to mimic this by describing "bad states" using predicates and requiring that some reachable state *satisfies* the bad predicate.

A key obstacle emphasized in QIL-style reasoning is that quantum program execution naturally produces *mixtures* (convex combinations) of states: branching, measurement, and nondeterministic choice lead to density operators that aggregate multiple behaviors into one operator. For projection-based (boolean) satisfaction $\rho \models P$, this aggregation can be too coarse for bug-catching: even if some bad branch exists, the overall mixture may fail to satisfy a predicate that was intended to describe that bad branch, simply because satisfaction requires *support inclusion* and therefore behaves like a "for all components" condition.

Intuitively: boolean satisfaction $\rho \models P$ expresses a *universal* guarantee ("the state is entirely inside P"). But bug-catching is existential: we want to certify that *some* bad behavior is possible. This explains the need for *under-approximation*; we want to express that the state has at least some component in P, rather than being entirely contained in P.

Definition 1.48. Let $\rho \sqsupseteq 0$ be a (partial) density operator on $\mathcal{H}$, and let P be a projection on $\mathcal{H}$. We say that P *under-approximates* ρ, written

$$P \preceq \rho,$$

if

$$\mathrm{Ran}(P) \subseteq \mathrm{supp}(\rho).$$

Equivalently, $P \preceq \rho$ iff $\Pi_\rho P = P$ (i.e. the support projector of ρ contains P).

The relation $P \preceq \rho$ should be read as: *the state ρ has at least the behaviors contained in subspace P*. This is an existential-style statement: ρ carries nonzero weight on every direction in $\mathrm{Ran}(P)$. In contrast, boolean satisfaction $\rho \models P$ means $\mathrm{supp}(\rho)$ is contained in P (a universal-style statement).

Lemma 1.49. *For $\rho \sqsupseteq 0$ and projection P, the following are equivalent:*

(i) $P \preceq \rho$.

(ii) $\mathrm{Ran}(P) \subseteq \mathrm{Ran}(\rho)$.

(iii) $P = \Pi_\rho P = P\Pi_\rho$.

(iv) $\mathrm{supp}(P) \subseteq \mathrm{supp}(\rho)$ *(viewing P itself as PSD).*

Lemma 1.50 (Monotonicity)**.** *Let $\rho, \sigma \sqsupseteq 0$ and let P, Q be projections.*

(i) If $P \leq Q$ (i.e. $\mathrm{Ran}(P) \subseteq \mathrm{Ran}(Q)$*) and $Q \preceq \rho$, then $P \preceq \rho$.*

(ii) If $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$ *and $P \preceq \rho$, then $P \preceq \sigma$.*

1.11 Connectives under under-approximation

Projection connectives behave differently under under-approximation than under boolean satisfaction.

Lemma 1.51. *Let $\rho_1, \rho_2 \sqsupseteq 0$ and let $\rho := \rho_1 + \rho_2$ (in particular, this covers convex mixtures up to scaling). Then for any projection P,*

$$P \preceq \rho \quad \Longleftrightarrow \quad \mathrm{Ran}(P) \subseteq \mathrm{supp}(\rho_1) + \mathrm{supp}(\rho_2) \quad \Longleftrightarrow \quad P \leq (\Pi_{\rho_1} \vee \Pi_{\rho_2}).$$

Equivalently, $P \preceq \rho$ means that every direction in P is reachable from some *component of the mixture, in the precise sense that P lies under the join of the component support projections.*

This lemma formalizes the intuition that mixtures represent "either branch may happen", so the *support* of a mixture is the span (join) of the branch supports (Lemma 1.19). Under-approximation turns this into a compositional rule: to show P is achievable from a mixture, it suffices to show P lies inside the span of supports of reachable components.

Lemma 1.52 (Conjunction/disjunction under under-approximation)**.** *Let $\rho \succeq 0$ and let P, Q be projections.*

(i) If $P \preceq \rho$ (or $Q \preceq \rho$), then $(P \wedge Q) \preceq \rho$. In particular, $P \preceq \rho$ and $Q \preceq \rho$ imply $(P \wedge Q) \preceq \rho$.

(ii) $(P \vee Q) \preceq \rho \iff \big(P \preceq \rho \ \wedge \ Q \preceq \rho\big)$.

Moreover, $(P \wedge Q) \preceq \rho$ does not imply $P \preceq \rho$ or $Q \preceq \rho$ in general.

Lemma 1.53. *Let $\rho \sqsupseteq 0$ and P a projection. In general, $P \preceq \rho$ does* not *imply $(\mathbf{1} - P) \not\preceq \rho$, and vice versa.*

1.12 Achieving

QIL-style reasoning treats program outcomes as sets (or distributions) of reachable partial states, often aggregated into a single (subnormalized) density operator representing the "accumulated" reachable mass.

At the prerequisites level (before full operational semantics), the key conceptual move is: a predicate is *achievable* if it under-approximates some mixture of reachable states.

Definition 1.54. Fix a program c and an initial state ρ. Let $\mathsf{Reach}(c, \rho)$ denote a collection of (partial) density operators representing states reachable along terminating exits (or along designated observation points), and let ρ_{mix} be any (subnormalized) mixture of these reachable operators, for instance a finite sum of the form $\rho_{\text{mix}} = \sum_i \rho_i$ with $\rho_i \in \mathsf{Reach}(c, \rho)$. A projection predicate Q is *achievable* from (c, ρ) if

$$Q \preceq \rho_{\text{mix}} \quad \text{for some such mixture } \rho_{\text{mix}}.$$

This definition isolates the idea that incorrectness logic is about *under-approximating* the set of behaviors a program can exhibit. The details of $\mathsf{Reach}(c, \rho)$ and what counts as an "exit" depend on the program semantics to be introduced later, but the algebraic shape is stable: reachability information composes by (subnormalized) summation/mixture, and claims about achievable predicates are expressed via support inclusion in the *reverse* direction.

Lemma 1.55. *If $Q \preceq \rho_{\text{mix}}$ and $\operatorname{supp}(\rho_{\text{mix}}) \subseteq \operatorname{supp}(\rho'_{\text{mix}})$, then $Q \preceq \rho'_{\text{mix}}$. In particular, adding additional reachable components to a mixture cannot invalidate an achievability claim.*

1.13 Wrap-up

The prerequisites above support two complementary tracks that we will develop in subsequent sections/papers.

Quantum Hoare Logic / CoqQ track. We will treat (partial) density operators as program states (Definition 1.11), and program commands as quantum operations, i.e. CP/TNI superoperators (Definition 1.27) with Kraus representations (Theorem 1.29). Assertions will primarily be effects $0 \sqsubseteq P \sqsubseteq \mathbf{1}$ (Definition 1.38), interpreted quantitatively via expectation $\operatorname{tr}(P\rho)$ (Definition 1.39), and ordered by Löwner entailment $P \sqsubseteq Q$ (Definition 1.40). This setup naturally supports weakest-precondition reasoning via the dual superoperator $\mathcal{E}^*$.

Quantum Incorrectness Logic track. We will treat sharp predicates as projections/subspaces (Definition 1.42) and reason using support $\mathrm{supp}(\rho)$ (Definition 1.15) and its calculus (Lemmas 1.18–1.19). Boolean satisfaction $\rho \models P$ (Definition 1.43) captures certainty, while incorrectness/reachability reasoning uses the under-approximation relation $P \preceq \rho$ (Definition 1.48) and its connective behavior under mixtures (Lemma 1.51). This separates “can happen” statements from “must hold” statements in a way that is robust under quantum mixing.