Introduction to Quantum Computing Ideas

Sai Vinjanampathy
Department of Physics, IIT Bombay

August 4, 2025

1 States and Transformations in Quantum Mechanics

1. $|\psi\rangle$: Quantum state as an example of a state.
   Other classical examples: (x, p), (P, V), etc.

   In physics, a **state** refers to a complete specification of a system at a given moment of time. This specification should contain enough information to determine how the system will evolve (in principle), according to the governing physical laws.
   For example, in classical physics, states are described using measurable quantities such as:

   - **Classical mechanics:** The state of a particle is described by its position and momentum (x, p).
   - **Thermodynamics:** A macroscopic system such as an ideal gas can be described by variables like pressure and volume (P, V).

2. Transformations are dynamics, dictated by linearity and symmetry.

3. Why linear? Stern–Gerlach, Young's Double-Slit Experiment, etc.
   Note:*Not* all linear theories are quantum mechanical.

4.

$$|\psi\rangle \to |\phi\rangle \quad \Rightarrow \quad |\phi\rangle = U\,|\psi\rangle \quad \text{From linearity} \tag{1}$$

5. Inner product preservation:

$$\langle\psi|\psi\rangle = \langle\phi|\phi\rangle \tag{2}$$

   This conditions stems from probability conservation (like in chemical reactions, mass is preserved). Equation (1) implies,

$$U^\dagger U = UU^\dagger = \mathbb{1} \tag{3}$$

6. In algebra, U is called a **unitary operator**.
   Lie group: $\mathrm{U}(N)$ — the unitary group.

7. In quantum computing: U represents all state transformations.
   U is composed of "primitive unitaries" called **gates**.

8. **Properties of Unitary Operators:**
   (a) $U^\dagger U = \mathbb{1}$.
   (b) $U = \exp[\text{anti-Hermitian matrix}]$.
   (c) Anti-Hermitian $= iH$, where $H^\dagger = H$ (i.e., H is Hermitian: Hamiltonian).
   (d) H has real eigenvalues and orthonormalizable eigenvectors.
   (e) Time evolution:

   $$U = \exp\left(-\frac{iHt}{\hbar}\right) \quad \text{(compact Lie groups)} \tag{4}$$

   Do a Taylor series expansion.
   (f) Note: For $H = \omega\hat{n} + g\hat{x}$, where $\hat{n}$ and $\hat{x}$ are number operator and position operator respectively, the group is **non-compact**.
   (g) Products of unitaries is unitary:

   $$U_1 \cdot U_2 \cdot U_3 \cdot \cdots \cdot U_n \in \mathcal{U}(N) \quad \text{if} \quad U_i \in \mathcal{U}(N) \tag{5}$$

   (h) Sum of Hermitian operators is Hermitian.
   This is helpful since if $H = \sum_i h_i$, $h_i^\dagger = h_i$, then,

   $$U = e^{iH} \in \mathcal{U}(N) \tag{6}$$

   (i) Unitary operators don't commute!

   $$U_1 U_2 \neq U_2 U_1 \tag{7}$$

   Proof: Let

   $$U_1 = e^{-i\theta H_1}, \quad U_2 = e^{-i\theta H_2} \tag{8}$$

   For small θ, do a Taylor series expansion and convince yourself that the two expressions are non-identical.

9. **Baker–Campbell–Hausdorff Lemma.**
   BCH asserts that,

   $$\mathcal{U} = e^{-i\theta A} B e^{i\theta A} = B - i\theta[A, B] + \frac{\theta^2}{2!}[A, [A, B]] + \ldots \tag{9}$$

   See Zassenhaus Formula.

10. As an application of the previous point, consider **Unitary frame (rotating frame, etc.)**
Consider the time-dependent Schrödinger equation (TDSE),

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle \tag{10}$$

Task: I want to write an equation for $|\varphi(t)\rangle = U(t)|\psi(t)\rangle$
Ans: Let,

$$|\varphi(t)\rangle = U(t)|\psi(t)\rangle \tag{11}$$

Differentiating the transformed state:

$$\begin{aligned}\partial_t|\varphi(t)\rangle &= (\partial_t U(t))|\psi(t)\rangle + U(t)\partial_t|\psi(t)\rangle \\ &= \dot{U}|\psi(t)\rangle - \frac{i}{\hbar}U(t)H(t)|\psi(t)\rangle \\ &= \dot{U}\underbrace{U^\dagger U}_{\mathbb{1}}|\varphi(t)\rangle - \frac{i}{\hbar}U(t)H(t)\underbrace{U^\dagger(t)U(t)}_{\mathbb{1}}|\varphi(t)\rangle \\ &= \left(\dot{U}U^\dagger - \frac{i}{\hbar}UHU^\dagger\right)|\varphi(t)\rangle\end{aligned}$$

So,

$$i\hbar\frac{d}{dt}|\varphi(t)\rangle = i\hbar\left(\dot{U}U^\dagger - \frac{i}{\hbar}UHU^\dagger\right)|\varphi(t)\rangle = \left(i\hbar\dot{U}U^\dagger + UHU^\dagger\right)|\varphi(t)\rangle \tag{12}$$

Define the new Hamiltonian in the rotating frame as,

$$X(t) = UHU^\dagger + i\hbar\dot{U}U^\dagger \tag{13}$$

The first term in the RHS of equation (13) is usually of the form $\boxed{e^{-i\theta A}He^{i\theta A}}$.

11. Counting principles and unitary operators.

    Let $U \in \mathcal{U}(N)$.
    Qn 1: How many "free elements" are in U?

    Counting degrees of freedom for 2×2 unitary matrices:

    Let

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{14}$$

Since a, b, c, d are complex, we have $4 \times 2 = 8$ real parameters.

Imposing unitarity: $U^\dagger U = \mathbb{1}$:

$$U^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}, \quad U^\dagger U = \begin{pmatrix} |a|^2 + |c|^2 & a^*b + c^*d \\ ab^* + cd^* & |b|^2 + |d|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{15}$$

This gives 4 constraints,

$$\begin{aligned} |a|^2 + |c|^2 &= 1 \\ |b|^2 + |d|^2 &= 1 \\ \mathrm{Re}(ac^* + bd^*) &= 0 \\ \mathrm{Im}(ac^* + bd^*) &= 0 \end{aligned}$$

So, total free parameters $= 8 - 4 = 4$ real parameters.

Also, for SU(2) (special unitary group), we impose:

$$\det U = ad - bc = +1 \tag{16}$$

which imposes 1 more constraint, leaving us with **3 real parameters**.

Thus, a general 2×2 unitary matrix can be expressed as a linear combination of Pauli matrices,

$$U = a\,\mathbb{1} + b \underbrace{\sigma_x}_{\sigma_1} + c \underbrace{\sigma_y}_{\sigma_2} + d \underbrace{\sigma_z}_{\sigma_3} \tag{17}$$

where,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{18}$$

These are Hermitian and unitary (up to phases), and they form a basis for 2×2 matrices.
From $U^\dagger U = 1$, we get,

$$a^2 + b^2 + c^2 + d^2 = 1 \tag{19}$$

This gives 3 independent real parameters if $a, b, c, d \in \mathbb{R}^1$.

In general, any Hermitian operator U can be expanded as:

$$U = \sum_i u_i \hat{O}_i \quad \text{where} \quad \hat{O}_i = \hat{O}_i^\dagger \tag{20}$$

with $\hat{O}_i$ forming a basis of Hermitian operators:

- Real symmetric part: $\dfrac{N(N+1)}{2}$ operators

- Real antisymmetric $\times i$: $\dfrac{N(N-1)}{2}$ operators

Total $= N^2$ operators. The expansion in equation (20) is known as the **Fano representation**.

12. **Bloch sphere representation**

Let

$$U = \begin{pmatrix} \cos\theta & \sin\theta\, e^{i\phi} \\ \sin\theta\, e^{-i\phi} & -\cos\theta \end{pmatrix} \tag{21}$$

Check unitarity:

$$U^\dagger U = \begin{pmatrix} c & s_+ \\ s_- & -c \end{pmatrix} \begin{pmatrix} c & s_+ \\ s_- & -c \end{pmatrix} = \begin{pmatrix} c^2 + s_+ s_- & cs_+ - s_+ c \\ cs_- - cs_- & s_- s_+ + c^2 \end{pmatrix} \tag{22}$$

(where $c = \cos\theta$, $s_\pm = \sin\theta e^{\pm i\phi}$)

Also, a general qubit state on the Bloch sphere,

$$U\,|0\rangle = \begin{pmatrix} s_+ \\ -c \end{pmatrix} = -[c_\theta\,|0\rangle - e^{i\phi} s_\theta\,|1\rangle] \tag{23}$$

Note: The Bloch sphere geometrically represents pure qubit states as points on the unit 2-sphere.

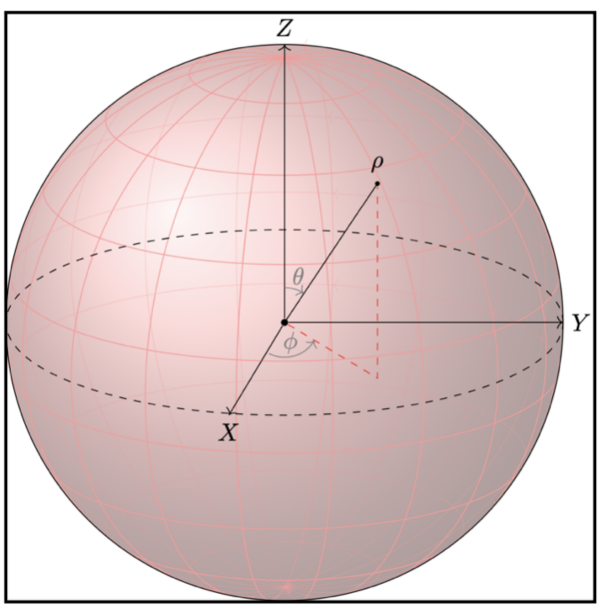


Figure 1: Bloch sphere

13. **Unitary Composed from Hamiltonians**

    Same question as "restricted unitaries".

    Consider the Hamiltonian,

$$H = \omega \sigma_z \tag{24}$$

    Question: Does this generate **all** unitaries on the Bloch sphere?

    Answer: No!
    Because $e^{i\theta\sigma_z}$ only generates a $U(1)$ *subgroup* of $SU(2)$!

    Takeaway: You cannot generate all unitaries if your Hamiltonian only spans a subgroup of SU(2).

    Real takeaway: We need the notion of *subgroups*.

14. **Bipartite unitaries: Tensor products**

    To write unitaries for two-qubit systems, you must work with **tensor products**.

    Tensor product: If A is an $m \times n$ matrix and B is a $p \times q$ matrix, the tensor (Kronecker) product $A \otimes B$ is an $mp \times nq$ matrix defined as,

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}. \tag{25}$$

    Linearity and tensor product structure: Linearity and the presence of more than one system (e.g., qubits or subsystems or atom) **demand tensor product structure**. The reason is that you can always ignore one subsystemn (atom),

$$\langle\psi_A| \otimes \langle\psi_B| (X_A \otimes 1_B) |\psi_A\rangle \otimes |\psi_B\rangle = \underbrace{\langle\psi_A| X_A |\psi_A\rangle}_{\text{Measured on } A} \cdot \underbrace{\langle\psi_B|\psi_B\rangle}_{\text{Did nothing on } B} \tag{26}$$

    Decomposition of Unitaries on Bipartite Systems:

    You can check that any unitary $\mathcal{U}$ acting on bipartite systems (A and B) can be expanded as:

$$\mathcal{U} = U_0 \, \mathbb{1}^A \otimes \mathbb{1}^B + \vec{a} \cdot \vec{O}^A \otimes \mathbb{1}^B + \mathbb{1}^A \otimes \vec{b} \cdot \vec{O}^B + \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} T_{ij} \, \hat{O}_i^A \otimes \hat{O}_j^B \tag{27}$$

    Here:

    - $\vec{O}^A = (\sigma_x, \sigma_y, \sigma_z)$ for qubits

- $\vec{O}^B$ can be generalized (e.g., Gell-Mann matrices for qutrits)

Generalization to multipartite systems:

$$\hat{O}_i^A \otimes \hat{O}_j^B \otimes \hat{O}_k^C \otimes \cdots \tag{28}$$

Example:

$$\vec{O}^A = (\sigma_x, \sigma_y, \sigma_z), \quad \vec{O}^B = \text{Gell-Mann matrices (8 operators)} \tag{29}$$

15. **Gate Composition of Unitary Operators**

   (a) In quantum computing (QC), we want the initial state to hold some "data" $|\psi_0\rangle$.

   (b) We want to "compute" it by unitary $U|\psi_0\rangle$, and reading some answer from it.

   (c) Why do we want to do this?
   Answer: Computational Complexity Hierarchy.

   Motivation includes:

   - Understanding which problems are in P, NP, BQP, etc.
   - Prime factorization is in BQP (known example of quantum advantage).
   - Connections to "Extended Church-Turing Hypothesis."

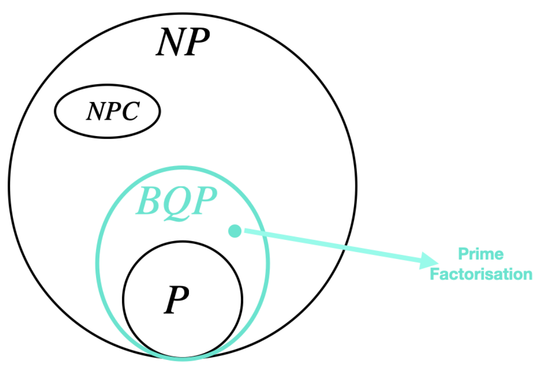


Figure 2: Complexity classes

   (d) The unitary U is an arbitrary element of $SU(2^n)$.
   We already know that we should not get stuck in subgroups!

   (e) But from the viewpoint of CS engineers, the Hamiltonian models are not standardized. They want "standard gates" that you can apply to get anything.

   (f) In classical electronics, the example is NAND and XOR gates.

→ In physics, we would answer the question of universality as:

"Arbitrary single-qubit rotations" + "One two-qubit gate".

→ In quantum computing, the answer is more subtle.

Hadamard Gate (H)

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

Pauli-X Gate (X)

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

Pauli-Y Gate (Y)

$$Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

Pauli-Z Gate (Z)

$$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

Phase Gate (S)

$$S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

$\pi/8$ **Gate (T)**

$$T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$
$$|[innersep = 4pt, minimumwidth = 1.5pt, minimumheight = 1.5pt]|$$

A universal gate set is given by,

$$\{H, S, \text{CNOT}\} + T \quad \text{(Other choices exist!)} \tag{30}$$

(e) **(H, S, T, CNOT) in detail:**

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & \sigma_x \end{pmatrix} \tag{31}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

This is a crucial step in an interferometer.

$$S^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

$$HZH = X \quad \text{and so forth.} \tag{32}$$

Comments:

1. H, S, CNOT generate the Pauli group:

$$\mathcal{P} = \{\pm 1, \pm i\} \times \{X, Y, Z\} \tag{33}$$

2. The Clifford group $\mathcal{C}$ normalizes $\mathcal{P}$:

$$(U \in \mathcal{C}) \quad \Rightarrow \quad \forall P_i \in \mathcal{P}, \quad UP_iU^\dagger \in \mathcal{P} \tag{34}$$

3. Clifford circuits generate **volume law** entanglement.

4. Clifford circuits are easy to **"track"** $\Rightarrow$ Stabilizer eigenvalues.

5. Adding T gates makes circuits classically difficult to simulate.

6. Good reference: Daniel Gottesman's book *"How to Survive the Classical World as a Quantum Computer"*.

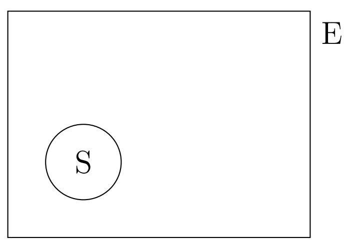
   Available online and free.

2 Lecture II: Open Quantum Systems

1.
$$\ddot{q} + \gamma \dot{q} + \omega_0^2 q = 0 \tag{35}$$
where γ is a phenomenological damping parameter.

2. Same with QM, but a bit subtle.
$$\begin{aligned} \dot{q} &= p \\ \dot{p} &= -\gamma p - \omega_0^2 q \end{aligned} \tag{36}$$
Let's look at the commutation relation.
$$\begin{aligned} [q,p] = i\hbar \quad \Rightarrow \quad & \frac{\mathrm{d}}{\mathrm{d}t}[q,p] = -\gamma[q,p] \\ & \Rightarrow [q(t),p(t)] = e^{-\gamma t}[q(0),p(0)] = e^{-\gamma t} i\hbar \end{aligned}$$
$\Rightarrow$ "Decays" canonical commutation relation, which is clearly a nonsense.

3. System-Environment Approach



$$\begin{aligned} |\psi_{SE}\rangle &= \sum_{i,j} C_{ij}\, |i\rangle \otimes |j\rangle \\ C &= U_{i\alpha}\lambda_{\alpha\alpha}V_{\alpha j} \quad , \quad \lambda \geq 0 \quad \text{(Singular Value Decomposition)} \\ |\psi_{SE}\rangle &= \sum_{\alpha} \lambda_\alpha\, |u_\alpha\rangle \otimes |v_\alpha\rangle \quad \text{(Schmidt coeffs.)} \end{aligned}$$
Entanglement exists if $\#\{\lambda_\alpha\} > 1$, i.e., there is **more than one non-zero Schmidt coefficient**.

$$\begin{aligned} \langle A_S\rangle &= \sum_{\alpha,\beta} \lambda_\alpha\lambda_\beta \langle u_\alpha|A|u_\beta\rangle\langle v_\alpha|v_\beta\rangle \\ &= \sum_\alpha \lambda_\alpha^2 \langle u_\alpha|A|u_\alpha\rangle \\ &= \mathrm{Tr}(A\rho) \quad (\text{where } \rho = \sum_\alpha \lambda_\alpha^2 |u_\alpha\rangle\langle u_\alpha|) \end{aligned} \tag{37}$$

Conjecture: Elevate $\hat{\rho}$ to a *fundamental object.*

4. How does $\hat{\rho}$ *transform*?

2.1 Kraus Operators and Stinespring Dilation from the System-Environment Approach

Consider a bipartite pure state of a system S and its environment E,

$$|\psi_{SE}\rangle = \sum_\alpha \lambda_\alpha |u_\alpha\rangle \otimes |v_\alpha\rangle \,, \tag{38}$$

where $\{\lambda_\alpha\}$ are the non-negative Schmidt coefficients, and $|u_\alpha\rangle$ and $|v_\alpha\rangle$ are orthonormal bases for $\mathcal{H}_S$ and $\mathcal{H}_E$ respectively. We assume that $|\psi_{SE}\rangle$ arises from a combined unitary evolution U_{SE} acting on a system-environment product state,

$$|\psi_{SE}\rangle = U_{SE}(|\psi\rangle_S \otimes |e_0\rangle_E), \tag{39}$$

where $|\psi\rangle_S$ is an arbitrary pure state of the system and $|e_0\rangle_E$ is a fixed pure state of the environment.

Tracing over the environment yields the reduced density matrix of the system,

$$\rho_S = \mathrm{Tr}_E\left[|\psi_{SE}\rangle\langle\psi_{SE}|\right] = \sum_\alpha \lambda_\alpha^2 |u_\alpha\rangle\langle u_\alpha| \,. \tag{40}$$

Entanglement exists if and only if more than one λ_α is non-zero.

Let us now describe how the system evolves when the environment is not observed. To do this, consider an orthonormal basis $|e_k\rangle$ for the environment's Hilbert space $\mathcal{H}_E$. We define a set of operators $\{K_k\}$—called **Kraus operators**—that act only on the system, by projecting the joint unitary U_{SE} onto the environment basis state $|e_k\rangle$,

$$K_k := \langle e_k|U_{SE}|e_0\rangle \,. \tag{41}$$

Intuitively, K_k tells us how the system evolves when the environment is found in the state $|e_k\rangle$ after interacting with it initially in state $|e_0\rangle$.

Using these operators, we can write the reduced evolution of the system (i.e., after tracing out the environment) as,

$$\mathcal{E}(\rho_S) = \sum_k K_k \rho_S K_k^\dagger. \tag{42}$$

This is the **operator-sum representation** or **Kraus representation** of the quantum channel $\mathcal{E}$. It describes a completely general evolution of a quantum system interacting unitarily with an environment that is initially uncorrelated with the system.

2.2 Stinespring Dilation

The Kraus representation of a quantum channel may seem abstract at first, but it has a deep and physically meaningful origin. This is formalized by the **Stinespring dilation theorem**, which provides a structural explanation for all completely positive, trace-preserving (CPTP) maps.

Theorem 1 (Stinespring Dilation)**.** *Let $\mathcal{E} : \mathcal{B}(\mathcal{H}_S) \to \mathcal{B}(\mathcal{H}_S)$ be a quantum channel. Then there exists:*

- *an auxiliary Hilbert space $\mathcal{H}_E$ (the* environment*),*
- *a pure state $|e_0\rangle \in \mathcal{H}_E$,*
- *and a unitary operator U_{SE} on $\mathcal{H}_S \otimes \mathcal{H}_E$,*

such that for any input state ρ_S of the system, the action of $\mathcal{E}$ can be written as

$$\mathcal{E}(\rho_S) = \mathrm{Tr}_E \left[U_{SE} \left(\rho_S \otimes |e_0\rangle\langle e_0| \right) U_{SE}^\dagger \right]. \tag{43}$$

This result tells us something remarkable: *any* quantum process—no matter how noisy or irreversible it seems—can always be seen as part of a larger, reversible unitary evolution, provided we allow the system to interact with an extended environment.

To see how this connects to the Kraus representation, suppose $\{|e_k\rangle\}$ is an orthonormal basis of $\mathcal{H}_E$. Then the partial trace over the environment can be evaluated as

$$\begin{aligned} \mathcal{E}(\rho_S) &= \sum_k \langle e_k| \, U_{SE} \left(\rho_S \otimes |e_0\rangle\langle e_0| \right) U_{SE}^\dagger \, |e_k\rangle \\ &= \sum_k \left(\langle e_k|U_{SE}|e_0\rangle \right) \rho_S \left(\langle e_k|U_{SE}|e_0\rangle \right)^\dagger . \end{aligned} \tag{44}$$

We define the Kraus operators K_k acting on $\mathcal{H}_S$ by

$$K_k := \langle e_k|U_{SE}|e_0\rangle \, , \tag{45}$$

so that the channel takes the familiar form:

$$\mathcal{E}(\rho_S) = \sum_k K_k \rho_S K_k^\dagger. \tag{46}$$

In summary, Stinespring dilation tells us that every quantum channel is physically realizable as a unitary evolution on a larger system. The Kraus operators arise directly by projecting the unitary U_{SE} onto the initial and final states of the environment. This provides an operational understanding of quantum dynamics.