41076: Methods in Quantum Computing

'Introduction to Quantum Mechanics' Module

Min-Hsiu Hsieh

Centre for Quantum Software & Information, Faculty of Engineering and Information Technology, University of Technology Sydney

Abstract

Contents to be covered in this lecture are

1. Linear algebra in Dirac notation;
2. Quantum postulates;
3. No-cloning theorem.

1 Linear Algebra in Dirac notation

The aim of this section is to let the readers be familiar with the notations used in the quantum community. In particular, we will adopt the bra-ket notation invented by Paul Dirac in 1939.

A d-dimensional Hilbert space $\mathcal{H}$ is a vector space equipped with an inner product. Let $\{\boldsymbol{e}_i\}_{i=0}^{d-1}$ be the computational basis, where $\boldsymbol{e_i}$ is a column vector of zeros except a '1' at the $(i+1)$-th entry. Any vector $\boldsymbol{v} \in \mathcal{H}$ can be expressed as

$$\boldsymbol{v} = \sum_{i=0}^{d-1} v_i \boldsymbol{e}_i, \tag{1}$$

for some complex number $v_i \in \mathbb{C}$. The inner product (or dot product) '$\cdot$' of two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in $\mathcal{H}$ is defined as

$$\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u}^\dagger \boldsymbol{v} = \sum_{i=0}^{d-1} u_i^* v_i, \tag{2}$$

where $\dagger$ denotes transpose and conjugate.

Now we are ready to introduce the bra-ket notation. Throughout this subject, we will denote $|i\rangle \equiv \boldsymbol{e}_i$ and write $\boldsymbol{v}$ as $|v\rangle$:

$$|v\rangle = \sum_{i=0}^{d-1} v_i |i\rangle. \tag{3}$$

The inner product of $|u\rangle$ and $|v\rangle$ in $\mathcal{H}$ becomes

$$\langle u|v\rangle = \sum_{i,j} u_i^* v_j \langle i|j\rangle = \sum_i u_i^* v_i \tag{4}$$

where $\langle u| \equiv |u\rangle^\dagger$ is now a row vector and $\langle i|j\rangle = \delta_{i,j}$.

For a Hilbert space $\mathcal{H}$, we denote $\mathcal{L}(\mathcal{H})$ the collection of linear operators $L : \mathcal{H} \to \mathcal{H}$. We denote the identity operator $I = \sum_{i=0}^{d-1} |i\rangle\langle i|$. Given an linear operator L, there is an equivalent matrix representation $[L_{i,k}]$ in the basis spanned by $\{|i\rangle\langle k|\}$:

$$L = \sum_{i,k=0}^{d-1} L_{i,k}|i\rangle\langle k|, \tag{5}$$

where $L_{i,k} = \langle i|L|k\rangle$.

An linear operator $H \in \mathcal{L}(\mathcal{H})$ is called *Hermitian* if and only if $H^\dagger = H$. For a Hermitian matrix H, the *spectral theorem* states that there exists an orthonormal basis $\{|\nu_i\rangle\}$ and real numbers $\{\lambda_i\} \in \mathbb{R}$ so that

$$H = \sum_i \lambda_i |\nu_i\rangle\langle\nu_i|. \tag{6}$$

Equivalently, $\{\lambda_i\}$ and $\{|\nu_i\rangle\}$ are known as eigenvalues and eigenvectors of H, respectively.

A Hermitian operator $P \in \mathcal{L}(\mathcal{H})$ is *positive*, denoted as $P \geq 0$, if and only if $\langle v|P|v\rangle \geq 0$ for all $|v\rangle \in \mathcal{H}$. We denote $\mathcal{L}(\mathcal{H})_+ = \{P \geq 0 : P \in \mathcal{L}(\mathcal{H})\}$ the set of positive semi-definite operators on $\mathcal{H}$.

Exercise 1. *Define the Hadamard product of two matrices $A, B \in \mathcal{L}(\mathcal{H})$:*

$$A \circ B = \sum_{i,j=0}^{d-1} A_{i,j}B_{i,j}|i\rangle\langle j|. \tag{7}$$

Show that if $A, B \in \mathcal{L}(\mathcal{H})_+$, then $A \circ B \in \mathcal{L}(\mathcal{H})_+$.

For any continuous function $f : \mathbb{R} \to \mathbb{R}$, we define the matrix function $f(H)$ on a Hermitian matrix H by

$$f(H) = \sum_i f(\lambda_i)|\nu_i\rangle\langle\nu_i|, \tag{8}$$

where H has the spectral decomposition in Eq. (6).

Exercise 2. *Let*

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Compute e^H.

We say f is *convex* if

$$f((1-p)A + pB) \leq (1-p)f(A) + pf(B) \tag{9}$$

for all Hermitian matrices A and B and for $0 \leq p \leq 1$. We say f is *monotone* if $f(A) \geq f(B)$ whenever $A \geq B$.

Exercise 3.

- *For $f(x) = \frac{1}{x}$, f is convex on $\mathcal{L}(\mathcal{H})_+$.*
- *For $f(x) = x^r$, f is convex on $\mathcal{L}(\mathcal{H})_+$ for $1 \leq r \leq 2$.*
- *For $f(x) = x^r$, f is monotone on $\mathcal{L}(\mathcal{H})_+$ for $0 \leq r \leq 1$.*
- *For $f(x) = x^3$, show that f is not convex on $\mathcal{L}(\mathcal{H})_+$ with an example.*

1.1 Tensor product of Hilbert spaces

Given two vectors $|u\rangle \in \mathcal{H}_A$ and $|v\rangle \in \mathcal{H}_B$, the tensor product '$\otimes$' of them is

$$|u\rangle \otimes |v\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} u_i v_j |i\rangle \otimes |j\rangle, \tag{10}$$

a vector of $d_A d_B$-dimension. If $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then $\{|i\rangle_A \otimes |j\rangle_B\}$, $i \in \{0, \cdots, d_A - 1\}$ and $j \in \{0, \cdots, d_B - 1\}$, forms an orthonormal basis in $\mathcal{H}_A \otimes \mathcal{H}_B$. The inner product on the space $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined by

$$(\langle v_2|_B \otimes \langle u_2|_A)(|u_1\rangle_A \otimes |v_1\rangle_B) = \langle u_2|u_1\rangle\langle v_2|v_1\rangle. \tag{11}$$

This definition extends to tensor product of linear operators in $\mathcal{L}(\mathcal{H})$:

$$\begin{aligned} L \otimes M &= \left(\sum_{i,j=0}^{d_A-1} L_{i,j}|i\rangle\langle j|\right) \otimes \left(\sum_{k,\ell=0}^{d_B-1} M_{k,\ell}|k\rangle\langle \ell|,\right) \\ &= \sum_{i,j=0}^{d_A-1} \sum_{k,\ell=0}^{d_B-1} L_{i,j} M_{k,\ell} |i\rangle\langle j| \otimes |k\rangle\langle \ell|. \end{aligned} \tag{12}$$

Useful properties of tensor product are summarised as follows.

1. $(A_1 \otimes \cdots \otimes A_k)(B_1 \otimes \cdots \otimes B_k) = (A_1 B_1 \otimes \cdots \otimes A_k B_k)$
2. $(A_1 \otimes \cdots \otimes A_k)^{-1} = A_1^{-1} \otimes \cdots \otimes A_k^{-1}$
3. $(A_1 \otimes \cdots \otimes A_k)^\dagger = A_1^\dagger \otimes \cdots \otimes A_k^\dagger$
4. If $\lambda_1, \cdots, \lambda_k$ are eigenvalues of $A_1, \cdots, A_k$ with eigenvectors $|u_1\rangle, \cdots, |u_k\rangle$, respectively, then $\prod_{i=1}^k \lambda_i$ is an eigenvector of $A_1 \otimes \cdots \otimes A_k$ with respect to the eigenvector $|u_1\rangle \otimes \cdots \otimes |u_k\rangle$.

1.2 Trace and Partial Trace

The trace $\mathrm{Tr} : \mathcal{L}(\mathcal{H}) \to \mathbb{C}$ is a linear map defined by

$$\mathrm{Tr}\,|j\rangle\langle k| = \langle k|j\rangle = \delta_{k,j}. \tag{13}$$

Extended by linearity, the trace of a linear operator L is then

$$\begin{aligned} \mathrm{Tr}\,L &= \mathrm{Tr}\left(\sum_{i,k=0}^{d-1} L_{i,k}|i\rangle\langle k|\right) \\ &= \sum_{i,k=0}^{d-1} L_{i,k}\,\mathrm{Tr}\,|i\rangle\langle k| \qquad (14) \\ &= \sum_{i,k=0}^{d-1} \langle i|L|k\rangle \delta_{i,k} \qquad (15) \\ &= \sum_{i=0}^{d-1} \langle i|L|i\rangle. \qquad (16) \end{aligned}$$

Exercise 4 (Cyclic property)**.** *Show that* $\operatorname{Tr} LM = \operatorname{Tr} ML$.

Note that $\operatorname{Tr} L^\dagger M$ defines an inner product on the space of $\mathcal{L}(\mathcal{H})$, and is known as the Hilbert-Schmidt inner product.

The partial trace $\operatorname{Tr}_A : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_B)$ is defined by

$$\operatorname{Tr}_A(|i\rangle\langle j|_A \otimes |k\rangle\langle \ell|_B) = \langle j|i\rangle |k\rangle\langle \ell|_B = \delta_{i,j} |k\rangle\langle \ell|_B. \tag{17}$$

Exercise 5. *Let* $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$*. Compute* $\operatorname{Tr}_A(|\Phi\rangle\langle\Phi|_{AB})$*.*

2 Quantum Postulates

2.1 Quantum States

Before defining what a quantum state looks like, we start with the classical notion of information. The basic unit of classical information is a bit $b \in \mathbb{Z} := \{0, 1\}$ that takes value of either '0' or '1'. The classical bit b can be generated randomly with a certain distribution P satisfying

$$\Pr\{b = 0\} = 1 - \Pr\{b = 1\} = p \in [0, 1].$$

However the bit b could never take non-binary value.

A quantum generalization of the classical bit, called a quantum bit or *qubit*, is mathematically defined as

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{18}$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Instead of using the vector form in Eq. (18), we will adopt the notation convention, the Dirac notation introduced in Section 1. Specifically, we will use the ket notation $|\cdot\rangle$ to denote a column vector of length one, e.g.,

$$|b\rangle := \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{19}$$

and use the bra notation $\langle\cdot|$ to denote the hermitian conjugate of $|\cdot\rangle$:

$$\langle b| := \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}. \tag{20}$$

We will also denote the computational basis of a d dimensional Hilbert space as $\{|0\rangle, |1\rangle, \cdots, |d{-}1\rangle\}$, where $|i\rangle$ is a column vector of zeros except a '1' in the $(i + 1)$-th entry. The qubit $|b\rangle$ in Eq. (18) can be written as

$$|b\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{21}$$

The quantum state $|b\rangle$ is viewed as in a *superposition* of states $|0\rangle$ and $|1\rangle$, a phenomenon unique in quantum mechanics. Generally, a quantum state in a d-dimensional Hilbert space can be expressed

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \tag{22}$$

where the *amplitude* α_i satisfies $\sum_i |\alpha_i|^2 = 1$.

A quantum state can also be randomly prepared: with probability p_i, the state $|\psi_i\rangle$ is prepared. The resulting quantum *ensemble* $\mathcal{E} : \{p_i, |\psi_i\rangle\}$ can be denoted by a density operator

$$\sigma_{\mathcal{E}} := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{23}$$

which is essentially a positive semi-definite matrix with trace one. We will denote by $\mathcal{D}(\mathcal{H})$ the collection of positive semi-definite matrices with trace one on the Hilbert space $\mathcal{H}$. The density matrix representation of a quantum state is considered to be the most general form in the following sense. If the ensemble only contains one entry, namely, $\sigma_{\mathcal{E}} \equiv |\psi_0\rangle\langle\psi_0|$ is of rank one, we say that the quantum state is *pure*. Otherwise, it is *mixed*.

Exercise 6. *For a density operator $\sigma \in \mathcal{D}(\mathcal{H})$, show that $\operatorname{Tr}\sigma^2 \leq 1$ with equality if and only if σ is pure.*

The density matrix representation also incorporates the notion of classical random bit; namely if $\sigma_{\mathcal{E}}$ is diagonal

$$\sigma_{\mathcal{E}} := \begin{pmatrix} p_0 & 0 \\ 0 & p_1 \end{pmatrix}, \tag{24}$$

then this means that the state $\sigma_{\mathcal{E}}$ is prepared in $|0\rangle$ with probability p_0 and in $|1\rangle$ with probability p_1.

Take Home

A quantum state can be represented by a positive semi-definite matrix with trace one.

2.2 Composite Quantum Systems

Again, let us start with the classical systems. It is rather easy and trivial to describe a joint classical state. Say the first bit is 0 and the second bit is 1, then its composite (or joint) classical system is a bit string $(0, 1)$. Such a joint rule is described by the *Cartesian product* ×, i.e., composition of two sets A and B, denoted $A \times B$, is

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}. \tag{25}$$

We can extend the Cartesian product to include n classical systems, which is represented by an n-dimensional string, where each element is an n-tuple.

Given two quantum states $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, the joint quantum state is $|\varphi\rangle_{AB} \equiv |\psi\rangle_A \otimes |\phi\rangle_B \in \mathcal{H} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$, where $\otimes$ is the *tensor product* . Tensor product can also extend a joint quantum system to include n subsystems. If one of the subsystems, say $\mathcal{H}_A$, is lost from $|\varphi\rangle_{AB}$, the residue quantum state returns to

$$|\phi\rangle\langle\phi|_B = \operatorname{Tr}_A |\varphi\rangle\langle\varphi|. \tag{26}$$

What is interesting in quantum mechanics is that there exist pure quantum states in $\mathcal{H}$ that cannot be decomposed into tensor product of two pure states in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A most notable example is the Bell state

$$|\Phi_+\rangle_{AB} := \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B). \tag{27}$$

Such a state is called an *entangled* state, a quantum state that contains *entanglement*. For an entangled state, if its partial system is lost, then it will decay into a mixed state.

Take Home

A bipartite pure quantum state is *entangled* if and only if it cannot be decomposed into tensor product of two local pure quantum state.

Exercise 7 (Schmidt decomposition)**.** *Show that a bipartite pure state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written as*

$$|\psi\rangle_{AB} = \sum_i \lambda_i |\nu_i\rangle_A \otimes |\xi_i\rangle_B \tag{28}$$

where $\lambda_i \geq 0$, $\sum_i |\lambda_i|^2 = 1$ and $\{|\nu_i\rangle_A\}$ and $\{|\xi_i\rangle_B\}$ are some orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

Exercise 8 (Purification)**.** *Show that a mixed state $\sigma_A = \sum_i \lambda_i |\nu_i\rangle\langle\nu_i|$ can be purified as follows. There exists a bipartite pure state $|\psi_\sigma\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}'_\mathcal{A}$ so that*

$$|\psi_\sigma\rangle = \sum_i \sqrt{\lambda_i} |\nu_i\rangle_A \otimes |\xi_i\rangle_{A'}, \tag{29}$$

where $\{|\xi_i\rangle\}$ is any orthonormal set of vectors in $\mathcal{H}_{A'}$.

Let us return to the scenario of a quantum ensemble $\mathcal{E} : \{p_x, |\psi_x\rangle\}_{x\in\mathcal{X}}$. Suppose that the person, say Alice, who prepares this ensemble can keep track of 'which state' she prepared. In other words, she has the additional classical label $|x\rangle\langle x|$ attached to the state $\sigma_x \in \mathcal{D}(\mathcal{H}_B)$, where $\{|x\rangle\}$ forms an orthonormal basis of $\mathcal{H}_X$. Such a hybrid classical-quantum system can be described as

$$\sigma_{XB} = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|. \tag{30}$$

This is an example of *the Church of the Larger Hilbert Space*. Forgetting (or lost) the classical information will result in

$$\sigma_B = \mathrm{Tr}_X\, \sigma_{XB} = \sum_{x\in\mathcal{X}} p_x |\psi_x\rangle\langle\psi_x|,$$

given in Eq. (23).

Consider a general mixed state $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we say σ_{AB} is *separable* if

$$\sigma_{AB} = \sum_i p_i \sigma_A^i \otimes \sigma_B^i \tag{31}$$

where $\sum_i p_i = 1$. In other words, σ_{AB} is *separable* if it can be written as convex combination of product states.

Take Home

A bipartite mixed quantum state is *entangled* if and only if it is not separable.

Exercise 9. *Argue why separable states do not contain entanglement.*

2.3 Quantum Evolution

The time evolution of a close quantum system is modelled by a unitary U; namely,

$$\rho \to U\rho U^\dagger. \tag{32}$$

The unitary evolution can be viewed as solving the Schrodinger equation

$$i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle \tag{33}$$

where $\hbar$ is the Planck constant and H is the system *Hamiltonian.*

We will describe the general (or noisy) evolution, i.e., quantum channels, in the second lecture.

2.4 Quantum Measurement

Quantum measurement is a process to observe the classical information within a quantum state. It can destroy the superposition property of a quantum state. The quantum measurement postulate evolves from *Born's rule* in his seminal paper in 1926, which states that "the probability density of finding a particle at a given point is proportional to the square of the magnitude of the particle's wave function at that point". Given the qubit state $|b\rangle$ in Eq. (21), Born's rule says that we can observe this qubit in state $|0\rangle$ with probability $|\alpha|^2$ and in state $|1\rangle$ with probability $|\beta|^2$. Furthermore, after the measurement, the qubit state $|b\rangle$ will disappear and collapse to the observed state $|0\rangle$ or $|1\rangle$.

In general, a quantum measurement is mathematically described by a collection of $\Upsilon := \{M_i\}$, where each measurement operator $M_i \in \mathcal{L}(\mathcal{H})$ satisfies

$$\sum_i M_i^\dagger M_i = I. \tag{34}$$

The probability of obtaining an outcome i on a quantum state ρ is

$$p_i := \mathrm{Tr}(M_i\rho M_i^\dagger) \tag{35}$$

and the residue quantum state becomes

$$\rho_i := \frac{M_i\rho M_i^\dagger}{p_i}.$$

The nomarlised condition in Eq. (34) guarantees that

$$\begin{aligned}\sum_i p_i &= \sum_i \mathrm{Tr}(M_i\rho M_i^\dagger)\\ &= \mathrm{Tr}\left(\sum_i M_i^\dagger M_i\rho\right)\\ &= \mathrm{Tr}\,\rho = 1.\end{aligned} \tag{36}$$

Projective Measurement and Observables

A special instance of quantum measurements is the *projective* measurement. A projective measurement Υ is a collection of projectors $\{P_0, P_1, \cdots, P_{L-1}\}$ which sum to identity. Note that $P_iP_j = 0$ for $i \neq j$ and $P_i^2 = P_i$. When we measure a quantum state $|\phi\rangle$ with Υ, we will get the outcome j with probability

$$p_j := \mathrm{Tr}(P_j|\phi\rangle\langle\phi|)$$

and the resulting state

$$\frac{P_j|\phi\rangle}{\sqrt{p_j}}.$$

A projective measurement $\Upsilon = \{P_i\}$ with the corresponding measurement outcomes $\{\lambda_i\} \in \mathcal{R}$ can be efficiently represented by a Hermitian matrix $H = \sum_i \lambda_i P_i$. Such a matrix is called an *observable.* In physics, an observable is a physical quantity that can be measured. Examples of *observables* of a physical system include the position or momentum of a particle, among many others.

Measuring the observable H means that performing the projective measurement $\Upsilon = \{P_i\}$ on a quantum state $|\phi\rangle$. It follows that the expected value of the outcomes if we measure the state $|\phi\rangle$ with $\Upsilon = \{P_i\}$ is

$$\langle H\rangle := \sum_i \lambda_i \,\mathrm{Tr}\, P_i|\phi\rangle\langle\phi| = \langle\phi|H|\phi\rangle. \tag{37}$$

If each projector $P_i \in \Upsilon$ is of rank one, $P_i = |i\rangle\langle i|$, where $\{|i\rangle\}_{i\in\mathcal{X}}$ forms a basis for $\mathcal{H}_X$, we will often call such a projective measurement Υ a *von Neumann measurement.* With the von Neumann measurement $\Upsilon = \{|i\rangle\langle i|\}$, we can then argue the *operational* equivalence between a quantum ensemble $\mathcal{E} = \{p_x, |\psi_x\rangle\}_{x\in\mathcal{X}}$ and the corresponding hybrid classical-quantum state σ_{XB} in Eq. (30):

1. Measuring the subsystem X with the von Neumann measurement Υ will leave subsystem B in the state $|\psi_i\rangle$ with probability p_i, for $i \in \mathcal{X}$. This results in the quantum ensemble $\mathcal{E} = \{p_x, |\psi_x\rangle\}_{x\in\mathcal{X}}$.

2. Conversely, given a quantum ensemble $\mathcal{E}$, we have stated how one can prepare the hybrid classical-quantum state σ_{XB} in Eq. (30).

Positive-operator-valued Measure (POVM)

POVM is a collection of subnormalised positive semi-definite matrices $\{\Lambda_i\}$ where each $I \geq \Lambda_i \geq 0$ and $\sum_i \Lambda_i = I$. It allows us to only focus on the probability distribution of the measurement outcomes. Recall that in Eq. (35), we can equate $\Lambda_i = M_i^\dagger M_i$. Hence the probability of obtaining the outcome i on the quantum state $|\phi\rangle$ is given by

$$p_i = \mathrm{Tr}(\Lambda_i|\phi\rangle\langle\phi|).$$

Exercise 10. *Show that every POVM can be constructed by a projective measurement on a larger Hilbert space.*

Quantum measurement can be used to distinguish a set of quantum states. We will elaborate a fundamental result, i.e., quantum state discrimination, in the second lecture.

Further Reading

A very good lecture note by Ronald de Wolf can be downloaded here [1].

3 No Cloning Theorem

In classical domain, a classical bit can be copied as many times as we want. However, it was shown to be impossible to copy an arbitrary unknown quantum state. This no-go theorem of quantum mechanics was first popularized by Wootters and Zurek in their Nature paper [3], but later realised that the idea has been proposed in [2].

Suppose that we have two quantum systems of equal size $\mathcal{H}_A = \mathcal{H}_B$. Given a quantum state $|\phi\rangle_A \in \mathcal{H}_A$, if quantum mechanics allows the operation of 'copying', then this copying operation U_{copy} should achieve

$$U_{\text{copy}}(|\phi\rangle_A \otimes |0\rangle_B) = |\phi\rangle_A \otimes |\phi\rangle_B. \tag{38}$$

In other words, the copying operation should produce a second copy of $|\phi\rangle$ in $\mathcal{H}_B$ (that was initially prepared in some ground state $|0\rangle_B$.)

Theorem 11 (No-Cloning theorem)**.** *There is no unitary operation U_{copy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that for all $|\psi\rangle_A \in \mathcal{H}_A$ and $|0\rangle_B \in \mathcal{H}_B$*

$$U_{\text{copy}}(|\phi\rangle_A \otimes |0\rangle_B) = e^{if(\phi)}|\phi\rangle_A \otimes |\phi\rangle_B \tag{39}$$

for some number $f(\phi)$ that depends on the initial state $|\phi\rangle$.

Proof. We can prove this theorem by contradiction. Assume such a coping operation U_{copy} exists. Then for any two states $|\psi\rangle_A, |\phi\rangle_A \in \mathcal{H}_A$, the following holds

$$\begin{aligned} U_{\text{copy}}(|\phi\rangle_A \otimes |0\rangle_B) &= e^{if(\phi)}|\phi\rangle_A \otimes |\phi\rangle_B & (40)\\ U_{\text{copy}}(|\psi\rangle_A \otimes |0\rangle_B) &= e^{if(\psi)}|\psi\rangle_A \otimes |\psi\rangle_B. & (41)\end{aligned}$$

Now

$$\begin{aligned} (\langle 0|_B \otimes \langle\phi|_A)U_{\text{copy}}^{\dagger}U_{\text{copy}}(|\psi\rangle_A \otimes |0\rangle_B) &= \langle\phi|\psi\rangle_A & (42)\\ &= e^{i(f(\psi)-f(\phi))}\langle\phi|\psi\rangle_A\langle\phi|\psi\rangle_B. & (43)\end{aligned}$$

The first equality follows because $U_{\text{copy}}^{\dagger}U_{\text{copy}} = I$ and $\langle 0|0\rangle_B = 1$. Hence

$$|\langle\phi|\psi\rangle_A|^2 = |\langle\phi|\psi\rangle_A|, \tag{44}$$

which implies that either $|\langle\phi|\psi\rangle_A| = 1$ or $|\langle\phi|\psi\rangle_A| = 0$. This allows us to conclude that not a single universal copying operation U_{copy} exists for two arbitrary states. □

References

[1] Ronald de Wolf, *Quantum computing: Lecture notes*, 2019.

[2] James L. Park, *The concept of transition in quantum mechanics*, Foundations of Physics **1** (March 1970), no. 1, 23–33.

[3] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (October 1982), no. 5886, 802–803.