Introduction to Quantum Information
CS 4331/5331 – Spring 2024
Lecture Notes

Contents

1 Qubits

Basic definitions and results

A single qubit is a two-state system. For example, the states $|h\rangle$ and $|v\rangle$ of the horizontal and vertical polarization of a photon can be considered as a two-state system.

The underlying Hilbert space for the qubit is $\mathbb{C}^2$. An arbitrary orthonormal basis for $\mathbb{C}^2$ is denoted by $\{|0\rangle, |1\rangle\}$, where

$$\begin{aligned} \langle 0|0\rangle &= \langle 1|1\rangle = 1, && (1) \\ \langle 0|1\rangle &= \langle 1|0\rangle = 0. && (2) \end{aligned}$$

In general, the vectors $\langle\phi|$ and $|\psi\rangle$ are called bra and ket vectors, which are row and column vectors, respectively. The notation $\langle\phi|\psi\rangle$ denotes the inner product (scalar product) of the two vectors. Any pure quantum state $|\psi\rangle$ of this (one qubit) system can be written as linear combination of the states (superposition) as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad (3)$$

where

$$|\alpha|^2 + |\beta|^2 = 1, \qquad \alpha, \beta \in \mathbb{C}. \qquad (4)$$

The classical boolean states, 0 and 1, can be represented by a fixed pari of orthonormal states of the qubit. The standard basis in $\mathbb{C}^2$ is given by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad (5)$$

and the Hadamard basis in $\mathbb{C}^2$ is given by

$$|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \qquad |1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}. \tag{6}$$

For any orthonormal basis $\{|0\rangle, |1\rangle\}$ in $\mathbb{C}^2$, we have

$$|0\rangle\langle 0| + |1\rangle\langle 1| = I_2, \tag{7}$$

where I_2 is the 2×2 identity matrix.

Let $|\psi\rangle \in \mathbb{C}^2$ and normalized, then

$$\rho = |\psi\rangle\langle\psi| \tag{8}$$

is a density matrix known as pure state. Pure state has the property

$$\rho^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{9}$$

Another parametrization of one qubit

Using $\alpha = \cos(\theta)$, $\beta = \sin(\theta)$ and the identity $\cos(\theta)^2 + \sin(\theta)^2 = 1$ for any $\phi, \theta \in R$, we have

$$|\psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\mathrm{e}^{i\phi}\cos(\theta)\\\sin(\theta)\end{pmatrix}, \tag{10}$$

where ϕ is an arbitrary phase, $\mathrm{e}^{-i\phi}\mathrm{e}^{i\phi} = 1$, and $i = \sqrt{-1}$.

In terms of the above parametrization, let's try to obtain the density matrix $\rho = |\psi\rangle\langle\psi|$, its trace $\mathrm{tr}(\rho)$, and ρ^2. Since

$$\langle\psi| = (\mathrm{e}^{-i\phi}\cos(\theta), \sin(\theta)), \tag{11}$$

we obtain the 2×2 density matrix as

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2(\theta) & \mathrm{e}^{i\phi}\sin(\theta)\cos(\theta) \\ \mathrm{e}^{-i\phi}\sin(\theta)\cos(\theta) & \sin^2(\theta) \end{pmatrix}. \tag{12}$$

Therefore,

$$\mathrm{tr}(\rho) = \cos^2(\theta) + \sin^2(\theta) = 1. \tag{13}$$

By the fact that $\langle\psi|\psi\rangle = 1$, we obtain

$$\rho^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{14}$$

As expected, $|\psi\rangle$ is a pure state.

Walsh-Hadamard transform

Let $|0\rangle$, $|1\rangle$ be an orthonormal basis in $\mathbb{C}^2$. The Walsh-Hadamard transform is a 1-qubit operation, denoted by U_H, that performs the linear transform

$$\begin{aligned} |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & (15) \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). & (16) \end{aligned}$$

The unitary operator U_H that implements H with respect to the basis $\{|0\rangle, |1\rangle\}$ is obviously

$$\begin{aligned} U_H &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| && (17) \\ &= \frac{1}{\sqrt{2}}|0\rangle(\langle 0| + \langle 1|) + \frac{1}{\sqrt{2}}|1\rangle(\langle 0| - \langle 1|). && (18) \end{aligned}$$

Since the U_H is unitary and its inverse is given by itself $U_H^{-1} = U_H^\dagger = U_H$.

Now consider the standard basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{19}$$

the matrix representation of U_H in terms of this basis is given by

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{20}$$

For the Hadamard basis

$$|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \tag{21}$$

the matrix representation of U_H is given by

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{22}$$

We see that the matrix representation for each of the two bases are the same.

Finally, by using (1) and (2), we can verify that

$$U_H U_H = |0\rangle \langle 0| + |1\rangle \langle 1| = I_2, \tag{23}$$

which is known as the completeness relation (of a single qubit).

Qubit trine

For an orthonormal basis $\{|0\rangle, |1\rangle\}$, the qubit trine is defined by the following states

$$\begin{aligned} |\psi_0\rangle &= |0\rangle && (24) \\ |\psi_1\rangle &= -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle && (25) \\ |\psi_2\rangle &= -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\,. && (26) \end{aligned}$$

As an example, we can obtain the following probabilities (related to the later discussion of measurement) by using (1) and (2) as

$$\begin{aligned} |\langle\psi_0|\psi_1\rangle|^2 &= \frac{1}{4} && (27) \\ |\langle\psi_1|\psi_2\rangle|^2 &= \frac{1}{4} && (28) \\ |\langle\psi_2|\psi_0\rangle|^2 &= \frac{1}{4}. && (29) \end{aligned}$$

Pauli spin matrices

The Pauli spin matrices are a set of three 2 × 2 (Hermitian and unitary) complex matrices given by

$$\begin{aligned} \sigma_1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} && (30) \\ \sigma_2 &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} && (31) \\ \sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. && (32) \end{aligned}$$

Let $n = (n_1, n_2, n_3)$ be a unit vector in $\mathbb{R}^3$,

$$n_1^2 + n_2^2 + n_3^2 = 1, \tag{33}$$

we define the operator

$$\Sigma = n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3. \tag{34}$$

It is easy to see that Σ is Hermitian $\Sigma^\dagger = \Sigma$ since σ_1, σ_1, and σ_3 are Hermitian. We will show that Σ is in fact unitary by showing additionally that $\Sigma^2 = I_2$ as follows. By using the fact that

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = I_2 \tag{35}$$

and

$$\begin{aligned} \sigma_1\sigma_2 + \sigma_2\sigma_1 &= 0_2 && (36) \\ \sigma_1\sigma_3 + \sigma_3\sigma_1 &= 0_2 && (37) \\ \sigma_2\sigma_3 + \sigma_3\sigma_2 &= 0_2, && (38) \end{aligned}$$

we obtain

$$\begin{aligned}
\Sigma^2 &= (n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3)^2 & (39)\\
&= (n_1^2 + n_2^2 + n_3^2)I_2 + n_1n_2(\sigma_1\sigma_2 + \sigma_2\sigma_1) + \\
&\quad n_1n_3(\sigma_1\sigma_3 + \sigma_3\sigma_1) + n_2n_3(\sigma_2\sigma_3 + \sigma_3\sigma_2) & (40)\\
&= I_2. & (41)
\end{aligned}$$

Since Σ is Hermitian and unitary, its eigenvalues λ_1 and λ_2 can only be ±. By the fact that

$$\mathrm{tr}(\Sigma) = 0 = \lambda_1 + \lambda_2, \tag{42}$$

we obtain that the two eigenvalues are -1 and $+1$.

As an example, let's compute the state $\Sigma\left|\psi\right\rangle$ and the probability $|\left\langle\psi\right|\Sigma\left|\psi\right\rangle|^2$ for the state

$$\left|\psi\right\rangle = \begin{pmatrix}1\\0\end{pmatrix}. \tag{43}$$

We find

$$\Sigma\left|\psi\right\rangle = n_1\begin{pmatrix}0\\1\end{pmatrix} + n_2\begin{pmatrix}0\\i\end{pmatrix} + n_3\begin{pmatrix}1\\0\end{pmatrix}, \tag{44}$$

and it follows that

$$|\left\langle\psi\right|\Sigma\left|\psi\right\rangle|^2 = n_3^2. \tag{45}$$

Distances between states

Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two normalized states in a Hilbert space $\mathcal{H}$. A distance d with $0 \leq d \leq \pi/2$ can be defined as

$$\cos^2(d) = |\langle\psi_1|\psi_2\rangle|^2. \tag{46}$$

For example, let $\mathcal{H} = \mathbb{C}^2$ and consider the normalized states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \qquad |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \tag{47}$$

by the fact that $\langle\psi_1|\psi_2\rangle = 0$, one has $\cos^2(d) = 0$. Therefore, the distance equals $d = \pi/2$.

One can also consider the variance

$$V_H(|\psi\rangle) = \langle\psi| H^2 |\psi\rangle - \langle\psi| H |\psi\rangle^2 \tag{48}$$

of a state $|\psi\rangle$ with respect to a symmetric matrix H over $\mathbb{R}$ as a distance metric.

For example, we consider a 2×2 symmetric matrix

$$H = \begin{pmatrix}h_{11} & h_{12}\\ h_{12} & h_{22}\end{pmatrix} \tag{49}$$

and the normalized state

$$|\psi\rangle = \begin{pmatrix}\cos(\theta)\\ \sin(\theta)\end{pmatrix}, \tag{50}$$

the corresponding variance is calculated as follows. We find

$$\begin{aligned} \langle\psi| H^2 |\psi\rangle &= h_{11}^2 \cos^2(\theta) + h_{22}^2 \sin^2(\theta) + h_{12}^2 + \\ &\quad 2h_{12}(h_{11} + h_{22}) \cos(\theta) \sin(\theta) \end{aligned} \tag{51}$$

and

$$\begin{aligned} \langle\psi| H |\psi\rangle^2 &= h_{11}^2 \cos^4(\theta) + h_{22}^2 \sin^4(\theta) + 2h_{11}h_{22} \cos^2(\theta) \sin^2(\theta) + \\ &\quad 4h_{11}h_{12} \cos^3(\theta) \sin(\theta) + 4h_{22}h_{12} \cos(\theta) \sin^3(\theta). \end{aligned} \tag{52}$$

Thus,

$$\begin{aligned} V_H(|\psi\rangle) &= (h_{11}^2 + h_{22}^2 - 2h_{11}h_{22}) \sin^2(\theta) \cos^2(\theta) + \\ &\quad h_{12}^2(1 - 4\sin^2(\theta) \cos^2(\theta)) + \\ &\quad 2h_{12}h_{11} \sin(\theta) \cos(\theta)(1 - 2\cos^2(\theta)) + \\ &\quad 2h_{12}h_{22} \sin(\theta) \cos(\theta)(1 - 2\sin^2(\theta)). \end{aligned} \tag{53}$$

2 Tensor Product

Basic definitions and results

Let A be an $m \times n$ matrix and B be an $r \times s$ matrix, the tensor (Kronecker) product of A and B is defined as the $mr \times ns$ matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}. \tag{54}$$

We have the following properties

- If A, B are Hermitian matrices, then $A \otimes B$ is a Hermitian matrix.

- If A, B are unitary matrices, then $A \otimes B$ is a unitary matrix.

- If A, B are projection matrices, then $A \otimes B$ is a projection matrix.

- The conjugate transpose is distributive

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger \tag{55}$$

- If A, B invertible, then $A \otimes B$ is invertible with

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}. \tag{56}$$

- Let A, B, C, D be matrices and assume that the matrix products AC and BD exist. Then

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD). \tag{57}$$

- Let A be an $m \times m$ matrix and B be an $n \times n$ matrix. Then

$$\begin{aligned} \mathrm{tr}(A \otimes B) &= \mathrm{tr}(A)\mathrm{tr}(B) && (58) \\ \mathrm{tr}(A \otimes I_n + I_m \otimes B) &= n\mathrm{tr}(A) + m\mathrm{tr}(B). && (59) \end{aligned}$$

Now let's try to verify some of the properties of tensor products by considering Pauli matrices σ_1 and σ_3 (Hermitian and unitary). One computes

$$\sigma_1 \otimes \sigma_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \tag{60}$$

and

$$\sigma_3 \otimes \sigma_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \tag{61}$$

where it can be easily verified that $\sigma_1 \otimes \sigma_3$ and $\sigma_3 \otimes \sigma_1$ are both Hermitian and unitary as expected.

Basis construction beyond $\mathbb{C}^2$

The set $\{|\phi_1\rangle, |\phi_2\rangle\}$,

$$|\phi_1\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |\phi_2\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{62}$$

forms a basis in $\mathbb{C}^2$, that is, the standard basis. The standard basis in $\mathbb{C}^4$ can be constructed from that in $\mathbb{C}^2$ by computing the tensor products as

$$|\phi_1\rangle \otimes |\phi_1\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \qquad |\phi_1\rangle \otimes |\phi_2\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \tag{63}$$

$$|\phi_2\rangle \otimes |\phi_1\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \qquad |\phi_2\rangle \otimes |\phi_2\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{64}$$

Similarly, for the orthonormal basis in $\mathbb{C}^2$

$$|\psi_1\rangle = \begin{pmatrix}\mathrm{e}^{i\phi}\cos(\theta)\\ \sin(\theta)\end{pmatrix}, \qquad |\psi_2\rangle = \begin{pmatrix}-\sin(\theta)\\ \mathrm{e}^{-i\phi}\cos(\theta)\end{pmatrix}, \tag{65}$$

the corresponding basis $\mathbb{C}^4$ is given by

$$\{|\psi_1\rangle \otimes |\psi_1\rangle\,,\;\; |\psi_1\rangle \otimes |\psi_2\rangle\,,\;\; |\psi_2\rangle \otimes |\psi_1\rangle\,,\;\; |\psi_2\rangle \otimes |\psi_2\rangle\} \tag{66}$$

since

$$(\langle\psi_j| \otimes \langle\psi_k|)(|\psi_m\rangle \otimes |\psi_n\rangle) = \delta_{jm}\delta_{kn} \tag{67}$$

for $j, k, m, n = 1, 2$.

A system of n-qubit can be represented by a finite-dimensional Hilbert space over the complex numbers of dimensions 2^n. A state $|\psi\rangle$ of the system is a superposition of the basic states

$$|\psi\rangle = \sum_{j_1, j_2, \ldots, j_n = 0}^{1} c_{j_1 j_2 \cdots j_n} |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle\,. \tag{68}$$

In a short hand notation, this state is written as

$$|\psi\rangle = \sum_{j_1, j_2, \ldots, j_n = 0}^{1} c_{j_1 j_2 \cdots j_n} |j_1 j_2 \cdots j_n\rangle\,. \tag{69}$$

For example, when $n = 2$ one has a 2-qubit state as

$$|\psi\rangle = c_{00}\,|00\rangle + c_{01}\,|01\rangle + c_{10}\,|10\rangle + c_{11}\,|11\rangle\,. \tag{70}$$

Consider a special case of the above state

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) && (71) \\ &= \frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) && (72) \end{aligned}$$

in the Hilbert space $\mathcal{H} = \mathbb{C}^4$. It can be seen that this state can be written as a product state as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{73}$$

indicating no entanglement.

Hilbert-Schmidt norm

Let A, B be $n \times n$ matrices over $\mathbb{C}$. A scalar product can be defined as

$$\langle A, B\rangle = \mathrm{tr}(AB^\dagger). \tag{74}$$

The scalar product implies a norm

$$\|A\|^2 = \langle A, A\rangle = \mathrm{tr}(AA^\dagger), \tag{75}$$

which is known as the Hilbert-Schmidt norm.

In particular, the two matrices are called orthogonal to each other if its Hilbert-Schmidt norm is zero. For example, consider the Dirac matrices

$$\gamma_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{76}$$

$$\gamma_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \tag{77}$$

we find that

$$\langle \gamma_0, \gamma_1 \rangle = \mathrm{tr}(\gamma_0 \gamma_1^\dagger) = 0. \tag{78}$$

Thus, γ_0 and γ_1 are orthogonal to each other.

The Hilbert-Schmidt norm is invariant under unitary transformation, that is, for any unitary matrix U,

$$\langle UA, UB \rangle = \langle A, B \rangle. \tag{79}$$

This is because

$$\mathrm{tr}(UA(UB)^\dagger) = \mathrm{tr}(UAB^\dagger U^\dagger) = \mathrm{tr}(U^\dagger UAB^\dagger) = \mathrm{tr}(AB^\dagger), \tag{80}$$

where we have used the cyclic property of matrix trace.

One also has the identity

$$\langle A \otimes C, B \otimes D \rangle = \langle A, B \rangle \langle C, D \rangle, \tag{81}$$

since

$$\begin{aligned}\mathrm{tr}((A\otimes C)(B\otimes D)^\dagger) &= \mathrm{tr}((A\otimes C)(B^\dagger\otimes D^\dagger)) && (82)\\ &= \mathrm{tr}((AB^\dagger)\otimes(CD^\dagger)) && (83)\\ &= \mathrm{tr}(AB^\dagger)\mathrm{tr}(CD^\dagger). && (84)\end{aligned}$$

Bell states

In the product Hilbert space $\mathbb{C}^4 \cong \mathbb{C}^2 \otimes \mathbb{C}^2$, the Bell states are given by

$$\begin{aligned}|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle) && (85)\\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle) && (86)\\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle+|1\rangle\otimes|0\rangle) && (87)\\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle-|1\rangle\otimes|0\rangle), && (88)\end{aligned}$$

which form an orthonormal basis in $\mathbb{C}^4$. Here, $\{|0\rangle, |1\rangle\}$ is an arbitrary orthonormal basis in the Hilbert space $\mathbb{C}^2$.

If we choose standard basis for $|0\rangle$ and $|1\rangle$, that is,

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \tag{89}$$

the Bell states take the form

$$|\Phi^+\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix} \tag{90}$$

$$|\Psi^+\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}. \tag{91}$$

The four Bell states with spin J ($J = 1/2, 1, 3/2, 2, \ldots$) are given by

$$|B_1\rangle \;=\; \frac{1}{\sqrt{2J+1}}\sum_{k=0}^{2J} |k\rangle \otimes |k\rangle \tag{92}$$

$$|B_2\rangle \;=\; \frac{1}{\sqrt{2J+1}}\sum_{k=0}^{2J} (-1)^k |k\rangle \otimes |k\rangle \tag{93}$$

$$|B_3\rangle \;=\; \frac{1}{\sqrt{2J+1}}\sum_{k=0}^{2J} |k\rangle \otimes |2J-k\rangle \tag{94}$$

$$|B_4\rangle \;=\; \frac{1}{\sqrt{2J+1}}\sum_{k=0}^{2J} (-1)^k |k\rangle \otimes |2J-k\rangle\,. \tag{95}$$

For $J = 1/2$, the above reduces to the standard Bell basis in $\mathbb{C}^4$, which form an orthonormal basis in $\mathbb{C}^4$.

For $J = 1$, the Bell states are

$$\begin{aligned} |B_1\rangle &= \frac{1}{\sqrt{3}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle) && (96) \\ |B_2\rangle &= \frac{1}{\sqrt{3}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle) && (97) \\ |B_3\rangle &= \frac{1}{\sqrt{3}}(|0\rangle \otimes |2\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |0\rangle) && (98) \\ |B_4\rangle &= \frac{1}{\sqrt{3}}(|0\rangle \otimes |2\rangle - |1\rangle \otimes |1\rangle + |2\rangle \otimes |0\rangle), && (99) \end{aligned}$$

which is effectively a 3-qubit system and shall not form a basis in $\mathbb{C}^4$. Indeed, let $c_1, c_2, c_3, c_4 \in \mathbb{C}$, then the equation

$$c_1 |B_1\rangle + c_2 |B_2\rangle + c_3 |B_3\rangle + c_4 |B_4\rangle = \mathbf{0} \qquad (100)$$

permits a solution $c_2 = -c_1$, $c_3 = -c_1$, $c_4 = c_1$ with c_1 arbitrary. Therefore, the four states are not linearly independent. In fact, it can be shown that

$$\begin{aligned} \langle B_1|B_2\rangle &= \frac{1}{3}, \qquad \langle B_1|B_3\rangle = \frac{1}{3} && (101) \\ \langle B_1|B_4\rangle &= -\frac{1}{3}, \qquad \langle B_2|B_3\rangle = -\frac{1}{3} && (102) \\ \langle B_2|B_4\rangle &= \frac{1}{3}, \qquad \langle B_3|B_4\rangle = \frac{1}{3}. && (103) \end{aligned}$$

3 Density Operators

Basic linear algebra results

Let A be an $n \times n$ matrix over $\mathbb{C}$. λ is an eigenvalue of A if there exists $\mathbf{x} \neq \mathbf{0}$ such that

$$A\mathbf{x} = \lambda\mathbf{x}, \tag{104}$$

where $\mathbf{x}$ is the corresponding eigenvector associated with λ. Eigenvalues can be obtained by finding the roots of the characteristic polynomials of A defined as

$$p_n(\lambda) = \det(\lambda I_n - A), \tag{105}$$

which is a polynomial of degree n in λ. Thus, A has n eigenvalues.

Let A and B be two $n \times n$ matrices over $\mathbb{C}$. If there exists a non-singular $n \times n$ matrix X such that $A = XBX^{-1}$, then A and B are said to be similar matrices. The two matrices have the same set of eigenvalues since

$$\begin{aligned}
\det(A - \lambda I_n) &= \det(XBX^{-1} - X\lambda I_n X^{-1}) && (106)\\
&= \det(X(B - \lambda I_n)X^{-1}) && (107)\\
&= \det(X)\det(B - \lambda I_n)\det(X^{-1}) && (108)\\
&= \det(B - \lambda I_n). && (109)
\end{aligned}$$

A Hadamard matrix H_n of dimension 2^n can be recursively defined as

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \tag{110}$$

which also satisfy the property that

$$H_n H_n^\dagger = 2^n I_{2^n}. \tag{111}$$

We will show below, by induction, that the eigenvalues of H_n are given by $2^{n/2}$ and $-2^{n/2}$ each with multiplicity 2^{n-1}. For $n = 1$, it can be easily obtained that H_1 has eigenvalues $\{-\sqrt{2}, \sqrt{2}\}$. For $n \geq 2$, we have

$$\begin{aligned} \det(\lambda I - H_n) &= \det \begin{pmatrix} \lambda I - H_{n-1} & -H_{n-1} \\ -H_{n-1} & \lambda I + H_{n-1} \end{pmatrix} && (112) \\ &= \det((\lambda I - H_{n-1})(\lambda I + H_{n-1}) - H_{n-1}^2) \\ &= \det\left(\lambda^2 I - 2H_{n-1}^2\right) && (113) \\ &= \det(\lambda I - \sqrt{2} H_{n-1}) \det(\lambda I + \sqrt{2} H_{n-1}). \end{aligned}$$

This shows that each eigenvalue μ of H_{n-1} generates two eigenvalues $\pm\sqrt{2}\mu$ of H_n. The statement then follows by the induction hypothesis: H_{n-1} has eigenvalues $2^{(n-1)/2}$ and $-2^{(n-1)/2}$ each with multiplicity 2^{n-2}.

For an $n \times n$ matrix A, the eigenvalues can be also obtained as solutions of the equations

$$\begin{aligned} \mathrm{tr}(A) &= \lambda_1 + \lambda_2 + \cdots + \lambda_n && (114) \\ \mathrm{tr}(A^2) &= \lambda_1^2 + \lambda_2^2 + \cdots + \lambda_n^2 && (115) \\ &\vdots \\ \mathrm{tr}(A^n) &= \lambda_1^n + \lambda_2^n + \cdots + \lambda_n^n. && (116) \end{aligned}$$

For example, consider the matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad (117)$$

since $\mathrm{tr}(H) = 0$ and $\mathrm{tr}(H^2) = 2$, we have

$$\begin{aligned} \lambda_1 + \lambda_2 &= 0 && (118) \\ \lambda_1^2 + \lambda_2^2 &= 2, && (119) \end{aligned}$$

from which we obtain the eigenvalues $\lambda_1 = -1$, $\lambda_2 = 1$.

Let A and B be two $n \times n$ matrices over $\mathbb{C}$. We introduce a new scalar product

$$\langle A, B \rangle = \frac{1}{n} \mathrm{tr}(AB^\dagger). \qquad (120)$$

The Lie group $SU(n)$ is defined by the collection of complex $n \times n$ matrices U as

$$SU(n) = \{U : U^\dagger U = UU^\dagger = I_n,\ \det(U) = 1\}. \tag{121}$$

The semi-simple Lie algebra $su(n)$ is defined by the collection of complex $n \times n$ matrices X as

$$su(n) = \{X : X^\dagger = -X,\ \mathrm{tr}(X) = 0\}. \tag{122}$$

Clearly, for an arbitrary $n \times n$ matrix A and any $U \in SU(n)$, one has $\langle U, U\rangle = 1$ and $\langle UA, UA\rangle = \langle A, A\rangle$.

As an example, we give a basis (w.r.t. the above defined scalar product) of Lie algebra $su(2)$ as shown below

$$\tau_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}. \tag{123}$$

It can be verified that the matrices are indeed linear independent, traceless, skew-hermitian, and orthogonal to each other.

Two orthonormal bases in an n-dimensional complex Hilbert space $\mathbb{C}^n$,

$$\{|\mathbf{u}_j\rangle : j = 1, 2, \ldots, n\} \tag{124}$$

$$\{|\mathbf{v}_j\rangle : j = 1, 2, \ldots, n\} \tag{125}$$

are called mutually unbiased if the inner products between all possible pairs of vectors taken from distinct bases have the same magnitude, that is,

$$|\langle \mathbf{u}_j | \mathbf{v}_k \rangle| = \frac{1}{\sqrt{n}}, \qquad \text{for all } j, k \in \{1, 2, \ldots, n\}. \tag{126}$$

The bases are unbiased in the sense that if a system is prepared in a state belonging to one of the bases, then all outcomes of the measurement with respect to the other basis are predicted to occur with equal probability.

In the Hilbert space $\mathbb{C}^2$, an example of the two mutually unbiased bases are

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \mathbf{u}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{127}$$

and

$$\mathbf{v}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \tag{128}$$

where another option for the second basis is

$$\mathbf{v}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad \mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \tag{129}$$

In the Hilbert space $\mathbb{C}^3$, an example of the two mutually unbiased bases are

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{u}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{u}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{130}$$

and

$$\mathbf{v}_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathbf{v}_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} -1 \\ (1+\sqrt{3})/2 \\ (1-\sqrt{3})/2 \end{pmatrix}, \tag{131}$$

$$\mathbf{v}_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} (-1+i\sqrt{3})/2 \\ (-1-i\sqrt{3})/2 \\ 1 \end{pmatrix}. \tag{132}$$

Definition and properties of density matrices

A density matrix (or density operator) ρ is a positive semi-definite operator on a Hilbert space with unit trace $\mathrm{tr}(\rho) = 1$. An operator is positive semi-definite if it is Hermitian and all of its eigenvalues are greater than or equal to zero. A density matrix is used in quantum theory to describe the statistical state of a quantum system.

Recall that if we have a pure state $|\psi\rangle$ in a Hilbert space with $\langle\psi|\psi\rangle = 1$ then

$$\rho = |\psi\rangle\langle\psi| \tag{133}$$

defines a density matrix with

$$\rho^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{134}$$

The expected value of an observable A is given by

$$\langle A\rangle = \mathrm{tr}(A\rho). \tag{135}$$

For a mixed state, we have the spectral representation

$$\rho = \sum_{j=1}^{n} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|, \tag{136}$$

where

$$p_j \geq 0, \qquad \sum_{j=1}^{n} p_j = 1, \tag{137}$$

and

$$\langle\psi_j|\psi_k\rangle = \delta_{jk}. \tag{138}$$

The expected value of an observable A over the mixed density matrix is

$$\mathrm{tr}(\rho A) = \sum_{j=1}^{n} p_j \left\langle\psi_j\right| A \left|\psi_j\right\rangle \tag{139}$$

We also have the following properties of density matrices

- If ρ_1 and ρ_2 are density matrices, then $\rho_1 \otimes \rho_2$ and $\rho_1 \oplus \rho_2$ are density matrices.

- If ρ_1 and ρ_2 are pure states, then $\rho_1 \otimes \rho_2$ and $\rho_1 \oplus \rho_2$ are pure states.

- If ρ is a density matrix and U is an unitary, then $U\rho U^\dagger$ is a density matrix.

- The eigenvalues of an $n \times n$ density matrix of pure state are 1 and $n-1$ of 0.

Some examples of density matrices

Let A be an arbitrary nonzero $n \times n$ matrix, then

$$\rho = \frac{AA^\dagger}{\mathrm{tr}(AA^\dagger)} \tag{140}$$

is a density matrix. The density matrix is also invariant under the unitary transformation $A \to AU$.

The 2×2 matrix

$$\rho = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} \tag{141}$$

is a density matrix and a pure state. This is because $\mathrm{tr}(\rho) = 1$ and the matrix is Hermitian with its eigenvalues being 0 and 1. The corresponding state is

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \tag{142}$$

where $\rho = |\psi\rangle \langle\psi|$.

Let $r \geq 0$. We will decide the conditions on r, θ, ϕ so that the

2×2 matrix

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + r\cos(\theta) & r\sin(\theta)\mathrm{e}^{-i\phi} \\ r\sin(\theta)\mathrm{e}^{i\phi} & 1 - r\cos(\theta) \end{pmatrix} \tag{143}$$

can be a density matrix. We first see that $\mathrm{tr}(\rho) = 1$ and the fact that the matrix is Hermitian. Thus, the eigenvalues are real, which are computed as

$$\lambda_1 = \frac{1}{2} - \frac{1}{2}r, \qquad \lambda_2 = \frac{1}{2} + \frac{1}{2}r. \tag{144}$$

Therefore, the condition that ρ is a density matrix requires $-1 \leq r \leq 1$. There is no requirement on θ or ϕ.

Consider the 2×2 matrix

$$\rho = \begin{pmatrix} 3/4 & \sqrt{2}\mathrm{e}^{-i\phi}/4 \\ \sqrt{2}\mathrm{e}^{i\phi}/4 & 1/4 \end{pmatrix}, \tag{145}$$

which clearly has $\mathrm{tr}(\rho) = 1$ and is Hermitian. The eigenvalues are calculated as

$$\lambda_1 = \frac{2 - \sqrt{3}}{4}, \qquad \lambda_2 = \frac{2 + \sqrt{3}}{4}, \tag{146}$$

which are non-negative. Thus, ρ is a density matrix. The eigenvalues show that the state mixed, which can be also verified by the fact $\rho^2 \neq \rho$.

The density matrix $\rho = |\psi\rangle \langle\psi|$ of the Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{147}$$

is given by

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \tag{148}$$

Moreover, it can be shown that the density matrix ρ can be written as a linear combinations of the matrices

$$\begin{aligned} \Lambda_{00} &= \frac{1}{2}I_2 \otimes I_2, \qquad \Lambda_{11} = \frac{1}{2}\sigma_1 \otimes \sigma_1 & (149) \\ \Lambda_{22} &= \frac{1}{2}\sigma_2 \otimes \sigma_2, \qquad \Lambda_{33} = \frac{1}{2}\sigma_3 \otimes \sigma_3, & (150) \end{aligned}$$

as

$$\rho = \frac{1}{2}\Lambda_{00} + \frac{1}{2}\Lambda_{11} - \frac{1}{2}\Lambda_{22} + \frac{1}{2}\Lambda_{33}, \tag{151}$$

where σ_1, σ_2, σ_3 are the Pauli matrices.

Consider the following matrix representation of N qubits in terms of tensor products of Pauli matrices

$$\rho = \frac{1}{2^N} \sum_{j_0=0}^{3} \sum_{j_1=0}^{3} \cdots \sum_{j_{N-1}=0}^{3} c_{j_0 j_1 \cdots j_{N-1}} \sigma_{j_0} \otimes \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_{N-1}}, \quad (152)$$

where $\sigma_0 = I_2$. Let's find the conditions of the expansion coefficients $c_{j_0 j_1 \cdots j_{N-1}}$ under which ρ satisfies the properties

$$\rho^\dagger = \rho, \qquad \mathrm{tr}(\rho) = 1. \quad (153)$$

For $\rho^\dagger = \rho$, since

$$\sigma_0^\dagger = \sigma_0, \quad \sigma_1^\dagger = \sigma_1, \quad \sigma_2^\dagger = \sigma_2, \quad \sigma_3^\dagger = \sigma_3, \quad (154)$$

the expansion coefficients must be real numbers.

For $\mathrm{tr}(\rho) = 1$, by using

$$\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B) \quad (155)$$

and the fact that

$$\mathrm{tr}(\sigma_1) = \mathrm{tr}(\sigma_2) = \mathrm{tr}(\sigma_3) = 0, \qquad \mathrm{tr}(I_2) = 2, \quad (156)$$

we must require that $c_{00\ldots0} = 1$.

Distances between density matrices

The Hilbert-Schmidt distance between two density matrices ρ_1 and ρ_2 is given by the Frobenius norm of the difference as

$$D_{HS}(\rho_1, \rho_2) = \sqrt{\mathrm{tr}(\rho_1 - \rho_2)^2} \quad (157)$$

For example, considering the density matrices

$$\rho_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{158}$$

the Hilbert-Schmidt distance is obtained as

$$D_{HS}(\rho_1, \rho_2) = \sqrt{2}. \tag{159}$$

Another distance is the Bures distance. The Bures distance between two density matrices ρ_1 and ρ_2 is defined as

$$D_B(\rho_1, \rho_2) = \sqrt{2\left(1 - \mathrm{tr}\left((\rho_1^{1/2}\rho_2\rho_1^{1/2})^{1/2}\right)\right)}. \tag{160}$$

For example, let's find the Bures distance when considering the density matrices

$$\rho_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \tag{161}$$

acting on the Hilbert space $\mathbb{C}^2$. Since

$$\rho_1^{1/2} = \rho_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{162}$$

we obtain

$$\rho_1^{1/2}\rho_2\rho_1^{1/2} = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix}. \tag{163}$$

Thus, the distance is given by

$$D_B(\rho_1, \rho_2) = \sqrt{2(1 - 1/\sqrt{2})}. \tag{164}$$

In addition, the trace distance between two density matrices ρ_1 and ρ_2 is

$$D_T(\rho_1, \rho_2) = \frac{1}{2}\mathrm{tr}\left(\sqrt{(\rho_1 - \rho_2)(\rho_1 - \rho_2)^\dagger}\right). \tag{165}$$

Partial trace of density matrices

Partial trace plays a central role in quantum computing. It gives rise to the model of entanglement in quantum bipartite systems. For a finite dimensional quantum system consisting of two subsystems A and B, its Hilbert space $\mathcal{H}$ is given by the tensor product of the individual Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$. Let ρ be the density matrix of the full system, and N_A and N_B be the dimensions of subsystems A and B, by using partial trace we can define the density matrices ρ_A and ρ_B in the space $\mathcal{H}_A$ and $\mathcal{H}_B$ as

$$\rho_A = \mathrm{tr}_B(\rho) = \sum_{j=1}^{N_B} (I_A \otimes \langle\phi_j|)\rho(I_A \otimes |\phi_j\rangle) \tag{166}$$

and

$$\rho_B = \mathrm{tr}_A(\rho) = \sum_{j=1}^{N_A} (\langle\psi_j| \otimes I_B)\rho(|\psi_j\rangle \otimes I_B), \tag{167}$$

where

$$|\phi_j\rangle\,, \quad j = 1, 2, \ldots, N_B \tag{168}$$

is an orthonormal basis in $\mathcal{H}_B$ and

$$|\psi_j\rangle\,, \quad j = 1, 2, \ldots, N_A \tag{169}$$

is an orthonormal basis in $\mathcal{H}_A$. One may choose the standard bases in the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$.

For example, consider the entangled state in $\mathbb{C}^4 \cong \mathbb{C}^2 \otimes \mathbb{C}^2$,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right), \tag{170}$$

let's find the partial traces $\rho_A = \mathrm{tr}_B(\rho)$ and $\rho_B = \mathrm{tr}_A(\rho)$, where $\rho = |\psi\rangle\langle\psi|$.

We have

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \tag{171}$$

thus

$$\rho = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{172}$$

Using the basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{173}$$

and the basis

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{174}$$

the partial traces are obtained as

$$\rho_A = \rho_B = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{175}$$

As another example, consider the Greenberger-Horne-Zeilinger (GHZ) entangled state in the Hilbert space $\mathbb{C}^8 \cong \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right), \tag{176}$$

which can be compactly represented as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |000\rangle). \tag{177}$$

The corresponding density matrix is given by

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{178}$$

The partial trace $\rho_{AB} = \mathrm{tr}_C(\rho)$ with respect to the basis

$$I_4 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad I_4 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{179}$$

is calculated as

$$\begin{aligned} \rho_{AB} = \mathrm{tr}_C(\rho) \;=\; & \left(I_4 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)^\dagger \rho \left(I_4 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) + \\ & \left(I_4 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)^\dagger \rho \left(I_4 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \end{aligned} \tag{180}$$

$$= \frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} \tag{181}$$

$$= \frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}. \tag{182}$$

4 Boolean Functions and Quantum Gates

Basic concepts

A truth table is tabular description of a combinational circuit listing all possible states of the input variables together with the output variables for each of those possible states. The truth table for the AND gate (denoted by $\cdot$), OR gate (denoted by $+$), XOR gate (denoted by $\oplus$), and NOT gate (denoted by $\overline{x}$) are

AND		
0	0	0
0	1	0
1	0	0
1	1	1

OR		
0	0	0
0	1	1
1	0	1
1	1	1

XOR		
0	0	0
0	1	1
1	0	1
1	1	0

NOT	
0	1
1	0

Let $X = \{0,1\}$ and $x_j \in X$, a boolean function f with n input variable $x_1, x_2, \ldots, x_n$ and n output variables $y_1, y_2, \ldots, y_n$ is a function $f : X^n \to X^n$ such that

$$f(x_1, \ldots, x_n) \to (y_1, \ldots, y_n). \qquad (183)$$

Here, $(x_1, \ldots, x_n) \in X^n$ is called the input vector and $(y_1, \ldots, y_n) \in X^n$ is called the output vector. An n input and n output boolean function f is reversible if it maps each input vector to a unique output vector, that is, the map is bijection. A reversible gate has a corresponding quantum version, whose properties are completely defined by the truth table of the classical version. Reversible gates are candidates as universal building blocks, which also require reduced power in implementation.

Feynman gate

The Feynman gate is a 2-input and 2-output gate given by

$$x_1' = x_1, \qquad x_2' = x_1 \oplus x_2. \tag{184}$$

From the definition, the truth table is obtained as

x_1	x_2	x_1'	x_2'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

From the truth table we can see that the transformation is invertible, that is, the mapping is a bijection. Formally, the inverse transformation can be found as follows. Since $x_1 \oplus x_1 = 0$, we have

$$x_1' \oplus x_2' = x_1 \oplus x_1 \oplus x_2 = 0 \oplus x_2 = x_2. \tag{185}$$

Thus, the inverse transform is given by

$$x_1 = x_1', \qquad x_2 = x_1' \oplus x_2'. \tag{186}$$

In the special case $x_2 = 0$, we have $x'_2 = x_1 \oplus 0 = x_1$. Thus, the gate implements copying.

In the special case $x_2 = 1$, we have $x'_2 = x_1 \oplus 1 = \overline{x_1}$. Thus, the gate can also implement complement.

Let $|0\rangle$, $|1\rangle$ be the standard basis in the Hilbert space $\mathbb{C}^2$, the unitary transform that implements the Feynman gate

$$|x_1\rangle \otimes |x_2\rangle \to |x_1\rangle \otimes |x_1 \oplus x_2\rangle\,, \qquad x_1, x_2 \in \{0,1\}, \tag{187}$$

is given by

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{188}$$

which is obtained by the fact that

$$\begin{aligned} |0\rangle \otimes |0\rangle \;&\to\; |0\rangle \otimes |0\rangle\,, \qquad |0\rangle \otimes |1\rangle \to |0\rangle \otimes |1\rangle & (189)\\ |1\rangle \otimes |0\rangle \;&\to\; |1\rangle \otimes |1\rangle\,, \qquad |1\rangle \otimes |1\rangle \to |1\rangle \otimes |0\rangle\,. & (190)\end{aligned}$$

Here, the notation of direct sum of matrices

$$A \oplus B = \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix} \tag{191}$$

shall be distinguishable by the context from that of the XOR gate.

Toffoli gate

The Toffoli gate is a boolean function $T : \{0, 1\}^3 \to \{0, 1\}^3$,

$$T(x_1, x_2, x_3) = (x_1, x_2, (x_1 \cdot x_2) \oplus x_3), \tag{192}$$

where $x_1, x_2, x_3 \in \{0, 1\}$. Its truth table is

x_1	x_2	x_3	x'_1	x'_2	x'_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

and the unitary matrix implementation of the gate is

$$U = I_6 \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{193}$$

As a special case, the NOT gate can be realized in terms of the Toffoli gate as

$$\mathrm{NOT}(a) = \mathrm{BIT3}(T(a, a, 1)) = a \oplus 1, \tag{194}$$

where $\mathrm{BIT3}(a, b, c) = c$. The result follows from the fact that $a \cdot a = a$ and $T(a, a, 1) = (a, a, a \oplus 1)$.

As another special case, the AND gate can be implemented in terms of the Toffoli gate as

$$\mathrm{AND(a,b)} = \mathrm{BIT3}(T(a,b,0)) = a \cdot b, \tag{195}$$

where we used the fact that $a \oplus 0 = a$.

Fredkin gate

The Fredkin gate is a boolean function $F : \{0,1\}^3 \to \{0,1\}^3$,

$$F(a,b,c) = (a, \overline{a} \cdot b + a \cdot c, \overline{a} \cdot c + a \cdot b). \tag{196}$$

The truth table is

x_1	x_2	x_3	x'_1	x'_2	x'_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

and the unitary matrix implementation is

$$U = I_5 \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus I_1. \tag{197}$$

In other words, the Fredkin gate maps the boolean patterns

$$(a, b, c) \to (a, c, b) \tag{198}$$

if and only if $a = 1$, otherwise it passes the boolean pattern unchanged.

One Fredkin gate is sufficient to implement the XOR gate as shown below. Choose $b = \overline{c}$, the Fredkin gate yields

$$(a, b, c) \to (a, \overline{a} \cdot b + a \cdot \overline{b}, \overline{a} \cdot c + a \cdot \overline{c}) = (a, a \oplus b, a \oplus c) \tag{199}$$

Thus, we can apply the Fredkin gate to $(a, b, \overline{b})$ and use the second bit to obtain $a \oplus b$ or equivalently apply the Fredkin gate to $(a, \overline{c}, c)$ and use the third bit to obtain $a \oplus c$.

Other related gates

Let $x \in \{0, 1\}$ and $|0\rangle$, $|1\rangle$ be the standard basis in $\mathbb{C}^2$. Consider the map

$$|x\rangle \otimes |0\rangle \to |x\rangle \otimes |\overline{x}\rangle \,, \tag{200}$$

the unitary transform U that implements the map can be found as follows. We have to satisfy

$$U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |1\rangle \,, \tag{201}$$

which is

$$U \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{202}$$

as well as

$$U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |0\rangle \,, \tag{203}$$

which is

$$U \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}. \tag{204}$$

A solution is

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{205}$$

For the boolean function

$$(x_1, x_2) \to (x_1 \oplus 1, x_1 \oplus x_2), \tag{206}$$

the unitary gate U that implements the resulting map

$$U(|x_1\rangle \otimes |x_2\rangle) = |x_1 \oplus 1\rangle \otimes |x_1 \oplus x_2\rangle \tag{207}$$

is obtained by solving the linear equations

$$U\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \qquad U\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{208}$$

$$U\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \qquad U\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \tag{209}$$

as

$$U=\begin{pmatrix}0&0&0&1\\0&0&1&0\\1&0&0&0\\0&1&0&0\end{pmatrix}. \tag{210}$$

For the map

$$|x_1\rangle\otimes|x_2\rangle\otimes|x_3\rangle\to|x_1\rangle\otimes|x_2\rangle\otimes|x_3\oplus(x_1\cdot\overline{x_2})\rangle\,, \tag{211}$$

the corresponding unitary transform that implements this map is

$$U=I_4\oplus\begin{pmatrix}0&1\\1&0\end{pmatrix}\oplus I_2, \tag{212}$$

which can be obtained by list all the transforms

$$
\begin{aligned}
|0\rangle\,|0\rangle\,|0\rangle &\rightarrow |0\rangle\,|0\rangle\,|0\rangle & (213)\\
|0\rangle\,|0\rangle\,|1\rangle &\rightarrow |0\rangle\,|0\rangle\,|1\rangle & (214)\\
|0\rangle\,|1\rangle\,|0\rangle &\rightarrow |0\rangle\,|1\rangle\,|0\rangle & (215)\\
|0\rangle\,|1\rangle\,|1\rangle &\rightarrow |0\rangle\,|1\rangle\,|1\rangle & (216)\\
|1\rangle\,|0\rangle\,|0\rangle &\rightarrow |1\rangle\,|0\rangle\,|1\rangle & (217)\\
|1\rangle\,|0\rangle\,|1\rangle &\rightarrow |1\rangle\,|0\rangle\,|0\rangle & (218)\\
|1\rangle\,|1\rangle\,|0\rangle &\rightarrow |1\rangle\,|1\rangle\,|0\rangle & (219)\\
|1\rangle\,|1\rangle\,|1\rangle &\rightarrow |1\rangle\,|1\rangle\,|1\rangle & (220)
\end{aligned}
$$

Consider the 3-input and 3-output gate given by

$$x_1' = x_1, \quad x_2' = x_1 \oplus x_2, \quad x_3' = x_3 \oplus (x_1 \cdot x_2). \qquad (221)$$

From the definition, the truth table is obtained as

x_1	x_2	x_3	x'_1	x'_2	x'_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	1	0
1	0	1	1	1	1
1	1	0	1	0	1
1	1	1	1	0	0

From the truth table we can see that the transformation is invertible. The inverse transform is in fact given by

$$\begin{aligned} x_1 &= x'_1 && (222) \\ x_2 &= x'_1 \oplus x'_2 && (223) \\ x_3 &= x'_3 \oplus (x'_1 \cdot (x'_1 \oplus x'_2)). && (224) \end{aligned}$$

The unitary transform that implements the gate

$$|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \rightarrow |x'_1\rangle \otimes |x'_2\rangle \otimes |x'_3\rangle \qquad (225)$$

can be similarly obtained as in previous examples.

5 Unitary Transforms and Quantum Gates

Definitions and basic properties

Quantum gates are realized by unitary transformations. A linear operator U in a Hilbert space is unitary if

$$U^\dagger = U^{-1}. \tag{226}$$

Equivalently, it requires

$$U^\dagger U = UU^\dagger = I. \tag{227}$$

We also point out the following results

- If U_1, U_2 are $n \times n$ unitary matrices, then $U_1 U_2$ is an unitary matrix. Thus, all $n \times n$ unitary matrices form a group under matrix multiplication.

- Each of the eigenvalues of a unitary matrix has the absolute value equal to 1, that is, $|\lambda| = 1$. Thus, $|\det(U)| = 1$.

- An important subgroup of unitary matrices is the collection of all $n \times n$ unitary matrices with $\det(U) = 1$. It is a subgroup because if $\det(U_1) = 1$ and $\det(U_2) = 1$, then $\det(U_1 U_2) = 1$.

- Another important subgroup is the collection of binary matrices or permutation matrices, some of which appeared in the last chapter.

Hadamard gate, CNOT gate, and phase gate

The Hadamard gate can be compactly represented as

$$U_H \left|k\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^k \left|1\right\rangle), \quad k \in \{0,1\}. \tag{228}$$

The controlled NOT gate is defined as

$$U_{CNOT}(\left|a\right\rangle \otimes \left|b\right\rangle) = \left|a\right\rangle \otimes \left|a \oplus b\right\rangle, \tag{229}$$

where a is the control bit and b is the target bit. Equivalently, it can also be represented by

$$U_{CNOT} = \left|00\right\rangle \left\langle 00\right| + \left|01\right\rangle \left\langle 01\right| + \left|10\right\rangle \left\langle 11\right| + \left|11\right\rangle \left\langle 10\right| \tag{230}$$

or

$$U_{CNOT} = \left|0\right\rangle \left\langle 0\right| \otimes I_2 + \left|1\right\rangle \left\langle 1\right| \otimes U_{NOT}, \tag{231}$$

where

$$U_{NOT} = \left|0\right\rangle \left\langle 1\right| + \left|1\right\rangle \left\langle 0\right| \tag{232}$$

is the NOT gate. The phase gate is given by

$$U_P(\theta) = \left|00\right\rangle \left\langle 00\right| + \left|01\right\rangle \left\langle 01\right| + \left|10\right\rangle \left\langle 10\right| + \mathrm{e}^{i\theta} \left|11\right\rangle \left\langle 11\right|. \tag{233}$$

We will see that various quantum computing tasks can be performed via combinations of the above gates. Define

$$A = \left|0\right\rangle \left\langle 0\right| - \left|1\right\rangle \left\langle 1\right|, \tag{234}$$

we first compute

$$
\begin{aligned}
U_H A U_H \left|j\right\rangle &= \frac{1}{\sqrt{2}} U_H A(\left|0\right\rangle + (-1)^j \left|1\right\rangle) && (235)\\
&= \frac{1}{\sqrt{2}} U_H(\left|0\right\rangle + (-1)^{j+1} \left|1\right\rangle) && (236)\\
&= \frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle + (-1)^{j+1} \left|0\right\rangle + (-1)^{j+2} \left|1\right\rangle) && (237)\\
&= \left|j \oplus 1\right\rangle = \left|\bar{j}\right\rangle . && (238)
\end{aligned}
$$

In other words, $U_H A U_H$ implements the NOT gate. This result will be frequently utilized in the discussion below.

Recall the notation $\left|jk\right\rangle = \left|j\right\rangle \otimes \left|k\right\rangle$, we now compute

$$
\begin{aligned}
& (U_H \otimes U_H) U_{CNOT} (U_H \otimes U_H) \left|jk\right\rangle && (239)\\
=\ & \frac{1}{2}(U_H \otimes U_H) U_{CNOT} (\left|0\right\rangle + (-1)^j \left|1\right\rangle) \otimes (\left|0\right\rangle + (-1)^k \left|1\right\rangle) \\
=\ & \frac{1}{2}(U_H \otimes U_H)(\left|00\right\rangle + (-1)^k \left|01\right\rangle + (-1)^j \left|11\right\rangle + (-1)^{j+k} \left|10\right\rangle) \\
=\ & \frac{1}{2}(U_H \otimes U_H)(\left|0\right\rangle \otimes (\left|0\right\rangle + (-1)^k \left|1\right\rangle) + \\
& (-1)^j \left|1\right\rangle \otimes (\left|1\right\rangle + (-1)^k \left|0\right\rangle) && (240)\\
=\ & \frac{1}{2}(U_H \otimes U_H)(\left|0\right\rangle \otimes (\left|0\right\rangle + (-1)^k \left|1\right\rangle) + \\
& (-1)^{j+k} \left|1\right\rangle \otimes (\left|0\right\rangle + (-1)^k \left|1\right\rangle) && (241)\\
=\ & \frac{1}{2}(U_H \otimes U_H)(\left|0\right\rangle + (-1)^{j+k} \left|1\right\rangle) \otimes (\left|0\right\rangle + (-1)^k \left|1\right\rangle) && (242)\\
=\ & \left|j \oplus k\right\rangle \otimes \left|k\right\rangle . && (243)
\end{aligned}
$$

Thus, the above operation $(U_H \otimes U_H) U_{CNOT} (U_H \otimes U_H) |jk\rangle$ leads to a variant of the CNOT gate, where the second bit k is the control bit and the first bit j is the target bit.

Similarly, one computes

$$\begin{aligned} & (I_2 \otimes U_H) U_P(\pi) (I_2 \otimes U_H) |jk\rangle & (244) \\ = & \frac{1}{\sqrt{2}} (I_2 \otimes U_H) U_P(\pi) |j\rangle \otimes (|0\rangle + (-1)^k |1\rangle) & (245) \\ = & \frac{1}{\sqrt{2}} (I_2 \otimes U_H) |j\rangle \otimes (|0\rangle + (-1)^{j+k} |1\rangle) & (246) \\ = & \frac{1}{2} |j\rangle \otimes |j \oplus k\rangle , & (247) \end{aligned}$$

which is in fact the U_{CNOT} gate, and

$$(I_2 \otimes U_H) U_{CNOT} (I_2 \otimes U_H) |jk\rangle = (-1)^{j \cdot k} |jk\rangle , \qquad (248)$$

which recovers the $U_P(\pi)$ gate.

Finally, we consider $U_{CNOT}(U_H \otimes I_2) |jk\rangle$, which is computed for all cases as

$$\begin{aligned} U_{CNOT}(U_H \otimes I_2) |00\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) & (249) \\ U_{CNOT}(U_H \otimes I_2) |01\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) & (250) \\ U_{CNOT}(U_H \otimes I_2) |10\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) & (251) \\ U_{CNOT}(U_H \otimes I_2) |11\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle), & (252) \end{aligned}$$

which are the Bell states. In other words, from the non-entanglement states, we have generated the entangled states.

Other examples of unitary gates

Let U be a 2×2 unitary matrix, we will show that the 4×4 matrix

$$V = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes U + \begin{pmatrix} \mathrm{e}^{i\alpha} & 0 \\ 0 & 0 \end{pmatrix} \otimes I_2 \tag{253}$$

is a unitary matrix. Since

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{e}^{i\alpha} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{e}^{i\alpha} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \tag{254}$$

and $UU^\dagger = I_2$, we obtain

$$\begin{aligned} VV^\dagger &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes I_2 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes I_2 && (255) \\ &= I_2 \otimes I_2 = I_4. && (256) \end{aligned}$$

The following matrix, known as the magic gate in quantum computing, is an unitary matrix

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & i & -1 \\ 1 & -i & 0 & 0 \end{pmatrix}. \tag{257}$$

It can also be shown that the magic gate admits the representation

$$M = U(I_2 \otimes U_H)(U_P \otimes U_P), \tag{258}$$

where

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{259}$$

and

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{260}$$

and

$$U_P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{261}$$

are Hadamard gate and a phase gate, respectively.

Given an orthonormal basis in $\mathbb{C}^N$,

$$|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{N-1}\rangle . \tag{262}$$

By the definition $\langle\phi_j|\phi_k\rangle = \delta_{jk}$, it can be verified that the matrix

$$U = \sum_{k=0}^{N-2} |\phi_k\rangle \langle\phi_{k+1}| + |\phi_{N-1}\rangle \langle\phi_0| \tag{263}$$

is an unitary matrix. We also see that

$$\mathrm{tr}(U) = 0 \tag{264}$$

as no term of the form $|\phi_k\rangle \langle\phi_k|$ appears in the sum. Since U maps the state $|\phi_k\rangle$ to the state $|\phi_{k-1}\rangle$ cyclically, applying the map N times leads to

$$U^N = I_N. \tag{265}$$

Consider the 8×8 matrix

$$U(\alpha) = \frac{\mathrm{e}^{i\alpha}}{\sqrt{2}}(I_2 \otimes I_2 \otimes I_2 + i\sigma_1 \otimes \sigma_1 \otimes \sigma_1), \tag{266}$$

where σ_1 is a Pauli matrix. By using the fact that

$$\sigma_1^\dagger = \sigma, \qquad \sigma_1^2 = I_2, \tag{267}$$

one can verify that $U(\alpha)$ is an unitary matrix. Moreover, for the product state

$$|\psi\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{268}$$

let's compute the action of the gate $U(\alpha)$ on the state. For convenience, we use the shorthand notations

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\uparrow\rangle\,, \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow\rangle \tag{269}$$

one has

$$\begin{aligned} U(\alpha)\,|\psi\rangle &= \frac{\mathrm{e}^{i\alpha}}{\sqrt{2}}(I_2 \otimes I_2 \otimes I_2 + i\sigma_1 \otimes \sigma_1 \otimes \sigma_1)(|\downarrow\rangle \otimes |\downarrow\rangle \otimes |\downarrow\rangle) \\ &= \frac{\mathrm{e}^{i\alpha}}{\sqrt{2}}(|\downarrow\rangle \otimes |\downarrow\rangle \otimes |\downarrow\rangle + i\,|\uparrow\rangle \otimes |\uparrow\rangle \otimes |\uparrow\rangle), \end{aligned} \tag{270}$$

which is related to a GHZ state.

Recall the Bell states,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{271}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \tag{272}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \tag{273}$$

$$|\Psi^-\rangle \;=\; \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle). \tag{274}$$

It can be directly verified that the Bell states can be transformed to each other under local unitary transforms (that is, tensor product $U \otimes V$ of 2×2 unitary matrices) as

$$\begin{aligned}
|\Phi^-\rangle &= (I_2 \otimes \sigma_3)\,|\Phi^+\rangle && (275)\\
|\Psi^+\rangle &= (I_2 \otimes \sigma_1)\,|\Phi^+\rangle && (276)\\
|\Psi^-\rangle &= (I_2 \otimes (-i\sigma_2))\,|\Phi^+\rangle\,. && (277)
\end{aligned}$$

Let $|0\rangle\,, |1\rangle\,, \ldots, |d-1\rangle$ be an orthonormal basis in the Hilbert space $\mathbb{C}^d$. Consider two normalized states $|\psi\rangle$, $|\phi\rangle$ in $\mathbb{C}^d$, the matrix

$$S = \sum_{j,k=0}^{d-1} (|j\rangle\,\langle k|) \otimes (|k\rangle\,\langle j|) \tag{278}$$

is the swap operator that performs the task

$$S(|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle \tag{279}$$

as shown below.

Indeed, we have

$$\begin{aligned}
& S(|\psi\rangle \otimes |\phi\rangle) && (280)\\
= & \sum_{j,k=0}^{d-1} ((|j\rangle \langle k|) \otimes (|k\rangle \langle j|))(|\psi\rangle \otimes |\phi\rangle) && (281)\\
= & \sum_{j,k=0}^{d-1} (|j\rangle \langle k|\psi\rangle) \otimes (|k\rangle \langle j|\phi\rangle) && (282)\\
= & \sum_{j,k=0}^{d-1} \langle k|\psi\rangle \langle j|\phi\rangle (|j\rangle \otimes |k\rangle) && (283)\\
= & \sum_{j,k=0}^{d-1} \langle k|\phi\rangle \langle j|\psi\rangle (|k\rangle \otimes |j\rangle) && (284)\\
= & \left(\sum_{k=0}^{d-1} \langle k|\phi\rangle |k\rangle\right) \otimes \left(\sum_{j=0}^{d-1} \langle j|\psi\rangle |j\rangle\right) && (285)\\
= & |\phi\rangle \otimes |\psi\rangle . && (286)
\end{aligned}$$

Quantum Fourier transform

Quantum Fourier transform is the foundation of quantum algorithms and computation. Consider the Hilbert space $\mathbb{C}^{2^n}$. Let $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$ be an orthonormal basis in this Hilbert space. The linear operator

$$U_{QFT} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \mathrm{e}^{-i2\pi kj/2^n} \left|k\right\rangle \left\langle j\right| \tag{287}$$

is defined as the quantum Fourier transform.

We first show that U_{QFT} is indeed a unitary gate. From the definition, we have

$$U_{QFT}^{\dagger} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \mathrm{e}^{i2\pi kj/2^n} \left|j\right\rangle \left\langle k\right|, \tag{288}$$

and therefore,

$$U_{QFT}^{\dagger} U_{QFT} \tag{289}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \sum_{l=0}^{2^n-1} \sum_{m=0}^{2^n-1} \mathrm{e}^{i2\pi(kj-lm)/2^n} \left|j\right\rangle \left\langle k|l\right\rangle \left\langle m\right| \tag{290}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \sum_{m=0}^{2^n-1} \mathrm{e}^{i2\pi(kj-km)/2^n} \left|j\right\rangle \left\langle m\right|. \tag{291}$$

For $j = m$, since

$$\mathrm{e}^{i2\pi(kj-km)/2^n} = 1, \tag{292}$$

one has

$$\sum_{k=0}^{2^n-1} \left(\mathrm{e}^{i2\pi(j-m)/2^n}\right)^k = 2^n. \tag{293}$$

For $j \neq m$, we have

$$\sum_{k=0}^{2^n-1} \left(\mathrm{e}^{i2\pi(j-m)/2^n} \right)^k = \frac{1 - \mathrm{e}^{i2\pi(j-m)}}{1 - \mathrm{e}^{i2\pi(j-m)/2^n}} = 0. \tag{294}$$

Therefore,

$$U_{QFT}^{\dagger} U_{QFT} = \sum_{j=0}^{2^n-1} |j\rangle \langle j| = I_{2^n}, \tag{295}$$

where the last equality is the completeness relation.

As an example, if we apply the quantum Fourier transform to the following state in Hilbert space $\mathbb{C}^8$ $(n = 3)$

$$|\psi\rangle = \frac{1}{2} \sum_{i=0}^{7} \cos(2\pi i/8) |i\rangle, \tag{296}$$

the resulting state is given by

$$U_{QFT} |\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |7\rangle). \tag{297}$$

Another related transform over the orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ in $\mathbb{C}^n$ is

$$U = \sum_{j=0}^{n-1} \mathrm{e}^{2\pi i j/n} |j\rangle \langle j|, \tag{298}$$

which can be similarly shown to be a unitary gate.

Inversion about average operator

In quantum search algorithm, an important ingredient is the inversion about average operator

$$U_{IA} = \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \left(\frac{2}{2^n} - \delta_{jk} \right) |k\rangle \langle j| \,, \tag{299}$$

which is an unitary gate as shown below.

By the fact that

$$U_{IA}^{\dagger} = \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \left(\frac{2}{2^n} - \delta_{jk} \right) |k\rangle \langle j| = U_{IA}, \tag{300}$$

we have

$$\begin{aligned} & U_{IA} U_{IA}^{\dagger} && (301) \\ = & \sum_{j,k,l,m=0}^{2^n-1} \left(\frac{2}{2^n} - \delta_{jk} \right) \left(\frac{2}{2^n} - \delta_{lm} \right) |k\rangle \langle j|m\rangle \langle l| && (302) \\ = & \sum_{j,k,l=0}^{2^n-1} \left(\frac{2}{2^n} - \delta_{jk} \right) \left(\frac{2}{2^n} - \delta_{lj} \right) |k\rangle \langle l| \,. && (303) \end{aligned}$$

Furthermore, we find

$$\sum_{j=0}^{2^n-1} \left(\frac{2}{2^n} - \delta_{jk} \right) \left(\frac{2}{2^n} - \delta_{lj} \right) \tag{304}$$

$$
\begin{aligned}
&= \sum_{j=0}^{2^n-1}\left(\frac{4}{2^{2n}} - \frac{2}{2^n}\delta_{jk} - \frac{2}{2^n}\delta_{lj} + \delta_{jk}\delta_{lj}\right) && (305)\\
&= \frac{4}{2^n} - \frac{2}{2^n} - \frac{2}{2^n} + \sum_{j=0}^{2^n-1}\delta_{jk}\delta_{lj} && (306)\\
&= \delta_{kl}. && (307)
\end{aligned}
$$

Therefore,

$$
U_{IA}U_{IA}^{\dagger} = \sum_{k=0}^{2^n-1} |k\rangle\langle k| = I_{2^n}. \qquad (308)
$$

6 Measurement

Basic concept and definitions

The concept of measurement is based on probability interpretation of quantum mechanics. Given a physical system in the state $|\psi\rangle$, the probability that it is in the state $|\chi\rangle$ is

$$0 \leq |\left\langle\psi|\chi\right\rangle|^2 \leq 1. \tag{309}$$

A positive operator-valued measure (POVM) is a collection of positive semi-definite operators

$$\{E_j : j = 1, 2, \ldots, n\} \tag{310}$$

that satisfies

$$\sum_{j=1}^{n} E_j = I_n. \tag{311}$$

In other words, a partition of identity operator by non-negative operators is called a POVM. When a state $|\psi\rangle$ is subject to such a POVM, the outcome j occurs with probability

$$p(j) = \left\langle\psi|E_j|\psi\right\rangle. \tag{312}$$

For example, consider the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{313}$$

as measured by the POVM

$$E_1 = |0\rangle\langle 0|\,, \qquad E_2 = |1\rangle\langle 1|\,. \tag{314}$$

The measurements are

$$p(1) \;=\; \langle\psi|E_1|\psi\rangle = \frac{1}{2} \tag{315}$$

$$p(2) \;=\; \langle\psi|E_2|\psi\rangle = \frac{1}{2}. \tag{316}$$

Consider the Hilbert space $\mathbb{C}^d$, a symmetric, informationally complete, positive operator-valued measure (SIC-POVM) consists of d^2 outcomes that are sub-normalized projection matrices Π_j on pure states

$$\Pi_j = \frac{1}{d}\,|\psi_j\rangle\langle\psi_j| \tag{317}$$

for $j, k = 1, \ldots, d^2$ such that

$$|\langle\psi_j|\psi_k\rangle|^2 = \frac{1 + d\delta_{jk}}{1+d}. \tag{318}$$

As an example, the following states form a SIC-POVM for $d = 2$,

$$|\psi_1\rangle \;=\; \begin{pmatrix} \sqrt{(3+\sqrt{3})/6} \\ \mathrm{e}^{i\pi/4}\sqrt{(3-\sqrt{3})/6} \end{pmatrix} \tag{319}$$

$$|\psi_2\rangle \;=\; \begin{pmatrix} \sqrt{(3+\sqrt{3})/6} \\ -\mathrm{e}^{i\pi/4}\sqrt{(3-\sqrt{3})/6} \end{pmatrix} \tag{320}$$

$$|\psi_3\rangle \;=\; \begin{pmatrix} \mathrm{e}^{i\pi/4}\sqrt{(3-\sqrt{3})/6} \\ \sqrt{(3+\sqrt{3})/6} \end{pmatrix} \tag{321}$$

$$|\psi_4\rangle \;=\; \begin{pmatrix} -\mathrm{e}^{i\pi/4}\sqrt{(3-\sqrt{3})/6} \\ \sqrt{(3+\sqrt{3})/6} \end{pmatrix}. \tag{322}$$

Examples of measurement computation

Consider the state

$$|\psi\rangle = \frac{1}{\sqrt{3}}\,|00\rangle + \sqrt{\frac{2}{3}}\,|11\rangle \tag{323}$$

and the state

$$|\phi\rangle = |11\rangle\,, \tag{324}$$

the probability of finding $|\psi\rangle$ in the state $|\phi\rangle$ is computed as

$$p = |\,\langle\psi|\phi\rangle\,|^2 = \frac{2}{3}, \tag{325}$$

where we have used the fact that

$$\langle 11|00\rangle = 0, \qquad \langle 11|11\rangle = 1. \tag{326}$$

Consider the Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \tag{327}$$

in $\mathbb{C}^4$ and the states

$$\begin{aligned} |\alpha\rangle &= \cos(\alpha)\,|0\rangle + \sin(\alpha)\,|1\rangle && (328) \\ |\beta\rangle &= \cos(\beta)\,|0\rangle + \sin(\beta)\,|1\rangle && (329) \end{aligned}$$

in $\mathbb{C}^2$, we will find the probability

$$p(\alpha, \beta) = |(\langle\alpha| \otimes \langle\beta|)\,|\psi\rangle\,|^2. \tag{330}$$

Since

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = \langle 0|1\rangle = 0, \tag{331}$$

it follows that

$$\begin{aligned} (\langle 0| \otimes \langle 1|)(|0\rangle \otimes |1\rangle) &= 1 && (332) \\ (\langle 1| \otimes \langle 0|)(|1\rangle \otimes |0\rangle) &= 1. && (333) \end{aligned}$$

Thus, we find

$$\begin{aligned} p(\alpha, \beta) &= \frac{1}{2}(\cos(\alpha)\sin(\beta) - \sin(\alpha)\cos(\beta))^2 && (334) \\ &= \frac{1}{2}\sin^2(\alpha - \beta). && (335) \end{aligned}$$

We conclude that the probability $p(\alpha, \beta)$ is no more than 1/2 as $\sin^2(\phi) \leq 1$ for all $\phi \in \mathbb{R}$.

Consider the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{336}$$

and the state $\langle 0| \otimes I_2$, a simple calculation shows that

$$(\langle 0| \otimes I_2) |\psi\rangle = \frac{1}{\sqrt{2}} |1\rangle . \tag{337}$$

The above result is interpreted as that the system is measured with probability 1/2, which collapses to the state $|1\rangle$ after the measurement. This is known as partial measurement.

7 Entropy and Entanglement

von Neumann entropy and basic properties

For any density operator

$$\rho = \sum_{j=1}^{n} \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right|, \qquad \lambda_j \geq 0, \qquad \sum_{j=1}^{n} \lambda_j = 1 \tag{338}$$

with $\langle\psi_j|\psi_k\rangle = \delta_{jk}$, the von Neumann entropy is defined as

$$S(\rho) = -\mathrm{tr}(\rho \ln(\rho)) \tag{339}$$

or equivalently

$$S(\rho) = -\sum_{j=1}^{n} \lambda_j \ln(\lambda_j), \tag{340}$$

where $\ln(\cdot)$ denotes logarithm of base 2. Thus, the von Neumann entropy is equal to the Shannon entropy of the eigenvalues.

We have

$$S(\rho) \geq 0 \tag{341}$$

with equality if and only if ρ is a pure state, that is $\rho = \left|\psi\right\rangle \left\langle\psi\right|$. Furthermore, we have the inequality

$$S(\rho) \leq \ln(n), \tag{342}$$

where n is the dimension of ρ. We find equality if and only if

$$\rho = \frac{1}{n} I, \tag{343}$$

where I is the identity operator.

The entropy is unchanged under unitary transformation

$$S(U\rho U^\dagger) = S(\rho). \tag{344}$$

For a composite system AB, we have

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B). \tag{345}$$

As an example, let's consider the density matrix of a pure state

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \end{pmatrix}. \tag{346}$$

As can be easily obtained, the eigenvalues of ρ are 0 and 1. Therefore, the von Neumann entropy is computed as

$$S(\rho) = 0, \tag{347}$$

where we have used the fact

$$0\ln(0) = 0, \qquad 1\ln(1) = 0. \tag{348}$$

Consider another example of density matrix of a mixed state

$$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}, \tag{349}$$

since $\ln(1/2) = -1$, the von Neumann entropy is obtained as

$$S(\rho) = 1. \tag{350}$$

Information capacity

Let ρ_{AB} be a density matrix defined on a $N \times N$-dimensional Hilbert space $\mathcal{H} \otimes \mathcal{H}$. The information capacity is defined as

$$C(\rho) = \ln(N) + S(\rho_B) - S(\rho_{AB}), \tag{351}$$

where ρ_B is the reduced density matrix obtained by the partial trace $\rho_B = \mathrm{tr}_A(\rho_{AB})$ and $S(\rho)$ is the von Neumann entropy.

Consider the example of a Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle), \tag{352}$$

the corresponding information capacity is computed as follows. We first find density matrix of the pure state as

$$\rho_{AB} = |\psi\rangle \langle\psi| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{353}$$

By using the partial trace formula (167), we obtain

$$\rho_B = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}. \tag{354}$$

With $N = 2$ and $S(\rho_{AB}) = 0$, it follows that (details left as an exercise)

$$C(\rho) = \ln(N) + S(\rho_B) - S(\rho_{AB}) = 2. \tag{355}$$

Mutual information

Consider the normalized states $|\psi_k\rangle$, $k = 0, 1, \ldots, N-1$ in the Hilbert space $\mathbb{C}^N$. A positive operator valued measure is specified by a decomposition of the identity matrix I_N into M positive semidefinite matrices P_m, that is

$$I_N = \sum_{m=0}^{M-1} P_m. \tag{356}$$

The mutual information is defined by

$$I = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} p_{nm} \ln_N \left(\frac{p_{nm}}{p_{n\cdot} p_{\cdot m}} \right), \tag{357}$$

where $p_{nm} = \langle \psi_n | P_m | \psi_n \rangle$ are the joint probabilities and

$$p_{n\cdot} = \sum_{m=0}^{M-1} p_{nm}, \qquad p_{\cdot m} = \sum_{n=0}^{N-1} p_{nm} \tag{358}$$

are the marginals.

Consider the example of $M = N = 2$ with the states

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \qquad |\psi_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{359}$$

and the decomposition of I_2,

$$P_0 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad P_1 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{360}$$

the mutual information is calculated as follows. Straightforward computation leads to (details left as an exercise)

$$p_{00} = \langle\psi_0|P_0|\psi_0\rangle = 0, \qquad p_{10} = \langle\psi_1|P_0|\psi_1\rangle = \frac{1}{2} \tag{361}$$

$$p_{01} = \langle\psi_0|P_1|\psi_0\rangle = 1, \qquad p_{11} = \langle\psi_1|P_1|\psi_1\rangle = \frac{1}{2}. \tag{362}$$

Thus,

$$p_{0\cdot} = 1, \;\; p_{1\cdot} = 1, \;\; p_{\cdot 0} = \frac{1}{2}, \;\; p_{\cdot 1} = \frac{3}{2}, \tag{363}$$

which leads to

$$I = 0. \tag{364}$$

Quantum Entanglement

Entanglement is the characteristic trait of quantum mechanics, which enforces its entire departure from classical lines of thought. Entanglement is the physical phenomenon, the medium, and, most importantly, the resources that enable quantum computing and other quantum technologies.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two finite-dimensional Hilbert spaces and let $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Then $|\psi\rangle$ is said to be disentangled, separable or a product state if there exist states $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ such that

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,, \tag{365}$$

and otherwise $|\psi\rangle$ is said to be entangled.

For example, the normalized state in $\mathbb{C}^4$

$$\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{366}$$

is a product state.

An example of entangled state is a polarization state

$$\frac{1}{\sqrt{2}}\left(|H\rangle \otimes |V\rangle + \mathrm{e}^{i\phi}\,|V\rangle \otimes |H\rangle\right), \tag{367}$$

where H denotes horizontal polarization and V denotes vertical polarization. This is one of the Bell states.

In fact, the four Bell states (85)-(88) are all entangled states. As an example, let's take a closer look at the Bell state

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle). \tag{368}$$

This state can not be written as a product state. Assume that it would

$$\begin{aligned} & (c_0\,|0\rangle + c_1\,|1\rangle) \otimes (d_0\,|0\rangle + d_1\,|1\rangle) \\ = \; & \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle), \end{aligned} \tag{369}$$

where $|c_0|^2 + |c_1|^2 = 1$ and $|d_0|^2 + |d_1|^2 = 1$. Then, we obtain the system of four equations

$$c_0 d_0 = 0, \quad c_0 d_1 = \frac{1}{\sqrt{2}}, \quad c_1 d_0 = -\frac{1}{\sqrt{2}}, \quad c_1 d_1 = 0. \tag{370}$$

The set of equations admits no solution. Thus, the Bell state (368) is entangled.

Consider the 2×2 unitary matrix

$$U(\theta,\phi) = \begin{pmatrix} \cos(\theta/2) & \mathrm{e}^{-i\phi}\sin(\theta/2) \\ -\mathrm{e}^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \tag{371}$$

we will show that the state

$$(U(\theta_1,\phi_1) \otimes U(\theta_2,\phi_2)) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{372}$$

is entangled. We use the fact that the vector $(x_1, x_2, x_3, x_4)^T \in \mathbb{C}^4$ is separable if and only if $x_1x_4 = x_2x_3$. We obtain

$$U(\theta_1,\phi_1)\begin{pmatrix}1\\0\end{pmatrix} \otimes U(\theta_2,\phi_2)\begin{pmatrix}1\\0\end{pmatrix} + U(\theta_1,\phi_1)\begin{pmatrix}0\\1\end{pmatrix} \otimes U(\theta_2,\phi_2)\begin{pmatrix}0\\1\end{pmatrix}$$
$$= \begin{pmatrix} \cos(\theta_1/2)\cos(\theta_2/2) + \mathrm{e}^{-i(\phi_1+\phi_2)}\sin(\theta_1/2)\sin(\theta_2/2) \\ \cos(\theta_2/2)\mathrm{e}^{-i\phi_1}\sin(\theta_1/2) - \cos(\theta_1/2)\mathrm{e}^{i\phi_2}\sin(\theta_2/2) \\ \cos(\theta_1/2)\mathrm{e}^{-i\phi_2}\sin(\theta_2/2) - \cos(\theta_2/2)\mathrm{e}^{i\phi_1}\sin(\theta_1/2) \\ \cos(\theta_1/2)\cos(\theta_2/2) + \mathrm{e}^{i(\phi_1+\phi_2)}\sin(\theta_1/2)\sin(\theta_2/2) \end{pmatrix}.$$

Hence, $x_1x_4 \neq x_2x_3$ and the state is entangled.

We can also test whether a state is entangled or not by calculating the von Neumann entropy (340) by using the criterion (341).

For example, consider the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ and the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \tag{373}$$

we now calculate the von Neumann entropy of the subsystems

$$S(\rho_A) = -\mathrm{tr}(\rho_A \ln(\rho_A)), \qquad S(\rho_B) = -\mathrm{tr}(\rho_B \ln(\rho_B)). \tag{374}$$

We first compute the density matrix ρ as

$$\rho = |\psi\rangle \langle\psi| = \frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{375}$$

We then choose the standard basis in $\mathbb{C}^2$ to calculate the partial trace as

$$\begin{aligned} \rho_A \;&=\; I_2 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rho \left(I_2 \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) + \\ &\quad\; I_2 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rho \left(I_2 \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) \end{aligned} \tag{376}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \rho \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rho \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{377}$$

$$= \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{378}$$

In the same manner, we obtain

$$\rho_B = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{379}$$

Thus, in this case $\rho_A = \rho_B$. The eigenvalues of ρ_A found to be 0 and 1. Therefore, by using the fact that $0 \ln(0) = 0, 1 \ln(1) = 0$, the von Neumann entropy is

$$S(\rho_A) = S(\rho_B) = 0. \tag{380}$$

We then conclude that the state $|\psi\rangle$ is not entangled.

As another example, consider the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \tag{381}$$

we now compute von Neumann entropy of the subsystem $\mathcal{H}_A$,

$$S(\rho_A) = -\mathrm{tr}(\rho_A \ln(\rho_A)) \tag{382}$$

where $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. The density matrix ρ is obtained as

$$\rho = |\psi\rangle \langle\psi| = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}. \tag{383}$$

We choose the standard basis in $\mathbb{C}^2$ to calculate the partial trace as (details left as an exercise)

$$\rho_A = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{384}$$

The von Neumann entropy is then obtained as

$$S(\rho_A) = -\frac{1}{2} \ln(1/2) - \frac{1}{2} \ln(1/2) = 1. \tag{385}$$

Therefore, the state $|\psi\rangle$ is entangled.

8 Teleportation

Basic concept and definitions

Teleportation is the transmission of quantum information using a classical channel and entanglement. It demonstrates the use of entanglement as a communication resource. The simplest case is to consider the teleportation of a single qubit using two bits of classical communication and one entangled pair. Quantum teleportation is the transport of an unknown quantum state from one place to another.

The key idea is that two distant operators, Alice (A) at a sending station and Bob (B) at a receiving terminal, share an entangled quantum bipartite state and exploit its nonlocal character as a quantum resource. The resource state can be a Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B \right), \tag{386}$$

where qubit 1 is given to Alice and qubit 2 is given to Bob. Alice intends to transport an unknown state of a third qubit to Bob. She performs a complete projective measurement on the joint system consisting of qubits 1 and 3 and then conveys its outcome to Bob via a classical communication channel. Bob makes use of the information transmitted classically by Alice to transform its reduced state into an output that is an accurate replica of the original unknown input.

To illustrate the above description, consider the task of teleporting one qubit of the state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \qquad |a|^2 + |b|^2 = 1 \tag{387}$$

via an entangled resource state shared by Alice and Bob as

$$|\phi\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{388}$$

The task is to show how the measurement of the first two qubits of the state $|\phi\rangle$ can be used to obtain the state $|\psi\rangle$ as the last qubit. Recall that Alice has the first qubit of $|\phi\rangle$ and Alice and Bob share the second and third qubits of $|\phi\rangle$. We first need to show that the state $|\phi\rangle$ can be written as (details left as an exercise)

$$\begin{aligned} |\phi\rangle \;=\; & \frac{1}{2\sqrt{2}}(|00\rangle + |11\rangle) \otimes (a\,|0\rangle + b\,|1\rangle) + \\ & \frac{1}{2\sqrt{2}}(|00\rangle - |11\rangle) \otimes (a\,|0\rangle - b\,|1\rangle) + \\ & \frac{1}{2\sqrt{2}}(|01\rangle + |10\rangle) \otimes (a\,|1\rangle + b\,|0\rangle) + \\ & \frac{1}{2\sqrt{2}}(|01\rangle - |10\rangle) \otimes (a\,|1\rangle - b\,|0\rangle). \end{aligned} \tag{389}$$

From the state $|\phi\rangle$, we can see that the first two qubits are in each of the Bell states

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{390}$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{391}$$

with equal probability. Thus, if we measure the first two qubits in the Bell basis we obtain a result corresponding to each of the Bell states. At the same time, we can perform a transform to obtain $|\psi\rangle$ in the last qubit according to the following table

Bell State	Transform
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	I_2
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\|0\rangle \langle 0\| - \|1\rangle \langle 1\|$
$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	U_{NOT}
$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	$\|0\rangle \langle 1\| - \|1\rangle \langle 0\|$

After measurement and applying the corresponding transform we obtain $|\psi\rangle$ as the last qubit.

Unitary transformation is often used in the entangled resource state in teleporting qubits. To see the use of unitary transformations in preparing the teleportation, we consider the following examples. For the state in the Hilbert space $\mathcal{H} = \mathbb{C}^{16}$,

$$|\psi_0\rangle = |0101\rangle \,, \tag{392}$$

let

$$\begin{aligned} |\psi_1\rangle &= B\,|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |0110\rangle) && (393) \\ |\psi_2\rangle &= U\,|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle) && (394) \\ |\psi_3\rangle &= S\,|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0101\rangle - |1010\rangle) && (395) \\ |\psi_4\rangle &= U^\dagger\,|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0101\rangle - |0110\rangle) && (396) \\ |\psi_5\rangle &= B^\dagger\,|\psi_4\rangle = -\,|0110\rangle \,, && (397) \end{aligned}$$

the corresponding unitary transformations B and U are found as follows. Notice first that B and U are 16×16 unitary matrices, where the above equations do not determine B and U uniquely. These equations tell us that

$$\begin{aligned} B\,|0101\rangle &= \frac{1}{\sqrt{2}}(|0101\rangle + |0110\rangle) && (398) \\ U\frac{1}{\sqrt{2}}(|0101\rangle + |0110\rangle) &= \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle) && (399) \\ U^\dagger\frac{1}{\sqrt{2}}(|0101\rangle - |1010\rangle) &= \frac{1}{\sqrt{2}}(|0101\rangle - |0110\rangle) && (400) \\ B^\dagger\frac{1}{\sqrt{2}}(|0101\rangle - |0110\rangle) &= -\,|0110\rangle \,. && (401) \end{aligned}$$

For the matrix B, we have

$$\begin{aligned} B\left|0101\right\rangle &= \left|01\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle) & (402) \\ B\left|0110\right\rangle &= \left|01\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|10\right\rangle - \left|01\right\rangle). & (403) \end{aligned}$$

One solution is

$$B = \frac{1}{\sqrt{2}} I_4 \otimes (\left|\gamma\right\rangle\left\langle 01\right| + \left|\delta\right\rangle\left\langle 10\right| + \left|\alpha\right\rangle\left\langle 00\right| + \left|\beta\right\rangle\left\langle 11\right|), \qquad (404)$$

where

$$\begin{aligned} \left|\alpha\right\rangle = \left|00\right\rangle + \left|11\right\rangle, &\qquad \left|\beta\right\rangle = \left|00\right\rangle - \left|11\right\rangle & (405) \\ \left|\gamma\right\rangle = \left|01\right\rangle + \left|10\right\rangle, &\qquad \left|\delta\right\rangle = \left|10\right\rangle - \left|01\right\rangle. & (406) \end{aligned}$$

This means that B maps from the computational basis to the Bell basis in the first two qubits.

For the matrix U, we have

$$\begin{aligned} U\left(\left|01\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)\right) &= \frac{1}{\sqrt{2}}(\left|0101\right\rangle + \left|1010\right\rangle) & (407) \\ U\left(\left|01\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)\right) &= \frac{1}{\sqrt{2}}(\left|0101\right\rangle - \left|1010\right\rangle), & (408) \end{aligned}$$

which leads to

$$U\left|0101\right\rangle = \left|0101\right\rangle, \qquad U\left|0110\right\rangle = \left|1010\right\rangle. \qquad (409)$$

A solution for U is then

$$U = I_{16} + (|1010\rangle - |0110\rangle)(\langle 0110| - \langle 1010|), \qquad (410)$$

that is, U is an identity matrix except on the subspace spanned by $|0110\rangle$ and $|1010\rangle$, where U swaps $|0110\rangle$ and $|1010\rangle$.

References

The lecture notes are largely based on the following two books.

[1] W.-H. Steeb and Y. Hardy, *Problems and Solutions in Quantum Computing and Quantum Information (4th edition).* Singapore: World Scientific Publishing Company, 2018.

[2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 2010.