Some important entangled states

Example The Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

are entangled states and form an orthonormal basis for the two qubit systems.

Example In the 3 qubit system, we have that GHZ state and W state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad \text{and} \quad |W\rangle\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle).$$

Example One can do measurement of the first qubit for a state vector in a n qubit system. For instance,

$$|x\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1.$$

We measure the first qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. Set

$$|x\rangle = |0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(c|0\rangle + d|1\rangle)$$

$$= u|0\rangle((a/u)|0\rangle + (b/u)|1\rangle) + v|1\rangle((c/v)|0\rangle + (d/v)|1\rangle),$$

where $u = \sqrt{|a|^2 + |b|^2}$ and $v = \sqrt{|c|^2 + |d|^2}$. We can measure the first qubit, say, by setting $A = (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes I_2$ so that

$$M_0 = |0\rangle\langle 0| \otimes I_2, \quad M_1 = |1\rangle\langle 1| \otimes I_2.$$

Applying M_0 and M_1, we obtain 0 with probability $\langle x|M_0|x\rangle = u^2$ and 1 with probability v^2; the state $|x\rangle$ collapses to

$$|0\rangle \otimes ((a/u)|0\rangle + (b/u)|1\rangle) \text{ and } |1\rangle \otimes ((c/v)|0\rangle + (d/v)|1\rangle), \text{ r}$$

espectively, upon measurement.

Einstein-Podolsky-Rosen (EPR) Phenomenon

- Consider the EPR state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

  Alice gets the first particle and Bob gets the second one.

- When Alice measures, Bob's particle will change instantaneously to $|1\rangle$ or $|0\rangle$ depending on the measured outcome of Alice being $|0\rangle$ or $|1\rangle$.

- For example, set up the apparatus for the observable

$$A = |0\rangle\langle 0| \otimes I_2 - |1\rangle\langle 1| \otimes I_2.$$

- If Alice sees the reading 1, then Bob's qubit is to $|1\rangle$; if Alice sees the reading -1, then Bob's qubit is $|0\rangle$.

- Alice cannot control her measurement and hence the reading of Bob! So, it does not violate the special theory of relativity. (It is impossible that information travels faster than light!)

- However, they can measure their individual states around the same time, and decide to make a move according to $|01\rangle$ or $|10\rangle$ occur.

- Bell proposed an experiment which confirmed that there cannot be a hidden rule governing the measurement of the entangled pair.

Bell inequality

About 30 years after the EPR paper was published, an experiment test was proposed to check whether the measurement of entangled pairs follow a certain predetermined rule imposed by Nature, or the postulate of quantum mechanics.

Here is the proposed experiments. Suppose Charlie prepares an entangled pair of qubits (photons or particles) and sends the first one to Alice and the second one to Bob. Alice will apply one of her two measurement schemes, say, Q and R, each will produce a measured value in $\{1, -1\}$. Bob will also apply one of his two measurement schemes, say, S and T, each will produce a measured value in $\{1, -1\}$.

Let us consider

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T.$$

Because $R, Q \in \{1, -1\}$, it follows that either $(Q + R)S = 0$ or $(R - Q)T = 0$. As a result, $QS + RS + RT - QT \in \{2, -2\}$.

Suppose there is a hidden rule governing the measurement outcomes, and $p(q, r, s, t)$ is the probability that, *before* the measurements are performed, the system is in the state $(Q, R, S, T) = (q, r, s, t)$. Then the expectation value $E(QS + RS + RT - QT) = E(QS) + E(RS) + E(RT) - E(QT)$ satisfies

$$\begin{aligned} |E(QS + RS + RT - QT)| &= \sum_{(q,r,s,t)} p(q, r, s, t)|qs + rs + rt - qt| \\ &\leq \sum_{(q,r,s,t)} p(q, r, s, t) \cdot 2 = 2. \end{aligned}$$

So, we get the **Bell inequality**

$$|E(QS) + E(RS) + E(RT) - E(QT)| \leq 2. \tag{0.1}$$

Suppose Charlie prepares an entangled state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

and gives Alice the first qubit, and Bob the second one. Alice uses the measurement operators $Q = \sigma_z$ and $R = \sigma_x$, and Bob uses the measurement operators $S = \frac{-1}{\sqrt{2}}(\sigma_z + \sigma_x)$ and $T = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$. Then

$$E(QS) = \langle\Psi^-|Q \otimes S|\Psi^-\rangle = \frac{1}{\sqrt{2}}, \quad E(RS) = \langle\Psi^-|R \otimes S|\Psi^-\rangle = \frac{1}{\sqrt{2}},$$

$$E(RT) = \langle\Psi^-|R \otimes T|\Psi^-\rangle = \frac{1}{\sqrt{2}}, \quad E(QT) = \langle\Psi^-|Q \otimes T|\Psi^-\rangle = \frac{-1}{\sqrt{2}},$$

and hence

$$E(QS + RS + RT - QT) = 4/\sqrt{2} = 2\sqrt{2}. \qquad (0.2)$$

This equality clearly violates the Bell inequality.

To determine whether (0.1) or (0.2) is valid, Alice and Bob can estimate $E(QS)$ by performing measurements on many copies of $|\Psi^-\rangle$, and record their results. After the experiments, they can multiply their measurements when they used the measurement schemes Q and S, respectively. Similarly, they can estimate $E(RS), E(RT), E(QT)$, so as to obtain an estimate of $E(QS + RS + RT - QT)$.

Experimental results showed strong support to (0.2). Hence, the EPR proposal that there is a hidden rule governing the measurement results of entangled pair was ruled out.

Measurements

For each outcome m, construct a measurement operator M_m so that the probability of obtaining outcome m in the state $|x\rangle$ is computed by

$$p(m) = \langle x|M_m^\dagger M_m|x\rangle$$

and the state immediately after the measurement is

$$|m\rangle = \frac{M_m|x\rangle}{\sqrt{p(m)}}.$$

Example Let $M = \{M_0, M_1\}$ with $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Then for $|x\rangle = a|0\rangle + b|1\rangle$ with $a \neq 0$, $p(0) = |a|^2$, $M_0|x\rangle = a|0\rangle/|a|$, which is the same as the vector state $|0\rangle$.

- In general, suppose an observable M is given with measurement operators M_m. Then setting $P_i = M_i^\dagger M_i$, we require that $\sum_m P_m = I_n$.
- If there are many copy of a state $|x\rangle$, then the expected value of M is

  $$E(M) = \langle M\rangle = \sum_m mp(m) = \sum_m m\langle x|P_m|x\rangle = \langle x|M|x\rangle.$$

  Here M can be identified with $\sum_m mP_m$.
- The standard derivation is

  $$\Delta(M) = \sqrt{\langle (M - \langle M\rangle)^2} = \sqrt{\langle M^2\rangle - \langle M\rangle^2}.$$

- The variance (square of standard deviation) is

  $$\langle (M - \langle M\rangle)^2\rangle = \langle x|M^2|x\rangle - \langle x|M|x\rangle^2.$$

Another proof of no-cloning theorem

The no-cloning theorem may be proved by using the special theory of relativity, which assumes no information can propagate faster than the speed of light.

Suppose Alice and Bob share a Bell state

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

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Readers are encouraged to verify the second equality. Alice keeps the first qubit while Bob keeps the second. If Alice wants to send Bob a bit "0", she measures her qubit in $\{|0\rangle, |1\rangle\}$ basis while if she wants to send "1", she employs $\{|+\rangle, |-\rangle\}$ basis for her measurement. Bob always measures his qubit in $\{|0\rangle, |1\rangle\}$ basis.

After Alice's measurment and before Bob's measurment, Bob's qubit is $|0\rangle$ or $|1\rangle$ if Alice sent "0" while it is $|+\rangle$ or $|-\rangle$ if Alice sent "1".

Suppose Bob is able to clone his qubit. He makes many copies of his qubit and measures them in $\{|0\rangle, |1\rangle\}$ basis. If Alice sent "0", Bob will obtain $0, 0, 0, \ldots$ or $1, 1, 1, \ldots$ while if she sent "1", Bob will obtain approximately 50% of 0's and 50% of 1's. Suppose Bob received $|\pm\rangle$ and made N clones, then the probability of obtaining the same outcome is $1/2^{N-1}$, which is negligible if N is sufficiently large. Note that Bob obtains the bit Alice wanted to send immediately after Alice's measurement assuming it does not take long to clone his qubit. This could happen even if Alice and Bob are separated many light years apart, thus in contradiction with the special theory of relativity. □

Mixed States and Density Matrices

- A system is in a mixed state if there is a (classical) probability p_i that the system is in state $|x_i\rangle$ for $i = 1, \ldots, N$.
- If there is only one possible state, i.e., $p_1 = 1$, then the system is in pure state.
- The expectation value (mean) of the measurement of the system corresponding to the observable described by the Hermitian matrix A is

$$\langle A \rangle = \sum_{j=1}^{N} p_j \langle x_j | A | x_j \rangle = \mathrm{tr}\,(A\rho),$$

  where

$$\rho = \sum_{j=1}^{N} p_j |x_j\rangle\langle x_j|$$

  is a density operator (matrix).

Example $\frac{1}{2}(|e_1\rangle\langle e_1| + |e_2\rangle\langle e_2|) = \frac{1}{2} I_2$ is a maximally mixed state.

It is the mixed state of $\frac{1}{2}(|e_1\rangle\langle e_1| + |e_2\rangle\langle e_2|)$ with

$$|e_1\rangle = (\cos\theta, \sin\theta)^t \quad \text{and} \quad |e_2\rangle = (\sin\theta, -\cos\theta)^t, \qquad \theta \in [0, 2\pi).$$

Definition A (Hermitian) matrix $A \in M_n$ is positive semidefinite if

$$\langle x|A|x\rangle \geq 0 \text{ for all } |x\rangle \in \mathbb{C}^n.$$

Proposition Let $A \in M_n$.

(a) The matrix $A \in M_n$ is positive semidefinite if and only if it has nonnegative eigenvalues.

(b) The matrix A is a density matrix if and only if it is positive semi-definite with trace 1.

Proof. (a) Let $A = UDU^\dagger$. If A has a negative eigenvalues λ with unit eigenector $|\lambda\rangle$, then $\langle\lambda|A|\lambda\rangle = \lambda < 0$.

If A has nonnegative eigenvalues, then for any $|x\rangle \in \mathbb{C}^n$ we can let $|y\rangle = U^\dagger|x\rangle$ so that $\langle x|A|x\rangle = \langle y|D|y\rangle = \sum_{j=1}^n \lambda_j |y_|^2 \geq 0$.

(b) If $A = \sum_{j=1}^r p_r |v_j\rangle\langle v_j|$ is a density matrix, then

$$\langle x|A|x\rangle = \sum_{j=1}^r p_r |\langle x|v_j\rangle|^2 \geq 0,$$

and $\mathrm{tr}\,(A) = \sum_{j=1}^r p_j \mathrm{tr}\, |v_j\rangle\langle v_j| = \sum_{j=1}^r p_j = 1$.

If A is positive semidefinite with trace 1, then

$A = \sum_{j=1}^n \lambda_j |\lambda_j\rangle\langle\lambda_j|$ with $\sum_{j=1}^n \lambda_j = 1$. □

Postulates of a quantum system in mixed states.

A1' A physical state is specified by a density matrix $\rho : \mathcal{H} \to \mathcal{H}$, which is positive semidefinite with trace equal to one.

A2' The mean value of an observable associate with the Hermitian matrix A is $\langle A \rangle = \mathrm{tr}\,(\rho A)$.

After a measurement, the mixed state ρ will collapses to one of the eigenstate ρ_j with a probability of $p_j = \mathrm{tr}\,(\rho\rho_j)$. Note that $\sum_j p_j = 1$.

A3' The temporal evolution of the density matrix is given by the Liouville-von Neumann equation

$$i\hbar\frac{d}{dt}\rho = [H, \rho] = H\rho - \rho H,$$

where H is the system Hamiltonian.

Theorem A state $\rho \in D_n$ is pure if and only if any one of the following condition holds.

$$\text{(a)} \quad \rho^2 = \rho. \qquad \text{(b)} \quad \operatorname{tr} \rho^2 = 1.$$

Proof. Suppose $\rho = |\psi\rangle\langle\psi|$ is a pure state.

Then $\rho^2 = (|\psi\rangle\langle\psi|)(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| = \rho$.

Thus, the condition (a) holds.

If (a) holds, then $\operatorname{tr} \rho^2 = \operatorname{tr} \rho = 1$. Thus, the condition (b) holds.

If (b) holds, and $\rho = \sum_{j=1}^n \lambda_j |\lambda_j\rangle\langle\lambda_j|$,

where $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$ and $\sum_{j=1}^n \lambda_j = 1$.

Then $\rho^2 = \sum_{j=1}^n \lambda_j^2 |\lambda_j\rangle\langle\lambda_j|$ has eigenvalues $\lambda_1^2, \ldots, \lambda_n^2$.

So, if $\operatorname{tr} \rho^2 = 1 = \operatorname{tr} \rho$, then

$$0 = \sum_{j=1}^n (\lambda_j - \lambda_j^2) = \sum_{j=1}^n \lambda_j (1 - \lambda_j)$$

so that all the nonnegative numbers $\lambda_j(1 - \lambda_j)$ is zero.

Thus, $\lambda_j \in \{0, 1\}$. Since $\sum_{j=1}^n \lambda_j = 1$, we see that

$\lambda_1 = 1$ and $\lambda_j = 0$ for $j > 1$.

Thus, $\rho = |\lambda_1\rangle\langle\lambda_1|$ is a pure state. □

Definition 2.1 Suppose $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. A state ρ is **uncorrelated** if $\rho = \rho_1 \otimes \rho_2$; it is **separable** if it is a **convex** combination of uncorrelated states, i.e.,

$$\rho = \sum_{j=1}^{r} p_j \rho_{1,j} \otimes \rho_{2,j}.$$

Otherwise, it is **inseparable** (or **entangled**).

Remark Every $A \in \mathcal{H}$ is a **linear** combination of product states with linear coefficient summing up to 1. But some of the coefficients may be negative.

Reason Suppose the basis $\mathcal{B}_1 \subseteq M_n$ contains the pure states:

$$|e_{1,j}\rangle\langle e_{1,j}|, 1 \leq j \leq m\}, \quad 1 \leq j \leq m,$$

and $\{|x\rangle\langle x|$ with

$$|x\rangle = \frac{1}{\sqrt{2}}(|e_{1,j} + |e_{1,k})\rangle, \frac{1}{\sqrt{2}}(|e_{1,j} + i|e_{1,k})\rangle, \quad 1 \leq j < k \leq m.$$

Then $\mathcal{B}_1$ is a basis for M_m. Similarly, there is a basis for M_n consisting of pure states. As a result, $\mathcal{B} = \{\rho_1 \otimes \rho_2 : \rho_j \in \mathcal{B}_j, j = 1, 2\}\}$ is a basis for $M_m \otimes M_n = M_{mn}$.

Remarks

The set of tensor states and separable states are small.

Separable states are closely related to product states.

Inseparable states are the resource for quantum computing.

Proposition Let $\rho \in D_{mn}$.

(a) Suppose ρ has rank one. Then ρ is separable if only only if $\rho = \rho_1 \otimes \rho_2$ for rank one matrices $\rho_1 \in D_m, \rho_2 \in D_n$.

(b) If $\rho \in D_{mn}$ is separable, then ρ is a convex combination of quantum states of the form $\rho_1 \in D_m, \rho_2 \in D_n$, where ρ_1, ρ_2 are pure states.

Partial transpose - a tool to determine inseparable sates

The **partial transpose** with respect to $\mathcal{H}_2$ is defined by

$$\rho^{\mathrm{pt}} = \rho_1 \otimes \rho_2^t.$$

Extend the map by linearity so that $\rho^{\mathrm{pt}} = \sum_{j=1} c_j \rho_{1,j} \otimes \rho_{2,j}^t$ if $\rho = \sum_{j=1}^k c_j \rho_{1,j} \otimes \rho_{2,j}$.

In matrix form, if $\rho = (P_{ij}) \in M_m(M_n)$, then $\rho^{\mathrm{pt}} = (P_{ij}^t)$.

Remark If ρ is separable, then so is ρ^{pt}.

If ρ^{pt} has negative eigenvalues, then ρ is not separable.

Define the **negativity** of $\rho \in \mathcal{H}_1 \otimes \mathcal{H}_2$ by

$$N(\rho) = (\sum_j |\lambda_i(\rho^{pt})| - 1)/2 \geq 0,$$

Then ρ^{pt} has nonnegative eigenvalues if and only if $N(\rho) = 0$.

Theorem If $\rho \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is separable, then $N(\rho) = 0$. The converse holds if $\dim \mathcal{H}_1 + \dim \mathcal{H}_2 \leq 5$.

Open problem Find a simple proof!

Example Let $\begin{pmatrix} \frac{1-p}{4} & 0 & 0 & 0 \\ 0 & \frac{1+p}{4} & \frac{-p}{2} & 0 \\ 0 & \frac{-p}{2} & \frac{1+p}{4} & 0 \\ 0 & 0 & 0 & \frac{1-p}{4} \end{pmatrix}$.

Theorem Let $\rho \in M_m \otimes M_n$. Then ρ is inseparable if and only if there is an entanglement witness F such that

$$\operatorname{tr}(F\rho) > 0 \geq \operatorname{tr}(F(\sigma_1 \otimes \sigma_2)) \qquad \text{for all } \sigma_1 \in D_m, \sigma_2 \in D_n.$$

It should be remarked that finding an entanglement witness of an inseparable state or showing the nonexistence could be a challenging problem.

Partial traces and Purification

Partial trace

Let $C = A \otimes B = (A_{ij}B) \in M_m \otimes M_n$.

(1) One can take the partial trace of the first system to get the matrix B in the second system by simply summing the diagonal blocks of C resulting in $A_{11}B + \cdots + A_{mm}B = (\operatorname{tr} A)B = B$.

(2) One can take the partial trace of the second system to get the matrix A in the first system by simply taking the trace of all the blocks of C resulting in $(A_{ij}\operatorname{tr}(B)) = (A_{ij}) = A$.

For a general state $\rho = (T_{rs})_{1\le r,s\le m}$ with $T_{rs} \in M_n$ for all r, s, the first partial trace and second partial traces are

$$\operatorname{tr}_1(\rho) = T_{11} + \cdots + T_{mm} \in M_n \quad \text{and} \quad \operatorname{tr}_2(\rho) = (\operatorname{tr} T_{ij}) \in M_m.$$

Let $A \in \mathcal{H}_1 \otimes \mathcal{H}_2$. The partial trace of A over $\mathcal{H}_2$ is an operator acting on $\mathcal{H}_1$ defined by

$$A_1 = \operatorname{tr}_2 A = \sum_{k=1}^{n} (I_m \otimes \langle e_{2,k}|) A (I_m \otimes |e_{2,k}\rangle),$$

where m, n are the dimension of $\mathcal{H}_1$ and $\mathcal{H}_2$.

In matrix form, if $\rho = (P_{ij}) \in M_m(M_n)$, then $\operatorname{tr}_2(\rho) = (\operatorname{tr} P_{ij}) \in M_n$. One can define $\operatorname{tr}_1(\rho_{ij}) = \rho_{11} + \cdots + \rho_{mm}$, which corresponds to

$$A_2 = \operatorname{tr}_1 A = \sum_{k=1}^{m} (\langle e_{1,k}| \otimes I_n) A (|e_{1,k}\rangle \otimes I_n).$$

Purification

Theorem Let $\rho_1 = \sum_{j=1}^r p_j |x_j\rangle\langle x_j|$. If $|\psi\rangle = \sum_{j=1}^r \sqrt{p}_j |x_j\rangle \otimes |y_j\rangle$, for an orthonromal set $\{|y_1\rangle, \ldots, |y_r\rangle\} \subseteq \mathbb{C}^r$, then

$$\operatorname{tr}_2(|\psi\rangle\langle\psi|) = \rho_1.$$

Example Let $\rho = \frac{1}{4}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \frac{3}{4}P_1 + \frac{1}{4}P_2$.

Let $\{|y_1\rangle, |y_2\rangle\} = \{|e_1\rangle, |e_2\rangle\}$.

Then $|\psi\rangle = \frac{1}{2\sqrt{2}}\begin{pmatrix} \sqrt{3} \\ 0 \\ \sqrt{3} \\ 0 \end{pmatrix} + \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}$ and

$$|\psi\rangle\langle\psi| = \frac{1}{8}\begin{pmatrix} 3 & \sqrt{3} & 3 & -\sqrt{3} \\ \sqrt{3} & 1 & \sqrt{3} & -1 \\ 3 & \sqrt{3} & 3 & -\sqrt{3} \\ -\sqrt{3} & -1 & -\sqrt{3} & 1 \end{pmatrix}.$$

Quantum operations on an open system

Quantum operations on a closed system with quantum state ρ has the form

$$\rho \mapsto U\rho U^\dagger,$$

for some unitary U.

A quantum system ρ always interact with other quantum systems (from the environment or by the introduction of an auxiliary system for quantum computing). We assume that σ is the quantum state for the environment or auxiliary system, and the initial state of the open system is $\sigma \otimes \rho$.

Then a general quantum operation will be obtained by taking a suitable partial trace of $U(\sigma \otimes \rho)U^\dagger$.

Theorem For every quantum operation on an open system $\Phi : M_n \to M_m$ there exist $r \in \mathbb{N}$ and $F_1, \ldots, F_r \in M_{m,n}$ such that $\sum_{j=1}^r F_j^\dagger F_j = I_n$ and

$$\Phi(A) = \sum_{j=1}^r F_j A F_j^\dagger \qquad \text{for all } A \in M_n.$$

This is called the operator sum representation of the quantum operation. The matrices $F_1, \ldots, F_r$ are called the Kraus operators of the operations.

Example Let $U_1, \ldots, U_r \in \mathrm{U}(n)$ and $p_1, \ldots, p_r$ be positive numbers summing up to 1. Then $\Phi : M_n \to M_n$ defined by

$$\Phi(A) = \sum_{j=1}^r p_j U_j A U_j^\dagger \quad \text{for all } A \in M_n$$

is a quantum channel known as the **random unitary channel** or **mixed unitary channel**.

Quantum channels and Measurements

When a quantum state ρ is transmitted through a quantum channel, it will interact with the external environment. So, we may regard the transmission as a process of letting the quantum state going through a quantum operation of an open system, and assume the received state has the form

$$\hat{\rho} = \sum_{j=1}^{r} F_j \rho F_j^{\dagger}.$$

Here $F_1, \ldots, F_r$ are the Kraus operators caused by the influence of the environment on ρ. In this context, $F_1, \ldots, F_r$ are known a the **error operators**.

Positive Operator-Valued Measure (POVM)

- Eigenprojections of A.
- Projective measurement.
- POVM.

Fidelity

Definition 2.2 The fidelity of two density matrices ρ_1 and ρ_2 is defined as

$$F(\rho_1, \rho_2) = \text{tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}.$$

Note that $\sqrt{\rho_1}\rho_2\sqrt{\rho_1}$ is positive semidefinite so that $\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}$ is well defined and $F(\rho_1, \rho_2) = \text{tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} \geq 0$.

Example $\rho_1 = \text{diag}\,(1/3, 2/3)$, $\rho_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Then

Remarks

1. If $A = \sum_j \lambda_j P_j$ with $\lambda_j \geq 0$, then $A^{1/2} = \sum_j \sqrt{\lambda_j} P_j$.

2. Let $R = \sqrt{\rho_1}\sqrt{\rho_2}$ with singular values $r_1, \dots, r_n$. Then $RR^\dagger = \sqrt{\rho_1}\rho_2\sqrt{\rho_1}$ has eigenvalues $r_1^2, \dots, r_n^2$ and

$$F(\rho_1, \rho_2) = \text{tr}\,(\sqrt{RR^*}) = r_1 + \cdots + r_n.$$

3. Note also that $R^\dagger R$ also has the same eigenvalues $r_1^2 \geq \cdots \geq r_n^2$. So,

$$F(\rho_2, \rho_1) = \text{tr}\,(R^* R) = \text{tr}\sqrt{\sqrt{\rho_2}\rho_1\sqrt{\rho_2}} = r_1 + \cdots + r_n = F(\rho_1, \rho_2).$$

4. For any unitary U, $F(U\rho_1 U^\dagger, U\rho_2 U^\dagger) = F(\rho_1, \rho_2)$. (Exercise 2.10).

5. Suppose ρ_1, ρ_2 have eigenvalues $a_1 \geq \cdots \geq a_n$ and $b_1 \geq \cdots \geq b_n$. Then

$$F(\rho_1, \rho_2) = \max\{|\text{tr}\,(\rho_1^{1/2}\rho_2^{1/2}U)| : U \text{ unitary}\} \leq \sum_{j=1}^{n} \sqrt{a_j b_j} \leq 1.$$

6. For any two density matrices ρ_1 and ρ_2, we have

$$0 \leq F(\rho_1, \rho_2) \leq 1.$$

   The first equality holds if and only if $\rho_1\rho_2 = 0$; the second equality holds if and only if $\rho_1 = \rho_2$.

Open problems

1. Let $A \in D_m, B \in D_n$. Determine $\mathcal{S}(A, B) = \{C \in D_{mn} : \text{tr}_1(C) = B, \text{tr}_2(C) = A\}$.

2. Determine $C \in \mathcal{S}(A, B)$ with maximum rank and minimum rank.

3. Determine $C \in \mathcal{S}(A, B)$ with maximum $S(C) = \mathrm{tr}\,(-C \ln C)$, von Neumann entropy.

4. More generally, one may consider tripartite system with states in $D_{n_1 n_2 n_3}$ and determine $\mathcal{S}(T_1, T_2) = \{C \in D_{n_1 n_2 n_3} : \mathrm{tr}_1(C) = T_1, \mathrm{tr}_2(C) = T_2\}$, where $T_1 \in D_{n_2 n_3}$ and $T_2 \in D_{n_1 n_3}$ are two given states.