Partial Trace and Purification

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

$$A_1 = \mathrm{tr}_2 A = \sum_u (I_m \otimes \langle u|) A (I_m \otimes |u\rangle).$$

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

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

$$A_2 = \mathrm{tr}_1 A = \sum_u (\langle u| \otimes I_n) A (|u\rangle \otimes I_n).$$

Theorem (Purification) Let $\rho_1 = \sum_{j=1}^n p_j |x_j\rangle\langle x_j|$. Suppose $|\psi\rangle = \sum_{j=1}^n \sqrt{p_j}|x_j\rangle \otimes |y_j\rangle$. Then $\mathrm{tr}_2(|\psi\rangle\langle\psi|) = \rho_1$.

Fidelity

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

$$F(\rho_1, \rho_2) = \operatorname{tr}\left((\rho_1^{1/2}\rho_2\rho_1^{1/2})^{1/2}\right) \geq 0.$$

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. If A, B are $m \times n$ and $n \times m$, then AB and BA have the same nonzero eigenvalues.

   Proof. Note that

   $$\begin{pmatrix} AB & 0 \\ B & 0_n \end{pmatrix} \begin{pmatrix} I_m & A \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} AB & ABA \\ B & BA \end{pmatrix} = \begin{pmatrix} I_m & A \\ 0 & I_n \end{pmatrix} \begin{pmatrix} 0_m & 0 \\ B & BA \end{pmatrix}.$$

   So, $\begin{pmatrix} AB & 0 \\ B & 0 \end{pmatrix}$ and $\begin{pmatrix} 0_m & 0 \\ B & BA \end{pmatrix}$ are similar. The result follows.

3. We have $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$ as $\rho_1^{1/2}\rho_2\rho_1^{1/2}$ and $\rho_2^{1/2}\rho_1\rho_2^{1/2}$ have the same eigenvalues.

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

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

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 $\rho_1 = \rho_2$.

$|\psi_1\rangle, \ldots, |\psi_r\rangle$

$p_1, \ldots, p_r$

$$\sum_{i=1}^{r} p_i \langle\psi_i|A|\psi_i\rangle = \operatorname{tr} A\rho$$

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$$

$$= \sum \lambda_i |\lambda_i\rangle\langle\lambda_i|$$

$\rho =$

$$\rho_1 = \frac{1}{3}\begin{pmatrix}1\\0\end{pmatrix}(1\ 0) + \frac{1}{3}\begin{pmatrix}0\\1\end{pmatrix}(0\ 1) + \frac{1}{3}\begin{pmatrix}1\\i\end{pmatrix}(1\ -i)$$

$|x_1\rangle \quad |x_2\rangle \quad |x_3\rangle$

$|\psi\rangle$ Choose $\{|y_1\rangle, |y_2\rangle, |y_3\rangle\} = \left\{\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$

$$|\psi\rangle = \frac{1}{\sqrt{3}}|x_1\rangle\otimes|y_1\rangle + \frac{1}{\sqrt{3}}|x_2\rangle|y_2\rangle + \frac{1}{\sqrt{3}}|x_3\rangle|y_3\rangle$$

$$= \frac{1}{\sqrt{3}}\begin{pmatrix}\\\\\end{pmatrix}_{|w_1\rangle} + \frac{1}{\sqrt{3}}\begin{pmatrix}\\\\\end{pmatrix}_{|w_2\rangle} + \frac{1}{\sqrt{3}}\begin{pmatrix}\\\\\end{pmatrix}_{|w_3\rangle} \in \mathbb{C}^6$$

$$\operatorname{tr}_2\left(|\psi\rangle\langle\psi|\right) = \operatorname{tr}_2\left(\frac{1}{3}\sum_{ij}|w_i\rangle\langle w_j|\right) \qquad |y_i\rangle\langle y_j| \to \begin{bmatrix}\cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot\end{bmatrix}$$

$$= \operatorname{tr}_2\left(\frac{1}{3}|w_1\rangle\langle w_1| + \frac{1}{3}|w_2\rangle\langle w_2| + \frac{1}{3}|w_3\rangle\langle w_3|\right)$$

$$\operatorname{tr}_2 \frac{1}{3}\sum_{i\neq j}|w_i\rangle\langle w_j|$$

$$= \frac{1}{3}|x_1\rangle\langle x_1| + \frac{1}{3}|x_2\rangle\langle x_2| + \frac{1}{3}|x_3\rangle\langle x_3|$$

$$+ 0 \cdot \sum |x_i\rangle\langle x_j| \langle y_j|y_i\rangle$$

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \frac{}{\sqrt{2}}$

3.2 Quantum Key Distribution (BB84 protocol)

Alice wants to send n bits to Bob securely. Eve is the notorious eavesdropper.

Alice and Bob will choose two randomly chosen systems:

(1) $0 \mapsto |e_1\rangle,\ 1 \mapsto |e_2\rangle$. $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

(2) $0 \mapsto (|e_1\rangle + |e_2\rangle)/\sqrt{2},\ 1 \mapsto (|e_1\rangle - |e_2\rangle)/\sqrt{2}$. $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \frac{}{\sqrt{2}}$ $\begin{pmatrix} 1 \\ -1 \end{pmatrix} \frac{}{\sqrt{2}}$

- Alice send $4n$ bits to Bob, each using the two systems randomly.
- Announce the types of systems; discard about $2n$ bits with wrong channel match.

  Probability for Alice and Bob use the same system: (1)(1), (2)(2), vs. (1)(2), (2)(1).
- Alice tells Bob n of two remaining bits to test whether they have not been tempered.

  Alice, Eve, Bob use channels

(1)(1)(1)	(1)(1)(2)	(1)(2)(1)	(1)(2)(2)	(2)(1)(1)	(2)(1)(2)	(2)(2)(1)	(2)(2)(2)
Y	N	Y	N	N	Y	N	Y
G	*	± G	*	*	± G	*	G

- If not, use the remaining n bits as the private key. Otherwise, repeat the process.

message = (0, 1) sequence $|0\rangle$, $|1\rangle$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Encrypt a sequence of length n by adding a private key, which is a (0, 1) sequence of length n shared between Alice & Bob. So that message $(i_1 \cdots i_n)$ will be encrypted by adding it to the private key $(k_1 \cdots k_n)$ under $\mathbb{Z}_2$ operation. i.e. $i_j + k_j = 1$ or 0 as $0+0=0=1+1$, $0+1=1=1+0$

Decryption is done again by adding $(k_1 \cdots k_n)$ to the received sequence.