Trace distance

$\rho_1 \; \rho_2$ $\quad TD(\rho_1, \rho_2)$ how distinguishable

SD is classical version

$TD(\rho_1,\rho_2) = tr|\rho_1 - \rho_2| \qquad |A| := \sqrt{A^\dagger A}$

$\frac{1}{2}\sum |eigenvalues| \qquad \sqrt{X}$ is uniqe $Y \geq 0$ st $Y^\dagger Y = X$

$E_1 = \{|0\rangle @ 1\} \qquad E_2 = \{|0\rangle @ \frac{1}{3}, |1\rangle @ \frac{2}{3}\}$

$\rho_1 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \rho_2 = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1| = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{2}{3} \end{pmatrix}$

$$TD(\rho_1,\rho_2) = tr|\rho_1 - \rho_2| = tr\left|\begin{pmatrix} \frac{2}{3} & 0 \\ 0 & -\frac{2}{3} \end{pmatrix}\right| = \frac{1}{2}\left(\left|\frac{2}{3}\right| + \left|-\frac{2}{3}\right|\right) = \frac{2}{3}$$

$E_1 = \{|0\rangle @ \frac{1}{2}+\varepsilon, |1\rangle @ \frac{1}{2}-\varepsilon\} \qquad E_2 = \{|+\rangle @ \frac{1}{2}+\varepsilon, |-\rangle @ \frac{1}{2}-\varepsilon\}$

$\varepsilon = 0 \quad TD(\rho_1,\rho_2) = 0$

$\varepsilon > 0 \quad TD(\rho_1,\rho_2) = ?$

$\rho_1 = (\frac{1}{2}+\varepsilon)|0\rangle\langle 0| + (\frac{1}{2}-\varepsilon)|1\rangle\langle 1| = \begin{pmatrix} \frac{1}{2}+\varepsilon & 0 \\ 0 & \frac{1}{2}-\varepsilon \end{pmatrix}$

$\rho_2 = (\frac{1}{2}+\varepsilon)|+\rangle\langle +| + (\frac{1}{2}-\varepsilon)|-\rangle\langle -| = \frac{1}{2}\begin{pmatrix} \frac{1}{2}+\varepsilon & \frac{1}{2}+\varepsilon \\ \frac{1}{2}+\varepsilon & \frac{1}{2}+\varepsilon \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{1}{2}-\varepsilon & \varepsilon-\frac{1}{2} \\ \varepsilon-\frac{1}{2} & \frac{1}{2}-\varepsilon \end{pmatrix} =$

$\frac{1}{2}\begin{pmatrix} 1 & 2\varepsilon \\ 2\varepsilon & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \varepsilon \\ \varepsilon & \frac{1}{2} \end{pmatrix}$

$$TD(\rho_1,\rho_2) = tr\left|\begin{pmatrix} \varepsilon & -\varepsilon \\ -\varepsilon & -\varepsilon \end{pmatrix}\right| = \frac{1}{2}\left(|\sqrt{2}\varepsilon| + |-\sqrt{2}\varepsilon|\right) = \sqrt{2}\varepsilon$$

$Av = \lambda I v$

$(A - \lambda I)v = 0$

$\det(A - \lambda I) = 0$

$$\det\begin{pmatrix} \varepsilon-\lambda & -\varepsilon \\ -\varepsilon & -\varepsilon-\lambda \end{pmatrix} = (\varepsilon-\lambda)(-\varepsilon-\lambda) - \varepsilon^2 = -\varepsilon^2 \cancel{-\varepsilon\lambda + \varepsilon\lambda} + \lambda^2 =$$

$= \lambda^2 - 2\varepsilon^2 = 0$

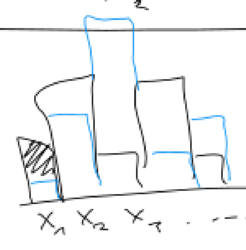
$\lambda^2 = 2\varepsilon^2$

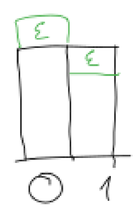
$\lambda_1 = \sqrt{2}\varepsilon$

$\lambda_2 = -\sqrt{2}\varepsilon$

$b' \leftarrow \{0,1\}$ biased towards 0 with ε

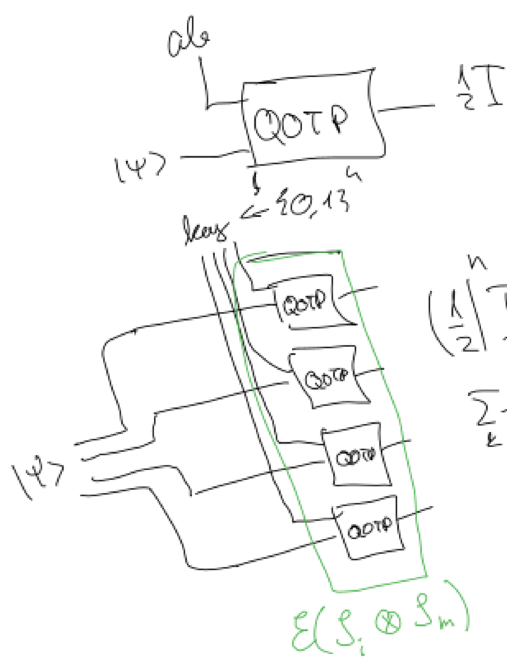
$\mathcal{E}_1 \to |0\rangle$ if $b=0$, $|1\rangle$ if $b=1$ $\qquad \mathcal{E}_2 \Rightarrow |+\rangle$ if $b=0$, $|-\rangle$ if $b=1$

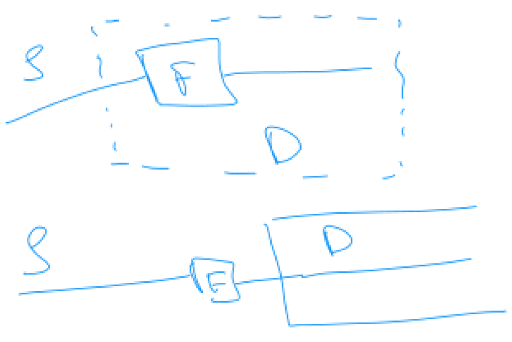


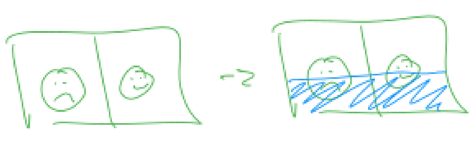


$\mathcal{E}_1(b') \overset{\varepsilon}{\approx} \mathcal{E}_1(b) \overset{0}{=} \mathcal{E}_2(b) \overset{\varepsilon}{\approx} \mathcal{E}_2(b')$ $\qquad \frac{1}{2}\sum |D_1(x) - D_2(x)|$

$SD(b, b') = \varepsilon \qquad TD(\mathcal{E}_1(b'), \mathcal{E}_2(b')) \leq 2\varepsilon$







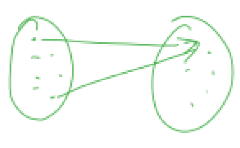
if key is 0 then $QOTP = ID$.
want to avoid 0 as key

$(\frac{1}{2})^n I$

$key' \leftarrow \{0,1\}^n \setminus \{0 \ldots 0\}$

$\sum_k \frac{1}{2^n}|k\rangle\langle k| = \rho_k \qquad \rho'_k = \sum_{k' \in K'} \frac{1}{2^n - 1}|k'\rangle\langle k'|$

$TD(F(\rho_1), F(\rho_2)) \leq TD(\rho_1, \rho_2)$



$$TD(\mathcal{E}(\rho_k \otimes \rho_m), \mathcal{E}(\rho_{k'} \otimes \rho_m)) \leq$$

$TD(\sigma \otimes \nu, \sigma' \otimes \nu) = TD(\sigma, \sigma')$

$$\leq TD(\rho_k \otimes \rho_m, \rho_{k'} \otimes \rho_m) \leq$$

$$TD(\rho_k, \rho_{k'}) = \frac{1}{2}\left(\sum_{k \neq 0}\left|\frac{1}{2^n} - \frac{1}{2^n-1}\right| + \frac{1}{2^n}\right) = \frac{1}{2}\left(\cancel{(2^n-1)} \cdot \left(\left|\frac{2^n - 1 - 2^n}{(2^n)\cancel{(2^n-1)}}\right|\right) + \frac{1}{2^n}\right) =$$

$\frac{1}{2^n}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \qquad \frac{1}{2^n-1}\begin{pmatrix} 0 & & \\ & 1 & \\ & & \ddots \; 1 \end{pmatrix}$

$$= \frac{1}{2}\left(\frac{1}{2^n} + \frac{1}{2^n}\right) = \frac{1}{2^n}$$

QOTP' (w/o 0)

$QOTP'(\rho_{k'} \otimes \rho_{m'}) \overset{2^{-n}}{=} QOTP(\rho_k \otimes \rho_{m'}) \overset{0}{=} QOTP(\rho_k \otimes \rho_m) \overset{2^{-n}}{=} QOTP'(\rho_{k'} \otimes \rho_m)$

$\leq 2 \cdot 2^{-n}$

$|\psi\rangle, |\varphi\rangle$ are orthogonal $\qquad TD(|0\rangle\langle 0|, |1\rangle\langle 1|) =$

$= tr\left|\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right| = \frac{1}{2}(|1| + |-1|) = 1$

$|\psi\rangle\langle\psi| = U|0\rangle\langle 0|U^\dagger$

$TD(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)$

$B = \{|\psi\rangle, |\varphi\rangle, \ldots\ldots\} \qquad U|0\rangle = |\psi\rangle, \; U|1\rangle = |\varphi\rangle$

$TD(\rho_1,\rho_2) = tr|\rho_1 - \rho_2| =$

$= tr|U\rho_1 U^\dagger - U\rho_2 U^\dagger| = tr|U(\rho'_1 - \rho'_2)U^\dagger| =$

comp. comp.

$= tr|\rho'_1 - \rho'_2| = tr\left|\begin{pmatrix} 1 & \\ & \ddots \; -1 \end{pmatrix}\right| = \frac{1}{2}(|1| + |-1|) = 1$

$|\psi\rangle$ and $|\varphi\rangle$ are <u>not</u> orthogonal

as a basis vector

$|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\psi\rangle\langle\psi| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$TD(|\varphi\rangle\langle\varphi|, |\psi\rangle\langle\psi|) = \qquad |\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad |\varphi\rangle\langle\varphi| = \begin{pmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{pmatrix}$

$tr\left|\begin{pmatrix} \alpha^2 - 1 & \alpha\beta \\ \alpha\beta & \beta^2 \end{pmatrix}\right| \qquad \alpha^2 + \beta^2 = 1$

$*$

$|0\rangle, |1\rangle \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \; TD = 1$

$|0\rangle, |+\rangle \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \; TD = \frac{1}{\sqrt{2}}$

$|-\rangle, |+\rangle \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \; TD = \frac{1}{\sqrt{2}}$

$B = \{|-\rangle, |+\rangle\} \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$|-\rangle \qquad |+\rangle$

$tr\,0 = e + f \Rightarrow e = -f$

$\det(A) = e \cdot f = (\alpha^2 - 1)\beta^2 - \alpha^2\beta^2 = \alpha^2\beta^2 - \beta^2 - \alpha^2\beta^2 = -\beta^2$

$e \cdot f = -\beta^2 \qquad TD(\ldots) = \frac{1}{2}\sum |eigenvalue| = \beta$

$-f^2 = -\beta^2$

$f_1 = \beta \quad e_1 = -\beta$

$f_2 = -\beta \quad e_2 = \beta$