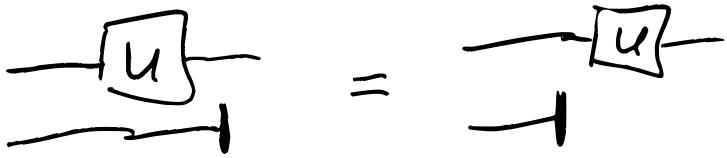
Partial Trace

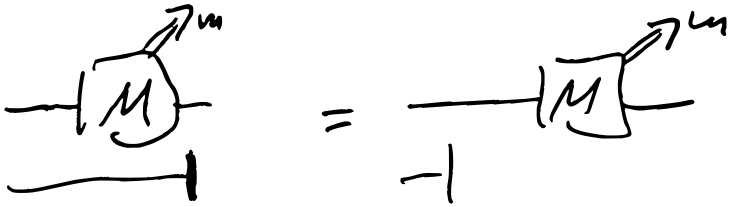
- remove part of a q. system
- throwing it away
- ignoring it forever

---

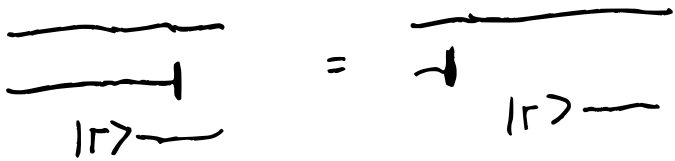
(1)



(2)



(3)



Def: $\mathrm{tr}_B \sigma \otimes \tau = \sigma \cdot \mathrm{tr}\,\tau$, $\forall_B$ linear

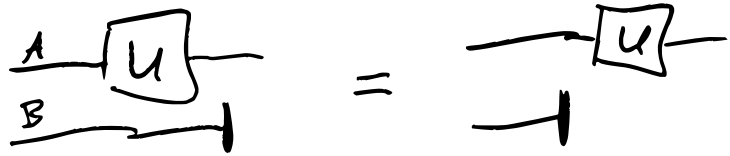
B: any matrices

Def: $\mathrm{tr}_B\, \sigma \otimes \tau = \sigma \cdot \mathrm{tr}\, \tau$, tr_B linear

σ, τ any matrices

---

(1)



$$\forall \rho : \mathrm{tr}_B (U \otimes I) \rho (U^\dagger \otimes I) = U (\mathrm{tr}_B \rho) U^\dagger$$

Sufficient to show this for $\rho = \sigma \otimes \tau$ (by linearity)

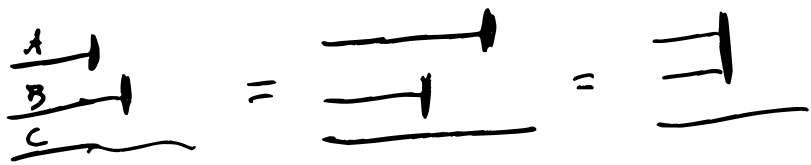
$$\mathrm{tr}_B (U \otimes I)(\sigma \otimes \tau)(U^\dagger \otimes I)$$

$$= \mathrm{tr}_B\, U \sigma U^\dagger \otimes \cancel{I} \tau \cancel{I}$$

$$= U \sigma U^\dagger \cdot \mathrm{tr}\, \tau$$

$$= U (\sigma \cdot \mathrm{tr}\, \tau) U^\dagger = U (\mathrm{tr}_B\, \sigma \otimes \tau) U^\dagger$$

Further facts:



$\mathcal{N}_B \circ \mathcal{N}_A = \mathcal{N}_A \circ \mathcal{N}_B = \mathcal{N}_{AB}$

Quantum operations

- General definition of arbitrary (adv) computations.
- Operation: $\mathbb{C}^{N \times N} \to \mathbb{C}^{M \times M}$
  (in particular, density ops to density ops)

Definitions

(1) $\mathcal{E}: \mathbb{C}^{N\times N} \to \mathbb{C}^{M\times M}$ is a q. op. iff it can be implemented as a q. circuit using: unitaries, partial tr., adding ancillas, measurements (that control further ops)

---

(2) $\mathcal{E}$ is q. op iff it can be written as

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

for some matrices E_k with $\sum E_k^\dagger E_k = I$

Kraus-op. repr.

---

(3) $\mathcal{E}$ is q. op. iff it can be written as:

$$\mathcal{E}(\rho) = \mathrm{tr}_B\left(U(\rho \otimes |0\rangle\langle 0|_C)U^\dagger\right)$$

for some B, C unitary U,

(4) $\mathcal{E}$ is q-op iff:

- $\mathcal{E}$ is linear
- $\mathcal{E}$ is trace-preserving
- $\mathcal{E}$ is completely positive

> $\mathcal{E}$ is pos. iff
> for pos. ρ, $\mathcal{E}(\rho)$ pos.
>
> $\mathcal{E}$ is compl. pos iff
> $\mathcal{E} \otimes I$ is pos.

A.k.a. completely positive trace-preserving map (CPTP M)

A.k.a. quantum channel

Tensor prod. of q. ops:

Def:

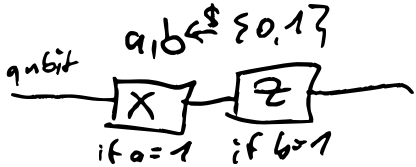
$$(\mathcal{E} \otimes \mathcal{F})(\sigma \otimes \tau) = \mathcal{E}(\sigma) \otimes \mathcal{F}(\tau)$$

$\mathcal{E} \otimes \mathcal{F}$ linear

Thm: this tensor prod. exists. and is q. op.

QOTP, revisited

The QOTP:



Writing QOTP as q. op:

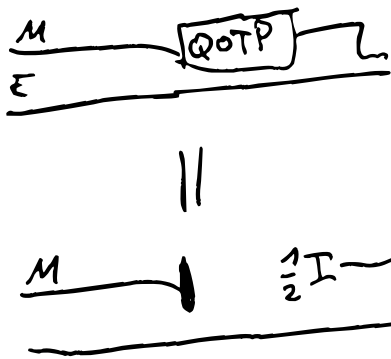
$$\rho \mapsto \frac{1}{4}\rho + \frac{1}{4} X\rho X^\dagger + \frac{1}{4} Z\rho Z^\dagger + \frac{1}{4}(ZX)\rho(ZX)^\dagger$$

$$= \sum E_k \rho E_k^\dagger \qquad E_1 = \frac{1}{4} I \quad E_2 = X\frac{1}{4}$$

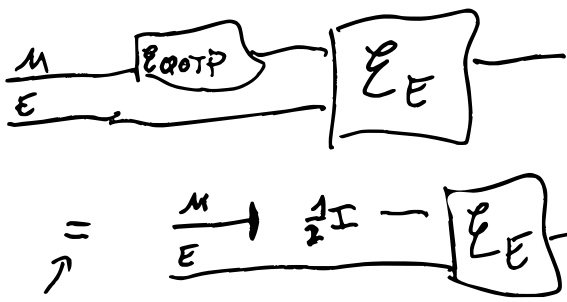
$$=: \mathcal{E}_{QOTP}(\rho) \qquad E_3 = Z\frac{1}{4} \quad E_4 = \frac{1}{4} ZX$$

Defining security

For all initial states of the system (including the msg to be sent, adv's state, possibly entangled), for adv E:



Formally: $\forall$ q. op. $\mathcal{E}_E$



as q. op.

$\mathcal{E}_E \circ (\mathcal{E}_{QOTP} \otimes id)$
$= \mathcal{E}_E \circ (\mathcal{E}' \otimes id)$

with
$\mathcal{E}'(\rho) := \frac{1}{2} I \cdot \mathrm{tr}\,\rho$

Nice fact:

Security wrt. of this def can be derived from sec. as we have shown so far

→ practice

Trace-distance

Motivating example

- Alice has secret bit b
- If $b=0$, A sends $|0\rangle$ @ 0.499 $|1\rangle$ @ 0.501
- If $b=1$, A sends $|+\rangle$ @ 0.499 $|-\rangle$ @ 0.501

Can B distinguish $b=0$, $b=1$?

$$\rho_1 = 0.499\, |0\rangle\langle 0| + 0.501\, |1\rangle\langle 1| = \begin{pmatrix} 0.499 & \\ & 0.501 \end{pmatrix}$$

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

$$\rho_2 = 0.499\, |+\rangle\langle +| + 0.501\, |-\rangle\langle -| = \begin{pmatrix} 1/2 & -0.01 \\ -0.01 & 1/2 \end{pmatrix}$$

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

$\Rightarrow$ not phys. indist.

Goal: (next time):

Definition of how different are two density ops.

"trace distance"

Will show: $TD(\rho_1, \rho_2) \approx 0$

Statistical distance

Given distribs / random variables X, Y

$$SD(X,Y) = \max_{A} \left| \Pr[A(X)=1] - \Pr[A(Y)=1] \right|$$

A: arbitrary prob. algorithm

$$SD(X,Y) = \max_{T} \left| \Pr[X \in T] - \Pr[Y \in T] \right|$$

T: set

$$SD(X,Y) = \frac{1}{2} \sum_{a} \left| \Pr[X=a] - \Pr[Y=a] \right|$$

Props

- SD is metric
  ($SD = 0$ iff $X = Y$
  $SD \geq 0$, triangle ineq.)
- $SD \leq 1$
- For any (possibly prob'ab.) function F:

$$SD(F(X), F(X)) \leq SD(X, Y)$$

- For any indep. Z

$$SD((X,Z), (Y,Z)) = SD(X, Y)$$