Centrum Wiskunde & Informatica

The Density Matrix Formalism, Quantum Channels, And More

CROSSING Winter School on Quantum Crypto

Serge Fehr

CWI Amsterdam

www.cwi.nl/~fehr

Dirac's Bra-Ket Notation

- $\mathscr{H}$: complex (finite-dimensional) *Hilbert space*
- Elements in $\mathscr{H}$ are denoted $|\varphi\rangle$, and called *ket-vectors*.
- *Inner product* of $|\varphi\rangle, |\psi\rangle \in \mathscr{H}$ is denoted $\langle\varphi|\psi\rangle$.

Example: $\mathscr{H} = \mathbb{C}^2$ with

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

where

$$\langle 0|0\rangle = 1 = \langle 1|1\rangle \quad \text{and} \quad \langle 0|1\rangle = 0$$

Dirac's Bra-Ket Notation

- $\mathscr{H}$: complex (finite-dimensional) *Hilbert space*
- Elements in $\mathscr{H}$ are denoted $|\varphi\rangle$, and called *ket-vectors*.
- *Inner product* of $|\varphi\rangle, |\psi\rangle \in \mathscr{H}$ is denoted $\langle\varphi|\psi\rangle$.
- For $|\varphi\rangle \in \mathscr{H}$, the *bra-vector* $\langle\varphi|$ is functional $\mathscr{H} \to \mathbb{C}$ s.t.

$$\langle\varphi||\psi\rangle = \langle\varphi|\psi\rangle \quad \forall\, |\psi\rangle \in \mathscr{H}$$

- For $|\varphi\rangle, |\psi\rangle \in \mathscr{H}$, the *outer product* $|\psi\rangle\langle\varphi| \in \mathrm{Lin}(\mathscr{H})$ is s.t.

$$|\psi\rangle\langle\varphi||\xi\rangle = |\psi\rangle\langle\varphi|\xi\rangle \quad \forall\, |\xi\rangle \in \mathscr{H}$$

- The *trace* is (unique) linear functional $\mathrm{tr}\colon \mathrm{Lin}(\mathscr{H}) \to \mathbb{C}$ s.t.

$$\mathrm{tr}(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle \quad \forall\, |\varphi\rangle, |\psi\rangle \in \mathscr{H}$$

Dirac's Bra-Ket Notation

- $\mathscr{H}$: complex (finite-dimensional) *Hilbert space*
- Elements in $\mathscr{H}$ are denoted $|\varphi\rangle$, and called *ket-vectors*.

Fact. tr is *cyclic*: $\mathrm{tr}(LR) = \mathrm{tr}(RL)\ \forall\ L,R \in \mathrm{Lin}(\mathscr{H})$.

Proof. For $R = |\psi\rangle\langle\varphi|$:

$$\mathrm{tr}(L|\psi\rangle\langle\varphi|) = \langle\varphi|\, L|\psi\rangle = \langle\varphi|L\,|\psi\rangle = \mathrm{tr}(|\psi\rangle\langle\varphi|L)$$

For general R: by linearity.

$$|\psi\rangle\langle\varphi|\xi\rangle = |\psi\rangle\langle\varphi|\xi\rangle \quad \forall\ |\xi\rangle \in \mathscr{H}$$

- The *trace* is (unique) linear functional tr: $\mathrm{Lin}(\mathscr{H}) \to \mathbb{C}$ s.t.

$$\mathrm{tr}(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle \quad \forall\ |\varphi\rangle, |\psi\rangle \in \mathscr{H}$$

Reminder: The State-Vector Formalism

- *Quantum system A*: Hilbert space $\mathscr{H}$ (or $\mathscr{H}_A \otimes \mathscr{H}_B$ etc.)
- *State* of *A*: norm-1 "state vector" $|\varphi\rangle \in \mathscr{H}$
- *(Unitary) operation*: $U \in \mathrm{Uni}(\mathscr{H})$. *Rule*: U maps $|\varphi\rangle$ to $U|\varphi\rangle$
- *Measurement*: $\{M_i\}_{i\in I}$ s.t. $\sum M_i^\dagger M_i = \mathbb{I}$. *Rule*:
  - observe i with probability

$$p_i = \langle\varphi| M_i^\dagger M_i |\varphi\rangle$$

Born's rule

  - state collapses to *post-measurement state* $M_i|\varphi\rangle / \sqrt{p_i}$.

In case of *rank-1 projective measurements*, i.e.,

"*measuring in a (orthonormal) basis* $\{|i\rangle\}_{i\in I}$",

$\{M_i\}_{i\in I}$ is given by $M_i = |i\rangle\langle i|$, and hence

$$p_i = \langle\varphi|M_i^\dagger M_i|\varphi\rangle = \langle\varphi||i\rangle\langle i||i\rangle\langle i||\varphi\rangle = \langle\varphi|i\rangle\langle i|i\rangle\langle i|\varphi\rangle$$

$$= \langle\varphi|i\rangle\langle i|\varphi\rangle = |\langle i|\varphi\rangle|^2 = |\alpha_i|^2$$

for $|\varphi\rangle = \sum_i \alpha_i|i\rangle$.

- *Measurement*: $\{M_i\}_{i\in I}$ s.t. $\sum M_i^\dagger M_i = \mathbb{I}$. *Rule*:
  - observe i with probability

    $$p_i = \langle\varphi|M_i^\dagger M_i|\varphi\rangle$$

    Born's rule
  - state collapses to *post-measurement state* $M_i|\varphi\rangle/\sqrt{p_i}$.

(First) Goal: A New Formalism

Motivation 1: Randomized States

Say: Alice prepares system *A* in state $|\varphi\rangle$ with probability p and in state $|\psi\rangle$ with probability $1-p$, and gives *A* to Bob.

Q: *What's a proper description of the state of A to Bob?*

A: The probability distribution over the state vectors:

"$|\varphi\rangle$ *with probability* p, *and* $|\psi\rangle$ *with probability* $1-p$"

Caveat: This representation is not unique!

Example

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Consider:

"$|0\rangle$ *with prob.* $1/2$, *and* $|1\rangle$ *with prob.* $1/2$"

versus

"$|+\rangle$ *with prob.* $1/2$, *and* $|-\rangle$ *with prob.* $1/2$".

Then, measuring in computational basis $\{|0\rangle,|1\rangle\}$:

observe a random bit as outcome,

and the same for the Hadamard basis $\{|+\rangle,|-\rangle\}$.

Actually, **cannot** be distinguished by **any** measurement.

As such, the two **states are identical**.

Motivation 2: Subsystems

Given: state $|\varphi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ of a bipartite system AB.

Q: *How to describe state of system B alone?*

Examples:

- If $|\varphi_{AB}\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$ then, quite obviously: $|\varphi_B\rangle$
- But if, say,

$$|\varphi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$$

then it's not clear - and it's **not** $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle$!!!

Towards Density Matrices

Consider: randomized state

"$|\varphi_k\rangle$ *with probability* ε_k $(k \in K)$"

Q: *How does it behave under measurement* $\{M_i\}_{i\in I}$ *?*

A: *Conditioned* on the state being $|\varphi_k\rangle$, observe i with prob.

$$p_{i|k} = \langle\varphi_k| M_i^\dagger M_i |\varphi_k\rangle = \mathrm{tr}\big(M_i^\dagger M_i |\varphi_k\rangle\langle\varphi_k|\big) \ ,$$

and thus, (on average) observe i with probability

$$\begin{aligned} p_i = \sum_k \varepsilon_k \, p_{i|k} &= \sum_k \varepsilon_k \, \mathrm{tr}\big(M_i^\dagger M_i |\varphi_k\rangle\langle\varphi_k|\big) \\ &= \mathrm{tr}\big(M_i^\dagger M_i \big(\sum_k \varepsilon_k |\varphi_k\rangle\langle\varphi_k|\big)\big) \end{aligned}$$

Thus: The matrix $\rho = \sum \varepsilon_k |\varphi_k\rangle\langle\varphi_k|$ carries **all** the information, and can be used to describe the state.

Density Matrices

The matrix $\rho = \sum \varepsilon_k |\varphi_k\rangle\langle\varphi_k|$ satisfies:

1. *Positivity*: $\forall\ |\psi\rangle \in \mathscr{H}$

$$\langle\psi|\rho|\psi\rangle = \sum \varepsilon_k \langle\psi|\varphi_k\rangle\langle\varphi_k|\psi\rangle = \sum \varepsilon_k |\langle\psi|\varphi_k\rangle|^2 \geq 0$$

2. *Normalization*:

$$\mathrm{tr}(\rho) = \sum \varepsilon_k \mathrm{tr}(|\varphi_k\rangle\langle\varphi_k|) = \sum \varepsilon_k \langle\varphi_k|\varphi_k\rangle = \sum \varepsilon_k = 1$$

Definition: Such $\rho \in \mathrm{Lin}(\mathscr{H})$ is called ***density matrix***. Write

$$\mathrm{Dens}(\mathscr{H}) := \{\rho \in \mathrm{Lin}(\mathscr{H}) \mid \rho \geq 0,\ \mathrm{tr}(\rho) = 1\}$$

Theorem: $\rho \in \mathrm{Lin}(\mathscr{H})$ is a density matrix iff $\rho = \sum \varepsilon_k |\varphi_k\rangle\langle\varphi_k|$ for $|\varphi_k\rangle \in \mathscr{H}$ with $\langle\varphi_k|\varphi_k\rangle = 1$, and $\varepsilon_k \geq 0$ with $\sum \varepsilon_k = 1$.

Density Matrices

Terminology:

- Such a “randomized state” is called ***mixed state***.
- A “deterministic state”, given by $|\varphi\rangle \in \mathscr{H}$, is called ***pure***. The corresponding density matrix is then

$$\rho = |\varphi\rangle\langle\varphi| \ .$$

Definition: Such $\rho \in \mathrm{Lin}(\mathscr{H})$ is called ***density matrix***. Write

$$\mathrm{Dens}(\mathscr{H}) := \{\rho \in \mathrm{Lin}(\mathscr{H}) \mid \rho \geq 0,\ \mathrm{tr}(\rho) = 1\}$$

Theorem: $\rho \in \mathrm{Lin}(\mathscr{H})$ is a density matrix iff $\rho = \sum \varepsilon_k |\varphi_k\rangle\langle\varphi_k|$ for $|\varphi_k\rangle \in \mathscr{H}$ with $\langle\varphi_k|\varphi_k\rangle = 1$, and $\varepsilon_k \geq 0$ with $\sum \varepsilon_k = 1$.

The Density-Matrix Formalism

- *Quantum system A*: Hilbert space $\mathscr{H}$ (or $\mathscr{H}_A \otimes \mathscr{H}_B$ etc.)
- *State* of *A*: density matrix $\rho_A \in \mathrm{Dens}(\mathscr{H})$
- *(Unitary) operation*: $U \in \mathrm{Uni}(\mathscr{H})$. *Rule*: maps ρ_A to $U\rho_A U^\dagger$
- *Measurement*: $\{M_i\}_{i\in I}$ s.t. $\sum M_i^\dagger M_i = \mathbb{I}$. *Rule*:
  - observe i with probability

$$p_i = \mathrm{tr}\left(M_i^\dagger M_i \rho_A\right) = \mathrm{tr}\left(M_i \rho_A M_i^\dagger\right)$$

  - state collapses to $\rho_A^i = M_i \rho_A M_i^\dagger / p_i$.

Born's rule

Example

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Consider:

"$|0\rangle$ *with prob.* $1/2$, *and* $|1\rangle$ *with prob.* $1/2$"

versus

"$|+\rangle$ *with prob.* $1/2$, *and* $|-\rangle$ *with prob.* $1/2$".

The former is given by the density matrix

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \ = \frac{1}{2}\,\mathbb{I}$$

and the latter by

$$\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$$
$$= \frac{1}{4}(|0\rangle+|1\rangle)(\langle 0|+\langle 1|) + \frac{1}{4}(|0\rangle-|1\rangle)(\langle 0|-\langle 1|) = \rho$$

Uniqueness of Density-Matrix Representation

Theorem: If $\rho,\sigma \in \mathrm{Dens}(\mathscr{H})$ are distinct, i.e. $\rho \neq \sigma$, then there exists a measurement $\{M_i\}_{i\in I}$ that "distinguishes" them:

$$\exists i\colon \mathrm{tr}\big(M_i^\dagger M_i \rho\big) \neq \mathrm{tr}\big(M_i^\dagger M_i \sigma\big)$$

Proof: Set $M_i = |i\rangle\langle i|$, where

$\{|i\rangle\}$ is an orthonormal eigenbasis of $\rho-\sigma$.

Then

$$\begin{aligned}\mathrm{tr}\big(M_i^\dagger M_i \rho\big) - \mathrm{tr}\big(M_i^\dagger M_i \sigma\big) &= \mathrm{tr}\big(M_i^\dagger M_i (\rho-\sigma)\big)\\ &= \mathrm{tr}\big(|i\rangle\langle i|i\rangle\langle i|(\rho-\sigma)\big) = \mathrm{tr}\big(|i\rangle\langle i|(\rho-\sigma)\big)\\ &= \langle i|(\rho-\sigma)|i\rangle = \lambda_i \langle i|i\rangle = \lambda_i\end{aligned}$$

which is non-zero for any eigenvalue $\lambda_i \neq 0$.

Motivation 2: Subsystems

Consider: bipartite system *AB.*
It's (possibly mixed) state is given by $\rho_{AB} \in \mathrm{Dens}(\mathscr{H}_A \otimes \mathscr{H}_B)$.

Q: *How to describe state of system B alone?*

A: By the *reduced density matrix*

$$\rho_B = \mathrm{tr}_A(\rho_{AB}) \in \mathrm{Dens}(\mathscr{H}_B)$$

where:

Definition. The ***partial trace*** tr_A is the linear map

$$\mathrm{tr}_A \colon \mathrm{Lin}(\mathscr{H}_A \otimes \mathscr{H}_B) \to \mathrm{Lin}(\mathscr{H}_B)$$

with the defining property that

$$\mathrm{tr}_A(|\psi\rangle\langle\varphi| \otimes |\xi\rangle\langle\eta|) = \langle\varphi|\psi\rangle\, |\xi\rangle\langle\eta| \,.$$

NB: In general, $\rho_B = \mathrm{tr}_A(\rho_{AB})$ is not pure, even if ρ_{AB} is.

An Equivalent Definition

Proposition: Partial trace tr_A is the unique linear map s.t.

$$\mathrm{tr}\big((\mathbb{I}\otimes L)R\big) = \mathrm{tr}\big(L\ \mathrm{tr}_A(R)\big)$$

for all $R \in \mathrm{Lin}(\mathscr{H}_A \otimes \mathscr{H}_B)$ and $L \in \mathrm{Lin}(\mathscr{H}_B)$.

Proof: Consider $R = |\psi\rangle\langle\varphi| \otimes |\xi\rangle\langle\eta|$. Then

$$\begin{aligned}
\mathrm{tr}\big(L\ \mathrm{tr}_A(R)\big) &= \mathrm{tr}\big(L\ \mathrm{tr}_A(|\psi\rangle\langle\varphi|\otimes|\xi\rangle\langle\eta|)\big) \\
&= \langle\varphi|\psi\rangle \cdot \mathrm{tr}\big(L|\xi\rangle\langle\eta|\big) \\
&= \mathrm{tr}\big(|\psi\rangle\langle\varphi|\big) \cdot \mathrm{tr}\big(L|\xi\rangle\langle\eta|\big) \\
&= \mathrm{tr}\big(|\psi\rangle\langle\varphi| \otimes L|\xi\rangle\langle\eta|\big) \\
&= \mathrm{tr}\big((\mathbb{I}\otimes L)(|\psi\rangle\langle\varphi|\otimes|\xi\rangle\langle\eta|)\big) \\
&= \mathrm{tr}\big((\mathbb{I}\otimes L)R\big)\ .
\end{aligned}$$

For a general R: by linearity

Justification for the Partial Trace

Say: state of *AB* is given by $\rho_{AB} \in \mathrm{Dens}(\mathscr{H}_A \otimes \mathscr{H}_B)$.

Want: measure *B* (alone) using measurement $\{M_i\}_{i \in I}$.

By applying Born's rule to ρ_{AB}, we get

$$\begin{aligned} p_i &= \mathrm{tr}\big((\mathbb{I} \otimes M_i)^\dagger (\mathbb{I} \otimes M_i)\, \rho_{AB}\big) \\ &= \mathrm{tr}\big((\mathbb{I} \otimes M_i^\dagger M_i)\, \rho_{AB}\big) \\ &= \mathrm{tr}\big(M_i^\dagger M_i\ \mathrm{tr}_A(\rho_{AB})\big) \end{aligned}$$

i.e., p_i can be computed (using Born's rule) from $\rho_B = \mathrm{tr}_A(\rho_{AB})$.

Example

Consider:

$$|\varphi_{AB}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\big)$$

Corresponding density matrix:

$$|\varphi_{AB}\rangle\langle\varphi_{AB}| = \frac{1}{2}\big(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\big)\big(\langle 0|\otimes\langle 0| + \langle 1|\otimes\langle 1|\big)$$
$$= \frac{1}{2}\big(|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |0\rangle\langle 1|\otimes|0\rangle\langle 1| + |1\rangle\langle 0|\otimes|1\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|\big)$$

Applying tr_A :

$$\mathrm{tr}_A\big(|\varphi_{AB}\rangle\langle\varphi_{AB}|\big) = \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big)$$

i.e., the state "$|0\rangle$ *with prob.* $1/2$*, and* $|1\rangle$ *with prob.* $1/2$"

Acting on a Subsystem

Fact: For any $\rho_{AB} \in \mathrm{Dens}(\mathscr{H}_A \otimes \mathscr{H}_B)$ and unitary $U \in \mathrm{Uni}(\mathscr{H}_A)$:

$$\mathrm{tr}_A\big((U \otimes \mathbb{I})\rho_{AB}(U \otimes \mathbb{I})^\dagger\big) = \mathrm{tr}_A(\rho_{AB})$$

Proof: Consider $|\psi\rangle\langle\varphi| \otimes |\xi\rangle\langle\eta| \in \mathrm{Lin}(\mathscr{H}_A \otimes \mathscr{H}_B)$. Then

$$\mathrm{tr}_A\big((U \otimes \mathbb{I})(|\psi\rangle\langle\varphi| \otimes |\xi\rangle\langle\eta|)(U \otimes \mathbb{I})^\dagger\big) = \mathrm{tr}_A(U|\psi\rangle\langle\varphi|U^\dagger \otimes |\xi\rangle\langle\eta|)$$

$$= \langle\varphi|U^\dagger U|\psi\rangle\,|\xi\rangle\langle\eta| = \langle\varphi|\psi\rangle\,|\xi\rangle\langle\eta| = \mathrm{tr}_A(|\psi\rangle\langle\varphi| \otimes |\xi\rangle\langle\eta|)$$

For a general $\rho_{AB} \in \mathrm{Dens}(\mathscr{H}_A \otimes \mathscr{H}_B)$: by linearity

Thus:

It is impossible to affect B by acting (unitarily) on A.

Acting on a Subsystem - Continued

The same holds for measurements:

Example: Measure system *A* of

$$|\varphi_{AB}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\big)$$

in computational basis:

State of *B* collapses to the state:

"$|0\rangle$ *with prob.* $1/2$, *and* $|1\rangle$ *with prob.* $1/2$"

which equals $\rho_B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \mathrm{tr}_A\big(|\varphi_{AB}\rangle\langle\varphi_{AB}|\big)$.

Thus, still:

nonsignaling principle

It is impossible to affect B by acting on A.

Purification

Have seen, in general:

tracing out A of **pure** state $|\varphi_{AB}\rangle$ gives a **mixed** state ρ_B .

Q: *Can **every** mixed state be obtained this way?*

A: *Yes!*

Theorem. $\forall\, \rho_B \in \mathrm{Dens}(\mathscr{H}_B)\ \exists\, |\varphi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ with $\mathscr{H}_A = \mathscr{H}_B$ s.t.

$$\rho_B = \mathrm{tr}_A(|\varphi_{AB}\rangle\langle\varphi_{AB}|) \ .$$

Purification

Theorem. $\forall\, \rho_B \in \mathrm{Dens}(\mathscr{H}_B)\ \exists\, |\varphi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ with $\mathscr{H}_A = \mathscr{H}_B$ s.t.

$$\rho_B = \mathrm{tr}_A\big(|\varphi_{AB}\rangle\langle\varphi_{AB}|\big)\ .$$

Proof. Write $\rho_B = \sum_{k=1}^{d} \varepsilon_k |\varphi_k\rangle\langle\varphi_k|$ (wlog: $d \leq \dim(\mathscr{H}_B)$)

Let $\{|k\rangle\}_{k=1..d}$ be an orthonormal basis of $\mathscr{H}_A = \mathscr{H}_B$, and set:

$$|\varphi_{AB}\rangle = \sum_k \sqrt{\varepsilon_k}\, |k\rangle \otimes |\varphi_k\rangle$$

Then:

$$|\varphi_{AB}\rangle\langle\varphi_{AB}| = \sum_{k,\ell} \sqrt{\varepsilon_k \varepsilon_\ell}\, |k\rangle\langle\ell| \otimes |\varphi_k\rangle\langle\varphi_\ell|$$

And so:

$$\mathrm{tr}_A\big(|\varphi_{AB}\rangle\langle\varphi_{AB}|\big) = \sum_{k,\ell} \sqrt{\varepsilon_k \varepsilon_\ell}\, \langle k|\ell\rangle\, |\varphi_k\rangle\langle\varphi_\ell|$$

$$= \sum_k \varepsilon_k |\varphi_k\rangle\langle\varphi_k| = \rho_B$$

Uniqueness of Purification

Q: *Is the purification **unique**?*

A: *No! Applying unitary U to **A** doesn't affect **B**:*

$$\mathrm{tr}_A\big((U\otimes\mathbb{I})|\varphi_{AB}\rangle\langle\varphi_{AB}|(U\otimes\mathbb{I})^\dagger\big) = \mathrm{tr}_A(|\varphi_{AB}\rangle\langle\varphi_{AB}|) = \rho_B\ .$$

But: *Unique up to a unitary U on **A**:*

Theorem. If

$$\mathrm{tr}_A(|\varphi_{AB}\rangle\langle\varphi_{AB}|) \stackrel{\approx}{=} \mathrm{tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$$

then $\exists\, U\in\mathrm{Uni}(\mathscr{H}_A)$ s.t.

$$|\psi_{AB}\rangle \stackrel{\approx}{=} (U\otimes\mathbb{I})|\varphi_{AB}\rangle.$$

(approximate version: Uhlman's Theorem)

Application: Impossibility of QBC

Commitment Schemes

- (Bit) commitment scheme = digital analogue of:
  - putting a message, or a bit, in a vault
  - and revealing it later

- Security properties:
  - *hiding*: Bob cannot see message/bit “inside” commitment
  - *binding*: Alice cannot change her mind

- Important cryptographic primitive, used for
  - coin tossing
  - zero-knowledge proofs
  - multiparty computation
  - etc.

Impossibility

- Classical (non-quantum) BC:
  scheme **cannot** be unconditionally *hiding* and *binding*

- Indeed: Unconditionally *binding*
  $\Rightarrow$ committed message is determined by Bob's info
  $\Rightarrow$ can in principle be computed
  $\Rightarrow$ not unconditionally *hiding*

- Reasoning doesn't apply in quantum setting
- After invention of QKD, strong believe in possibility of QBC
- Several schemes proposed in late 80's and early 90's.

- 1996/97: Mayers / Lo & Chau showed impossibility of QBC.

Impossibility Proof (Sketch)

- Consider potential QBC scheme
- Look at joint state after commit phase

  $|\varphi^0_{AB}\rangle$ or $|\varphi^1_{AB}\rangle$

  depending on whether honest Alice committed to 0 or 1

WLOG: may assume this state to be pure

- By *hiding* property:

$$\mathrm{tr}_A(|\varphi^0_{AB}\rangle\langle\varphi^0_{AB}|) \approx \mathrm{tr}_A(|\varphi^1_{AB}\rangle\langle\varphi^1_{AB}|)$$

- Thus, by Uhlmans Theorem:

$$\exists U \in \mathrm{Uni}(\mathscr{H}_A)\colon |\varphi^1_{AB}\rangle \approx (U \otimes \mathbb{I})|\varphi^0_{AB}\rangle.$$

- So, dishonest Alice can (honestly) commit to, say, 0, but can still "change her mind" by applying U to her state.

Back to theory...

Classical versus Quantum Information

Consider: non-empty finite set $\mathcal{X}$

We understand $x \in \mathcal{X}$ as ***classical*** *information*

Want: capture *classical* information using *quantum* formalism

For that,

- consider $\mathscr{H}_X = \mathbb{C}^{|\mathcal{X}|}$
- fix orthonormal basis $\{|x\rangle\}_{x \in \mathcal{X}}$ of $\mathscr{H}_X$
- identify $x \in \mathcal{X}$ with quantum state $|x\rangle \in \mathscr{H}_X$ (resp. $|x\rangle\langle x|$)

Holding *classical* x is **equivalent** to holding *quantum* state $|x\rangle$:
x can be recovered from $|x\rangle$ by measuring in basis $\{|x\rangle\}_{x \in \mathcal{X}}$.

Randomized Classical Information

Randomized *classical* info, given by random variable X, such that $X{=}x$ with prob. $P_X(x)$, is then identified with

$$\rho_X = \sum_x P_X(x)|x\rangle\langle x| \in \mathrm{Dens}(\mathscr{H}_X)$$

Finally, a hybrid of *classical* and *quantum* info, where

- $X{=}x$ with prob. $P_X(x)$,
- state of A is given by $\rho_A^x \in \mathrm{Dens}(\mathscr{H}_A)$

is then identified with

$$\rho_{XA} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_A^x \in \mathrm{Dens}(\mathscr{H}_X \otimes \mathscr{H}_A)$$

Example: Measurement

Let $\{M_x\}_{x\in\mathcal{X}}$ be a measurement on a system ***A***.

Applied to a state $\rho\in\mathrm{Dens}(\mathscr{H}_A)$:

- observe x with probability $p_x = \mathrm{tr}\big(M_x\rho M_x^\dagger\big)$
- state collapses to $\rho^x = M_x\rho M_x^\dagger/p_x$.

Captured by “hybrid state”:

$$\sum_x p_x|x\rangle\langle x|\otimes\rho^x = \sum_x |x\rangle\langle x|\otimes M_x\rho M_x^\dagger$$
$$= \sum_x (|x\rangle\otimes M_x)\,\rho\,(\langle x|\otimes M_x^\dagger)$$

where $|x\rangle\otimes M_x\colon \mathscr{H}_A\to\mathscr{H}_X\otimes\mathscr{H}_A$, $|\varphi\rangle\mapsto|x\rangle\otimes M_x|\varphi\rangle$ and

$$\sum(\langle x|\otimes M_x^\dagger)(|x\rangle\otimes M_x) = \sum\langle x|x\rangle M_x^\dagger M_x = \sum M_x^\dagger M_x = \mathbb{I}$$

CPTP Maps (or Quantum Channels)

Definition. $\mathcal{E}$: $\mathrm{Lin}(\mathscr{H}_A) \to \mathrm{Lin}(\mathscr{H}_{A'})$ is called a *CPTP map* if

$$\mathcal{E}(R) = \sum_i E_i R E_i^\dagger$$

or
quantum channel

where $E_i : \mathscr{H}_A \to \mathscr{H}_{A'}$ such that $\sum E_i^\dagger E_i = \mathbb{I}$.

Examples:

- measuring a quantum state: $\rho \mapsto \sum (|x\rangle \otimes M_x)\rho(\langle x| \otimes M_x^\dagger)$
- applying a unitary: $\rho \mapsto U\rho U^\dagger$
- appending a (fixed) state $|\varphi\rangle$:

$$\rho \mapsto \rho \otimes |\varphi\rangle\langle\varphi| = (\mathbb{I} \otimes |\varphi\rangle)\,\rho\,(\mathbb{I} \otimes \langle\varphi|)$$

- "throwing away" part of a state:

$$\rho_{AB} \mapsto \mathrm{tr}_A(\rho_{AB}) = \sum (\langle i| \otimes \mathbb{I})\,\rho_{AB}\,(|i\rangle \otimes \mathbb{I})$$

CPTP Maps (or Quantum Channels)

Definition. $\mathcal{E}$: $\mathrm{Lin}(\mathscr{H}_A) \to \mathrm{Lin}(\mathscr{H}_{A'})$ is called a *CPTP map* if

$$\mathcal{E}(R) = \sum_i E_i R E_i^\dagger$$

or
quantum channel

where $E_i : \mathscr{H}_A \to \mathscr{H}_{A'}$ such that $\sum E_i^\dagger E_i = \mathbb{I}$.

Thus:

Every quantum operation is described by a CPTP map.

And:

Every CPTP map describes a quantum operation.

- "throwing away" part of a state:

$$\rho_{AB} \mapsto \mathrm{tr}_A(\rho_{AB}) = \sum (\langle i| \otimes \mathbb{I})\, \rho_{AB}\, (|i\rangle \otimes \mathbb{I})$$

Characterizations of CPTP maps

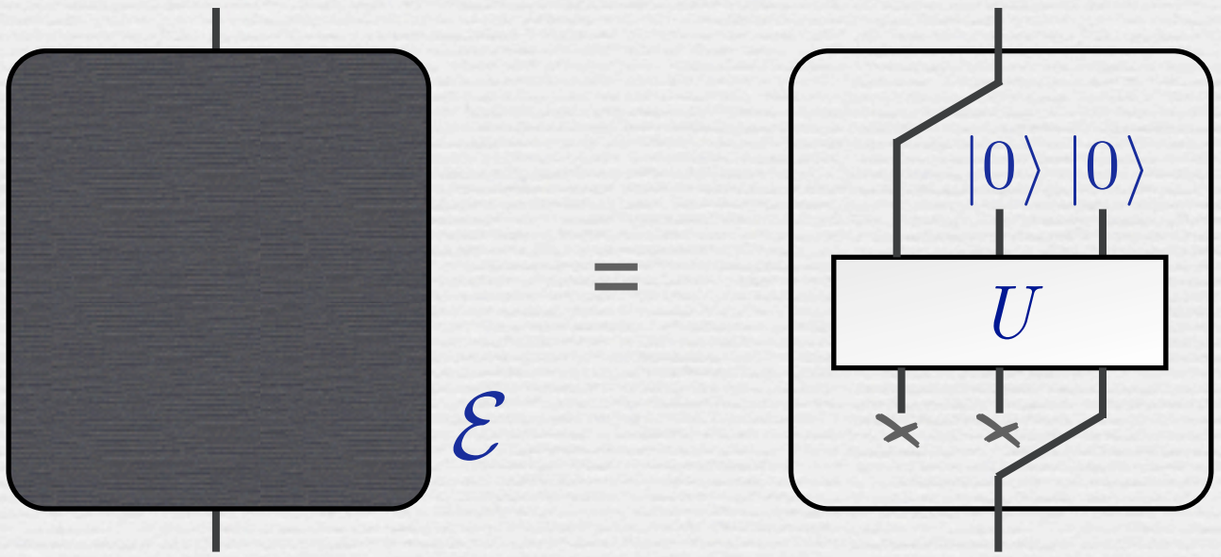
Theorem. Let $\mathcal{E}: \mathrm{Lin}(\mathscr{H}_A) \to \mathrm{Lin}(\mathscr{H}_{A'})$. The following are "⇔"

1. $\mathcal{E}$ is a CPTP map (i.e., $\mathcal{E}(R) = \sum E_i R E_i^\dagger$). *Kraus representation*
2. $\mathcal{E}$ is *completely positive* and *trace preserving.*
3. $\exists\ \mathscr{H}_E$ and $U \in \mathrm{Uni}(\mathscr{H}_A \otimes \mathscr{H}_E \otimes \mathscr{H}_{A'})$ s.t. $\forall\, \rho \in \mathrm{Dens}(\mathscr{H}_A)$:

$$\mathcal{E}(\rho) = \mathrm{tr}_{AE}\big(U(\rho \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|)\, U^\dagger\big)$$

Steinspring representation

where the $|0\rangle$'s are default state vectors in $\mathscr{H}_E$ and $\mathscr{H}_{A'}$.



Application: No-Cloning (Part II)

No-Cloning

Theorem. Let $\mathcal{E}$ be a CPTP map, and $|\varphi\rangle, |\psi\rangle$ state vectors. If

$$\mathcal{E}(|\varphi\rangle\langle\varphi|) = |\varphi\rangle\langle\varphi| \otimes |\varphi\rangle\langle\varphi| \text{ and } \mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \ .$$

then $|\langle\varphi|\psi\rangle| = 1$ (and thus $|\varphi\rangle\langle\varphi| = |\psi\rangle\langle\psi|$) or $\langle\varphi|\psi\rangle = 0$.

Proof:

- Consider Steinspring representation of $\mathcal{E}$ and the states $\mathcal{E}(|\varphi\rangle\langle\varphi|)$ and $\mathcal{E}(|\psi\rangle\langle\psi|)$ **before** the partial trace:

$$U|\varphi\rangle|0\rangle|0\rangle \text{ and } U|\psi\rangle|0\rangle|0\rangle.$$

- By uniqueness of purification, must be of the form

$$U|\varphi\rangle|0\rangle|0\rangle = |\varphi\rangle|\varphi\rangle|\varphi_o\rangle \text{ and } U|\psi\rangle|0\rangle|0\rangle = |\psi\rangle|\psi\rangle|\psi_o\rangle.$$

- But then: $\langle\varphi|\psi\rangle = \langle\varphi|\langle 0|\langle 0| U^\dagger U|\psi\rangle|0\rangle|0\rangle = \langle\varphi|\psi\rangle^2\langle\varphi_o|\psi_o\rangle$ which implies that $|\langle\varphi|\psi\rangle| = 1$ or $\langle\varphi|\psi\rangle = 0$.

No-Cloning

Theorem. Let $\mathcal{E}$ be a CPTP map, and $|\varphi\rangle, |\psi\rangle$ state vectors. If

$$\mathcal{E}(|\varphi\rangle\langle\varphi|) = |\varphi\rangle\langle\varphi| \otimes |\varphi\rangle\langle\varphi| \text{ and } \mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \ .$$

then $|\langle\varphi|\psi\rangle| = 1$ (and thus $|\varphi\rangle\langle\varphi| = |\psi\rangle\langle\psi|$) or $\langle\varphi|\psi\rangle = 0$.

Proof:

- Cons[illegible] state[illegible] [illegible]race:
- By uniqueness of purification, must be of the form

$$U|\varphi\rangle|0\rangle|0\rangle = |\varphi\rangle|\varphi\rangle|\varphi_o\rangle \text{ and } U|\psi\rangle|0\rangle|0\rangle = |\psi\rangle|\psi\rangle|\psi_o\rangle.$$

- But then: $\langle\varphi|\psi\rangle = \langle\varphi|\langle 0|\langle 0| U^\dagger U|\psi\rangle|0\rangle|0\rangle = \langle\varphi|\psi\rangle^2\langle\varphi_o|\psi_o\rangle$ which implies that $|\langle\varphi|\psi\rangle| = 1$ or $\langle\varphi|\psi\rangle = 0$.

Using Uhlman's Theorem:
Also approximate cloning is impossible

Back to theory: Distance between States

Trace-Norm and -Distance

Definition. The ***trace norm*** of a Hermitian $D \in \mathrm{Lin}(\mathscr{H})$ is

$$\|D\| := \sum |\lambda_i|$$

where $\lambda_1,\ldots,\lambda_d \in \mathbb{R}$ is the list of eigenvectors (w/ multiplicity).

Example: The λ_i's of $\rho \in \mathrm{Dens}(\mathscr{H})$ are ≥ 0 and add to 1. So:

$$\|\rho\| = 1 \,.$$

Definition. The ***trace distance*** of $\rho, \sigma \in \mathrm{Dens}(\mathscr{H})$ is

$$\delta(\rho,\sigma) := \frac{1}{2}\|\sigma - \rho\| \,.$$

The Classical Case

If P and Q are distributions over $\mathcal{X}$, and

$$\rho = \sum P(x)|x\rangle\langle x| \quad \text{and} \quad \sigma = \sum Q(x)|x\rangle\langle x|$$

the corresponding density matrix representations, then

$$\rho - \sigma = \sum \big(P(x) - Q(x)\big)|x\rangle\langle x|$$

and thus

$$\delta(\rho,\sigma) = \frac{1}{2}\sum |P(x) - Q(x)|$$

which is the *statistical distance* between P and Q, which captures exactly **how well P and Q can be distinguished**.

Trace Distance and Distinguishability

Theorem. Let $\mathcal{E}$ be a CPTP map and $\rho,\sigma \in \mathrm{Dens}(\mathscr{H})$, then

$$\delta\big(\mathcal{E}(\rho),\mathcal{E}(\sigma)\big) \leq \delta(\rho,\sigma).$$

In particular:

$\delta(\rho,\sigma)$ *bounds how well* ρ & σ *can be distinguished.*

Proposition. $\forall\ \rho,\sigma \in \mathrm{Dens}(\mathscr{H})$ $\exists$ measurement $\mathcal{M}$ s.t.

$$\delta\big(\mathcal{M}(\rho),\mathcal{M}(\sigma)\big) = \delta(\rho,\sigma).$$

Thus:

$\delta(\rho,\sigma)$ *captures exactly how well* ρ & σ *can be distinguished.*

Proof of Proposition

Proposition. $\forall\ \rho,\sigma \in \mathrm{Dens}(\mathscr{H})\ \exists$ measurement $\mathcal{M}$ s.t.

$$\delta\big(\mathcal{M}(\rho),\mathcal{M}(\sigma)\big) = \delta(\rho,\sigma).$$

Proof: Let $\mathcal{M}$ be measurement given by $\{M_i = |i\rangle\langle i|\}$, where $\{|i\rangle\}$ is an orthonormal eigenbasis of $\rho - \sigma$.

Then

$$\begin{aligned}
2\cdot\delta\big(\mathcal{M}(\rho),\mathcal{M}(\sigma)\big) &= \sum \big|\mathrm{tr}\big(|i\rangle\langle i|\,\rho\big) - \mathrm{tr}\big(|i\rangle\langle i|\,\sigma\big)\big| \\
&= \sum \big|\mathrm{tr}\big(|i\rangle\langle i|\,(\rho-\sigma)\big)\big| \\
&= \sum \big|\langle i|(\rho-\sigma)|i\rangle\big| \\
&= \sum \big|\lambda_i \langle i|i\rangle\big| \\
&= \sum |\lambda_i| \\
&= 2\cdot\delta(\rho,\sigma)
\end{aligned}$$

Almost done...

Take-Home Summary

- Quantum state is described by
  - a state vector for pure state, or
  - a density matrix for mixed states.
- ∃ mathematical rules for how the state behaves under:
  - unitary operation
  - measurement
  - appending a state
  - “throwing away” part
- Purification: every mixed state can be purified - uniquely.
- Classical info can be captured by quantum formalism.
- CPTP maps: captures all possible quantum operations
- Trace distance: captures how similarly states behave