

Unknown quantum operations: A de Finetti representation theorem

Rüdiger Schack

Royal Holloway, University of London

in collaboration with

Christopher A. Fuchs (Bell Labs)

Petra Scudo (Technion)

early project

- 1. What's the point of this story?
- 2. Why a representation theorem for quantum operations?
- **3. The classical de Finetti theorem**
- 4. The quantum de Finetti theorem
- 5. Bayesian quantum process tomography
- 6. De Finetti theorem for quantum operations

No randomness in no randomness out!

No randomness in no randomness out!

Any probability assignment p to the outcome 0 depends on some prior probability assignment.

Royal Holloway

No randomness in no randomness out!

Any probability assignment p to the outcome 0 depends on some prior probability assignment.

Royal Holloway

Bayesian probability theory: p is a degree of belief, not part of physical reality.

It certainly looks like it: A measurement in the basis $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$

yields the result $+$. The post-measurement state is

$$
\mathcal{F}(\rho) = \frac{|+\rangle\langle+|\rho|+\rangle\langle+|}{\langle+|\rho|+\rangle} = |+\rangle\langle+|.
$$

A subsequent measurement in the 0-1 basis gives $p=\Pr(0)=\frac{1}{2}.$

It certainly looks like it: A measurement in the basis $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ yields the result $+$. The post-measurement state is

$$
\mathcal{F}(\rho) = \frac{|+\rangle\langle+|\rho|+\rangle\langle+|}{\langle+|\rho|+\rangle} = |+\rangle\langle+|.
$$

A subsequent measurement in the 0-1 basis gives $p=\Pr(0)=\frac{1}{2}.$

Is p part of physical reality?

It certainly looks like it: A measurement in the basis $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ yields the result $+$. The post-measurement state is

$$
\mathcal{F}(\rho) = \frac{|+\rangle\langle+|\rho|+\rangle\langle+|}{\langle+|\rho|+\rangle} = |+\rangle\langle+|.
$$

A subsequent measurement in the 0-1 basis gives $p=\Pr(0)=\frac{1}{2}.$

F is part of physical reality $\implies |+\rangle$ is part of physical reality $\Longrightarrow p$ is part of physical reality.

Consider a mixture

$$
\rho = p|+\rangle\langle +| + (1-p)|-\rangle\langle -| ,
$$

where p is a Bayesian degree of belief, and $|\pm\rangle\langle\pm|$ are elements of physical reality.

But ρ can be rewritten

 $\rho = q|\psi\rangle\langle\psi| + (1 - q)|\phi\rangle\langle\phi|$.

What kind of probability is $q\, ?$

Preferred decomposition of density operators?

. . . all probabilities in quantum mechanics are taken to be Bayesian degrees of belief?

. . . all probabilities in quantum mechanics are taken to be Bayesian degrees of belief?

Then some quantum operations do not represent real states of affairs.

. . . all probabilities in quantum mechanics are taken to be Bayesian degrees of belief?

Then some quantum operations do not represent real states of affairs.

The argument:

F is part of physical reality $\implies |+\rangle$ is part of physical reality $\Longrightarrow p$ is part of physical reality.

Equivalently,

p is not part of physical reality $\implies |+\rangle$ is not part of physical reality $\implies \mathcal{F}$ is not part of physical reality.

Quantum process tomography: Determine ^a quantum operation by making measurements on the output for ^a set of well-chosen inputs.

What does it mean to determine an unknown quantum operation, $\mathcal F$, if $\mathcal F$ is not part of physical reality?

Needed: A Bayesian formulation of quantum process tomography.

Classical tomography

Result in 10 throws:

- 1 times $k=1$,
- **4** times $k=2$,
- 2 times $k=3$,
- 2 times $k=4$,
- 1 times $k=5$,
- **0** times $k=6$.

- 1 times $k = 1$,
- **4** times $k=2$,
- **2** times $k = 3$,
- **2** times $k = 4$,
- 1 times $k = 5$,
- **0 times** $k = 6$.

Question: What probability p do you assign to a 6 in the next throw?

Answer: It depends on your prior.

- 1 times $k = 1$,
- **4** times $k=2$,
- **2** times $k = 3$,
- **2** times $k = 4$,
- 1 times $k = 5$,
- **0 times** $k = 6$.

Question: What probability p do you assign to a 6 in the next throw?

Answer I: $p = 1/6$ if you believe that the die is fair.

- 1 times $k = 1$,
- **4** times $k=2$,
- **2** times $k = 3$,
- **2** times $k = 4$,
- 1 times $k = 5$,
- **0 times** $k = 6$.

Question: What probability p do you assign to a 6 in the next throw?

Answer II: $p = 1/12$ given a totally uninformative prior (Laplace's rule of succession).

- 1 times $k = 1$,
- **4** times $k=2$,
- **2** times $k = 3$,
- **2** times $k = 4$,
- 1 times $k = 5$,
- **0 times** $k = 6$.

Question: What probability p do you assign to a 6 in the next throw?

Answer III: $p = 0$ if you know the die came from a box that contains only trick dice of two types: type A never comes up 1, type B never comes up 6.

 $p^{(n)}(x_1,\ldots,x_n)$, $n=1,2,\ldots$ form an exchangeable sequence if

Royal Holloway

 $p^{(n)}(x_1,\ldots,x_n), n=1,2,\ldots$ form an exchangeable sequence if

(i) (symmetry) $p^{(n)}$ is permutation invariant;

Royal Holloway

 $p^{(n)}(x_1,\ldots,x_n), n=1,2,\ldots$ form an exchangeable sequence if

(i) (symmetry) $p^{(n)}$ is permutation invariant;

(ii) (extendibility) $p^{(n)}$ is the marginal of $p^{(n+1)}$.

Royal Holloway

 $p^{(n)}(x_1,\ldots,x_n), n=1,2,\ldots$ form an exchangeable sequence if

(i) (symmetry) $p^{(n)}$ is permutation invariant;

(ii) (extendibility) $p^{(n)}$ is the marginal of $p^{(n+1)}$.

For given N, we say that $p^{(N)}(x_1, \ldots, x_N)$ is exchangeable if it is part of an exchangeable sequence.

De Finetti's representation theorem (binary case)

 $p^{(N)}(x_1,\ldots,x_N)$ is exchangeable if and only if

$$
p^{(N)}(x_1, \dots, x_N) = \int_0^1 P(p) \, p^k (1-p)^{N-k} dp
$$

where $P(p)$ is unique and k is the number of zeroes in (x_1,\ldots,x_N) .

(i) Start from an exchangeable prior for $N + M$ trials.

(ii) Collect data for N trials.

(iii) Use Bayes' rule to obtain (posterior) probabilities for the remaining M trials.

(i) Start from an exchangeable prior for $N + M$ trials.

(ii) Collect data for N trials.

(iii) Use Bayes' rule to obtain (posterior) probabilities for the remaining M trials.

Two agents starting from different priors will always converge to ^a joint posterior in the limit of large N (under mild assumptions about the priors).

Key assumption: Exchangeability.

Exchangeability for quantum systems

A state $\rho^{(N)}$ of N systems is [exchangea](#page-53-0)ble if it is a member of an exchangeable sequence $\rho^{(n)}$, i.e.,

(i) (symmetry) each $\rho^{(n)}$ is invariant under permutations of the n systems on which it is defined; and

(ii) (extendibility) $\rho^{(n)} = \text{tr}_{n+1}\rho^{(n+1)}$ for all n, where tr_{n+1} denotes the partial trace over the $(n + 1)$ th system.

 $\rho^{(N)}$ is [exchangea](#page-53-0)ble if and only if

 $\rho^{(N)} = \int d\rho \ p(\rho) \rho^{\otimes N} = \int d\rho \ p(\rho) \rho \otimes \cdots \otimes \rho,$ where $p(\rho)\geq 0$ is unique.

(Hudson, Moody 1976; Caves, Fuchs, RS 2002)

 $p(\rho|\vec{\alpha})$ given by the [quantum](#page-54-0) Bayes rule.

 $\boxed{\rho^{(M)} = \int d\rho~p(\rho|\vec{\alpha})\,\rho^{\otimes M}}$

Royal Holloway

Two agents starting from different priors will always converge to a joint posterior in the limit of large N (under mild assumptions about the priors). 2002 – p.15

Any finite version of quantum process tomography depends ineluctably on ^a prior.

Wanted: A representation theorem for priors in the space of quantum operations on N copies of a system.

Bayesian quantum process tomography

We describe N uses of a quantum channel by a quantum operation (trace-preserving cpm)

 $\Phi^{(N)} : \mathcal{L}(\mathcal{H}^{\otimes N}) \longrightarrow \mathcal{L}(\mathcal{H}^{\otimes N})$

1. We start from an exchangeable prior $\Phi^{(N+M)}$.

- 1. We start from an exchangeable prior $\Phi^{(N+M)}$.
- 2. We send $N+M$ particles in a state $\rho_{\rm in} = \sigma^{(N)} \otimes \rho^{(M)}$ through the channel.

- 1. We start from an exchangeable prior $\Phi^{(N+M)}$.
- 2. We send $N+M$ particles in a state $\rho_{\rm in} = \sigma^{(N)} \otimes \rho^{(M)}$ through the channel.
- 3. The output state is $\rho_{\rm out} = \Phi^{(N+M)}(\rho_{\rm in})$.

- 1. We start from an exchangeable prior $\Phi^{(N+M)}$.
- 2. We send $N+M$ particles in a state $\rho_{\rm in} = \sigma^{(N)} \otimes \rho^{(M)}$ through the channel.
- 3. The output state is $\rho_{\rm out} = \Phi^{(N+M)}(\rho_{\rm in})$.
- 4. We do measurements on the first N particles.

- 1. We start from an exchangeable prior $\Phi^{(N+M)}$.
- 2. We send $N+M$ particles in a state $\rho_{\rm in} = \sigma^{(N)} \otimes \rho^{(M)}$ through the channel.
- 3. The output state is $\rho_{\rm out} = \Phi^{(N+M)}(\rho_{\rm in})$.
- 4. We do measurements on the first N particles.
- 5. We deduce $\Phi^{(M)}(\rho^{(M)})$.

Exchangeability

for quantum operations

A sequence $\Phi^{(n)}$ of quantum operations defined on $\mathcal{L}(\mathcal{H}^{\otimes n})$ is exchangeable if

Exchangeability

for quantum operations

A sequence $\Phi^{(n)}$ of quantum operations defined on $\mathcal{L}(\mathcal{H}^{\otimes n})$ is exchangeable if

1.) (symmetry) $\Phi^{(n)}(\rho^{(n)}) = \pi(\Phi^{(n)}(\pi^{-1}\rho^{(n)}))$ for any permutation π of the n systems and for any state $\rho^{(n)};$

Exchangeability

for quantum operations

A sequence $\Phi^{(n)}$ of quantum operations defined on $\mathcal{L}(\mathcal{H}^{\otimes n})$ is exchangeable if

1.) (symmetry) $\Phi^{(n)}(\rho^{(n)}) = \pi(\Phi^{(n)}(\pi^{-1}\rho^{(n)}))$ for any permutation π of the n systems and for any state $\rho^{(n)};$

2.) (Extendibility) $\Phi^{(n)}(\rho^{(n)}) = \text{tr}_{n+1}\Big(\Phi^{(n+1)}(\rho^{(n+1)})\Big)$ for any states $\rho^{(n)}$, $\rho^{(n+1)}$ such that $\rho^{(n)} = \text{tr}_{n+1}\rho^{(n+1)}$.

De Finetti representation for

quantum operations

 $\Phi^{(N)}$ is exchangeable (i.e., part of an exchangeable sequence)

if and only if

$$
\Phi^{(N)} = \int d\Phi \; p(\Phi) \; \Phi^{\otimes N}
$$

where the integral ranges over all single-system quantum operations $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, and where $p(\Phi) \geq 0$ is unique.

 Φ is a quantum operation on \mathcal{H}_d if it is a trace-preserving completely positive map (cpm), i.e.,

 Φ is a quantum operation on \mathcal{H}_d if it is a trace-preserving completely positive map (cpm), i.e.,

 Φ is a linear map on $\mathcal{L}(\mathcal{H}_d)$ with the properties

1.) $\Phi(\rho)$ is a density operator for any density operator ρ on \mathcal{H}_d ;

 Φ is a quantum operation on \mathcal{H}_d if it is a trace-preserving completely positive map (cpm), i.e.,

 Φ is a linear map on $\mathcal{L}(\mathcal{H}_d)$ with the properties

1.) $\Phi(\rho)$ is a density operator for any density operator ρ on \mathcal{H}_d ;

2.) $(I \otimes \Phi)(\rho^{(2)})$ is a density operator for any density operator $\rho^{(2)}$ on $\mathcal{H}_{d'} \otimes \mathcal{H}_{d}$ (d' arbitrary).

Let
$$
|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |e_j\rangle \otimes |e_j\rangle \in \mathcal{H}_d \otimes \mathcal{H}_d
$$

be a maximally entangled state.

Theorem [\(Jamiołkows](#page-55-0)ki):

A linear map Φ on \mathcal{H}_d is a cpm

if and only if

 $(I \otimes \Phi)(|\psi\rangle\langle\psi|)$ is a positive operator.

Denote by $\rho^{(N)}$ the [Jamiołkow](#page-55-0)ski density operator corresponding to the quantum operation $\Phi^{(N)}$.

 $\Phi^{(N)}$ exchangeable

- $\Longrightarrow \rho^{(N)}$ exchangeable
- \Longrightarrow unique de Finetti representation for $\rho^{(N)}$
- \Longrightarrow unique de Finetti representation for $\Phi^{(N)}$.

There exist non-trace-preserving cpm's Φ such that $(I \otimes \Phi)(|\psi\rangle\langle\psi|)$ is a density operator.

How does one see that the domain of the integral

$$
\Phi^{(N)} = \int d\Phi~p(\Phi)~\Phi^{\otimes N}
$$

includes only trace-preserving cpm's?

 $\Phi^{(N)}=\sum$ $\it i$ $p_i\; \Phi_i^{\otimes N}$, $p_i > 0$,

$$
\Phi^{(N)} = \sum_{i} p_i \, \Phi_i^{\otimes N}, \, p_i > 0,
$$
\n
$$
\text{implies } 1 = \sum_{i} p_i \big(\text{tr}[\Phi_i(\rho)]\big)^N \text{ for all } \rho.
$$

$$
\Phi^{(N)} = \sum_i p_i \ \Phi_i^{\otimes N}, \ p_i > 0,
$$

implies $1=\sum p_i\big(\text{tr}[\Phi_i(\rho)]\big)^N$ for all $\rho.$ $\it i$

Assume $\mathrm{tr}[\Phi_1(\rho)]\neq 1$ for some $\rho.$

$$
\Phi^{(N)} = \sum_i p_i \; \Phi_i^{\otimes N}, \, p_i > 0,
$$

implies $1=\sum p_i\big(\text{tr}[\Phi_i(\rho)]\big)^N$ for all $\rho.$ $\it i$

Assume $\mathrm{tr}[\Phi_1(\rho)]\neq 1$ for some $\rho.$

Then there is k such that $\mathrm{tr}[\Phi_k(\rho)]>1.$

$$
\Phi^{(N)} = \sum_i p_i \ \Phi_i^{\otimes N}, \ p_i > 0,
$$

implies $1=\sum p_i\big(\text{tr}[\Phi_i(\rho)]\big)^N$ for all $\rho.$ $\it i$

Assume $\mathrm{tr}[\Phi_1(\rho)]\neq 1$ for some $\rho.$

Then there is k such that $\mathrm{tr}[\Phi_k(\rho)]>1.$

Then $1\geq p_k\big(\text{tr}[\Phi_k(\rho)]\big)^N\to\infty$

- 1. We start from an exchangeable prior $\Phi^{(N+M)}$.
- 2. We send $N+M$ particles in a state $\rho_{\rm in} = \sigma^{(N)} \otimes \rho^{(M)}$ through the channel.
- 3. The output state is $\rho_{\rm out} = \Phi^{(N+M)}(\rho_{\rm in})$.
- 4. We do measurements on the first N particles.
- 5. We deduce $\Phi^{(M)}(\rho^{(M)})$.

1.) $\rho = \rho_1 \otimes \rho_2$ is not exchangeable for $\rho_1 \neq \rho_2$.

Royal Holloway

2.) $\rho_{\rm GHZ} = \frac{1}{2}(\ket{000} + \ket{111})(\bra{000} + \bra{111})$ is not exchangeable:

there exists no permutation-invariant $\rho^{(4)}$ such that $\rho_{\rm GHZ} = {\rm tr}_4(\rho^{(4)})$.

$$
p(\rho|\vec{\alpha}) = \frac{p(\rho)p(\vec{\alpha}|\rho)}{p_{\alpha}} \ ,
$$

where $p(\vec{\alpha}|\rho)=\text{tr} \big(\,\rho^{\otimes N}\,E_{\alpha_1}\otimes\cdots\otimes E_{\alpha_N}\big)$,

$$
\vec{\alpha}=(\alpha_1,\ldots,\alpha_N),
$$

 ${E_k}$ is a POVM,

and
$$
p_{\alpha} = \int d\rho \ p(\rho) p(\vec{\alpha}|\rho)
$$
.

University of London Jamiołkowski operator

Matrix elements of Φ :

$$
\Phi(|e_j\rangle\langle e_k|) = \sum_{l,m} S_{lj,mk} |e_l\rangle\langle e_m|
$$

Matrix elements of Jamiołkowski's ρ :

$$
\rho = (I \otimes \Phi)(|\psi\rangle\langle\psi|)
$$

= $\frac{1}{d} \sum_{l,j,m,k} S_{lj,mk}(|e_j\rangle \otimes |e_l\rangle)(\langle e_k| \otimes \langle e_m|)$

Let $\{E_1, \ldots, E_{d^2}\}\)$ be a minimal informationally complete POVM on d-dim. Hilbert space \mathcal{H}_d .

Then there is ^a one-to-one correspondence between states ρ and probabilities (p_1,\ldots,p_{d^2}) :

 $tr(\rho E_1) = p_1$ $tr(\rho E_2) = p_2$

.. .

 $tr(\rho E_{d^2}) = p_{d^2}$

Let $\{E_1, \ldots, E_{d^2}\}\)$ be a minimal informationally complete POVM on d-dim. Hilbert space \mathcal{H}_d .

Then there is ^a one-to-one correspondence between states ρ and probabilities (p_1,\ldots,p_{d^2}) :

 $tr(\rho E_1) = p_1$ $tr(\rho E_2) = p_2$

.. .

 $tr(\rho E_{d^2}) = p_{d^2}$

 $\{E_1, \ldots, E_{d^2}\}\;$ form a basis of the d^2 -dimensional vector space $\mathcal{L}(\mathcal{H}_d)$.

Results are random variables $\alpha_k \in \{1, \ldots, d^2\}$ with distribution

$$
p^{(N)}(\alpha_1,\ldots,\alpha_N) = \text{tr}\big(\, \rho^{(N)}\,E_{\alpha_1}\otimes\cdots\otimes E_{\alpha_N}\big)
$$

Results are random variables $\alpha_k \in \{1, \ldots, d^2\}$ with distribution

$$
p^{(N)}(\alpha_1,\ldots,\alpha_N)=\text{tr}\big(\,\rho^{(N)}\,E_{\alpha_1}\otimes\cdots\otimes E_{\alpha_N}\big)
$$

 $\rho^{(N)}$ exchangeable

- $\Longrightarrow p^{(N)}$ exchangeable
- \Longrightarrow classical de Finetti representation for $p^{(N)}$
- \Longrightarrow quantum de Finetti representation for $\rho^{(N)}.$

Construction of a minimal ICPOVM

1.) Let $\{|e_i\rangle\}$ be an orthonormal basis of \mathcal{H}_d . A basis of $\mathcal{L}(\mathcal{H}_d)$ is then given by the d^2 projectors Π_α of the form

 $\Pi_\alpha = |e_j\rangle\langle e_j|$ or $\,\Pi_{\alpha}$ $\alpha = \frac{1}{2}\Bigl({\vert e_{j} \rangle + \vert e_{k} \rangle } \Bigr) \Bigl(\langle e_{j} \vert + \langle e_{k} \vert \Bigr)$ or $\,\Pi_{\alpha}$ $\alpha = \frac{1}{2}\Bigl(|e_j\rangle + i|e_k\rangle\Bigr)\Bigl(\langle e_j|-i\langle e_k|\Bigr)$ **(1)**

Construction of a minimal ICPOVM

(2)

2.)
$$
G = \sum_{\alpha=1}^{d^2} \Pi_{\alpha}
$$
 is invertible.

3.) $X \to G^{-1/2} X G^{-1/2}$ is an invertible linear transformation.

4.)
$$
I = \sum_{\alpha=1}^{d^2} G^{-1/2} \Pi_{\alpha} G^{-1/2}
$$

Construction of a minimal ICPOVM

(2)

2.)
$$
G = \sum_{\alpha=1}^{d^2} \Pi_{\alpha}
$$
 is invertible.

3.) $X \to G^{-1/2} X G^{-1/2}$ is an invertible linear transformation.

4.)
$$
I = \sum_{\alpha=1}^{d^2} G^{-1/2} \Pi_{\alpha} G^{-1/2}
$$

5.) $E_{\alpha} = G^{-1/2} \Pi_{\alpha} G^{-1/2}$ form a minimal ICPOVM.