A Gaussian de Finetti theorem and application to truncations of random Haar matrices

*arXiv:*1612.05080

Anthony Leverrier

Inria Paris

Workshop on "Probabilistic techniques and Quantum Information Theory"

Outline of the talk

- de Finetti theorems: classical and quantum
- Representation of the unitary group on Fock spaces
- Which density matrices are unitarily-invariant?
- Truncation of Haar random unitaries

Outline of the talk

- de Finetti theorems: classical and quantum
- Representation of the unitary group on Fock spaces
- Which density matrices are unitarily-invariant?
- Truncation of Haar random unitaries

Finite de Finetti theorems (classical version)

infinite version due to Bruno de Finetti (Annales IHP 1937).

Classical version: Diaconis, Freedman (Annals of Prob 1980)

Let $P(x_1, \cdots, x_n)$ be a permutation invariant distribution on S^n:

$$P(x_1, \cdots, x_n) = P(x_{\pi(1)}, \cdots, x_{\pi(n)}) \quad \forall \pi \in \mathfrak{S}_n.$$

Let P_k be the law of $(x_1, \cdots, x_k)$ on S^k. Then, for $1 \leq k \leq n$, there exists a measure dm on distributions p on S such that

$$\|P_k - \int p^{\times k} dm(p)\|_{TV} \leq 2|S|\frac{k}{n}.$$

proof follows from the total variation distance between hypergeometric and multinomial distributions:

- bag with n balls of $|S|$ colors, pick k balls
- *without replacement:* hypergeometric distribution (P is a convex mixture of such distributions corresponding to different bags)
- *with replacement:* multinomial distribution

Finite de Finetti theorems (classical version)

infinite version due to Bruno de Finetti (Annales IHP 1937).

Classical version: Diaconis, Freedman (Annals of Prob 1980)

Let $P(x_1, \cdots, x_n)$ be a permutation invariant distribution on S^n:

$$P(x_1, \cdots, x_n) = P(x_{\pi(1)}, \cdots, x_{\pi(n)}) \quad \forall \pi \in \mathfrak{S}_n.$$

Let P_k be the law of $(x_1, \cdots, x_k)$ on S^k. Then, for $1 \leq k \leq n$, there exists a measure dm on distributions p on S such that

$$\|P_k - \int p^{\times k} dm(p)\|_{TV} \leq 2|S|\frac{k}{n}.$$

proof follows from the total variation distance between hypergeometric and multinomial distributions:

- bag with n balls of $|S|$ colors, pick k balls
- *without replacement:* hypergeometric distribution (P is a convex mixture of such distributions corresponding to different bags)
- *with replacement:* multinomial distribution

Finite de Finetti theorems (quantum version)

infinite version due to Caves, Fuchs, Schack (JMP 2002)

Quantum version: Christandl, König, Mitchison, Renner (CMP 2007)

Let ρ^{n} be a permutation invariant density operator on $(\mathbb{C}^{d})^{\otimes n}$:

$$\pi\rho^{n}\pi^{\dagger} = \rho^{n} \quad \forall \pi \in \mathfrak{S}_{n}.$$

Then there exists a measure dm on the set of mixed states on $\mathbb{C}^{d}$ such that

$$\|\mathrm{tr}_{n-k}\,\rho^{n} - \int \sigma^{\otimes k}\mathrm{dm}(\sigma)\|_{tr} \leq 2d^{2}\frac{k}{n}.$$

- d^2 improved to d if ρ^n is assumed to be pure
- implies the classical version
- *applications:* security of quantum cryptography (qkd), tomography of quantum states

Finite de Finetti theorems (quantum version)

infinite version due to Caves, Fuchs, Schack (JMP 2002)

Quantum version: Christandl, König, Mitchison, Renner (CMP 2007)

Let ρ^{n} be a permutation invariant density operator on $(\mathbb{C}^{\mathrm{d}})^{\otimes \mathrm{n}}$:

$$\pi \rho^{\mathrm{n}} \pi^{\dagger} = \rho^{\mathrm{n}} \quad \forall \pi \in \mathfrak{S}_{\mathrm{n}}.$$

Then there exists a measure dm on the set of mixed states on $\mathbb{C}^{\mathrm{d}}$ such that

$$\| \mathrm{tr}_{\mathrm{n}-\mathrm{k}} \rho^{\mathrm{n}} - \int \sigma^{\otimes \mathrm{k}} \mathrm{dm}(\sigma) \|_{\mathrm{tr}} \leq 2\mathrm{d}^2 \frac{\mathrm{k}}{\mathrm{n}}.$$

- d^2 improved to d if ρ^{n} is assumed to be pure
- implies the classical version
- *applications:* security of quantum cryptography (qkd), tomography of quantum states

beyond discrete distributions and permutation invariance

infinite version due to Schoenberg (1938)

Diaconis, Freedman (Annales IHP 1987)

Let $P(x_1, \cdots, x_n)$ be an *orthogonally invariant* distribution on $\mathbb{R}^n$:

$$P(\vec{x}) = P(R\vec{x}) \quad \forall R \in O(n).$$

Let P_k be the law of $(x_1, \cdots, x_k)$ on $\mathbb{R}^k$. Then, for $1 \leq k \leq n-3$, there exists a measure dm on $\mathbb{R}_+$ such that

$$\|P_k - \int p_\sigma^{\times} \, \mathrm{dm}(\sigma)\|_{TV} \leq 2\frac{k+3}{n-k-3}$$

with p_σ the law of a Gaussian variable $\mathcal{N}(0, \sigma^2)$

- ex: random vector on the sphere
- Similar results hold for other symmetries on $\mathbb{R}_+^n$ or $\mathbb{N}^n$, with normal distribution replaced by exponential or geometric.

beyond discrete distributions and permutation invariance

infinite version due to Schoenberg (1938)

Diaconis, Freedman (Annales IHP 1987)

Let $P(x_1, \cdots, x_n)$ be an *orthogonally invariant* distribution on $\mathbb{R}^n$:

$$P(\vec{x}) = P(R\vec{x}) \quad \forall R \in O(n).$$

Let P_k be the law of $(x_1, \cdots, x_k)$ on $\mathbb{R}^k$. Then, for $1 \leq k \leq n-3$, there exists a measure dm on $\mathbb{R}_+$ such that

$$\|P_k - \int p_\sigma^{\times} \, \mathrm{dm}(\sigma)\|_{TV} \leq 2\frac{k+3}{n-k-3}$$

with p_σ the law of a Gaussian variable $\mathcal{N}(0, \sigma^2)$

- ex: random vector on the sphere
- Similar results hold for other symmetries on $\mathbb{R}_+^n$ or $\mathbb{N}^n$, with normal distribution replaced by exponential or geometric.

quantum version for unitary invariance: baby version

(Easy) quantum version: Leverrier, Cerf (PRA 2009)

Let ρ^{n} be an n-mode quantum state invariant under the action of any passive interferometer (described by a unitary in $U(n)$). Then, there exists a measure dm on $\mathbb{R}_{+}$ such that

$$\|\mathrm{tr}_{n-k}\,\rho^{n} - \int \sigma_{x}^{\otimes k}\mathrm{dm}(x)\|_{tr} \leq 2\frac{n(2k+3)}{(n-k-1)(n-k-2)}$$

with σ_{x} is a thermal state with energy x.

- Follows essentially from one of the results of Diaconis and Freedman.
- a (much) stronger statement could be used to prove the security of continuous-variable qkd *(motivation for this work)*

quantum version for unitary invariance: baby version

(Easy) quantum version: Leverrier, Cerf (PRA 2009)

Let ρ^{n} be an n-mode quantum state invariant under the action of any passive interferometer (described by a unitary in $\mathrm{U}(\mathrm{n})$). Then, there exists a measure dm on $\mathbb{R}_+$ such that

$$\|\mathrm{tr}_{\mathrm{n}-\mathrm{k}}\,\rho^{\mathrm{n}} - \int \sigma_{\mathrm{x}}^{\otimes \mathrm{k}} \mathrm{dm}(\mathrm{x})\|_{\mathrm{tr}} \leq 2\frac{\mathrm{n}(2\mathrm{k}+3)}{(\mathrm{n}-\mathrm{k}-1)(\mathrm{n}-\mathrm{k}-2)}$$

with σ_{x} is a thermal state with energy x.

- Follows essentially from one of the results of Diaconis and Freedman.
- a (much) stronger statement could be used to prove the security of continuous-variable qkd *(motivation for this work)*

A further generalization

Let $X \in \mathbb{C}^{n\times p}$, $Y \in \mathbb{C}^{n\times q}$ be *unitarily invariant random matrices*:

$$P(UX, \overline{U}Y) = P(X, Y), \quad \forall U \in \mathcal{U}(n).$$

Let P_k be the distribution of the first k rows. What can we say about $P_k(X, Y)$?

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathrm{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$.

- Aaronson, Arkhipov (STOC 2011): $\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} = O\left(\frac{k^6}{n}\right)$
- expected right scaling (Jiang, Ma 2017): convergence for $k = o(n^{1/2})$
- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

A further generalization

Let $X \in \mathbb{C}^{n\times p}$, $Y \in \mathbb{C}^{n\times q}$ be *unitarily invariant random matrices*:

$$P(UX, \overline{U}Y) = P(X, Y), \quad \forall U \in \mathcal{U}(n).$$

Let P_k be the distribution of the first k rows. What can we say about $P_k(X, Y)$?

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathrm{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$.

- Aaronson, Arkhipov (STOC 2011): $\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} = O\left(\frac{k^6}{n}\right)$
- expected right scaling (Jiang, Ma 2017): convergence for $k = o(n^{1/2})$
- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

A further generalization

Let $X \in \mathbb{C}^{n\times p}$, $Y \in \mathbb{C}^{n\times q}$ be *unitarily invariant random matrices*:

$$P(UX, \overline{U}Y) = P(X, Y), \quad \forall U \in \mathcal{U}(n).$$

Let P_k be the distribution of the first k rows. What can we say about $P_k(X, Y)$?

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathrm{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$.

- Aaronson, Arkhipov (STOC 2011): $\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} = O\left(\frac{k^6}{n}\right)$
- expected right scaling (Jiang, Ma 2017): convergence for $k = o(n^{1/2})$
- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

Outline of the talk

- de Finetti theorems: classical and quantum
- Representation of the unitary group on Fock spaces
- Which density matrices are unitarily-invariant?
- Truncation of Haar random unitaries

Fock spaces

Let H be a finite-dimensional Hilbert space.

$$\mathcal{F}(\mathrm{H}) := \bigoplus_{\mathrm{k}=0}^{\infty} \mathbf{Sym}^{\mathrm{k}}(\mathrm{H}),$$

with $\mathbf{Sym}^{\mathrm{k}}(\mathrm{H})$: the symmetric part of $\mathrm{H}^{\otimes \mathrm{k}}$ (system with k excitations).

Ex: d*-mode space:* $\mathrm{H} \cong \mathbb{C}^{\mathrm{d}}$

- orthonormal basis of $\mathcal{F}(\mathbb{C}^{\mathrm{d}})$: $\{|\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_{\mathrm{d}}\rangle \,:\, \mathrm{k}_{\mathrm{i}} \in \mathbb{N}\}$
- a pair of annihilation/creation operators is associated with each mode: $[\mathrm{a}_{\mathrm{i}}, \mathrm{a}_{\mathrm{i}}^{\dagger}] = \mathbb{1}$.
- states can be expressed as functions of creation operators applied to the vacuum:
$$|\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_{\mathrm{d}}\rangle = \tfrac{1}{\sqrt{\mathrm{k}_1! \cdots \mathrm{k}_{\mathrm{d}}!}} (\mathrm{a}_1^{\dagger})^{\mathrm{k}_1} \cdots (\mathrm{a}_{\mathrm{d}}^{\dagger})^{\mathrm{k}_{\mathrm{d}}} |0\rangle$$

$$\mathcal{F}_{\mathrm{p,q,1}} := \mathcal{F}(\mathbb{C}^{\mathrm{p}} \oplus \mathbb{C}^{\mathrm{q}}) \qquad \mathcal{F}_{\mathrm{p,q,n}} := \mathcal{F}(\mathbb{C}^{\mathrm{p}} \oplus \mathbb{C}^{\mathrm{q}})^{\otimes \mathrm{n}} \cong \mathcal{F}(\mathbb{C}^{\mathrm{np}} \oplus \mathbb{C}^{\mathrm{nq}})$$

$\mathcal{F}_{\mathrm{p,q,n}}$ is an $\mathrm{n}(\mathrm{p}+\mathrm{q})$-mode Fock space.

Fock spaces

Let H be a finite-dimensional Hilbert space.

$$\mathcal{F}(\mathrm{H}) := \bigoplus_{\mathrm{k}=0}^{\infty} \mathbf{Sym}^{\mathrm{k}}(\mathrm{H}),$$

with $\mathbf{Sym}^{\mathrm{k}}(\mathrm{H})$: the symmetric part of $\mathrm{H}^{\otimes \mathrm{k}}$ (system with k excitations).

Ex: d*-mode space:* $\mathrm{H} \cong \mathbb{C}^{\mathrm{d}}$

- orthonormal basis of $\mathcal{F}(\mathbb{C}^{\mathrm{d}})$: $\{|\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_{\mathrm{d}}\rangle \,:\, \mathrm{k}_{\mathrm{i}} \in \mathbb{N}\}$
- a pair of annihilation/creation operators is associated with each mode: $[\mathrm{a}_{\mathrm{i}}, \mathrm{a}_{\mathrm{i}}^\dagger] = \mathbb{1}$.
- states can be expressed as functions of creation operators applied to the vacuum:
$$|\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_{\mathrm{d}}\rangle = \tfrac{1}{\sqrt{\mathrm{k}_1! \cdots \mathrm{k}_{\mathrm{d}}!}} (\mathrm{a}_1^\dagger)^{\mathrm{k}_1} \cdots (\mathrm{a}_{\mathrm{d}}^\dagger)^{\mathrm{k}_{\mathrm{d}}} |0\rangle$$

$$\mathcal{F}_{\mathrm{p,q,1}} := \mathcal{F}(\mathbb{C}^{\mathrm{p}} \oplus \mathbb{C}^{\mathrm{q}}) \qquad \mathcal{F}_{\mathrm{p,q,n}} := \mathcal{F}(\mathbb{C}^{\mathrm{p}} \oplus \mathbb{C}^{\mathrm{q}})^{\otimes \mathrm{n}} \cong \mathcal{F}(\mathbb{C}^{\mathrm{np}} \oplus \mathbb{C}^{\mathrm{nq}})$$

$\mathcal{F}_{\mathrm{p,q,n}}$ is an $\mathrm{n}(\mathrm{p}+\mathrm{q})$-mode Fock space.

Segal-Bargmann representation: $\mathcal{F}$ as a space of holomorphic functions

- $|\psi\rangle \in \mathcal{F}_{p,q,n}$ represented by a *holomorphic function* of $n(p+q)$ variables:

$$|\psi\rangle \quad \leftrightarrow \quad \psi : \mathbb{C}^{n\times p} \times \mathbb{C}^{n\times q} \to \mathbb{C}$$

- with norm: $\|\psi\|^2 := \frac{1}{\pi^{n(p+q)}} \int |\psi(X,Y)|^2 \exp(-\|X\|_2^2 - \|Y\|_2^2) dX dY < \infty$

Examples

- Glauber coherent state: $|\alpha\rangle = \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle = e^{\hat{a}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\alpha x} \quad (\alpha \in \mathbb{C})$

- Two-mode squeezed vacuum state:

$$\sum_{k=0}^{\infty} \lambda^k |k,k\rangle = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} \hat{a}^{\dagger k} \hat{b}^{\dagger k} = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\lambda xy} \quad (|\lambda| < 1)$$

- n 2-mode squeezed vacuum states:

$$\bigotimes_{i=1}^{n} \left(\sum_{k=0}^{\infty} \lambda^k |k,k\rangle \right) = e^{\lambda(\hat{a}_1^\dagger \hat{b}_1^\dagger + \cdots + \hat{a}_n^\dagger \hat{b}_n^\dagger)}|0\rangle \quad \leftrightarrow \quad e^{\lambda(x_1 y_1 + \cdots + x_n y_n)} \quad (|\lambda| < 1)$$

Segal-Bargmann representation: $\mathcal{F}$ as a space of holomorphic functions

- $|\psi\rangle \in \mathcal{F}_{p,q,n}$ represented by a *holomorphic function* of $n(p+q)$ variables:

$$|\psi\rangle \quad \leftrightarrow \quad \psi : \mathbb{C}^{n\times p} \times \mathbb{C}^{n\times q} \to \mathbb{C}$$

- with norm: $\|\psi\|^2 := \frac{1}{\pi^{n(p+q)}} \int |\psi(X,Y)|^2 \exp(-\|X\|_2^2 - \|Y\|_2^2) dX dY < \infty$

Examples

- Glauber coherent state: $|\alpha\rangle = \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle = e^{\hat{a}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\alpha x} \quad (\alpha \in \mathbb{C})$

- Two-mode squeezed vacuum state:

$$\sum_{k=0}^{\infty} \lambda^k |k,k\rangle = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} \hat{a}^{\dagger k} \hat{b}^{\dagger k} = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\lambda xy} \quad (|\lambda| < 1)$$

- n 2-mode squeezed vacuum states:

$$\bigotimes_{i=1}^{n} \left(\sum_{k=0}^{\infty} \lambda^k |k,k\rangle \right) = e^{\lambda(\hat{a}_1^\dagger \hat{b}_1^\dagger + \cdots + \hat{a}_n^\dagger \hat{b}_n^\dagger)}|0\rangle \quad \leftrightarrow \quad e^{\lambda(x_1 y_1 + \cdots + x_n y_n)} \quad (|\lambda| < 1)$$

Action of the unitary group on $\mathcal{F}_{\mathrm{p,q,n}}$

Mathematically: as a change of variables

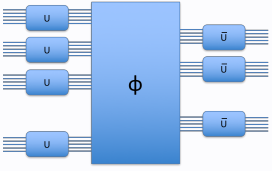
$\mathcal{F}_{\mathrm{p,q,n}}$ carries a representation $(\mathrm{u} \mapsto \mathrm{W_u})$ of the unitary group $\mathcal{U}(\mathrm{n})$:

$$\mathrm{W_u}\psi(\mathrm{X},\mathrm{Y}) := \psi(\mathrm{uX},\overline{\mathrm{u}}\mathrm{Y}), \quad \text{for } \mathrm{u} \in \mathcal{U}(\mathrm{n})$$

Physically: as a passive interferometer

Any n-mode passive interferometer (= *linear optical network*) consisting of beamsplitters and phase-shifters is described by a unitary $\mathrm{u} \in \mathcal{U}(\mathrm{n})$:

- each of the p blocks of n modes of X is processed by the interferometer u
- each of the q blocks of n modes of Y is processed by the interferometer $\overline{\mathrm{u}}$



Action of the unitary group on $\mathcal{F}_{p,q,n}$

Mathematically: as a change of variables

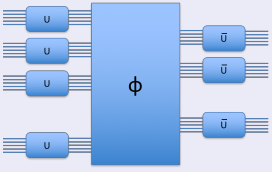
$\mathcal{F}_{p,q,n}$ carries a representation $(u \mapsto W_u)$ of the unitary group $\mathcal{U}(n)$:

$$W_u \psi(X, Y) := \psi(uX, \overline{u}Y), \quad \text{for } u \in \mathcal{U}(n)$$

Physically: as a passive interferometer

Any n-mode passive interferometer (= *linear optical network*) consisting of beamsplitters and phase-shifters is described by a unitary $u \in \mathcal{U}(n)$:

- each of the p blocks of n modes of X is processed by the interferometer u
- each of the q blocks of n modes of Y is processed by the interferometer $\overline{u}$



Outline of the talk

- de Finetti theorems: classical and quantum
- Representation of the unitary group on Fock spaces
- Which density matrices are unitarily-invariant?
- Truncation of Haar random unitaries

Restriction to pure states (for permutation-invariance)

Lemma (Christandl, König, Mitchison, Renner, CMP 2007)

Let ρ be a permutation-invariant density matrix on $\mathcal{H}^{\otimes n}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{K}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ (with $\mathcal{K} \cong \mathcal{H}$) such that

$$\pi|\psi\rangle = |\psi\rangle, \qquad \forall \pi \in \mathfrak{S}_n.$$

Proof.

Define $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle$ with $|\Phi\rangle = \left(\sum_i |i\rangle_{\mathcal{K}}|i\rangle_{\mathcal{H}}\right)^{\otimes n}$

- $\sqrt{\rho}$ and $|\Phi\rangle$ are permutation-invariant $\implies$ $|\psi\rangle$ is permutation-invariant
- $\mathrm{tr}_{\mathcal{K}^{\otimes n}}\left((\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle\langle\Phi|(\mathbb{1} \otimes \sqrt{\rho})^\dagger\right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\pi|\psi\rangle = |\psi\rangle, \quad \forall \pi \in \mathfrak{S}_n$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathrm{Sym}^n(\mathcal{H})$

Restriction to pure states (for permutation-invariance)

Lemma (Christandl, König, Mitchison, Renner, CMP 2007)

Let ρ be a permutation-invariant density matrix on $\mathcal{H}^{\otimes n}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{K}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ (with $\mathcal{K} \cong \mathcal{H}$) such that

$$\pi|\psi\rangle = |\psi\rangle, \qquad \forall \pi \in \mathfrak{S}_n.$$

Proof.

Define $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle$ with $|\Phi\rangle = \left(\sum_i |i\rangle_{\mathcal{K}}|i\rangle_{\mathcal{H}}\right)^{\otimes n}$

- $\sqrt{\rho}$ and $|\Phi\rangle$ are permutation-invariant $\implies$ $|\psi\rangle$ is permutation-invariant
- $\mathrm{tr}_{\mathcal{K}^{\otimes n}}\left((\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle\langle\Phi|(\mathbb{1} \otimes \sqrt{\rho})^\dagger\right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\pi|\psi\rangle = |\psi\rangle, \quad \forall \pi \in \mathfrak{S}_n$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathrm{Sym}^n(\mathcal{H})$

Restriction to pure states (for permutation-invariance)

Lemma (Christandl, König, Mitchison, Renner, CMP 2007)

Let ρ be a permutation-invariant density matrix on $\mathcal{H}^{\otimes n}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{K}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ (with $\mathcal{K} \cong \mathcal{H}$) such that

$$\pi|\psi\rangle = |\psi\rangle, \qquad \forall \pi \in \mathfrak{S}_n.$$

Proof.

Define $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle$ with $|\Phi\rangle = \left(\sum_i |i\rangle_{\mathcal{K}}|i\rangle_{\mathcal{H}}\right)^{\otimes n}$

- $\sqrt{\rho}$ and $|\Phi\rangle$ are permutation-invariant $\implies$ $|\psi\rangle$ is permutation-invariant
- $\mathrm{tr}_{\mathcal{K}^{\otimes n}}\left((\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle\langle\Phi|(\mathbb{1} \otimes \sqrt{\rho})^\dagger\right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\pi|\psi\rangle = |\psi\rangle, \quad \forall \pi \in \mathfrak{S}_n$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathrm{Sym}^n(\mathcal{H})$

Restriction to pure states (for permutation-invariance)

Lemma (Christandl, König, Mitchison, Renner, CMP 2007)

Let ρ be a permutation-invariant density matrix on $\mathcal{H}^{\otimes n}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{K}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ (with $\mathcal{K} \cong \mathcal{H}$) such that

$$\pi|\psi\rangle = |\psi\rangle, \qquad \forall \pi \in \mathfrak{S}_n.$$

Proof.

Define $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle$ with $|\Phi\rangle = \left(\sum_i |i\rangle_{\mathcal{K}}|i\rangle_{\mathcal{H}}\right)^{\otimes n}$

- $\sqrt{\rho}$ and $|\Phi\rangle$ are permutation-invariant $\implies$ $|\psi\rangle$ is permutation-invariant
- $\mathrm{tr}_{\mathcal{K}^{\otimes n}}\left((\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle\langle\Phi|(\mathbb{1} \otimes \sqrt{\rho})^\dagger\right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\pi|\psi\rangle = |\psi\rangle, \quad \forall \pi \in \mathfrak{S}_n$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathrm{Sym}^n(\mathcal{H})$

Restriction to pure states (for permutation-invariance)

Lemma (Christandl, König, Mitchison, Renner, CMP 2007)

Let ρ be a permutation-invariant density matrix on $\mathcal{H}^{\otimes n}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{K}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ (with $\mathcal{K} \cong \mathcal{H}$) such that

$$\pi|\psi\rangle = |\psi\rangle, \qquad \forall \pi \in \mathfrak{S}_n.$$

Proof.

Define $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle$ with $|\Phi\rangle = \left(\sum_i |i\rangle_{\mathcal{K}}|i\rangle_{\mathcal{H}}\right)^{\otimes n}$

- $\sqrt{\rho}$ and $|\Phi\rangle$ are permutation-invariant $\implies$ $|\psi\rangle$ is permutation-invariant
- $\mathrm{tr}_{\mathcal{K}^{\otimes n}}\left((\mathbb{1} \otimes \sqrt{\rho})|\Phi\rangle\langle\Phi|(\mathbb{1} \otimes \sqrt{\rho})^\dagger\right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\pi|\psi\rangle = |\psi\rangle, \quad \forall \pi \in \mathfrak{S}_n$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathrm{Sym}^n(\mathcal{H})$

Restriction to pure states (for unitarily-invariance)

Lemma (arXiv:1612.05080)

Let ρ be a *unitarily-invariant* density matrix on $\mathcal{F}_{\mathrm{p,q,n}}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{F}_{\mathrm{p+q,q+p,n}}$ such that

$$\mathrm{W_u} \otimes \mathrm{W_{\bar{u}}} |\psi\rangle = |\psi\rangle, \qquad \forall \mathrm{u} \in \mathcal{U}(\mathrm{n}).$$

Proof.

Similar argument with $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\mathrm{MES}\rangle$ with $|\mathrm{MES}\rangle =$ "maximally entangled state" between two copies of $\mathcal{F}_{\mathrm{p,q,n}} \cong \mathcal{F}_{\mathrm{q,p,n}}$ (doesn't really exist ...)

- $\sqrt{\rho}$ and $|\mathrm{MES}\rangle$ are unitarily-invariant $\implies$ $|\psi\rangle$ is unitarily-invariant
- $\mathrm{tr}_{\mathcal{F}_{\mathrm{q,p,n}}} \left((\mathbb{1} \otimes \sqrt{\rho})|\mathrm{MES}\rangle\langle\mathrm{MES}|(\mathbb{1} \otimes \sqrt{\rho})^\dagger \right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\mathrm{W_u}|\psi\rangle = |\psi\rangle, \quad \forall \mathrm{u} \in \mathcal{U}_\mathrm{n}$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathcal{F}^{\mathcal{U}(\mathrm{n})}_{\mathrm{p+q,p+q,n}}$

Restriction to pure states (for unitarily-invariance)

Lemma (arXiv:1612.05080)

Let ρ be a *unitarily-invariant* density matrix on $\mathcal{F}_{\mathrm{p,q,n}}$. Then there exists a purification $|\psi\rangle$ of ρ in $\mathcal{F}_{\mathrm{p+q,q+p,n}}$ such that

$$\mathrm{W_u} \otimes \mathrm{W_{\bar{u}}} |\psi\rangle = |\psi\rangle, \qquad \forall \mathrm{u} \in \mathcal{U}(\mathrm{n}).$$

Proof.

Similar argument with $|\psi\rangle = (\mathbb{1} \otimes \sqrt{\rho})|\mathrm{MES}\rangle$ with $|\mathrm{MES}\rangle =$ "maximally entangled state" between two copies of $\mathcal{F}_{\mathrm{p,q,n}} \cong \mathcal{F}_{\mathrm{q,p,n}}$ (doesn't really exist ...)

- $\sqrt{\rho}$ and $|\mathrm{MES}\rangle$ are unitarily-invariant $\implies$ $|\psi\rangle$ is unitarily-invariant
- $\mathrm{tr}_{\mathcal{F}_{\mathrm{q,p,n}}} \left((\mathbb{1} \otimes \sqrt{\rho})|\mathrm{MES}\rangle\langle\mathrm{MES}|(\mathbb{1} \otimes \sqrt{\rho})^\dagger \right) = \sqrt{\rho}\mathbb{1}\sqrt{\rho}^\dagger = \rho$

□

$\implies$ it is sufficient to consider pure states $|\psi\rangle$ such that $\mathrm{W_u}|\psi\rangle = |\psi\rangle, \quad \forall \mathrm{u} \in \mathcal{U}_\mathrm{n}$

i.e. $|\psi\rangle$ belongs to the *symmetric subspace* $\mathcal{F}^{\mathcal{U}(\mathrm{n})}_{\mathrm{p+q,p+q,n}}$

Symmetric subspaces

Permutation invariance

$$\mathrm{Sym}^{n}(\mathbb{C}^{d}) := \left\{ |\psi\rangle \in (\mathbb{C}^{d})^{\otimes n} \ : \ \pi|\psi\rangle = |\psi\rangle, \forall \pi \in \mathrm{S}_{n} \right\}$$

Properties:

- $\mathrm{Sym}^{n}(\mathbb{C}^{d}) = \mathrm{Span}\left\{ |\phi\rangle^{\otimes n} \quad : \quad |\phi\rangle \in \mathbb{C}^{d} \right\}$
- $|\phi\rangle^{\otimes n}$: $\mathrm{SU}(d)$ coherent states
- $\dim\left(\mathrm{Sym}^{n}(\mathbb{C}^{d})\right) = \mathrm{O}(n^{d})$ (for $d \ll n$)

Unitarily invariance

$$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)} := \{ |\psi\rangle \in \mathcal{F}_{p,q,n} \ : \ \mathrm{W}_{u}|\psi\rangle = |\psi\rangle, \forall u \in \mathfrak{S}_{n} \}$$

Theorem (arXiv:1612.05080)

$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)}$ is spanned by $\mathrm{SU}(p,q)$ *generalized coherent states*.

Symmetric subspaces

Permutation invariance

$$\mathrm{Sym}^{n}(\mathbb{C}^{d}) := \left\{ |\psi\rangle \in (\mathbb{C}^{d})^{\otimes n} \ : \ \pi|\psi\rangle = |\psi\rangle, \forall \pi \in \mathrm{S}_{n} \right\}$$

Properties:

- $\mathrm{Sym}^{n}(\mathbb{C}^{d}) = \mathrm{Span}\left\{ |\phi\rangle^{\otimes n} \quad : \quad |\phi\rangle \in \mathbb{C}^{d} \right\}$
- $|\phi\rangle^{\otimes n}$: $\mathrm{SU}(d)$ coherent states
- $\dim\left(\mathrm{Sym}^{n}(\mathbb{C}^{d})\right) = \mathrm{O}(n^{d})$ (for $d \ll n$)

Unitarily invariance

$$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)} := \{ |\psi\rangle \in \mathcal{F}_{p,q,n} \ : \ \mathrm{W}_{u}|\psi\rangle = |\psi\rangle, \forall u \in \mathfrak{S}_{n} \}$$

Theorem (arXiv:1612.05080)

$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)}$ is spanned by $\mathrm{SU}(p,q)$ *generalized coherent states*.

Symmetric subspaces

Permutation invariance

$$\mathrm{Sym}^{n}(\mathbb{C}^{d}) := \left\{ |\psi\rangle \in (\mathbb{C}^{d})^{\otimes n} \,:\, \pi|\psi\rangle = |\psi\rangle, \forall \pi \in \mathrm{S}_{n} \right\}$$

Properties:

- $\mathrm{Sym}^{n}(\mathbb{C}^{d}) = \mathrm{Span}\left\{ |\phi\rangle^{\otimes n} \quad : \quad |\phi\rangle \in \mathbb{C}^{d} \right\}$
- $|\phi\rangle^{\otimes n}$: $\mathrm{SU}(d)$ coherent states
- $\dim\left(\mathrm{Sym}^{n}(\mathbb{C}^{d})\right) = \mathrm{O}(n^{d})$ (for $d \ll n$)

Unitarily invariance

$$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)} := \{ |\psi\rangle \in \mathcal{F}_{p,q,n} \,:\, \mathrm{W}_{u}|\psi\rangle = |\psi\rangle, \forall u \in \mathfrak{S}_{n} \}$$

Theorem (arXiv:1612.05080)

$\mathcal{F}_{p,q,n}^{\mathcal{U}(n)}$ is spanned by $\mathrm{SU}(p,q)$ *generalized coherent states*.

Generalized coherent states

The states $|\phi\rangle^{\otimes n}$ with $|\phi\rangle \in \mathbb{C}^d$ are an example of generalized CS, associated to $\mathrm{SU}(d)$.

An example of Perelomov generalized CS construction for $\mathcal{H}^{\otimes n} \cong (\mathbb{C}^d)^{\otimes n}$

- a *Lie group* G, e.g $\mathrm{SU}(d)$, and a representation $(g \mapsto T_g)$ of G on $\mathcal{H}^{\otimes n}$

$$u \in \mathrm{SU}(d) \quad \mapsto u^{\otimes n} \quad \text{on} \quad (\mathbb{C}^d)^{\otimes n}$$

- a distinguished *vector* $\psi_0 \in \mathcal{H}^{\otimes n}$, e.g. $|0\rangle^{\otimes n}$
- generalized *G-coherent states*: $\{|\psi_g\rangle = T_g|\psi_0\rangle, g \in G\}$, e.g. $|\phi_u\rangle^{\otimes n} = u^{\otimes n}|0\rangle^{\otimes n}$
- CS labeled by elements of G/H, e.g. $\phi_u \in \mathrm{SU}(d)/\mathrm{SU}(d-1) \cong \mathcal{S}_1(\mathbb{C}^d)$
- with H: stationary subgroup $\left\{g \in G \,:\, T_g|\psi_0\rangle = e^{i\theta}|\psi_0\rangle\right\}$

$\mathrm{SU}(p,q)$ *coherent states*

The quadratic form $Z_{i,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$ is invariant under $X \to uX$, $Y \to \overline{u}Y$:

$$Z_{i,j} \to \sum_{k=1}^{n}\sum_{s=1}^{n}\sum_{t=1}^{n} u_{k,s} x_{s,i} \overline{u}_{k,t} y_{t,j} = \sum_{s=1}^{n}\sum_{t=1}^{n} (u^\dagger u)_{t,s} x_{s,i} y_{t,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$$

$\implies \phi_{\Lambda,n} := \det(1-\Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{p\times q}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$

Perelomov's construction (1972) applied to $G = \mathrm{SU}(p,q)$ *(noncompact group)*

$$\mathrm{SU}(p,q) := \left\{ A \in \mathrm{M}_{p+q}(\mathbb{C}) \,:\, A \mathbb{1}_{p,q} A^\dagger = \mathbb{1}_{p,q}, \quad \det A = 1 \right\} \quad \text{with} \quad \mathbb{1}_{p,q} = \begin{pmatrix} \mathbb{1}_p & 0 \\ 0 & -\mathbb{1}_q \end{pmatrix}$$

- $\Lambda \to (A^T \Lambda + C^T)(B^T \Lambda + D^T)^{-1}$ for $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SU}(p,q)$
- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,n}$ associated with $\Lambda \in G/H$
- $\phi_{\Lambda,n} = \phi_{\Lambda,1}^{\otimes n}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(\mathrm{p},\mathrm{q})$ *coherent states*

The quadratic form $\mathrm{Z}_{\mathrm{i,j}} = \sum_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{x}_{\mathrm{k,i}}\mathrm{y}_{\mathrm{k,j}}$ is invariant under $\mathrm{X} \to \mathrm{uX}, \mathrm{Y} \to \overline{\mathrm{u}}\mathrm{Y}$:

$$\mathrm{Z}_{\mathrm{i,j}} \to \sum_{\mathrm{k}=1}^{\mathrm{n}} \sum_{\mathrm{s}=1}^{\mathrm{n}} \sum_{\mathrm{t}=1}^{\mathrm{n}} \mathrm{u}_{\mathrm{k,s}}\mathrm{x}_{\mathrm{s,i}}\overline{\mathrm{u}}_{\mathrm{k,t}}\mathrm{y}_{\mathrm{t,j}} = \sum_{\mathrm{s}=1}^{\mathrm{n}} \sum_{\mathrm{t}=1}^{\mathrm{n}} (\mathrm{u}^\dagger\mathrm{u})_{\mathrm{t,s}}\mathrm{x}_{\mathrm{s,i}}\mathrm{y}_{\mathrm{t,j}} = \sum_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{x}_{\mathrm{k,i}}\mathrm{y}_{\mathrm{k,j}}$$

$\implies \phi_{\Lambda,\mathrm{n}} := \det(1 - \Lambda\Lambda^\dagger)^{\mathrm{n}/2} \exp(\lambda_{11}\mathrm{Z}_{11} + \cdots + \lambda_{\mathrm{p,q}}\mathrm{Z}_{\mathrm{pq}})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{\mathrm{p}\times\mathrm{q}}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_{\mathrm{p}}$

Perelomov's construction (1972) applied to $\mathrm{G} = \mathrm{SU}(\mathrm{p},\mathrm{q})$ *(noncompact group)*

$$\mathrm{SU}(\mathrm{p},\mathrm{q}) := \left\{ \mathrm{A} \in \mathrm{M}_{\mathrm{p+q}}(\mathbb{C}) \,:\, \mathrm{A}\mathbb{1}_{\mathrm{p,q}}\mathrm{A}^\dagger = \mathbb{1}_{\mathrm{p,q}}, \quad \det \mathrm{A} = 1 \right\} \quad \text{with} \quad \mathbb{1}_{\mathrm{p,q}} = \begin{pmatrix} \mathbb{1}_{\mathrm{p}} & 0 \\ 0 & -\mathbb{1}_{\mathrm{q}} \end{pmatrix}$$

- $\Lambda \to (\mathrm{A}^{\mathrm{T}}\Lambda + \mathrm{C}^{\mathrm{T}})(\mathrm{B}^{\mathrm{T}}\Lambda + \mathrm{D}^{\mathrm{T}})^{-1}$ for $\left(\begin{smallmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{smallmatrix}\right) \in \mathrm{SU}(\mathrm{p},\mathrm{q})$
- stationary subgroup: $\mathrm{H} = \mathrm{SU}(\mathrm{p}) \times \mathrm{SU}(\mathrm{q}) \times \mathrm{U}(1)$
- factor space $\mathrm{G/H}$: $\mathrm{p}\times\mathrm{q}$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_{\mathrm{p}}$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,\mathrm{n}}$ associated with $\Lambda \in \mathrm{G/H}$
- $\phi_{\Lambda,\mathrm{n}} = \phi_{\Lambda,1}^{\otimes \mathrm{n}}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(p,q)$ *coherent states*

The quadratic form $Z_{i,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$ is invariant under $X \to uX$, $Y \to \overline{u}Y$:

$$Z_{i,j} \to \sum_{k=1}^{n}\sum_{s=1}^{n}\sum_{t=1}^{n} u_{k,s} x_{s,i} \overline{u}_{k,t} y_{t,j} = \sum_{s=1}^{n}\sum_{t=1}^{n} (u^\dagger u)_{t,s} x_{s,i} y_{t,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$$

$\implies \phi_{\Lambda,n} := \det(1 - \Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{p\times q}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$

Perelomov's construction (1972) applied to $G = \mathrm{SU}(p,q)$ *(noncompact group)*

$$\mathrm{SU}(p,q) := \left\{ A \in \mathrm{M}_{p+q}(\mathbb{C}) \,:\, A \mathbb{1}_{p,q} A^\dagger = \mathbb{1}_{p,q}, \quad \det A = 1 \right\} \quad \text{with} \quad \mathbb{1}_{p,q} = \begin{pmatrix} \mathbb{1}_p & 0 \\ 0 & -\mathbb{1}_q \end{pmatrix}$$

- $\Lambda \to (A^T \Lambda + C^T)(B^T \Lambda + D^T)^{-1}$ for $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SU}(p,q)$
- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,n}$ associated with $\Lambda \in G/H$
- $\phi_{\Lambda,n} = \phi_{\Lambda,1}^{\otimes n}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(p,q)$ *coherent states*

The quadratic form $Z_{i,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$ is invariant under $X \to uX$, $Y \to \overline{u}Y$:

$$Z_{i,j} \to \sum_{k=1}^{n}\sum_{s=1}^{n}\sum_{t=1}^{n} u_{k,s} x_{s,i} \overline{u}_{k,t} y_{t,j} = \sum_{s=1}^{n}\sum_{t=1}^{n} (u^\dagger u)_{t,s} x_{s,i} y_{t,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$$

$\implies \phi_{\Lambda,n} := \det(1 - \Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{p\times q}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$

Perelomov's construction (1972) applied to $G = \mathrm{SU}(p,q)$ (noncompact group)

$$\mathrm{SU}(p,q) := \left\{ A \in \mathrm{M}_{p+q}(\mathbb{C}) \,:\, A \mathbb{1}_{p,q} A^\dagger = \mathbb{1}_{p,q}, \quad \det A = 1 \right\} \quad \text{with} \quad \mathbb{1}_{p,q} = \begin{pmatrix} \mathbb{1}_p & 0 \\ 0 & -\mathbb{1}_q \end{pmatrix}$$

- $\Lambda \to (A^T\Lambda + C^T)(B^T\Lambda + D^T)^{-1}$ for $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SU}(p,q)$
- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,n}$ associated with $\Lambda \in G/H$
- $\phi_{\Lambda,n} = \phi_{\Lambda,1}^{\otimes n}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(p,q)$ *coherent states*

The quadratic form $Z_{i,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$ is invariant under $X \to uX$, $Y \to \overline{u}Y$:

$$Z_{i,j} \to \sum_{k=1}^{n}\sum_{s=1}^{n}\sum_{t=1}^{n} u_{k,s} x_{s,i} \overline{u}_{k,t} y_{t,j} = \sum_{s=1}^{n}\sum_{t=1}^{n} (u^\dagger u)_{t,s} x_{s,i} y_{t,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$$

$\implies \phi_{\Lambda,n} := \det(1 - \Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{p\times q}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$

Perelomov's construction (1972) applied to $G = \mathrm{SU}(p,q)$ *(noncompact group)*

$$\mathrm{SU}(p,q) := \left\{ A \in \mathrm{M}_{p+q}(\mathbb{C}) \,:\, A \mathbb{1}_{p,q} A^\dagger = \mathbb{1}_{p,q}, \quad \det A = 1 \right\} \quad \text{with} \quad \mathbb{1}_{p,q} = \begin{pmatrix} \mathbb{1}_p & 0 \\ 0 & -\mathbb{1}_q \end{pmatrix}$$

- $\Lambda \to (A^T\Lambda + C^T)(B^T\Lambda + D^T)^{-1}$ for $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SU}(p,q)$
- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,n}$ associated with $\Lambda \in G/H$
- $\phi_{\Lambda,n} = \phi_{\Lambda,1}^{\otimes n}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(p,q)$ *coherent states*

The quadratic form $Z_{i,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$ is invariant under $X \to uX$, $Y \to \overline{u}Y$:

$$Z_{i,j} \to \sum_{k=1}^{n}\sum_{s=1}^{n}\sum_{t=1}^{n} u_{k,s} x_{s,i} \overline{u}_{k,t} y_{t,j} = \sum_{s=1}^{n}\sum_{t=1}^{n} (u^\dagger u)_{t,s} x_{s,i} y_{t,j} = \sum_{k=1}^{n} x_{k,i} y_{k,j}$$

$\implies \phi_{\Lambda,n} := \det(1-\Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{p\times q}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$

Perelomov's construction (1972) applied to $G = \mathrm{SU}(p,q)$ *(noncompact group)*

$$\mathrm{SU}(p,q) := \left\{ A \in \mathrm{M}_{p+q}(\mathbb{C}) \,:\, A \mathbb{1}_{p,q} A^\dagger = \mathbb{1}_{p,q}, \quad \det A = 1 \right\} \quad \text{with} \quad \mathbb{1}_{p,q} = \begin{pmatrix} \mathbb{1}_p & 0 \\ 0 & -\mathbb{1}_q \end{pmatrix}$$

- $\Lambda \to (A^T\Lambda + C^T)(B^T\Lambda + D^T)^{-1}$ for $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SU}(p,q)$
- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,n}$ associated with $\Lambda \in G/H$
- $\phi_{\Lambda,n} = \phi_{\Lambda,1}^{\otimes n}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

$\mathrm{SU}(\mathrm{p},\mathrm{q})$ *coherent states*

The quadratic form $\mathrm{Z}_{\mathrm{i,j}} = \sum_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{x}_{\mathrm{k,i}}\mathrm{y}_{\mathrm{k,j}}$ is invariant under $\mathrm{X} \to \mathrm{uX}, \mathrm{Y} \to \overline{\mathrm{u}}\mathrm{Y}$:

$$\mathrm{Z}_{\mathrm{i,j}} \to \sum_{\mathrm{k}=1}^{\mathrm{n}} \sum_{\mathrm{s}=1}^{\mathrm{n}} \sum_{\mathrm{t}=1}^{\mathrm{n}} \mathrm{u}_{\mathrm{k,s}}\mathrm{x}_{\mathrm{s,i}}\overline{\mathrm{u}}_{\mathrm{k,t}}\mathrm{y}_{\mathrm{t,j}} = \sum_{\mathrm{s}=1}^{\mathrm{n}} \sum_{\mathrm{t}=1}^{\mathrm{n}} (\mathrm{u}^\dagger\mathrm{u})_{\mathrm{t,s}}\mathrm{x}_{\mathrm{s,i}}\mathrm{y}_{\mathrm{t,j}} = \sum_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{x}_{\mathrm{k,i}}\mathrm{y}_{\mathrm{k,j}}$$

$\implies \phi_{\Lambda,\mathrm{n}} := \det(1 - \Lambda\Lambda^\dagger)^{\mathrm{n}/2} \exp(\lambda_{11}\mathrm{Z}_{11} + \cdots + \lambda_{\mathrm{p,q}}\mathrm{Z}_{\mathrm{pq}})$ is unitarily-invariant for $\Lambda \in \mathbb{C}^{\mathrm{p}\times\mathrm{q}}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_{\mathrm{p}}$

Perelomov's construction (1972) applied to $\mathrm{G} = \mathrm{SU}(\mathrm{p},\mathrm{q})$ *(noncompact group)*

$$\mathrm{SU}(\mathrm{p},\mathrm{q}) := \left\{ \mathrm{A} \in \mathrm{M}_{\mathrm{p+q}}(\mathbb{C}) \,:\, \mathrm{A}\mathbb{1}_{\mathrm{p,q}}\mathrm{A}^\dagger = \mathbb{1}_{\mathrm{p,q}}, \quad \det \mathrm{A} = 1 \right\} \quad \text{with} \quad \mathbb{1}_{\mathrm{p,q}} = \begin{pmatrix} \mathbb{1}_{\mathrm{p}} & 0 \\ 0 & -\mathbb{1}_{\mathrm{q}} \end{pmatrix}$$

- $\Lambda \to (\mathrm{A}^{\mathrm{T}}\Lambda + \mathrm{C}^{\mathrm{T}})(\mathrm{B}^{\mathrm{T}}\Lambda + \mathrm{D}^{\mathrm{T}})^{-1}$ for $\left(\begin{smallmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{smallmatrix}\right) \in \mathrm{SU}(\mathrm{p},\mathrm{q})$
- stationary subgroup: $\mathrm{H} = \mathrm{SU}(\mathrm{p}) \times \mathrm{SU}(\mathrm{q}) \times \mathrm{U}(1)$
- factor space $\mathrm{G/H}$: $\mathrm{p}\times\mathrm{q}$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_{\mathrm{p}}$ (spectral norm < 1)
- generalized coherent state $\phi_{\Lambda,\mathrm{n}}$ associated with $\Lambda \in \mathrm{G/H}$
- $\phi_{\Lambda,\mathrm{n}} = \phi_{\Lambda,1}^{\otimes \mathrm{n}}$: *i.i.d. Gaussian state* (exp. of a quadratic form in the creation operators)

Resolution of the identity

$$\begin{aligned}\phi_{\Lambda,\mathrm{n}} \leftrightarrow |\Lambda,\mathrm{n}\rangle &= \det(1-\Lambda\Lambda^\dagger)^{\mathrm{n}/2}\exp(\lambda_{11}\mathrm{Z}_{11}+\cdots+\lambda_{\mathrm{p,q}}\mathrm{Z}_{\mathrm{pq}})|0\rangle \\ &= |\Lambda,1\rangle^{\otimes \mathrm{n}}\end{aligned}$$

with $\mathrm{Z}_{\mathrm{ij}} := \sum_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{ki}}^\dagger \mathrm{b}_{\mathrm{kj}}^\dagger$

Defining property of coherent states

For $\mathrm{n} \geq \mathrm{p}+\mathrm{q}$,

$$\int_{\mathcal{D}} \left(|\Lambda,1\rangle\langle\Lambda,1|\right)^{\otimes \mathrm{n}} \mathrm{d}\mu_{\mathrm{n}}(\Lambda) = \mathbb{1}_{\mathrm{F}_{\mathrm{p,q,n}}^{\mathrm{U(n)}}},$$

with the invariant measure on $\mathcal{D} = \{\mathbb{C}^{\mathrm{p}\times\mathrm{q}} : \Lambda\Lambda^\dagger < \mathbb{1}_{\mathrm{p}}\}$

$$\mathrm{d}\mu_{\mathrm{n}}(\Lambda) = \mathrm{C}_{\mathrm{n}}[\det(\mathbb{1}_{\mathrm{p}}-\Lambda\Lambda^\dagger)]^{-(\mathrm{p}+\mathrm{q})} \prod_{\mathrm{i,j}}^{\mathrm{p}} \mathrm{d}\Lambda_{\mathrm{i,j}}$$

and

$$\mathrm{C}_{\mathrm{n}} := \frac{1}{\pi^{\mathrm{pq}}} \prod_{\mathrm{i}=0}^{\mathrm{q}-1} \frac{(\mathrm{n}-\mathrm{q}+\mathrm{i})!}{(\mathrm{n}-\mathrm{p}-\mathrm{q}+\mathrm{i})!}$$

Resolution of the identity

$$\begin{aligned}\phi_{\Lambda,n} \leftrightarrow |\Lambda, n\rangle &= \det(1-\Lambda\Lambda^\dagger)^{n/2} \exp(\lambda_{11} Z_{11} + \cdots + \lambda_{p,q} Z_{pq})|0\rangle \\ &= |\Lambda, 1\rangle^{\otimes n}\end{aligned}$$

with $Z_{ij} := \sum_{k=1}^{n} a_{ki}^\dagger b_{kj}^\dagger$

Defining property of coherent states

For $n \geq p+q$,

$$\int_{\mathcal{D}} \left(|\Lambda, 1\rangle\langle\Lambda, 1|\right)^{\otimes n} d\mu_n(\Lambda) = \mathbb{1}_{F_{p,q,n}^{U(n)}},$$

with the invariant measure on $\mathcal{D} = \{\mathbb{C}^{p\times q} : \Lambda\Lambda^\dagger < \mathbb{1}_p\}$

$$d\mu_n(\Lambda) = C_n[\det(\mathbb{1}_p - \Lambda\Lambda^\dagger)]^{-(p+q)} \prod_{i,j}^{p} d\Lambda_{i,j}$$

and

$$C_n := \frac{1}{\pi^{pq}} \prod_{i=0}^{q-1} \frac{(n-q+i)!}{(n-p-q+i)!}$$

de Finetti Theorem (arXiv:1612.05080)

Let n be an arbitrary integer and $k \geq p + q$. Let $\rho = |\psi\rangle\langle\psi|$ be a symmetric (pure) state in $\mathcal{F}^{U(n+k)}_{p,q,n+k}$. Then the state obtained after tracing out over $k(p+q)$ modes can be well approximated by a mixture of generalized coherent states:

$$\|\mathrm{tr}_k(\rho) - C_k \int \nu(\Lambda)(|\Lambda, 1\rangle\langle\Lambda, 1|)^{\otimes n} d\mu_{p,q}(\Lambda)\|_{tr} \leq \frac{3npq}{2(n+k-p-q)}.$$

special case of a result by König, Mitchison (JMP 2009)

proof adapted from Christandl, König, Mitchison, Renner (CMP 2007):

- relies on resolution of the identity and

$$1 - \frac{C_k}{C_{n+k}} \leq \frac{npq}{n+k-p-q}$$

de Finetti Theorem (arXiv:1612.05080)

Let n be an arbitrary integer and $k \geq p+q$. Let $\rho = |\psi\rangle\langle\psi|$ be a symmetric (pure) state in $\mathcal{F}^{U(n+k)}_{p,q,n+k}$. Then the state obtained after tracing out over $k(p+q)$ modes can be well approximated by a mixture of generalized coherent states:

$$\|\mathrm{tr}_k(\rho) - C_k \int \nu(\Lambda)(|\Lambda,1\rangle\langle\Lambda,1|)^{\otimes n} d\mu_{p,q}(\Lambda)\|_{tr} \leq \frac{3npq}{2(n+k-p-q)}.$$

special case of a result by König, Mitchison (JMP 2009)

proof adapted from Christandl, König, Mitchison, Renner (CMP 2007):

- relies on resolution of the identity and

$$1 - \frac{C_k}{C_{n+k}} \leq \frac{npq}{n+k-p-q}$$

Outline of the talk

- de Finetti theorems: classical and quantum
- Representation of the unitary group on Fock spaces
- Which density matrices are unitarily-invariant?
- Truncation of Haar random unitaries

Back to the initial problem of truncation of Haar random unitaries

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathsf{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

idea:

- find a quantum state and a measurement that yields a distribution arbitrarily close to $\mathrm{Haar}(\mathcal{U}(n))$
- looking at the k marginal yields $\mathcal{H}_{k,k}$
- use Gaussian de Finetti to argue that it is close to measuring a Gaussian state

Back to the initial problem of truncation of Haar random unitaries

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathrm{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

idea:

- find a quantum state and a measurement that yields a distribution arbitrarily close to $\mathrm{Haar}(\mathcal{U}(n))$
- looking at the k marginal yields $\mathcal{H}_{k,k}$
- use Gaussian de Finetti to argue that it is close to measuring a Gaussian state

Back to the initial problem of truncation of Haar random unitaries

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathsf{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

idea:

- find a quantum state and a measurement that yields a distribution arbitrarily close to $\mathsf{Haar}(\mathcal{U}(n))$
- looking at the k marginal yields $\mathcal{H}_{k,k}$
- use Gaussian de Finetti to argue that it is close to measuring a Gaussian state

Back to the initial problem of truncation of Haar random unitaries

Example: truncation of random Haar matrices

Let $\mathcal{H}_{k,k}$ be the distribution over $k \times k$ complex matrices obtained by drawing a random unitary $U \sim \mathsf{Haar}(\mathcal{U}(n))$ and outputting $\sqrt{n}U_{k,k}$ where $U_{k,k}$ is the $k \times k$ upper-left submatrix of U.

Let $\mathcal{G}^{k\times k}$ be the distribution over $k \times k$ complex matrices where each entry $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

- this work (with a quantum approach):

$$\|\mathcal{H}_{k,k} - \mathcal{G}^{k\times k}\|_{TV} \leq \frac{2k^3}{n-k}$$

idea:

- find a quantum state and a measurement that yields a distribution arbitrarily close to $\mathsf{Haar}(\mathcal{U}(n))$
- looking at the k marginal yields $\mathcal{H}_{k,k}$
- use Gaussian de Finetti to argue that it is close to measuring a Gaussian state

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k\times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k\times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Truncation of Haar random unitaries

- ρ_α^1 is the kn-mode pure state $\exp(\alpha x_{1,1} + \cdots + \alpha x_{k,k})$, a product of standard coherent states: measuring with heterodyne detection and renormalizing yields $\approx (e_1, \ldots, e_k)$
- $\rho_\alpha^2 = \int V_u \rho_\alpha^1 V_u^\dagger du$ (twirling $\implies$ unitarily invariant)
- trace out k rows, yields ρ_α^3 and measure with heterodyne detection (Husimi function):

$$\implies \text{approximates } \mathcal{H}_{k,k}$$

- purification of ρ_α^2 in $\mathcal{F}_{k,k,n}^{U(n)}$ (2nk modes)

$$\implies \text{Gaussian de Finetti applies with } p = q = k$$

proof skteck

- taking $\alpha \to \infty$ and renormalizing yields $\mathcal{H}_{k,k}$
- Gaussian de Finetti: ρ_α^3 is close to a mixture of Gaussian states
- when $\alpha \to \infty$, the mixture converges to a Dirac distribution
- the Husimi function of the Gaussian state tends to $\mathcal{G}^{k \times k}$

Conclusion

- de Finetti theorems are ubiquitous for studying large permutation-invariant multipartite systems / protocols
- but they fail to address infinite-dimensional systems (continuous variables)
- for some problems, a stronger invariance under U(n) is satisfied
  $\Longrightarrow$ ex: continuous-variable quantum cryptography
- open question: other applications?

Dualities

- Schur-Weyl duality:

$$\mathrm{SU(d)} \quad \leftrightarrow \quad \mathrm{S_n} \quad \text{on} \quad (\mathbb{C}^d)^{\otimes n} = \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$$

- this work:

$$\mathrm{SU(p,q)} \quad \leftrightarrow \quad \mathrm{U(n)} \quad \text{on} \quad \mathrm{F_{p,q,n}} = \mathrm{F_{p,q,1}} \otimes \cdots \otimes \mathrm{F_{p,q,1}}$$

thanks!

Conclusion

- de Finetti theorems are ubiquitous for studying large permutation-invariant multipartite systems / protocols
- but they fail to address infinite-dimensional systems (continuous variables)
- for some problems, a stronger invariance under $\mathrm{U}(n)$ is satisfied
  $\Longrightarrow$ ex: continuous-variable quantum cryptography
- open question: other applications?

Dualities

- Schur-Weyl duality:

$$\mathrm{SU}(d) \quad \leftrightarrow \quad \mathrm{S}_n \quad \text{on} \quad (\mathbb{C}^d)^{\otimes n} = \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$$

- this work:

$$\mathrm{SU}(p,q) \quad \leftrightarrow \quad \mathrm{U}(n) \quad \text{on} \quad \mathrm{F}_{p,q,n} = \mathrm{F}_{p,q,1} \otimes \cdots \otimes \mathrm{F}_{p,q,1}$$

thanks!

Conclusion

- de Finetti theorems are ubiquitous for studying large permutation-invariant multipartite systems / protocols
- but they fail to address infinite-dimensional systems (continuous variables)
- for some problems, a stronger invariance under $\mathrm{U(n)}$ is satisfied
  $\Longrightarrow$ ex: continuous-variable quantum cryptography
- open question: other applications?

Dualities

- Schur-Weyl duality:

$$\mathrm{SU(d)} \quad \leftrightarrow \quad \mathrm{S_n} \quad \text{on} \quad (\mathbb{C}^{\mathrm{d}})^{\otimes \mathrm{n}} = \mathbb{C}^{\mathrm{d}} \otimes \cdots \otimes \mathbb{C}^{\mathrm{d}}$$

- this work:

$$\mathrm{SU(p,q)} \quad \leftrightarrow \quad \mathrm{U(n)} \quad \text{on} \quad \mathrm{F_{p,q,n}} = \mathrm{F_{p,q,1}} \otimes \cdots \otimes \mathrm{F_{p,q,1}}$$

thanks!