SU(p, q) *coherent states and Gaussian de Finetti theorems*

*arXiv:*1612.05080
*arXiv:*1701.03393

Anthony Leverrier

Inria Paris

QIP 2017

Motivation

Generalize de Finetti reductions to problems with continuous variables

- de Finetti: permutation (S_n) invariance in $\mathcal{H}^{\otimes n}$ $\Longrightarrow$ i.i.d. $|\phi\rangle^{\otimes n} \in \mathcal{H}^{\otimes n}$
- but only if the local dimension is small
- what about continuous-variable systems (Fock space)?
- This work: unitary $U(n)$ invariance $\Longrightarrow$ Gaussian i.i.d.
  - mathematical framework: arXiv:1612.05080 (special thanks to Matthias Christandl!)
  - application to QKD with continuous variables: arXiv:1701.03393

Motivation

Generalize de Finetti reductions to problems with continuous variables

- de Finetti: permutation (S_n) invariance in $\mathcal{H}^{\otimes n}$ $\Longrightarrow$ i.i.d. $|\phi\rangle^{\otimes n} \in \mathcal{H}^{\otimes n}$
- but only if the local dimension is small
- what about continuous-variable systems (Fock space)?
- This work: unitary $U(n)$ invariance $\Longrightarrow$ Gaussian i.i.d.
  - mathematical framework: arXiv:1612.05080 (special thanks to Matthias Christandl!)
  - application to QKD with continuous variables: arXiv:1701.03393

Outline of the talk

1. The (usual) symmetric subspace and de Finetti theorems
2. Application to quantum key distribution
3. The “unitary” symmetric subspace and $\mathrm{SU}(p,q)$ coherent states
4. Gaussian de Finetti theorems

Outline of the talk

1. The (usual) symmetric subspace and de Finetti theorems
2. Application to quantum key distribution
3. The "unitary" symmetric subspace and $\mathrm{SU}(p,q)$ coherent states
4. Gaussian de Finetti theorems

The symmetric subspace

Let $\mathcal{H} = \mathbb{C}^d$, the space $\mathcal{H}^{\otimes n} = (\mathbb{C}^d)^{\otimes n}$ of n qudits is exponentially large.

$\implies$ the permutation group S_n acts by permuting the factors

Definition

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

Main properties

- It is as small as it can be: spanned by $SU(d)$ coherent states

$$\mathsf{Sym}^n(\mathbb{C}^d) = \mathsf{Span}\left\{ |\phi\rangle^{\otimes n} \quad : \quad |\phi\rangle \in \mathbb{C}^d \right\}$$

- It has polynomial dimension: $\mathsf{dim} = O(n^d)$ ... if $d \ll n$
- Symmetric operators admit a purification in the symmetric subspace of $(\mathcal{H} \otimes \mathcal{H})^{\otimes n}$
  $\implies$ we can restrict our attention to pure states

SU(d) *coherent states*

The states $|\phi\rangle^{\otimes n}$ with $|\phi\rangle \in \mathbb{C}^d$ are an example of generalized CS, associated to 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 SU(d), and a representation $(g \mapsto T_g)$ of G on $\mathcal{H}^{\otimes n}$

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

- 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. $|\phi_u\rangle^{\otimes n} = u^{\otimes n}|0\rangle^{\otimes n}$
- H: stationary subgroup $\{g \in G : T_g|\psi_0\rangle = e^{i\theta}|\psi_0\rangle\}$
- the CS are labeled by elements of G/H, e.g. $\phi_u \in SU(d)/SU(d-1) \cong \mathcal{S}_1(\mathbb{C}^d)$

This work: SU(p, q) CS are a natural generalization for bosonic systems ($\mathcal{H}$ = Fock space)

de Finetti theorem (Caves, Fuchs, Schack, Christandl, König, Mitchison, Renner, Chiribella ...)

Theorem

Tracing out a few subsystems of a symmetric density operator $\rho = |\Psi\rangle\langle\Psi|$ on $\mathcal{H}^{\otimes(n+k)}$ gives an approximate mixture of CS:

$$\mathrm{tr}_{\mathcal{H}_{n+1},\dots,\mathcal{H}_{n+k}}(\rho) \approx_\varepsilon \int (|\phi\rangle\langle\phi|)^{\otimes n} \nu(\phi) d\phi \quad \text{with} \quad \varepsilon = O\left(\frac{dn}{n+k}\right)$$

Main property of CS: they resolve the identity on $\mathrm{Sym}^{n+k}(\mathbb{C}^d)$:

$$\frac{1}{\dim(\mathrm{Sym})} \int_{\mathcal{S}_1(\mathbb{C}^d)} (|\phi\rangle\langle\phi|)^{\otimes(n+k)} d\psi = \mathbb{1}_{\mathrm{Sym}}$$

intuition.

- $|\Psi\rangle = \int |\phi\rangle^{\otimes(n+k)} \lambda(\phi) d\phi$
- $\mathrm{tr}_{\mathcal{H}_{n+1},\dots,\mathcal{H}_{n+k}}(|\Psi\rangle\langle\Psi|) = \int (|\phi\rangle\langle\psi|)^{\otimes n} (\langle\psi|\phi\rangle)^k \lambda(\phi) d\phi \lambda(\psi) d\psi$
- $(\langle\phi|\psi\rangle)^k \to \delta_{\phi,\psi}$ for $k \to \infty$.

□

de Finetti reduction: Christandl, König, Renner (2009)

Consider two CPTP maps $\mathcal{E}, \mathcal{F} : \mathcal{H}^{\otimes n} \to \mathcal{H}'$.

Diamond norm: $\|\mathcal{E} - \mathcal{F}\|_\diamond$

- natural notion of distance between 2 CPTP maps, with an operational meaning:
  - quantifies the maximal probability of distinguishing $\mathcal{E}$ and $\mathcal{F}$
- not easy to compute

$$\|\mathcal{E} - \mathcal{F}\|_\diamond := \sup_{\|\rho\|_1 \leq 1} \|((\mathcal{E} - \mathcal{F})_{\mathcal{H}^{\otimes n}} \otimes \mathbb{1}_{\mathcal{K}})\rho_{\mathcal{H}^{\otimes n}\mathcal{K}}\|_1 \qquad (\text{with } \mathcal{K} \cong \mathcal{H}^{\otimes n})$$

de Finetti reduction

If Δ is permutation-invariant, then

$$\|\Delta\|_\diamond \leq n^{\mathrm{poly}(d)} \, \| \, (\Delta \otimes \mathbb{1})\tau_{\mathcal{H}^n\mathcal{R}} \, \|_1 \quad \text{with} \quad \tau_{\mathcal{H}^n} = \int \sigma_{\mathcal{H}}^{\otimes n} \mu(\sigma_{\mathcal{H}})$$

$\Longrightarrow$ only needs to consider a specific i.i.d. state (de Finetti state)

Summary about the symmetric subspace

- useful to analyze protocols, systems with permutation invariance
- useful ansatz: the SU(d) coherent states, i.i.d. states $|\phi\rangle^{\otimes n}$
- these states are "sufficient": they resolve the identity on Sym
  - de Finetti theorem: the partial trace of a symmetric state is approx. a mixture of CS
  - de Finetti reduction: computing $\|\Delta\|_\diamond$ for Δ symmetric can be done by considering CS inputs
- the approach breaks down for large d (ex: continuous variables)

Outline of the talk

QKD protocols

with qubits (ex: BB84)

- Alice and Bob share n 2-qubit states.
- They measure their systems with $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.
- They each get n classical outcomes $(\text{basis}, \text{bit})$
- Parameter estimation, error correction, privacy amplification
- They obtain 2 keys

with continuous variables

- Alice and Bob share n 2-mode states.
- They measure their systems with hererodyne detection $\{|\alpha\rangle \,:\, \alpha \in \mathbb{C}\}$.
- They each get n classical outcomes $\alpha_i \in \mathbb{C}$
- Parameter estimation, error correction, privacy amplification
- They obtain 2 keys

Security proof via a de Finetti reduction

QKD protocol: completely-positive trace-preserving map $\mathcal{E} : \mathcal{H}_{\mathrm{AB}}^{\otimes \mathrm{n}} \to \mathcal{S}_{\mathrm{A}}\mathcal{S}_{\mathrm{B}}\mathcal{C}$

- maps an arbitrary state ρ_{AB} as input to keys $\mathrm{S}_{\mathrm{A}}, \mathrm{S}_{\mathrm{B}}$

Security of $\mathcal{E}$

- compare $\mathcal{E}$ to an ideal protocol $\mathcal{F}$ that either outputs identical, secret keys or aborts
- $\mathcal{E}$ is ε-secure if $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon \quad \Longrightarrow$ needs to consider all possible input states

de Finetti reduction: Christandl, König, Renner (2009)

If $\mathcal{E}, \mathcal{F}$ are permutation-invariant, then

$$\|(\mathcal{E} - \mathcal{F})\|_\diamond \leq \mathrm{n}^{\mathrm{poly}(\mathrm{d})} \, \| \, ((\mathcal{E} - \mathcal{F}) \otimes \mathbb{1})\tau_{\mathcal{H}^{\mathrm{n}}\mathcal{R}} \, \|_1 \quad \text{with} \quad \tau_{\mathcal{H}^{\mathrm{n}}} = \int \sigma_{\mathcal{H}}^{\otimes \mathrm{n}} \mu(\sigma_{\mathcal{H}})$$

The term $\|((\mathcal{E} - \mathcal{F}) \otimes \mathbb{1})\tau_{\mathcal{H}^{\mathrm{n}}\mathcal{R}}\|_1$ can be bounded by proving that the protocol is secure against collective attacks: inputs restricted to $(\sigma_{\mathrm{AB}})^{\otimes \mathrm{n}}$.

Continuous-variable protocols

Alice and Bob are not exchanging finite-dimensional systems, but rather standard (Glauber) coherent states:

- appealing from an implementation viewpoint: coherent states are easy to prepare and measure with coherent detection (homodyne detection): no need for photon counters
- $\mathcal{H}$: infinite-dimensional Fock space $\implies d = \infty$
- previous results have error term scaling as $n^{\mathrm{poly}(d)}$
- possible approach: truncate the Hilbert space, but $d = \Omega(\log n)$ is needed $\implies$ not good enough for applications

Solution

- exploit invariance of the protocol under the action of $U(n)$ (instead of S_n)

Outline of the talk

1. The (usual) symmetric subspace and de Finetti theorems
2. Application to quantum key distribution
3. The "unitary" symmetric subspace and $\mathrm{SU}(p,q)$ coherent states
4. Gaussian de Finetti theorems

Fock spaces

Fock space

Let H be a finite-dimensional Hilbert space.

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

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

n-*mode space:* $H = \mathbb{C}^n$

- orthonormal basis of $\mathcal{F}(H)$:

$$\{|k_1, k_2, \ldots, k_n\rangle \, : \, k_i \in \mathbb{N}\}$$

- a pair of annihilation/creation operators is associated with each mode: $[a_i, a_i^\dagger] = \mathbb{1}$.
- states can be expressed as functions of creation operators applied to the vacuum:
$$|k_1, k_2, \ldots, k_n\rangle = \frac{1}{\sqrt{k_1! \cdots k_n!}} (a_1^\dagger)^{k_1} \cdots (a_n^\dagger)^{k_n} |0\rangle$$

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

- Bras and kets are not well-suited to deal with states of many modes
- A better approach is to realize $\mathcal{F}(\mathbb{C}^n)$ as a space of functions of n variables:
  - $|\psi\rangle \quad \leftrightarrow \quad \psi(z_1, \ldots, z_n)$
  - with norm $\|\psi\|^2 := \langle \psi, \psi \rangle = \frac{1}{\pi^n} \int \exp(-|z|^2)|\psi(z)|^2 dz < \infty$
- to recover the bra-ket formalism: replace the z_k by $\hat{a}_k^\dagger$ and apply to the vac. state

Examples

- Glauber coherent state: $|\alpha\rangle = \sum_{k=0}^\infty \frac{\alpha^k}{\sqrt{k!}}|k\rangle = e^{\hat{a}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\alpha z}$
- Two-mode squeezed vacuum state:

$$\sum_{k=0}^\infty \lambda^k |k, k\rangle = \sum_{k=0}^\infty \frac{\lambda^k}{k!} \hat{a}^{\dagger k} \hat{b}^{\dagger k} = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|0\rangle \quad \leftrightarrow \quad e^{\lambda z z'}$$

- n 2-mode squeezed vacuum states:

$$\bigotimes_{i=1}^n \left(\sum_{k=0}^\infty \lambda^k |k, k\rangle \right) = e^{\lambda(\hat{a}_1^\dagger \hat{b}_1^\dagger + \cdots + \hat{a}_n^\dagger \hat{b}_n^\dagger)}|0\rangle \quad \leftrightarrow \quad e^{\lambda(z_1 z_1' + \cdots + z_n z_n')}$$

Action of the unitary group on $F_{p,q,n}$

Consider $(p+q)$ copies of $\mathcal{F}(\mathbb{C}^n)$

- $F_{p,q,n} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_p} \otimes \mathcal{H}_{B_1} \otimes \cdots \mathcal{H}_{B_q}$ with $\mathcal{H}_{A_i} \cong \mathcal{H}_{B_j} \cong \mathcal{F}(\mathbb{C}^n)$
- functions of $n(p+q)$ variables:

$$\underbrace{(z_{1,1} \dots z_{n,1})}_{\vec{z}_1}, \dots, \underbrace{(z_{1,p} \dots z_{n,p})}_{\vec{z}_p}; \underbrace{(z'_{1,1} \dots z'_{n,1})}_{\vec{z}_1{}'}, \dots, \underbrace{(z'_{1,q} \dots z'_{n,q})}_{\vec{z}_q{}'}$$

The unitary group $U(n)$ *acts in a natural way on* $F_{p,q,n} := F(\mathbb{C}^{np} \otimes \mathbb{C}^{nq})$

$$\vec{z}_i \mapsto u\vec{z}_i, \quad \vec{z}_j{}' \mapsto \bar{u}\vec{z}_j{}' \quad \text{(change of variables)}$$

$F_{p,q,n}$ carries a representation of $U(n)$:

$$V_u : \psi(\vec{z}_1, \dots, \vec{z}_p, \vec{z}_1{}', \dots, \vec{z}_q{}') \mapsto \psi(u\vec{z}_1, \dots, u\vec{z}_p, \bar{u}\vec{z}_1{}', \dots, \bar{u}\vec{z}_q{}')$$

- Physically, a unitary $u \in U(n)$ is a linear optical network made of phase-shifters and beamsplitters acting on n modes.
- The previous CV QKD protocol is invariant under $U(n)$.

The symmetric subspace $F_{p,q,n}^{U(n)}$

$$F_{p,q,n}^{U(n)} = \{|\psi\rangle \in F_{p,q,n} \,:\, V_u|\psi\rangle = |\psi\rangle, \forall u \in U(n)\}$$

$|\lambda\rangle^{\otimes n} = e^{\lambda(z_1 z_1' + \cdots + z_n z_n')} \in F_{1,1,n}^{U(n)}$ (n *two-mode squeezed vacuum states)*

The quadratic form $Z := z_1 z_1' + \ldots + z_n z_n'$ is invariant under the change of variable $z \to uz, z' \to \bar{u}z'$:

$$\sum_{k=1}^n (uz)_k (\bar{u}z')_k = \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n u_{k,i} z_i \bar{u}_{k,j} z_j' = \sum_{i=1}^n \sum_{j=1}^n z_i z_j' \sum_{k=1}^n u_{k,i} (u^\dagger)_{j,k} = \sum_{i=1}^n z_i z_i'$$

since $uu^\dagger = \mathbb{1}_n$.

Introduce the $p \times q$ operators: $Z_{i,j} = z_{1,i} z_{1,j}' + \cdots + z_{n,i} z_{n,j}' \quad \leftrightarrow \quad a_{1,i}^\dagger b_{1,j}^\dagger + \cdots + a_{n,i}^\dagger b_{n,i}^\dagger$

$\implies$ $Z_{i,j}$ corresponds to the coherent addition of a photon in $\mathcal{H}_{A_i}$ and $\mathcal{H}_{B_j}$.

- Obs.: $\psi(Z_{1,1}, \ldots, Z_{p,q}) \in F_{p,q,n}^{U(n)} \implies$ only $p \times q$ parameters, instead of $n(p+q)$
- Main technical contribution: these are the only states

SU(p, q) *coherent states*

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

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

- stationary subgroup: $H = \mathrm{SU}(p) \times \mathrm{SU}(q) \times \mathrm{U}(1)$
- factor space G/H: set $\mathcal{D}$ of $p \times q$ matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$ (spectral norm < 1)
- generalized coherent state associated with $\Lambda \in \mathcal{D}$

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

- $|\Lambda, n\rangle$ is an i.i.d. Gaussian state (exp. of a quadratic form in the creation operators).

Theorem (arXiv:1612.05080)

$$F^{U(n)}_{p,q,n} = \mathrm{Span}\{ |\Lambda, n\rangle \,:\, \Lambda \in \mathcal{D} \}$$

Outline of the talk

Gaussian de Finetti

de Finetti Theorem (arXiv:1612.05080)

Let $n, k \geq p + q$, $\rho = |\psi\rangle\langle\psi|$ symmetric (pure) state in $F^{U(n+k)}_{p,q,n+k}$. Then tracing out over $k(p+q)$ modes gives an approximate mixture of $SU(p,q)$ coherent states:

$$\mathrm{tr}_{k(p+q)}(\rho) \approx_\varepsilon \int \nu(\Lambda) |\Lambda, n\rangle\langle\Lambda, n| d\mu(\Lambda) \quad \text{with} \quad \varepsilon = O\left(\frac{pqn}{n+k}\right)$$

de Finetti reduction for $p = q = 2$, application to QKD (arXiv:1701.03393)

Let $\Delta : \mathrm{End}(F^{\leq K}_{1,1,n}) \to \mathrm{End}(\mathcal{H}')$ such that $\Delta \circ V_u = \Delta$ for all $u \in U(n)$, then

$$\|\Delta\|_\diamond \leq \frac{K^4}{50} \|(\Delta \otimes \mathrm{id})\tau^\eta_{\mathcal{H}\mathcal{N}}\|_1,$$

with $\tau^\eta_{\mathcal{H}}$ a mixture of $|\Lambda, n\rangle$.

$\Longrightarrow$ prefactor improved from $2^{\mathrm{polylog}(n)}$ to $O(n^4)$ compared to previous results

$\Longrightarrow$ sufficient to consider security for Gaussian i.i.d. input states

Gaussian de Finetti: proof technique

rather straightforward once we have defined the coherent states

Resolution of the identity on $F_{p,q,n}^{U(n)}$ *(arXiv:1612.05080)*

For $n \geq p + q$,

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

with the invariant measure on $\mathcal{D}$: $d\mu_n(\Lambda) = C_n[\det(\mathbb{1}_p - \Lambda\Lambda^\dagger)]^{-(p+q)} \prod_{i,j}^{p} d\Lambda_{i,j}$

Approximate version for bounded energy, $p = q = 2$ *(arXiv:1701.03393)*

For $n \geq 5$ and $\eta \in [0, 1[$, if $K \leq \frac{\eta N}{1-\eta}$ for $N = n - 5$, then

$$\int_{\mathcal{D}_\eta} |\Lambda, n\rangle\langle\Lambda, n| d\mu_n(\Lambda) \geq (1 - \varepsilon)\Pi_{\leq K}$$

with $\varepsilon = 2N^4(1 + K/N)^7 \exp(-ND(\frac{K}{K+N} \,\|\, \eta))$ and $\Pi_{\leq K}$ projector onto the finite subspace with less than K excitations in $F_{2,2,n}^{U(n)}$

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
  - the corresponding symmetric subspace is spanned by $SU(p,q)$ coherent states
  - Gaussian de Finetti: considering such Gaussian i.i.d. states is sufficient

  $\Longrightarrow$ ex: continuous-variable QKD

Dualities

- Schur-Weyl duality:

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

- this work:

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