On Exchangeable Continuous Variable Systems

Robert König\(^1\) and Michael M. Wolf\(^2,3\)

\(^1\)Institute for Quantum Information, Caltech, Pasadena, USA
\(^2\)Max-Planck-Institut für Quantenoptik, Garching, Germany
\(^3\)Niels Bohr Institute, Copenhagen, Denmark

(Dated: April 18, 2008)

We investigate permutation-invariant continuous variable quantum states and their covariance matrices. We provide a complete characterization of the latter with respect to permutation-invariance, exchangeability and representing convex combinations of tensor power states. On the level of the respective density operators this leads to necessary criteria for all these properties which become necessary and sufficient for Gaussian states. For these we use the derived results to provide de Finetti-type theorems for various distance measures.

I. INTRODUCTION

A k-partite density operator on \((\mathbb{C}^d)^{\otimes k}\) is called n-exchangeable if it is the partial trace of a permutation-invariant state on \((\mathbb{C}^d)^{\otimes n}\). According to the quantum de Finetti theorem, such states can be approximated by convex combinations of k-fold product states with error bounded by \(O(\frac{1}{n})\). This result has various applications in quantum information theory (e.g., in security proofs for cryptographic protocols [12] or the justification of mean-field approaches [3]) and relatives (the “monogamy” of entanglement (cf. [4, 5]) or the appearance of a local classical description under symmetries [4, 7, 8]).

Unfortunately, such de Finetti-type statements for finitely exchangeable states are no longer true when the Hilbert space \(\mathbb{C}^d\) of an individual (“local”) system is replaced by an infinite-dimensional Hilbert space—as it happens for instance when dealing with fields of light. Indeed, as shown in [9], there are n-exchangeable states on \((\mathbb{C}^d)^{\otimes k}\) whose distance from any convex combination of product states is at least \(\Omega(\frac{1}{\sqrt{n}})\). This outrules the possibility of there being a de Finetti theorem for all finitely exchangeable states on infinite-dimensional Hilbert spaces.

It is, however, still possible to find de Finetti-type results for infinite-dimensional systems by considering restricted classes of states or observables [23]. An example are the coherent cat-states for which a de Finetti theorem was obtained by D’Cruz, Osborne and Schack [10]; an “exponential” version thereof is provided in [11]. In the present work we will first restrict the set of observables and consider covariance matrices of canonical field operators (such as position and momentum or the groupings into position- and momentum coordinates. The symmetric group \(S_n\) acts on the \(n\)-fold tensor product \(\mathcal{H}^{\otimes n}_d\) by permuting the factors. A state \(\rho\) on \(\mathcal{H}^{\otimes n}_d\) is called symmetric if it is invariant under this action, i.e., if \(\pi\rho\pi^{-1} = \rho\) for all \(\pi \in S_n\).

II. PRELIMINARIES

This section will introduce the notation and recall basic results (cf. [15]) on covariance matrices and the corresponding continuous variable states. Consider a system of \(n\) sites, each of which with \(d\) canonical degrees of freedom (modes). Such a system can be described using a symplectic vector space, the phase space, \(\mathcal{V} \cong \mathbb{R}^{2d} \otimes \mathbb{R}^n\) of dimension \(2d \cdot n\). We choose canonical coordinates such that the symplectic matrix \(\sigma\) has the form

\[
\sigma = \begin{pmatrix} 0_d & -1_d \\ 1_d & 0_d \end{pmatrix} \otimes 1_n ,
\]

where \(0_d\) and \(1_d\) are the \(d \times d\)-zero and identity matrix respectively. Occasionally, we will denote with a slight abuse of notation the symplectic matrix for a subsystem (less than \(n\) sites) by \(\sigma\) as well. The block structure in Eq. (1) reflects the grouping into position- and momentum coordinates. The corresponding quantum system with Hilbert space \(\mathcal{H}^{\otimes n}_d \cong (\mathcal{L}^2)^{\otimes dn}\) is characterized by canonical position- and momentum operators \(\{R_i^x, R_i^\beta\}_{i=1}^{2d}\) for each site \(i = 1, \ldots, n\); here \(\{R_i^x, R_i^{x+\alpha}\}_1, 1 \leq \alpha \leq d\) are the position- and momentum-operator of the \(\alpha\)-th mode of the \(i\)-th site, acting non-trivially...
only on the \( i \)-th factor of the \( n \)-fold tensor product space \( \mathcal{H}_d^\otimes n \). These operators satisfy the canonical commutation relations (CCR)

\[
i[R^a_k,R^b_l] = \sigma_{(a,k),(b,l)} \mathbb{I} . \tag{2}
\]

Real linear transformations \( S : \mathcal{V} \rightarrow \mathcal{V} \) which preserve the CCR (i.e., \( S\sigma S^T = \sigma \)) are called symplectic. Affine transformations are obtained from the unitary Weyl operators

\[
W(\xi) := e^{i\xi^T \sigma R} \tag{25}
\]

which give rise to displacements:

\[
W(\xi)R^a_k W(\xi)^\dagger = R^a_k + \xi^a \mathbb{I} . \tag{3}
\]

These only alter the first moments of a state, collected in the covariance matrix (CM) \( \Gamma \) with entries

\[
\Gamma_{(i,i),(\beta,j)} = \text{tr} \left( \{ R^a_i - D^a_i \cdot \mathbb{I}, R^b_j - D^b_j \cdot \mathbb{I} \} + \rho \right) .
\]

Since the Weyl operators act locally in the sense that they factorize with respect to local systems we can w.l.o.g. typically assume \( D = 0 \). Positivity of the density matrices implies that any CM has to satisfy \( \Gamma \geq i\sigma \). Conversely, every real symmetric matrix fulfilling this requirement is a valid CM. In particular, there always exists a Gaussian state which is, up to displacements, completely characterized by this CM.

### III. CHARACTERIZATION OF COVARIANCE MATRICES

We are now ready to characterize covariance matrices with respect to permutation-invariance, exchangeability and power-state property. Clearly, we could express all results below in terms of Gaussian states. However, we want to logically separate the treatment of CMs, since it is neither necessary for the state to be Gaussian nor does the corresponding density matrix have to share the full symmetry of the CM.

We will say that a CM is a power-state CM if it corresponds to a mixture of states with product CMs of the form \( \gamma \otimes \mathbb{I}_n \). Similarly, we say that it is \( n \)-exchangeable if it is a sub-block of a permutation-invariant CM of \( n \) sites, and we call it separable if it corresponds to a mixture of states with product CMs of the form \( \bigoplus_{i=1}^n \gamma_i \).

The main ingredient of our analysis is the following one-to-one correspondence between permutation-invariant CMs and bipartite product CMs:

**Proposition 1 (Symmetric CMs).** Let \( X \) be any real orthogonal \( n \times n \) matrix for which \( X_{i,1} = 1/\sqrt{n} \) for all \( i = 1, \ldots, n \). Then \( S = \mathbb{I}_{2^d} \otimes X \) is a symplectic transformation on \( \mathcal{V} = \mathbb{R}^{2^d} \otimes \mathbb{R}^n \) which gives rise to a one-to-one mapping between permutation-invariant CMs \( \Gamma \) on \( \mathcal{V} \) and pairs of CMs \( E,F \) on \( \mathbb{R}^{2^d} \) such that

\[
\Gamma = \Gamma(E,F) = S(E \otimes \bigoplus_{i=2}^n F)S^T . \tag{4}
\]

**Proof.** Evidently, \( S \) is a symplectic transformation and therefore maps CMs onto CMs. In fact, it is a passive transformation, i.e., number preserving. We first show that every pair of CMs \( E,F \) leads to a permutation-invariant \( \Gamma \). For this we have to show that the entries of the latter are site-independent in the sense that

\[
\Gamma_{(\alpha,i),(\beta,j)} = A_{\alpha,\beta} , \quad \Gamma_{(\alpha,i),(\beta,k)} = B_{\alpha,\beta} \quad \text{for } i \neq j . \tag{5}
\]

The symmetric \( 2d \times 2d \) matrices \( A \) and \( B \) encode the local (on-site) and non-local (inter-site) correlations, respectively.

With some abuse of Dirac notation Eq.(4) can be written as

\[
\Gamma = E \otimes X |1\rangle\langle 1|X^T + F \otimes (\mathbb{1} - X |1\rangle\langle 1|X^T) . \tag{6}
\]

Exploiting the condition on the first column of \( X \) this leads to

\[
\Gamma_{(\alpha,i),(\beta,j)} = \frac{1}{n} E_{\alpha,\beta} + (\delta_{i,j} - \frac{1}{n}) F_{\alpha,\beta} , \tag{7}
\]

which is indeed permutation-invariant. This immediately implies that every permutation-invariant CM characterized by \( A,B \) can be obtained in the above way by choosing

\[
E = A + (n-1)B \quad \text{and} \quad F = A - B . \tag{8}
\]

We will now use this representation in order to characterize power-state and exchangeable CMs:

**Proposition 2 (Power-state CMs).** Let \( \Gamma(E,F) \) be a permutation-invariant CM on \( \mathbb{R}^{2^d} \otimes \mathbb{R}^n \). Then the following are equivalent: (i) \( \Gamma \) is a power-state CM, (ii) \( \Gamma \) is a separable CM, and (iii) there exists a CM \( \gamma \) of \( d \) modes such that \( E \geq \gamma \) and \( F \geq \gamma \).

**Proof.** Clearly, (i) implies (ii). The remaining proof closely follows the derivation of the separability criterion for Gaussian states in [16]. There it is shown that for every separable CM \( \Gamma \) there exist CMs \( \gamma_i \) such that \( \Gamma \geq \bigoplus_{i=1}^n \gamma_i \). Averaging over all permutations we obtain \( \Gamma \geq \gamma \otimes \mathbb{I}_n \) with \( \gamma = \frac{1}{n} \sum_i \gamma_i \). Applying the symplectic transformation of Prop.1 to this inequality leads to \( E,F \geq \gamma \) (since the r.h.s. has \( E = F = \gamma \)) and (iii) is equivalent to (ii). Finally, again following [16], \( \Gamma \geq \gamma \otimes \mathbb{I}_n \) implies that \( \Gamma \) is the CM of a mixture of states with CM \( \gamma \otimes \mathbb{I}_n \).

**Proposition 3 (Exchangeable CMs).** Let \( \Gamma \) be a permutation-invariant CM on \( \mathbb{R}^{2^d} \otimes \mathbb{R}^k \), \( k \leq n \). With the notation from Prop.1 \( \Gamma \) is \( n \)-exchangeable if and only if \( A + (n-1)B \geq i\sigma \) or equivalently \( E = \frac{1}{n} \mathbb{E} + (1 - \frac{1}{n})F \) with \( \mathbb{E} \) being any CM of \( d \) modes.

This follows in a straightforward way from Prop.1 and the relation Eq.(8). It is remarkable that Prop.3 gives a simple criterion for deciding \( n \)-exchangeability for any CM. Note that such a criterion is not known for general exchangeable states on finite-dimensional Hilbert spaces (cf. [17]).

We also point out that according to Prop.3 \( \Gamma \) admits a permutation-invariant super-system of \( n \) sites for all \( n \geq k \) if and only if \( E \geq F \); this is a stronger condition than the one for power-state CMs.
IV. DE FINETTI THEOREMS FOR GAUSSIAN STATES

We now step back from phase space to Hilbert space and derive upper bounds on the distance between exchangeable Gaussian states and the set of power-states. Note that the conditions for a Gaussian state to be exchangeable or a power-state are precisely those given in the previous section. We begin with the single-mode case ($d = 1$) and recall that the trace norm ($L^1$-norm) is defined by $\|A\|_1 = \text{tr}\sqrt{A^*A}$.

**Theorem 1** (Single-mode de Finetti). Let $\rho_{\Gamma(E,F)}$ be an $n$-exchangeable Gaussian density matrix describing a permutation-invariant $k \leq n$ mode system. Define $E' = \frac{n-k}{n-k} E$. Then $\rho_{\Gamma(E',F)}$ is a Gaussian power-state, and

$$\|\rho_{\Gamma(E',F)} - \rho_{\Gamma(E,F)}\|_1 \leq \left(\frac{n-k}{n} - \frac{1}{2}\right)^{-1}.$$  \hfill (9)

**Proof.** The matrix $E'$ defines a valid CM, since multiplying by a factor $\lambda := \frac{n-k}{n} \geq 1$ preserves the condition $E \geq \lambda \sigma$. Using $n$-exchangeability and the CM $E$ appearing in Prop.3 we can write $E' = \frac{n-k}{n} E + F$. Observe that $E$ is a positive semi-definite operator, which is implied by $E \geq \lambda \sigma$ (via complex conjugation and averaging). We conclude that $E' \geq F$. According to Prop.3 this implies that $\rho_{\Gamma(E',F)}$ is indeed a Gaussian power-state.

To compute the distance between $\rho_{\Gamma(E,F)}$ and $\rho_{\Gamma(E',F)}$, we use the tensor product form of the states in the basis of Prop.3 together with the stability property $\|\rho \otimes \sigma - \rho' \otimes \sigma\| = \|\rho - \rho'\|$ of the trace norm, so that

$$\|\rho_{\Gamma(E,F)} - \rho_{\Gamma(E',F)}\|_1 = \|\rho_{\Gamma(E,F)} - \rho_{\Gamma(E',F)}\|_1.$$  \hfill (10)

To evaluate this further we use that there is a canonical basis where $E = s \mathbb{1}_2$ for some $s \geq 1$ and thus $E' = \lambda s \mathbb{1}_2$. The corresponding density matrices are now simultaneously diagonal in Fock state basis (labeled by $\ell = 0, \ldots, \infty$) with eigenvalues $\mu_\ell(s) := 2(s-1)\ell/((s+1)\ell+1)$ and $\mu_\ell(\lambda s)$ respectively. Hence, we proceed with 26

$$\|\rho_{\Gamma(E,F)} - \rho_{\Gamma(E',F)}\|_1 = \sum_{\ell=0}^{\infty} |\mu_\ell(s) - \mu_\ell(\lambda s)|$$

$$= \max_{\ell \in \mathbb{N}} 2 \left[\frac{\lambda s - 1}{\lambda s + 1}\right]^{\ell+1} - \left[\frac{s - 1}{s + 1}\right]^{\ell+1}. \hfill (11)$$

In order to obtain a bound which is independent of $s$ we consider the worst case, i.e., we take the supremum over $s \geq 1$ which is achieved for $s = 1$ [27] for which $\ell = 0$ attains the maximum so that finally

$$\|\rho_{\Gamma(E,F)} - \rho_{\Gamma(E',F)}\|_1 \leq 2 \frac{\lambda - 1}{\lambda + 1} \left(\frac{n-k}{n} - \frac{1}{2}\right)^{-1}. \hfill (12)$$

Let us now consider Gaussian systems with several modes ($d \geq 1$). In principle we could follow the same route as above. However, computing the trace-norm distance directly appears to become cumbersome due to its non-additivity with respect to tensor products. For this reason we choose two different figures of merit for measuring the distance to the set of power-states: the relative entropy

$$S(\rho, \rho') = \text{tr} \left[ \rho (\log \rho - \log \rho') \right]$$

and the fidelity

$$F(\rho, \rho') = \text{tr} \sqrt{\rho' \rho}.$$  \hfill (13)

Both have benign behavior under taking tensor products (they are additive and multiplicative, respectively) and both yield bounds for the trace norm distance since

$$\frac{1}{2} ||\rho - \rho'||^2 \leq \left\{ \begin{array}{c} S(\rho, \rho') \geq 2 - 2F(\rho, \rho')^2. \end{array} \right.$$  \hfill (14)

**Theorem 2** (Multi-mode de Finetti). Let $\rho_{\Gamma(E,F)}$ be an $n$-exchangeable Gaussian density matrix describing a permutation-invariant system of $k \leq n$ sites of $d$ modes each. Then the Gaussian power-state $\rho_{\Gamma(E',F)}$ with $E' = \frac{n-k}{n-k} E$ satisfies

$$S(\rho_{\Gamma(E',F)}, \rho_{\Gamma(E,F)}) \leq \log \frac{(n-k/2)^d}{(n-k)}, \hfill (15)$$

$$F(\rho_{\Gamma(E',F)}, \rho_{\Gamma(E,F)}) \geq \frac{(n-k/2)^{d/2}}{(n-k/2)}. \hfill (16)$$

**Proof.** It is clear from the arguments in Thm.1 that $\Gamma(E', F)$ indeed corresponds to a Gaussian power-state. We again exploit that the distance between $\rho_{\Gamma(E,F)}$ and $\rho_{\Gamma(E',F)}$ equals that between $\rho\in \rho_{\Gamma(E,F)}$. Moreover, we can simultaneously diagonalize the latter two states such that $\rho = \bigotimes_{\alpha=1}^d \rho(s_\alpha)$ where each $\rho(s_\alpha) = \sum_{\ell=0}^{\infty} \mu_\ell(s_\alpha) |\ell\rangle\langle\ell|$ is a thermal Gaussian state with $s_\alpha \mathbb{1}_2$ and the $s_\alpha \geq 1$ are the symplectic eigenvalues of $E$. For $E'$ we only have to replace $s_\alpha$ by $\lambda s_\alpha$, with $\lambda = n/(n-k)$. For the relative entropy, summing up the series leads to

$$S(\rho_{\Gamma(E',F)}, \rho_{\Gamma(E,F)}) = \sum_{\alpha=1}^d S(\rho(s_\alpha), \rho(\lambda s_\alpha)) \hfill (17)$$

$$= \frac{1}{2} \sum_{\alpha=1}^d \left[ (s_\alpha - 1) \log(s_\alpha - 1) - (s_\alpha + 1) \log(s_\alpha + 1) + (s_\alpha + 1) \log(\lambda s_\alpha + 1) - (s_\alpha - 1) \log(\lambda s_\alpha - 1) \right]. \hfill (18)$$

For every $\lambda \geq 1$ each summand is a decreasing function in $s_\alpha$ such that the supremum is again obtained for $s_\alpha = 1$, i.e.,

$$\sup_{s_\alpha \geq 1} S(\rho(s), \rho(\lambda s)) = \log \frac{1+\lambda}{2} \hfill (19)$$

which concludes the proof for the relative entropy upon inserting $\lambda$. In a similar vein we can evaluate the fidelity:

$$F(\rho_{\Gamma(E',F)}, \rho_{\Gamma(E,F)}) = \prod_{\alpha=1}^d F(\rho(s_\alpha), \rho(\lambda s_\alpha)) \hfill (20)$$

$$= \sum_{\ell=0}^{\infty} \sqrt{\mu_\ell(s) \mu_\ell(\lambda s)} \hfill (21)$$

$$= \frac{2}{\sqrt{(s+1)(\lambda s + 1) - (s-1)(\lambda s - 1)}}. \hfill (22)$$

Again the worst case, now the infimum over $s \geq 1$, is attained at $s = 1$ which leads to the desired result. \hfill \Box
V. CONCLUSIONS & OPEN PROBLEMS

The bounds given in Thm[1] and Thm[2] are tight for the given class of ansatz states and the proofs allow for any explicitly given CM $E$ to compute the exact distance to this class. Whether the chosen class is optimal or yields at least an optimal scaling remains open. Similarly, the question for which figure of merit a power-state closest to a given $n$-exchangeable Gaussian state can again be chosen to be Gaussian remains open as standard arguments, e.g. based on the central limit theorem (CLT) [19], do not immediately apply. Some kind of marriage between the CLT and the de Finetti theorem would also be desirable in order to extend the latter in a reasonable way beyond the class of Gaussian states.

Another interesting direction of future research could be to use more general approximating states than Gaussian power-states in the de Finetti theorem. In this way it might be possible to obtain an exponentially small error as in the “almost-product” de Finetti theorem for finite-dimensional systems [1] (see also [11, 20]). This would be important for applications to continuous-variable quantum key distribution, for example [21].

Acknowledgments

RK would like to thank the Max-Planck-Institute for its hospitality, and Ignacio Cirac and Geza Giedke for helpful discussions. He acknowledges partial support by NSA under ARO contract no. W911NF-05-1-0294 and by NSF under contract no. PHY-0456720.

[1] R. Renner, Ph.D. thesis, ETH Zurich (2005), arXiv:quant-ph/0512258.
[2] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Phys. Rev. Lett. 100, 110502 (2008), arXiv:quant-ph/0712.2265.
[3] G. A. Raggio and R. F. Werner, Helv. Phys. Acta 62, 980 (1989).
[4] T. Osborne and F. Verstraete, Phys. Rev. Lett. 96, 220503 (2006).
[5] M. Wolf, F. Verstraete, and J. Cirac, Phys. Rev. Lett. 92, 087903 (2006).
[6] R. Werner, Lett. Math. Phys. 17, 359 (1989).
[7] M. Wolf, F. Verstraete, and J. Cirac, Int. Journal of Quantum Information 1, 465 (2003).
[8] B. Terhal, A. Doherty, and D. Schwab, Phys. Rev. Lett. 90, 157903 (2003).
[9] M. Christandl, R. König, G. Mitchison, and R. Renner, Comm. Math. Phys. 273, 473 (2007).
[10] C. D’Cruz, T. J. Osborne, and R. Schack, Phys. Rev. Lett 98, 160406 (2007), arXiv:quant-ph/0606139.
[11] R. König and G. Mitchison, A most compendious and facile quantum de finetti theorem (2007), arXiv:quant-ph/0703210.
[12] R. L. Hudson and G. R. Moody, Z. Wahrschein. verw. Geb. 33, 343 (1976).
[13] E. Størmer, J. Funct. Anal. 3, 48 (1969).
[14] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. 43, 4537 (2002), arXiv:quant-ph/0104088.
[15] A. S. Holevo, Probabilistic and statistical aspects of quantum theory (North-Holland Publishing Company, New York, 1982).
[16] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. 86, 3658 (2001).
[17] M. Fannes and C. Vandenplas, Journal of Physics A: Mathematical and General 39, 13843 (2006), arXiv:quant-ph/0605216.
[18] M. Ohya and D. Petz, Quantum Entropy and Its Use, Texts and Monographs in Physics (Springer, 2004).
[19] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. 96, 080502 (2006).
[20] R. Renner, Nature Physics 3, 645 (2007), arXiv:quant-ph/0703069.
[21] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. 97, 190503 (pages 4) (2006).
[22] M. Christandl and B. Toner, Finite de finetti theorem for conditional probability distributions describing physical theories (2007), arXiv:quant-ph/0712.0916.
[23] J. Barrett and M. Leifer, The de finetti theorem for test spaces (2007), arXiv:quant-ph/0712.2265.
[24] See [23] for a different direction of generalization of the basic de Finetti claim for quantum states.
[25] Here we assume, as usual, the Weyl system to be irreducible and strongly continuous.
[26] Eq.(10) is evaluated by first noting that $\mu_\ell(s)$ and $\mu_\ell(\lambda s)$ are normalized geometric series such that one is larger than the other up to some specific $\ell$. In this way the absolute value can be expressed as a difference of two geometric series.
[27] For this we need to evaluate the expression at the optimal $\ell$ which is one of the two integers next to

\[
\left(\log \frac{\log \nu(s)}{\log \nu(\lambda s)}\right) / \log \left(\frac{\nu(\lambda s)}{\nu(s)}\right) - 1,
\]

with $\nu(s) := (s - 1)/(s + 1)$. 