PHYSICAL REVIEW A **80**, 010102(R) (2009)

Quantum de Finetti theorem in phase-space representation

Anthony Leverrier
Institut Telecom/Telecom ParisTech, CNRS LTCI, 46 rue Barrault, 75634 Paris Cedex 13, France

Nicolas J. Cerf
Quantum Information and Communication, Ecole Polytechnique, Université Libre de Bruxelles, CP 165/59, 50 Av. F. D. Roosevelt, B-1050 Brussels, Belgium
and MIT, Research Laboratory of Electronics, Cambridge, Massachusetts 02139, USA

(Received 30 April 2009; published 28 July 2009)

The quantum versions of de Finetti's theorem derived so far express the convergence of n-partite symmetric states, i.e., states that are invariant under permutations of their n parties, toward probabilistic mixtures of independent and identically distributed (IID) states of the form $\sigma^{\otimes n}$. Unfortunately, these theorems only hold in finite-dimensional Hilbert spaces, and their direct generalization to infinite-dimensional Hilbert spaces is known to fail. Here, we address this problem by considering invariance under orthogonal transformations in *phase space* instead of permutations in *state space*, which leads to a quantum de Finetti theorem particularly relevant to continuous-variable systems. Specifically, an n-mode bosonic state that is invariant with respect to this continuous symmetry in phase space is proven to converge toward a probabilistic mixture of IID Gaussian states (actually, n identical thermal states).

DOI: 10.1103/PhysRevA.80.010102 PACS number(s): 03.65.Ca, 03.70.+k, 42.50.−p

I. INTRODUCTION

There has been a renewed interest in de Finetti's theorem [1] over the recent years, especially in the context of quantum information theory (see, e.g., [2]). In a classical setting, de Finetti's theorem addresses the statistics of large composite systems obeying some fundamental symmetry (e.g., invariance under permutations of its parts), stating that its parts can be well approximated by identical independent subsystems. In the language of probability theory, a permutation-invariant joint probability distribution of n random variables is shown to approach a probabilistic mixture of *independent and identically distributed* (IID) variables. In a quantum setting, the theorem makes the connection between two types of n-mode states in $\mathcal{H}^{\otimes n}$: symmetric states, i.e., states that are invariant under permutations of their subsystems (ρ such that $\rho=\pi\rho\pi^{\dagger}$ for any permutation $\pi\in\mathcal{S}_n$), and mixtures of IID states of the form $\sigma^{\otimes n}$ for some state $\sigma\in\mathcal{H}$. Whereas an IID state is obviously symmetric, the converse is not true in general. This situation is rather frustrating as the symmetry of a state is often known or can be easily enforced by application of a random permutation of the subsystems, while it rather is the IID property that one wishes to have as it considerably simplifies the analysis (an IID state is fully described in $\mathcal{H}$ instead of $\mathcal{H}^{\otimes n}$). According to the quantum de Finetti theorem [3,4], a symmetric state becomes increasingly close to a mixture of IID states as one traces out more of its parts. Attempts at characterizing the speed of convergence toward an IID state are more recent, both in the classical case [5] and quantum case [6,7]: the trace distance between the partial trace over $(n-k)$ parties of an n-partite symmetric state and a mixture of k-partite IID states is bounded from above by $2d^2k/n$, where d is the dimension of the Hilbert space.

Interestingly, a striking difference with the classical case is that the trace distance in the quantum case necessarily depends on the dimension of the Hilbert space. In particular, this rules out the possibility of a direct generalization of the theorem to an infinite-dimensional Hilbert space. This was proven in Ref. [7], where a counterexample was exhibited: the n-dimensional generalization of the singlet state $1/\sqrt{n!}\Sigma_{\pi}\mathrm{sgn}(\pi)\pi(|0\rangle\otimes|1\rangle\otimes\cdots\otimes|n-1\rangle)$ is symmetric but any bipartite part, being a mixture of singlet states, cannot be approximated by a mixture of IID states. Even if a general quantum de Finetti theorem does not hold in infinite dimension, it is still possible to establish interesting versions of the theorem by restricting the set of states considered. For instance, such results can be obtained for coherent Schrödinger cat (macroscopic quantum superposition) states [8] and Gaussian states [9].

In this Rapid Communication, we follow a rather different approach by considering a symmetry group different from the permutations over the n subsystems of a state in $\mathcal{H}^{\otimes n}$. We investigate the properties of *orthogonally invariant* states ρ, i.e., states that are invariant under the action of any n-mode Gaussian unitary operator corresponding to a real symplectic orthogonal transformation in the $2n$-dimensional phase space of ρ. In [10], we had touched this question in the asymptotic limit $n\to\infty$ and exhibited the connection between orthogonally invariant states and (probabilistic mixtures of) IID thermal states. Here, we prove a finite version of this result, which leads to a genuine quantum continuous-variable de Finetti theorem in phase-space representation.

The outline of the Rapid Communication is as follows. In Sec. II, we introduce the concept of orthogonally invariant quantum states and give an alternative characterization of these states in the Fock state representation. Then, in Sec. III, we prove a quantum de Finetti theorem for orthogonally invariant n-mode states, which bounds the convergence speed toward IID thermal states for finite n. Finally, in Sec. IV, we discuss the perspectives of this continuous-variable quantum de Finetti theorem and draw conclusions.

II. ORTHOGONALLY INVARIANT STATES

The state ρ of an n-mode bosonic quantum system can be completely characterized by its Wigner function W in the $2n$-dimensional phase space parametrized by the quadratures $x_1, p_1, \ldots, x_n, p_n$. The Wigner function is well known to be a quasiprobability distribution, not a genuine probability distribution as it can take negative values. However, by integrating it over one quadrature (x or p) for each mode, one obtains the n-variate probability distribution characterizing the outcomes of the n homodyne measurements (one performed on each mode).

One is of course not restricted to measuring quadratures x_k or p_k but can also measure rotated quadratures with any angle θ_k in phase space. Thus, from a Wigner function, one can always construct a genuine probability distribution $p(r_1, \ldots, r_n)$, where r_k corresponds to a particular rotated quadrature of the kth mode. In addition, one can also mix several modes with the help of a passive linear interferometer before performing the homodyne measurements, which means that the variables r_k become (normalized) linear combinations of the quadratures $x_1, p_1, \ldots, x_n, p_n$. In summary, starting with an arbitrary Wigner function, one can always construct a family of n-variate probability distributions $p(r_1, \ldots, r_n)$ using the following procedure: first, one processes the n modes through a passive linear interferometer (a network of beam splitters and phase shifters), and then one measures one fixed quadrature for each output mode.

Let us now consider possible symmetries of the joint probability distribution characterizing the n random variables r_k. A first symmetry, which is standard in the context of de Finetti's theorem, is the invariance under permutations of the variables. This means that $p(r_1, \ldots, r_n) = p(r_{\pi(1)}, \ldots, r_{\pi(n)})$ for any permutation $\pi \in \mathcal{S}_n$, where $\mathcal{S}_n$ denotes the group of permutations on $\{1, \ldots, n\}$. Another symmetry, which has not been explored so far in the quantum context, emerges naturally for the real-valued random vector $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$. Note that the previous permutation symmetry simply means that the distribution probability is not affected by reordering the coordinates. As we work in $\mathbb{R}^n$, however, it seems more appropriate to substitute a discrete symmetry group such as $\mathcal{S}_n$ with a continuous symmetry group. A natural choice in this respect is the orthogonal group $O(n)$, that is, the group of orthogonal transformations (or isometries) acting on vector $\mathbf{r}$. Note that applying an orthogonal transformation on $\mathbf{r}$ precisely corresponds to inserting an n-mode passive linear interferometer before performing the n homodyne measurements.

In classical probability theory, distributions that are invariant under orthogonal transformations are referred to as orthogonally invariant distributions. It has long been known that such probability distributions tend to mixtures of IID Gaussian distributions in the limit $n \to \infty$, or, more formally, that the first k coordinates of a random point that is uniformly distributed on the n-dimensional sphere are asymptotically normal. (An historical perspective of this property, going back to Poincaré, Borel, and Maxwell, can be found in Ref. [11], where the authors also derive a sharp bound for the theorem). In what follows, we consider the natural quantum counterpart of these distributions, namely, n-mode states ρ for which the probability distribution $p(r_1, \ldots, r_n)$ that results from measuring n quadratures of ρ is unaffected by an n-mode passive interferometer preceding the measurement. This is equivalent to the condition that the state ρ is itself invariant under passive symplectic transformations, or, more physically, that ρ remains unchanged after being processed via any n-mode passive linear interferometer. In what follows, we will refer to these states as orthogonally invariant in phase space.

This orthogonal invariance in phase space clearly encompasses the permutation invariance in state space since permuting the coordinates in phase space is just a special case of an orthogonal transformation. Since we are considering a continuous instead of a discrete symmetry group, this invariance in phase space might appear quite restrictive, and we may question whether there exist interesting orthogonally invariant states. This is fortunately the case as, for example, any multimode thermal state is orthogonally invariant. This can be readily checked by considering its Wigner function which is given by a $2n$-partite Gaussian distribution with variance σ^2, $W_{\mathrm{th}}(x_1, p_1, \ldots, x_n, p_n) \propto e^{-(x_1^2+p_1^2+\cdots+x_n^2+p_n^2)/2\sigma^2}$ which is clearly invariant under orthogonal transformations of the coordinates. Note that such a multimode thermal state is nothing but a product of identical thermal states, which, in fact, plays the same role for the invariance under orthogonal transformations as IID states for the usual invariance under permutations. Another class of orthogonally invariant states is the multimode extension of Fock states that we will consider in the following.

Let us now give two alternative characterizations of the set of orthogonally invariant states. The most natural one relies on phase-space representation since this is how the symmetry is expressed. In order to be invariant under orthogonal transformations in phase space, these states must simply have a Wigner function that only depends on one single parameter, namely, the modulus $\|\mathbf{r}\| = (x_1^2 + p_1^2 + \cdots + x_n^2 + p_n^2)^{1/2}$. The characterization of this set of states in the Fock state representation is slightly more involved. We note that this set is convex as any mixture of orthogonally invariant states remains invariant under orthogonal transformations. It is, therefore, completely characterized by its extremal points, which can be shown to be the states

$$\sigma_p^n = \frac{1}{a_p^n} \sum_{\substack{p_1 \cdots p_n \\ \text{st } \sum_i p_i = p}} |p_1 \cdots p_n\rangle\langle p_1 \cdots p_n|, \tag{1}$$

with $a_p^n = \binom{n+p-1}{n-1}$. These extremal states are the multimode generalization of number states $|p\rangle$, that is, they correspond to the (normalized) projectors onto the various eigenspaces of the total number operator $\hat{n} = \hat{n}_1 + \cdots + \hat{n}_n$. For instance, σ_p^n, which is proportional to the projector onto the eigenspace of $\hat{n}$ with eigenvalue p, physically corresponds to a state with p photons distributed over n modes. The normalization factor a_p^n simply coincides with the number of ways of distributing p photons over n modes. These extremal states σ_p^n form a discrete infinite set of mixed states parametrized by p (or pure states for $n=1$ as $\sigma_p^1 = |p\rangle\langle p|$). Importantly, any pure eigenstate chosen in the eigenspace corresponding to a given

total photon number p is generally not orthogonally invariant; only the uniform mixture of them fulfills this invariance (Schur's lemma), which is why the extremal states σ_p^n are mixed for $n>1$.

III. QUANTUM DE FINETTI THEOREM FOR ORTHOGONALLY INVARIANT STATES

As mentioned above, a classical de Finetti theorem exists for classical orthogonally invariant probability distributions. The theorem states that, in the limit of infinite sequences $X_1,\ldots,X_n$ with $n\to\infty$, the first k variables are exactly mixtures of IID Gaussian distributions. This result only holds approximately for finite sequences [11]: if the distribution of $X_1,\ldots,X_n$ is invariant under orthogonal transformations in $\mathbb{R}^n$, then the marginal distribution of the first k coordinates $X_1,\ldots,X_k$ is close to a mixture of IID Gaussian distributions. Here, the "closeness" is measured in the sense that the variation distance is bounded from above by $2(k+3)/(n-k-3)$ for $1\leq k\leq n-3$.

Let us now formulate our main result, which is the quantum counterpart of the previous result.

Theorem 1. If ρ^n is an n-mode orthogonally invariant quantum state, its partial trace over any $(n-k)$ modes $\mathrm{tr}_{n-k}(\rho^n)$ can be approximated by a mixture of k-mode thermal states $\rho_{\mathrm{th}}^k(x)$, that is,

$$\left\|\mathrm{tr}_{n-k}(\rho^n)-\int\rho_{\mathrm{th}}^k(x)\mu(dx)\right\|_1\leq 2\left(\frac{n^2}{(n-k-1)(n-k-2)}-1\right),$$

where $\rho_{\mathrm{th}}^k(x)$ is the tensor product of k thermal states with a mean number of x photons per mode, and μ is a probability measure.

The idea of our proof is inspired from that of the classical version of the theorem for geometric probability distributions, as described in [11]. If $X_1,\ldots,X_n$ are integer classical random variables whose joint distribution is invariant under transformations that keep the sum $X_1+\cdots+X_n$ constant, then the marginal law of the first k coordinates $X_1,\ldots,X_k$ is close, in the sense of the variation distance, to a mixture of IID geometric distributions. The link with our quantum problem comes from the fact that in the Fock basis, any passive linear interferometer redistributes the photons among the modes in such a way that the total photon number is kept constant since the energy is conserved. The invariance under orthogonal transformations in phase space therefore translates into the invariance under transformations that keep the total photon number constant in the Fock basis. As a consequence, the asymptotic state in our theorem is characterized by a geometric distribution in the Fock basis, which precisely is the signature of a thermal state. Our proof will thus consist in bounding the convergence of an n-mode state that is invariant under a redistribution of photons among the n modes (with a constant total photon number) toward a mixture of thermal states.

Proof. We start from the fact that any n-mode orthogonally invariant state ρ^n can be written as a convex mixture of the multimode number states σ_p^n as defined in Eq. (1), namely, $\rho^n=\Sigma_{p=0}^{\infty}c_p\sigma_p^n$ with arbitrary weights c_p satisfying $0\leq c_p\leq 1$ and $\Sigma_p c_p=1$. Now, using the convexity of the trace-norm distance $\left\|\mathrm{tr}_{n-k}(\rho^n)-\int\rho_{\mathrm{th}}^k(x)\mu(dx)\right\|_1\leq\Sigma_{p=0}^{\infty}c_p\left\|\mathrm{tr}_{n-k}(\sigma_p^n)-\int\rho_{\mathrm{th}}^k(x)\mu(dx)\right\|_1$, we see that it is sufficient to prove the theorem for the extremal states σ_p^n. More precisely, we will upper bound the quantity $\left\|\mathrm{tr}_{n-k}(\sigma_p^n)-\rho_{\mathrm{th}}^k(p/n)\right\|_1$.

The reduced state $\mathrm{tr}_{n-k}(\sigma_p^n)$ is obviously orthogonally invariant in the remaining space of k modes, which implies that it can be written as a mixture of k-mode number states, $\mathrm{tr}_{n-k}(\sigma_p^n)=\Sigma_{l=0}^{p}f(l)\sigma_l^k$ where a simple combinatorial argument shows that $f(l)=a_l^k a_{p-l}^{n-k}/a_p^n$. The k-mode thermal state $\rho_{\mathrm{th}}^k(x)$ is defined as the product of k single-mode thermal states with x photons per mode, namely, $\rho_{\mathrm{th}}^k(x)=\rho_{\mathrm{th}}(x)^{\otimes k}$, with $\rho_{\mathrm{th}}(x)=\Sigma_{l=0}^{\infty}\frac{x^l}{(1+x)^{l+1}}|l\rangle\langle l|$. A straightforward calculation shows that $\rho_{\mathrm{th}}^k(x)=\Sigma_{l=0}^{\infty}g(l)\sigma_l^k$, with $g(l)=a_l^k\frac{x^l}{(1+x)^{l+k}}$ which confirms that it is also orthogonally invariant.

Since both $\mathrm{tr}_{n-k}(\sigma_p^n)$ and $\rho_{\mathrm{th}}^k(x)$ are diagonal in the basis of k-mode number states, their trace-norm distance is given by the variation distance between the classical probability distributions f and g, that is, $\left\|\mathrm{tr}_{n-k}(\sigma_p^n)-\rho_{\mathrm{th}}^k(p/n)\right\|_1=\Sigma_{l=0}^{\infty}|f(l)-g(l)|=2\Sigma_{l=0}^{\infty}(\frac{f(l)}{g(l)}-1)^+g(l)$ where the function $(x)^+=\max(x,0)$. It follows that

$$\left\|\mathrm{tr}_{n-k}(\sigma_p^n)-\rho_{\mathrm{th}}^k(p/n)\right\|_1\leq 2(\sup_l h(l)-1), \tag{2}$$

where $h(l)\equiv\frac{f(l)}{g(l)}=\frac{a_{p-l}^{n-k}(1+p/n)^{l+k}}{a_p^n(p/n)^l}$. Expanding the binomials in a_{p-l}^{n-k} and a_p^n, one gets $h(l)=\Pi_{t=1}^{k}(1-\frac{t}{n})\Pi_{t=1}^{l-1}(1-\frac{t}{p})/\Pi_{t=1}^{k+l}(1-\frac{t}{n+p})$. The logarithm of $h(l)$ can be expressed as

$$\ln h(l)=-S(n,k)-S(p,l-1)+S(n+p,k+l), \tag{3}$$

where $S(n,k)\equiv-\Sigma_{t=0}^{k}\ln(1-\frac{t}{n})$. For the function $x\mapsto-\ln(1-x)$ being monotonically increasing on $[0,1]$, one has

$$nJ\left(\frac{k}{n}\right)\leq S(n,k)\leq nJ\left(\frac{k+1}{n}\right), \tag{4}$$

where $J(x)\equiv-\int_0^x\ln(1-t)dt=x+(1-x)\ln(1-x)$. Let us introduce the two reduced variables $u=k/n$ and $v=l/p$, which both belong to the interval $[0,1]$. Since the function $J(x)$ is convex on $[0,1]$, we have $J[\alpha u+(1-\alpha)v]\leq\alpha J(u)+(1-\alpha)J(v)$, where $0\leq\alpha\leq 1$. If we choose $\alpha=n/(n+p)$, this equation translates into $(n+p)J(\frac{k+l}{n+p})\leq nJ(\frac{k}{n})+pJ(\frac{l}{p})$ whose left-(right-)hand side term can be lower (upper) bounded thanks to Eq. (4). This yields $S(n+p,k+l-1)\leq S(n,k)+S(p,l)$. Substituting k with $k+2$ and l with $l-1$, we get the equivalent inequality $S(n+p,k+l)\leq S(n,k+2)+S(p,l-1)$, which, together with Eq. (3), gives $\ln h(l)\leq S(n,k+2)-S(n,k)$. Hence, $h(l)\leq\frac{n^2}{(n-k-1)(n-k-2)}$ which, using Eq. (2), concludes the proof of our theorem. ■

IV. CONCLUSION

We have investigated the invariance under orthogonal transformations in phase-space representation in the context of quantum de Finetti theorems. This approach seems to be particularly relevant to study the properties of continuous-variable systems, going beyond the standard approach based on permutation invariance in state space representation. Just like orthogonally invariant n-partite probability distributions

are known to tend to IID. Gaussian distributions, we have shown that orthogonally invariant n-mode states tend to IID thermal states. More precisely, we have derived a finite version of a quantum de Finetti theorem for this class of states, which puts an upper bound on the distance between the partial trace of orthogonally invariant states and mixtures of multimode thermal states. Physically, the invariance under orthogonal transformations in phase space corresponds to the fact that the state is unchanged by a passive linear interferometer. Since this operation amounts to redistributing photons while keeping their number constant, our quantum de Finetti theorem is connected to the classical de Finetti theorem for geometric distributions [11].

Let us conclude by suggesting two potentially interesting extensions of this de Finetti theorem, which arise in the context of continuous-variable quantum key distribution [12]. First, one would like to generalize our results to bipartite states, i.e., states ρ_{AB} that are invariant under (conjugate) orthogonal transformations applied to systems A and B, respectively. As we explained in Ref. [10], the legitimate parties (Alice and Bob) can always enforce such symmetry in phase space. Their global state ρ_{AB} can therefore be assumed to be a bipartite orthogonally invariant state in phase space. In other words, ρ_{AB} is invariant if both parts $\rho_A=\mathrm{tr}_B\ \rho_{AB}$ and $\rho_B=\mathrm{tr}_A\ \rho_{AB}$ are processed via (conjugate) passive linear interferometers. Note that the resulting local states held by each party, ρ_A and ρ_B, are then another example of orthogonally invariant states. The second question one might want to answer is whether the theorem presented here has an exponential version in analogy to Ref. [2], that is, such that only a small number of modes needs to be traced out in order to get a reduced state that is well approximated by (almost) a mixture of thermal states.

ACKNOWLEDGMENTS

A.L. thanks Renato Renner and Johan Åberg for fruitful discussions. The authors acknowledge financial support of the European Union under the FET-Open project COMPAS (Grant No. 212008), the Agence Nationale de la Recherche under projects PROSPIQ (Grant No. ANR-06-NANO-041-05) and SEQURE (Grant No. ANR-07-SESU-011-01), and the Brussels-Capital Region under project CRYPTASC.

[1] B. De Finetti, Ann. I.H.P. Probab. Stat. **7**, 1 (1937).
[2] R. Renner, Nat. Phys. **3**, 645 (2007).
[3] R. Hudson and G. Moody, Probab. Theory Relat. Fields **33**, 343 (1976).
[4] C. Caves, C. Fuchs, and R. Schack, J. Math. Phys. **43**, 4537 (2002).
[5] P. Diaconis and D. Freedman, Ann. Probab. **8**, 745 (1980).
[6] R. König and R. Renner, J. Math. Phys. **46**, 122108 (2005).
[7] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[8] C. D'Cruz, T. J. Osborne, and R. Schack, Phys. Rev. Lett. **98**, 160406 (2007).
[9] R. König and M. Wolf, J. Math. Phys. **50**, 012102 (2009).
[10] A. Leverrier, E. Karpov, P. Grangier, and N. Cerf, e-print arXiv:0907.3696.
[11] P. Diaconis and D. Freedman, Ann. Inst. Henri Poincare, Sect. A **23**, 397 (1987).
[12] N. Cerf and P. Grangier, J. Opt. Soc. Am. B **24**, 324 (2007).