Extremal quantum cloning machines

G. Chiribella, G. M. D'Ariano,* and P. Perinotti
QUIT Quantum Information Theory Group of the INFM, unità di Pavia and Dipartimento di Fisica "A. Volta," via Bassi 6, I-27100 Pavia, Italy

N. J. Cerf
QUIC, Ecole Polytechnique, Université Libre de Bruxelles, 1050 Brussels, Belgium

(Received 14 July 2005; published 28 October 2005)

We investigate the problem of cloning a set of states that is invariant under the action of an irreducible group representation. We then characterize the cloners that are *extremal* in the convex set of group covariant cloning machines, among which one can restrict the search for optimal cloners. For a set of states that is invariant under the discrete Weyl-Heisenberg group, we show that all extremal cloners can be unitarily realized using the so-called *double-Bell states*, whence providing a general proof of the popular *ansatz* used in the literature for finding optimal cloners in a variety of settings. Our result can also be generalized to *continuous-variable* optimal cloning in infinite dimensions, where the covariance group is the customary Weyl-Heisenberg group of displacements.

DOI: 10.1103/PhysRevA.72.042336 PACS number(s): 03.67.Hk, 03.65.Ta

I. INTRODUCTION

The impossibility of preparing several exact copies of an unknown quantum state, encapsulated by the *no-cloning* theorem [1], is one of the most remarkable features of quantum mechanics. In addition to being of fundamental interest, it is also a pivotal ingredient in many practical applications, first among them quantum cryptography, where the impossibility of perfect cloning crucially poses limitations to eavesdropping.

From the discovery of the no-cloning theorem to now, a main research focus in the literature has been to find the best approximation of ideal quantum cloning with physical transformations allowed by quantum mechanics. Many relevant cases have been studied, and, depending on the set of states to be cloned, different optimal machines have been found [2–7]. In particular, much attention has been devoted to the situation in which the set of states to be cloned is invariant under a group of unitary transformations, the so-called *group covariant cloning* [8].

Despite the variety of cloning transformations that is known today, it is remarkable that the overwhelming majority of optimal covariant cloning machines shares some common features, which relate their structure to a particular superposition of *double-Bell states*. This observation, which was originally formulated in an ansatz [9,10], has since then often been exploited to find optimal cloners along with their physical realizations (see, e.g., Refs. [11–13]). Although the double-Bell ansatz has been shown to be correct in many cases, no general proof has been provided of its validity, yet and the common features of these optimal cloning machines are still just a surprising coincidence.

The aim of this paper is to provide a formal proof of this double-Bell ansatz in a covariant context, analyzing the physical meaning of the related implicit assumptions. This analysis *a posteriori* explains in a general way the appearance of double-Bell states in the optimal one-to-two covariant cloners, and also allows us to connect several cloning problems [e.g., the cloning of the four states involved in the Bennett-Brassard Protocol (BB84) to the phase-covariant cloning of equatorial states].

In Sec. II, we set the problem of cloning an invariant set of states in the language of quantum operations, and define the covariance and strong covariance conditions. In Sec. III, we characterize the set of extremal covariant cloners, and show that it includes the set of strongly covariant cloners. In Sec. IV, we analyze the special case of covariant cloners under the discrete Weyl-Heisenberg group, and show that all extremal covariant cloners are then necessarily also strongly covariant. This result is shown to imply the double-Bell ansatz, which is then used to derive the optimal cloners in various settings for qubits, *d*-dimensional, or infinite-dimensional states. Finally, the conclusions are drawn in Sec. V.

II. CLONING AS A QUANTUM OPERATION

A. Cloning an invariant set of states

Consider a machine $\mathcal{M}$ that takes states in the Hilbert space $\mathcal{H}$ of a quantum system to states in $\mathcal{H}\otimes\mathcal{H}$. The task of the cloning machine is to provide two approximate copies of a state picked up from a given set of density matrices $\mathsf{S}\subset\mathcal{B}(\mathcal{H})$ which is invariant under the action of some group of symmetry transformations. The action of the group—call it $\mathbf{G}$—is specified by a unitary representation $\{U_g | g\in\mathbf{G}\}$, and the set of states S enjoys the invariance property

$$U_g \mathsf{S} U_g^\dagger = \mathsf{S}, \quad \forall\, g\in\mathbf{G}, \tag{1}$$

where $U_g\mathsf{S}U_g^\dagger=\{U_g\rho U_g^\dagger | \rho\in\mathsf{S}\}$. It is important to stress that here, in contrast to the usual definition, we do not require the

*Also at Center for Photonic Communication and Computing, Department of Electrical and Computer Engineering, Northwestern University, Evanston, IL 60208.

set S to be the group orbit of a fixed input state $\rho_0 \in \mathsf{S}$, that is, $\mathsf{S}=\{U_g \rho_0 U_g^\dagger | g \in \mathbf{G}\}$. In fact, in what follows, the sole invariance of the set S will be sufficient.

The quality of the cloning machine is judged by introducing a figure of merit, usually the Uhlmann fidelity [18], which measures how close the joint output state $\mathcal{M}(\rho)$ is to two exact copies of the input state ρ. Sometimes, instead, it is more interesting to evaluate the single-clone fidelity, which measures how close the state of each clone is to the input state ρ. The results we are going to present hold for both kinds of fidelity and, more generally, for any figure of merit $F[\rho, \mathcal{M}(\rho)]$ satisfying the invariance property

$$F[U_g \rho U_g^\dagger, \quad U_g^{\otimes 2} \mathcal{M}(\rho) U_g^{\dagger \otimes 2}] = F[\rho, \mathcal{M}(\rho)], \tag{2}$$

for any $g \in \mathbf{G}$.

In this setting, the optimization problem is to maximize the average value of the figure of merit

$$\langle F \rangle = \int_S \mathrm{d}\mu(x) F[\rho_x, \mathcal{M}(\rho_x)], \tag{3}$$

where x parametrizes the input states and $\mathrm{d}\mu(x)$ is an invariant probability distribution over the set of input states, i.e.,

$$\mathrm{d}\mu(gx) = \mathrm{d}\mu(x), \quad \forall\, g \in \mathbf{G}, \quad \forall\, x \in \mathsf{S}. \tag{4}$$

B. Covariance condition

As a consequence of the invariance of the set of input states (1), of the figure of merit (2), and of the probability distribution (4), there is no loss of generality in assuming the cloning machine $\mathcal{M}$ to be *covariant*, that is

$$\mathcal{M}(U_g \rho U_g^\dagger) = U_g^{\otimes 2} \mathcal{M}(\rho) U_g^{\dagger \otimes 2}, \quad \forall\, g \in \mathbf{G}, \quad \forall\, \rho. \tag{5}$$

In fact, for any noncovariant cloning machine $\mathcal{N}$, there is always a covariant one which has the same average fidelity, namely $\mathcal{M}=\int \mathrm{d}g U_g^{\dagger \otimes 2} \mathcal{N}(U_g \rho U_g^\dagger) U_g^{\dagger 2}$, where $\mathrm{d}g$ is the normalized Haar measure on the group.

A convenient tool for the study of optimal cloning is the formalism of quantum operations (QO). A cloning machine is described by a completely positive trace-preserving map $\mathcal{M}$ that takes states in a Hilbert space $\mathcal{H}$ to states in the Hilbert space $\mathcal{H} \otimes \mathcal{H}$. According to Refs. [19,20], this map $\mathcal{M}$ can be put in one-to-one correspondence with a positive operator R on $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, where the indices 1 and 2 stand for the two output clones, while index 3 stands for the input system (all spaces are isomorphic to $\mathcal{H}$). Specifically, by fixing a basis $\mathcal{B}=\{|n\rangle | n=1, \ldots, d\}$ for the d-dimensional Hilbert space $\mathcal{H}$, the correspondence is given by

$$R = (\mathcal{M} \otimes \mathbb{1}) |\mathbb{1}\rangle\rangle\langle\langle \mathbb{1}|, \tag{6}$$

where $|\mathbb{1}\rangle\rangle \in \mathcal{H}^{\otimes 2}$ is (up to normalization) the maximally entangled state $|\mathbb{1}\rangle\rangle = \Sigma_{n=1}^d |n\rangle|n\rangle$. In terms of the operator R, the action of the QO on states is given by

$$\mathcal{M}(\rho) = \mathrm{Tr}_3[\mathbb{1}_1 \otimes \mathbb{1}_2 \otimes \rho_3^T R], \tag{7}$$

where T denotes transposition with respect to the fixed basis $\mathcal{B}$.

Notice that, since the map $\mathcal{M}$ is completely positive, the operator R defined by Eq. (6) is positive. Moreover, according to Eq. (7), the trace-preservation condition $\mathrm{Tr}[\mathcal{M}(\rho)] = 1 \,\forall\, \rho$ becomes

$$\mathrm{Tr}_{1,2}[R] = \mathbb{1}_3, \tag{8}$$

that is, the trace of R over the two output spaces gives the identity in the input space. Finally, the covariance condition (5) translates into [20]

$$[R, U_g \otimes U_g \otimes U_g^*] = 0, \quad \forall\, g \in \mathbf{G}, \tag{9}$$

with $*$ denoting complex conjugation with respect to the fixed basis $\mathcal{B}$.

C. Strong covariance condition

In this section, we introduce a stronger requirement than simple covariance, which we will call *strong covariance*. This requirement concerns the unitary realization of the cloning machine with an ancilla, and corresponds to imposing that the ancilla transforms under the action of the group as the time reversal of the transformation undergone by each of the two clones.

The explicit form of the strong covariance condition can be introduced by purifying the QO describing the cloning machine. The operator R introduced in Eq. (6) is (up to normalization) the output state resulting from the application of the map $\mathcal{M}$ on a maximally entangled state. Such an output state is not pure in general, but it can always be purified by introducing an ancillary system. In this way, the QO is realized as a unitary transformation (isometry) on the extended Hilbert space. Let us define $|\Psi\rangle \in \mathcal{H}^{\otimes 4}$ as the (normalized) pure state of the two clones, the input system, and the ancilla after the cloning transformation. The operator R of Eq. (6) is then given by

$$R = d\, \mathrm{Tr}_4[|\Psi\rangle\langle\Psi|], \tag{10}$$

the index 4 denoting the ancilla.

We say that the unitary realization of a cloning machine is *strongly covariant* if the joint output state $|\Psi\rangle$ satisfies the property [21]

$$U_g \otimes U_g \otimes U_g^* \otimes U_g^* |\Psi\rangle = |\Psi\rangle, \quad \forall\, g \in \mathbf{G}. \tag{11}$$

In other words, a strongly covariant realization of cloning requires that (i) the ancilla transforms under the group with the time-reversed unitary U_g^*, and (ii) the joint output state is invariant under the action of the group. From a physical point of view, this corresponds intuitively to assuming a kind of “conservation law” in the cloning process, where the ancilla undergoes a time-reversed transformation in order to balance the corresponding transformation of the two clones.

We will name as *strongly covariant* a map that admits a strongly covariant unitary realization. It is easy to see that a strongly covariant map is always covariant, but the converse is not necessarily true. The puzzle is now that all the known optimal covariant cloners satisfy this additional property. In the following, we will investigate the meaning of this strong covariance condition, showing in particular that the strongly covariant maps coincide with the extremal covariant maps in the case of the (discrete or continuous) Weyl-Heisenberg group, which happens to be a symmetry of the set of input states in the vast majority of cloners considered in the literature.

III. EXTREMAL COVARIANT CLONING MACHINES

A. Characterization of extremal covariant QOs

The set of covariant QO is a convex set, namely the convex combination of two such QO is still a covariant QO. In the same way, the set of positive operators R defined by (6) and satisfying the relations (8) and (9) is a convex set. We will call $\mathcal{C}$ such a convex set of "covariant operators".

Since for a pure input state the Uhlmann fidelity—either global or single-clone—is a linear functional of the QO, the search for the optimal covariant cloner can be restricted without loss of generality to the extremal points of this convex set, i.e., those QOs that cannot be written as convex combinations of other QOs. The convex structure of the set of covariant QOs then greatly simplifies the optimization problem. Although finding a characterization of the extremal covariant maps is, in general, a rather complicated issue [15–17], here we can give a simple characterization of the extremal covariant maps in the special case where the representation $\{U_g | g \in \mathbf{G}\}$ acting on the input states is irreducible.

In order to deal with the covariance condition (9), it is useful to decompose the Hilbert space $\mathcal{H}^{\otimes 3}$ into irreducible subspaces

$$\mathcal{H}^{\otimes 3} = \bigoplus_{\mu \in \mathsf{D}} \bigoplus_{i=1}^{m_\mu} \mathcal{H}_i^{(\mu)}. \tag{12}$$

Here, the index μ runs over the set D of the inequivalent representations that show up in the Clebsch-Gordan decomposition of the representation $\{U_g \otimes U_g \otimes U_g^*\}$, while the index i distinguishes m_μ different subspaces carrying equivalent representations. We recall that, by definition, two irreducible subspaces $\mathcal{H}_i^{(\mu)}$ and $\mathcal{H}_j^{(\mu)}$ of a given representation $\{V_g\}$ carry equivalent representations if and only if there exists an isomorphism $T_{ij}^{(\mu)}:\mathcal{H}_j^{(\mu)} \to \mathcal{H}_i^{(\mu)}$ such that $[T_{ij}^{(\mu)}, V_g] = 0$, $\forall g \in \mathbf{G}$.

Using Schur's lemma, it is possible to prove (see, e.g., Ref. [20]) that the general expression of a positive operator satisfying the commutation relation (9) is

$$R = \bigoplus_{\mu \in \mathsf{D}} \bigoplus_{i,j} r_{ij}^{(\mu)} T_{ij}^{(\mu)}, \tag{13}$$

where each $r^{(\mu)}$ is a positive $m_\mu \times m_\mu$ matrix. Moreover, by diagonalizing the matrix $r^{(\mu)}$, we can write

$$R = \bigoplus_{\mu \in \mathsf{D}} \bigoplus_{i} \lambda_i^{(\mu)} P_i^{(\mu)}, \tag{14}$$

where $\lambda_i^{(\mu)} \geqslant 0$, and $P_i^{(\mu)}$ is the projection onto an irreducible subspace $\mathcal{K}_i^{(\mu)}$ carrying the representation μ. The diagonalization of the matrix $r_{ij}^{(\mu)}$ corresponds to switching from the decomposition (12) to a *new decomposition* of the Hilbert space $\mathcal{H}^{\otimes 3}$

$$\mathcal{H}^{\otimes 3} = \bigoplus_{\mu \in \mathsf{D}} \bigoplus_{i=1}^{m_\mu} \mathcal{K}_i^{(\mu)}, \tag{15}$$

where $\{\mathcal{K}_i^{(\mu)}\}$ is a new set of irreducible subspaces. In fact, due to the presence of equivalent representations, there is a freedom in the choice of irreducible subspaces that decompose the Hilbert space [14].

Theorem 1. *If the representation $\{U_g\}$ is irreducible, then a covariant operator $R \in \mathcal{C}$ is extremal if and only if it is proportional to a projection onto an irreducible subspace, namely*

$$R = \frac{d}{d_\mu} P_i^{(\mu)}, \tag{16}$$

where $P_i^{(\mu)}$ is the projection onto the irreducible subspace $\mathcal{K}_i^{(\mu)}$ whose dimension is d_μ.

Proof. Let R be a covariant operator in $\mathcal{C}$. Since R is a positive operator commuting with the group action (9), it has the form (14) with a suitable decomposition of the Hilbert space. On the other hand, any projection $P_i^{(\mu)}$ in the sum satisfies $[P_i^{(\mu)}, U_g^{\otimes 2} \otimes U_g^*] = 0$ $\forall g$; therefore, its partial trace $\mathrm{Tr}_{1,2}[P_i^{(\mu)}]$ commutes with the irreducible representation $\{U_g^*\}$. By Schur's lemma, the partial trace is proportional to the identity in $\mathcal{H}_3$, namely $\mathrm{Tr}_{1,2}[P_i^{(\mu)}] = k_\mu \mathbb{1}_3$. Taking traces on both sides, we can evaluate the proportionality constant, $k_\mu = d_\mu / d$. As a consequence, any positive operator defined by $R_i^{(\mu)} = (d/d_\mu) P_i^{(\mu)}$ satisfies both (8) and (9), when it is itself a covariant operator in $\mathcal{C}$. On the other hand, Eq. (14) yields the convex decomposition of R in terms of the extremal points $\{R_i^{(\mu)}\}$ proportional to the orthogonal projectors $P_i^{(\mu)}$. ■

Remark. When the set of input states is invariant under an irreducible representation, Theorem 1 greatly simplifies the search for optimal cloners, since one just needs to find the irreducible subspaces $\mathcal{K}_i^{(\mu)}$ of $\mathcal{H}^{\otimes 3}$ and find out which operator $R_i^{(\mu)}$ projecting on $\mathcal{K}_i^{(\mu)}$ maximizes the fidelity.

B. Characterization of strongly covariant QOs

Theorem 1 allows understanding of the meaning of the strong covariance condition in the case where the group representation $\{U_g\}$ is irreducible. In this case, we will show that the strongly covariant maps form a special subset of the set of extremal covariant QOs.

Theorem 2. *Denote by ω the irreducible representation $\{U_g\}$ transforming the input states. Then, the strong covariance condition amounts to restricting to extremal QOs of the form*

$$R = P_i^{(\omega)}. \tag{17}$$

In other words, the strongly covariant maps are the extremal maps with $\mu = \omega$ in Eq. (16). (Notice that, by definition, $d/d_\omega = 1$.) To find such maps, one has to select among the irreducible subspaces of $\mathcal{H}^{\otimes 3}$ those carrying a representation equivalent to $\{U_g\}$ (the representation transforming the input states).

Proof. Consider a pure joint state $|\Psi\rangle \in \mathcal{H}^{\otimes 4}$ satisfying the strong covariance condition (11). Since any $P_i^{(\mu)} \in \mathcal{B}(\mathcal{H}^{\otimes 3})$ in

(14) commutes with the representation $\{U_g^{\otimes 2}\otimes U_g^*\}$, the vector $|\Psi_i^{(\mu)}\rangle=(P_i^{(\mu)}\otimes\mathbb{1})|\Psi\rangle$ also satisfies the strong covariance condition, namely

$$U_g^{\otimes 2}\otimes U_g^{*\otimes 2}|\Psi_i^{(\mu)}\rangle=|\Psi_i^{(\mu)}\rangle, \quad \forall\, g\in\mathbf{G}. \tag{18}$$

On the other hand, $|\Psi_i^{(\mu)}\rangle$ transforms with the representation $\mu\otimes\omega^*$, corresponding to $P_i^{(\mu)}(U_g^{\otimes 2}\otimes U_g^*)P_i^{(\mu)}$ for μ and U_g^* for ω^*. Therefore, the Clebsch-Gordan series of $\mu\otimes\omega^*$ must contain the trivial representation μ_0, where the action of any group element is given by multiplication by the number 1. In terms of the characters $\chi_\mu(g)$, $\chi_\omega(g)$, and $\chi_{\mu_0}(g)\equiv 1$ of the three representations, this amounts to saying that the character of the trivial representation is not orthogonal to the character of the tensor product $\mu\otimes\omega^*$, namely

$$\langle\chi_{\mu_0},\chi_\mu\times\chi_\omega^*\rangle=\int_{\mathbf{G}} \mathrm{d}g\;\chi_\mu(g)\chi_\omega^*(g)\neq 0. \tag{19}$$

Since the characters of irreducible representations are orthonormal, the value of the integral (19) is the Kronecker delta $\delta_{\mu\omega}$. Therefore, the tensor product $\mu\otimes\omega^*$ contains the trivial representation μ_0 if and only if $\mu=\omega$. According to this, the operator $R=d\,\mathrm{Tr}_4[|\Psi\rangle\langle\Psi|]$ must have a special block form

$$R=\bigoplus_i \lambda_i^{(\omega)}P_i^{(\omega)}, \tag{20}$$

that is, the sum (14) runs only on the projections with $\mu=\omega$. Finally, we can prove that R is also extremal. Since $R=d\,\mathrm{Tr}_4[|\Psi\rangle\langle\Psi|]$, the rank of R is the Schmidt number of the pure state $|\Psi\rangle$ with respect to the bipartition ancilla versus clones+input, where it cannot be larger than the dimension of the ancilla, that is, $\mathrm{rank}(R)\leqslant d$. On the other hand, from Eq. (20), we have $\mathrm{rank}(R)=d\times n$, where n is the number of blocks in the direct sum. By comparison, we obtain $n=1$, i.e., R is proportional to just one irreducible projection. Exploiting the characterization of Theorem 1, we know that such an operator is extremal. ■

Remark. Theorem 2 thus implies that imposing strong covariance instead of covariance corresponds to considering a special class of extremal covariant QOs. In general, an extremal covariant map with respect to some group is not necessarily strongly covariant with respect to that group. However, strong covariance becomes simply equivalent to covariance together with extremality in the special case of the discrete Weyl-Heisenberg group. This is the topic of the next section.

IV. EXTREMAL CLONERS FOR THE WEYL-HEISENBERG GROUP

A. Covariance vs strong covariance

Let us consider the class of cloning machines characterized by the fact that the set of states S to be cloned is invariant under the discrete Weyl-Heisenberg group, namely the set of unitary operators

$$U_{pq}=\sum_{k=0}^{d-1} e^{(2\pi i/d)kq}|k\oplus p\rangle\langle k|, \quad p,q=0,\ldots,d-1, \tag{21}$$

where $\{|k\rangle\,|\,k=0,\ldots,d-1\}$ is an orthonormal basis of a d-dimensional Hilbert space, and $\oplus$ denotes the addition modulo d. This class includes for instance the universal cloning machines [4], the Fourier-covariant cloning machines [11], or the phase-covariant cloning machines [7,13,22–25], as well as these three cases for generic asymmetry between the clones. Indeed, in all these cases, due to the invariance of the set of input states one can assume without loss of generality that the cloner is covariant under the Weyl-Heisenberg group.

Theorem 3. *For the discrete Weyl-Heisenberg group, all extremal covariant cloners are also strongly covariant.*

Proof. Since the action of the discrete Weyl-Heisenberg group is irreducible in the d-dimensional Hilbert space $\mathcal{H}$, we can exploit the characterization of Theorem 1. The decomposition (12) of the Hilbert space $\mathcal{H}^{\otimes 3}$ into irreducible subspaces of the representation $\{U_{pq}\otimes U_{pq}\otimes U_{pq}^*\}$ now reads

$$\mathcal{H}^{\otimes 3}=\bigoplus_{r,s=0}^{d-1}\mathcal{H}_{rs}, \tag{22}$$

where

$$\mathcal{H}_{rs}=\mathcal{H}\otimes|U_{rs}\rangle\rangle. \tag{23}$$

Here, $\mathcal{H}\otimes|U_{rs}\rangle\rangle$ denotes the subspace of vectors of the form $|\psi\rangle|U_{rs}\rangle\rangle$, where $|\psi\rangle\in\mathcal{H}$ and

$$|U_{rs}\rangle\rangle=\sum_{k=0}^{d-1}e^{(2\pi i/d)ks}|k\oplus r\rangle|k\rangle \tag{24}$$

are the d-dimensional Bell states. The orthogonal subspaces $\mathcal{H}_{rs}$ all carry the same representation, namely for any couple of spaces $\mathcal{H}_{rs}$ and $\mathcal{H}_{r's'}$, one has the isomorphism

$$T_{rs,r's'}=\frac{1}{d}U_{rs}^\dagger U_{r's'}\otimes|U_{rs}\rangle\rangle\langle\langle U_{r's'}|, \tag{25}$$

that commutes with the representation $\{U_{pq}^{\otimes 2}\otimes U_{pq}^*\}$. Moreover, since $U_{pq}\otimes U_{pq}^*|\mathbb{1}\rangle\rangle=|\mathbb{1}\rangle\rangle$, $\forall p,q$, the space $\mathcal{H}_{00}=\mathcal{H}\otimes|\mathbb{1}\rangle\rangle$ carries the representation $\{U_{pq}\}$. Summarizing, all irreducible subspaces in the decomposition of $\mathcal{H}^{\otimes 3}$ carry the same representation, which is equivalent to $\{U_{pq}\}$, the representation acting on the input states. Therefore, all the extremal maps in Theorem 1 are also strongly covariant, according to Theorem 2. ■

The result of Theorem 3 shows that, if the set of input states is invariant with respect to the discrete Weyl-Heisenberg group, then one can assume strong covariance without loss of generality, since it provides a parametrization of all extremal covariant QO. Moreover, in the following we will see that the the strongly covariant cloning machines (with respect to the discrete Weyl-Heisenberg group) can be parametrized in terms of "double-Bell" states, thus explaining with a general argument the presence of a recurrent structure that characterizes the known optimal cloners.

B. Parametrization with double-Bell states

Using Theorem 3, we can parametrize explicitly all the extremal quantum cloning transformations that are covariant with respect to the discrete Weyl-Heisenberg group. Since the operator R associated with an extremal map is the projection onto an irreducible subspace [see Eq. (17)], it is enough to write the most general form of such a projection, which has the form

$$P_{\mathbf{a}} = \sum_{r,s,r',s'=0}^{d-1} a_{rs} a^{*}_{r's'} T_{rs,r's'}, \tag{26}$$

with $\mathbf{a}=\{a_{rs}\}$ such that $\Sigma_{r,s}|a_{rs}|^2=1$. Remarkably, the irreducible projections are in one-to-one correspondence with the pure states in $\mathcal{H}\otimes\mathcal{H}$. As a matter of fact, the convex structure of covariant QOs is exactly the same as the convex structure of states on $\mathcal{H}\otimes\mathcal{H}$.

By inserting Eq. (25) in Eq. (26), we obtain

$$R = \sum_{r,s,r',s'=0}^{d-1} \frac{a_{rs}a_{r's'}}{d} U^{\dagger}_{rs} U_{r's'} \otimes |U_{rs}\rangle\rangle\langle\langle U_{r's'}|, \tag{27}$$

thus giving the explicit parametrization of a generic extremal covariant map. Finally, by purifying R we can characterize the (strongly covariant) unitary realization of the extremal cloning machine with the pure output state of the double-Bell form

$$|\Psi\rangle = \sum_{r,s=0}^{d-1} a_{rs} \frac{|U^{\dagger}_{rs}\rangle\rangle_{1,4}}{\sqrt{d}} \frac{|U_{rs}\rangle\rangle_{2,3}}{\sqrt{d}}. \tag{28}$$

This proves the double-Bell ansatz [9,10], which captures the characteristic feature of all the above-mentioned optimal cloners [4,7,11,13,22,24,25]. The expression (28) for the optimal cloner can then be assumed without loss of generality whenever the set of input states is invariant under the Weyl-Heisenberg group. Indeed, such an invariance is very common, therefore the form (28) covers most of the one-to-two cloning machines considered in the literature. Moreover, Theorem 3 and the double-Bell form can be extended in a direct way to the case of the continuous Weyl-Heisenberg group in infinite dimension (see Sec. IV E).

C. Optimal qubit cloners

In this section we review the main examples of qubit cloners in the framework drawn in the previous sections. Theorem 3 greatly simplifies the search for optimal cloners, and explains some interesting relations among different cloning machines.

1. Cloning of the BB84 states

The study of the optimal cloning as a possible cryptographic attack is crucial for the security analysis of the BB84 cryptographic protocol. In this case, the aim of an eavesdropper is to clone with the same fidelity two mutually unbiased bases, corresponding to the eigenvectors of the Pauli matrices σ_x and σ_y. Such discrete set of states describes a square in the equatorial plane of the Bloch sphere, and it is clearly invariant under the action of the discrete Weyl-Heisenberg group, which in dimension 2 is just the Pauli group

$$U_{0,0} = \mathbb{1}, \quad U_{0,1} = \sigma_z, \quad U_{1,0} = \sigma_x, \quad U_{1,1} = -i\sigma_y. \tag{29}$$

Using the double-Bell form (28), and optimizing coefficients, one finds the optimal asymmetric cloner of Ref. [12]

$$\begin{aligned}|\Psi\rangle = \frac{1}{2}\{&F_B|\mathbb{1}\rangle\rangle_{1,4}|\mathbb{1}\rangle\rangle_{2,3} + (1-F_B)|\sigma_z\rangle\rangle_{1,4}|\sigma_z\rangle\rangle_{2,3}\\ &+ \sqrt{F_B(1-F_B)}(|\sigma_x\rangle\rangle_{1,4}|\sigma_x\rangle\rangle_{2,3} + |\sigma_y\rangle\rangle_{1,4}|\sigma_y\rangle_{2,3})\}.\end{aligned} \tag{30}$$

Here, F_B is the fixed fidelity of Bob's clone (Hilbert space $\mathcal{H}_2$). The fidelity of Eve's clone is given by $F_E=1/2+\sqrt{F_B(1-F_B)}$, so that the symmetric cloner has a fidelity $1/2+1/\sqrt{8}$.

2. Phase-covariant qubit cloning

The general theory allows us to assume again the double-Bell expression of Eq. (28), since the equatorial states $1/\sqrt{2}(|0\rangle+e^{i\phi}|1\rangle)$ are invariant under the action of the Pauli group. This implies that the asymmetric cloning obtained in Ref. [12] is actually optimal, and in particular, the popular conjecture that phase-covariant equatorial cloning [22] is indeed equivalent to the BB84-states cloning [12] is now proved. Clearly, the double-Bell form is exactly the same as in Eq. (30).

3. Six states cloning

This cloning problem is linked to the security of the six-state quantum cryptographic protocol [26]. The states to be cloned are the six eigenstates of the three Pauli matrices, which are invariant under the Pauli group (i.e., the discrete Weyl-Heisenberg group in dimension 2). Therefore, one can use again the double-Bell form, and the expression for the optimal asymmetric cloning is [10]

$$\begin{aligned}|\Psi\rangle = \frac{1}{2}\Bigg\{&\sqrt{\frac{3F_B-1}{2}}|\mathbb{1}\rangle\rangle_{1,4}|\mathbb{1}\rangle\rangle_{2,3}\\ &+\sqrt{\frac{1-F_B}{2}}\left(\sum_{i=1}^{3}|\sigma_i\rangle\rangle_{1,4}|\sigma_i\rangle\rangle_{2,3}\right)\Bigg\},\end{aligned} \tag{31}$$

where F_B is the fixed fidelity of Bob's clone. The fidelity of Eve's clone is then given by $F_E=1-F_B/2+\sqrt{(3F_B-1)(1-F_B)}/2$, so that the symmetric cloner has the fidelity $5/6$.

4. Universal cloning

In the case of universal cloning, it is straightforward to see that the set of input states (the whole surface of the Bloch sphere) is invariant under the Pauli group. Similarly to the case of phase-covariant cloning, using the double-Bell form (28), we obtain the same optimal cloner as in the case of the six states, thus proving the equivalence between the six-state cloning and the universal cloning. Accordingly, the double-

Bell expression for the optimal universal cloner is the same as in Eq. (31).

5. Cubic cloning

Using the present method, we can analyze easily all cloning problems with the set of input states invariant under the Pauli group, which in the Bloch sphere corresponds to invariance under π rotation around the three reference axes. As a new example, let us consider the cloning of eight pure states forming a cube in the Bloch sphere. By performing a suitable rotation, we can always bring the vertexes of the cube in the positions specified by the Bloch vectors $\{\pm 1/\sqrt{3}, \pm 1/\sqrt{3}, \pm 1/\sqrt{3}\}$, so that the states to be cloned become

$$\rho = \frac{1}{2}\left(\mathbb{1} \pm \frac{1}{\sqrt{3}}\sigma_x \pm \frac{1}{\sqrt{3}}\sigma_y \pm \frac{1}{\sqrt{3}}\sigma_z\right). \tag{32}$$

This set of states is clearly invariant under the Pauli group. Starting from a general double-Bell form

$$|\Psi\rangle = \frac{1}{2}\sum_{i=0}^{3} a_i |\sigma_i\rangle\rangle_{1,4}|\sigma_i\rangle\rangle_{2,3}, \tag{33}$$

where $\sigma_0 = \mathbb{1}$ and $\Sigma_i |a_i|^2 = 1$, one gets the following expressions for the fidelities of the two clones:

$$F_B = |a_0|^2 + \frac{1}{3}\sum_{i=1}^{3}|a_i|^2, \quad F_A = \frac{2}{3} + \frac{1}{3}\left|\sum_{i=0}^{3} a_i\right|^2. \tag{34}$$

It is clear that one can take all the coefficients a_i as non-negative without affecting F_B, and seek the maximum of F_A only for $a_i \geqslant 0$. Using the method of Lagrange multipliers, one can then maximize F_B for fixed F_B, thus obtaining

$$a_0 = \sqrt{\frac{3F_B - 1}{2}}, \quad a_i = \sqrt{\frac{1 - F_B}{2}}. \tag{35}$$

Comparing these values with the corresponding ones in Eq. (31), we see that the optimal cloning of a cube in the Bloch sphere is performed by the same machine that gives the optimal cloning of the six-state- and the optimal universal cloning.

D. Optimal *d*-dimensional cloners

1. Cloning of two Fourier-transformed bases

The d-dimensional generalization of the cloning of BB84 states gives rise to the problem of cloning two bases that are Fourier transformed, namely the computational basis $\{|m\rangle\}$ and the dual basis $\{|e_m\rangle\}$, where

$$|e_m\rangle = \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1} e^{2\pi i m p/d}|p\rangle. \tag{36}$$

The invariance of S under the action of the discrete Heisenberg group is straightforward, and the optimal asymmetric cloning corresponds to the following double-Bell form [11]:

$$|\Psi\rangle = \frac{1}{d}\left\{ F_B|\mathbb{1}\rangle\rangle|\mathbb{1}\rangle\rangle + \frac{1-F_B}{d-1}\sum_{p,q=1}^{d-1}|U_{pq}^{\dagger}\rangle\rangle|U_{pq}\rangle\rangle + \sqrt{\frac{F_B(1-F_B)}{d-1}}\sum_{p=1}^{d-1}\left(|U_{p0}^{\dagger}\rangle\rangle|U_{p0}\rangle\rangle + |U_{0p}^{\dagger}\rangle\rangle|U_{0p}\rangle\rangle\right)\right\}. \tag{37}$$

The fidelity of Eve's clone is given by

$$F_E = \frac{F_B}{d} + \frac{(d-1)(1-F_B)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)}, \tag{38}$$

so that the symmetric cloner has the fidelity $(1+1/\sqrt{d})/2$.

2. Multiple phase-covariant cloning

The optimal cloning of states of the form $(1/\sqrt{d})(|0\rangle + \Sigma_{k=1}^{d-1} e^{i\phi_k}|k\rangle)$ fits the constraints for the validity of the double-Bell form, since the set S is clearly invariant under the discrete Heisenberg group. For the double-Bell form for the optimal cloner, see Ref. [13].

3. Universal cloning

In this case, the set S of states to be cloned is the whole set of pure states in a d-dimensional Hilbert space, which is clearly invariant under all the unitaries in the discrete Weyl-Heisenberg group. The optimal universal cloning [2,4] corresponds indeed to the following double-Bell form:

$$|\Psi\rangle = \frac{1}{d}\left\{ \sqrt{\frac{(d+1)F_B - 1}{d}}|\mathbb{1}\rangle\rangle_{1,4}|\mathbb{1}\rangle\rangle_{2,3} + \sqrt{\frac{1-F_B}{d(d-1)}}\sum_{(p,q)\neq(0,0)}|U_{p,q}^{\dagger}\rangle\rangle_{1,4}|U_{pq}\rangle\rangle_{2,3}\right\}, \tag{39}$$

as derived in Ref. [10]. The fidelity of Eve's clone is given by

$$F_E = 1 - \frac{(d^2-2)F_B + 2 - d}{d^2} + \frac{2\sqrt{d-1}}{d^2}\sqrt{(1-F_B)[(d+1)F_B - 1]}, \tag{40}$$

so that the symmetric cloner has a fidelity $F = 1/2 + 1/(d+1)$.

E. Cloning of continuous variables

Theorem 3 and the double-Bell form can be extended to the continuous-variable case, where the set of states to be cloned lies in an infinite dimensional Hilbert space and is invariant under the Weyl-Heisenberg representation of the displacements in the complex plane, i.e., under the set of unitaries

$$\{D(\alpha) = e^{\alpha a^{\dagger} - \bar{\alpha} a} | \alpha \in \mathbb{C}\}, \tag{41}$$

where $[a, a^{\dagger}] = 1$. The Weyl-Heisenberg representation can be regarded indeed as the continuous-variable version of the discrete Weyl-Heisenberg group, where the couple of integers (p,q) is replaced by the complex number $\alpha \in \mathbb{C}$. In this case, one can decompose the Hilbert space $\mathcal{H}^{\otimes 3}$ (two clones+input system) by substituting formally the direct sum (22) with a direct integral

$$\mathcal{H}^{\otimes 3} = \int_{\mathbb{C}} \mathrm{d}^2\alpha\, \mathcal{H}_\alpha, \tag{42}$$

where

$$\mathcal{H}_\alpha = \mathcal{H} \otimes |D(\alpha)\rangle\rangle, \tag{43}$$

and $|D(\alpha)\rangle\rangle = \Sigma_{m,n=0}^{\infty} \langle m|D(\alpha)|n\rangle|m\rangle|n\rangle$ for a fixed orthonormal basis $\{|n\rangle | n=0,1,\ldots\}$. The subspaces $\mathcal{H}_\alpha$ are orthogonal in the Dirac sense and carry all the same representation. The continuous variable version of the isomorphism (25) is

$$T_{\alpha\beta} = \frac{1}{\pi} D(\alpha)^\dagger D(\beta) \otimes |D(\alpha)\rangle\rangle\langle\langle D(\beta)|. \tag{44}$$

According to the characterization of Theorem 1 and generalizing (26), an extremal QO is then represented by

$$R = \int_{\mathbb{C}} \mathrm{d}^2\alpha \int_{\mathbb{C}} \mathrm{d}^2\beta\, \phi(\alpha)\phi^*(\beta)\; T_{\alpha\beta}, \tag{45}$$

where $\int_{\mathbb{C}} d^2\alpha\, |\phi(\alpha)|^2 = 1$. Again, the convex structure of covariant QO is the same as the convex structure of states on $\mathcal{H}\otimes\mathcal{H}$. Moreover, it is still possible to give the purification of the cloning machine as

$$|\Psi\rangle = \int_{\mathbb{C}} \mathrm{d}^2\alpha\, \phi(\alpha) \frac{|D(\alpha)^\dagger\rangle\rangle_{1,4}}{\sqrt{\pi}} \frac{|D(\alpha)\rangle\rangle_{2,3}}{\sqrt{\pi}}, \tag{46}$$

according to the continuous-variable version of the double-Bell ansatz. This special form of the unitary realization is indeed the unifying feature of the known continuous-variable cloners [5,6].

V. CONCLUSION

We have analyzed the problem of cloning a set of states that is invariant under the action of a given symmetry group. If we use a figure of merit that is invariant with respect to this group, such as the Uhlman fidelity, then the optimal cloning transformation (i.e., the transformation that maximizes the average fidelity over the set of input states) can be chosen to be group covariant. We have shown that substituting this covariance condition with a strong covariance condition implies that the resulting cloning transformation is extremal. The converse is not true in general, that is, an extremal covariant transformation is not necessarily strongly covariant. However, when the considered invariance group is the (discrete or continuous) Weyl-Heisenberg group, the converse also holds, so that the set of strongly covariant cloners is equivalent to the set of extremal covariant cloners. Since the covariant cloners form a convex set, and since the fidelity is linear in the cloning transformation, this equivalence greatly simplifies the search for optimal cloners: it is sufficient to search among the set of extremal cloners. Luckily, the set of strongly covariant (hence extremal) cloners with respect to the Weyl-Heisenberg group can be parametrized in a very compact form, which coincides with the so-called double-Bell ansatz. In this form, the cloner only depends on d^2 real parameters for a d-dimensional input state. As a consequence of the simplification of the optimization problem, one can easily derive a large variety of optimal cloning transformations. As an illustration of the power of the method, we proved the optimality of several cloners that have been described in the literature, including the continuous-variable cloners. As a side result, we proved that the optimal cloner of the four states involved in the BB84 protocol (six states involved in the six-state protocol) is the phase-covariant (universal) cloner. We also showed that the optimal cloner of any eight states forming a cube on the Bloch sphere is the universal cloner.

ACKNOWLEDGMENTS

This work has been supported by INFM under PRA-2002-CLON, and has been cofunded by the EC and Ministero Italiano dell'Università e della Ricerca (MIUR) through the cosponsored ATESIT project IST-2000-29681 and Cofinanziamento 2003. G.M.D. acknowledges partial support from the Multiple Universities Research Initiative (MURI) program administered by the U.S. Army Research Office under Grant No. DAAD1900-1-0177. N.J.C. also acknowledges hospitality of the QUIT group, as well as partial support from MIUR, from the Action de Recherche Concertée de la Communauté Française de Belgique, from the IUAP program of the Belgian Federal Governement under Grant V-18, and from the EC through projects RESQ (IST-2001-37559) and SECOQC (IST-2003-506813).

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).

[2] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[3] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[4] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).

[5] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).

[6] N. J. Cerf and S. Iblisdir, Phys. Rev. Lett. **87**, 247903 (2001).

[7] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).

[8] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).

[9] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); Proc. First NASA International Conference QCQC'98, Palm Springs, February 1998.

[10] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); J. Mod. Opt. **47**,

187 (2000).

[11] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[12] N. J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002).

[13] L.-P. Lamoureux and N. J. Cerf, Quantum Inf. Comput. **5**, 32 (2005).

[14] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. A **70**, 062105 (2004).

[15] H. Scutaru, Rep. Math. Phys. **16**, 79 (1979).

[16] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).

[17] G. M. D'Ariano, J. Math. Phys. **45**, 3620 (2004).

[18] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1974).

[19] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[20] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (1998).

[21] P. Navez and N. J. Cerf, Phys. Rev. A **68**, 032313 (2003).

[22] D. Bruss, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).

[23] H. Fan, H. Imai, K. Matsumoto, and X.-B. Wang, Phys. Rev. A **67**, 022317 (2003).

[24] F. Buscemi, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).

[25] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **60**, 2764 (1999).

[26] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).