Economical realization of phase-covariant devices in arbitrary dimensions (Invited)

Francesco Buscemi, Giacomo Mauro D'Ariano, and Chiara Macchiavello

Quantum Information Theory Group, Dipartimento di Fisica "A. Volta," Università di Pavia, via Bassi 6, I-27100 Pavia, Italy

Received May 19, 2006; accepted June 5, 2006;
posted July 27, 2006 (Doc. ID 71095); published January 26, 2007

We describe a unified framework of phase-covariant multiuser quantum transformations for d-dimensional quantum systems. We derive the optimal phase-covariant cloning and transposition transformations for multiphase states. We show that for some particular relations between the input and output number of copies, they correspond to economical transformations, which can be achieved without the need of auxiliary systems. We prove a relation between the optimal phase-covariant cloning and transposition maps and optimal estimation of multiple phases for equatorial states. © 2007 Optical Society of America

OCIS codes: 000.1600, 000.3860, 270.0270.

1. INTRODUCTION

The possibility of employing quantum systems with a (finite) dimension higher than two in quantum information has recently triggered much interest. In particular, it has been shown that an increase in the dimension leads to a better performance of various quantum information protocols, such as, for example, quantum cryptography[1–3] and some problems in distributed quantum computing.[4] Moreover, considerable experimental progress has been recently reported in the generation, manipulation, and detection of quantum systems with higher dimensions.[5–7]

In this work we consider the case of phase-covariant transformations where the information is encoded into phase properties of states with arbitrary finite dimension d. Encoding information into phase shifts has important applications in quantum computation and quantum information. For example, it was shown that the existing quantum algorithms can be described in a unified way as quantum interference processes among different computational paths where the result of the computation is retrieved from a phase shift.[8]

We will describe in a unified framework the features of multiuser phase-covariant transformations in arbitrary dimension d, where typically an arbitrary number of input systems N described by the same quantum state is transformed into a larger number of output systems M, which are still described by the same output density operators. We will then specify this description to two tasks of interest in quantum information, namely, cloning and phase conjugation.

The no-cloning theorem[9] states the impossibility of perfectly cloning unknown quantum states selected from a nonorthogonal set and is the basis of the security of quantum cryptography.[10,11] Approximate quantum cloning has been extensively studied in past years[12] and has led to relevant results in quantum cryptography. The eavesdropping strategies in quantum key distribution protocols that are known to be optimal so far are actually based on cloning attacks.[2,3,13,14] Moreover, quantum cloning allows one to study the sharing of quantum information among several parties and it may be applied also to study the security of multiparty cryptographic schemes.[15]

Perfect phase conjugation of the density operator of an unknown input state, or equivalently ideal time reversal, is also forbidden by the laws of quantum mechanics. Such a transformation has also recently attracted much interest in connection with the problem of entanglement, in regards to the so-called positive partial transpose criterion.[16,17] Since phase conjugation cannot be achieved unitarily, one can try to approximate the transformation with a physical channel, optimizing the fidelity of the output state with the complex-conjugated input. In the case of qubits ($d=2$), phase conjugation is unitarily equivalent to the NOT operation.[18] For the set of all pure states the resulting universal optimal channel is classical,[18,19] namely, it can be achieved by state estimation followed by state preparation. In contrast, as we will show in this paper, for equatorial pure states the optimal phase-covariant conjugation map is a purely quantum transformation (for any number of input copies), generalizing to the case of many copies the analogous result already proved for a single input system.[20]

The paper is organized as follows. In Section 2 we describe in a unified framework the operation of multiuser phase-covariant transformations in arbitrary finite dimension d. In Section 3 we review the concept of economical maps. In Sections 4 and 5 we derive the optimal phase-covariant cloning and phase conjugation maps, respectively, for equatorial input states, and show that for some particular relations between the input and output number of copies the optimal transformations can be achieved economically. In Section 6 we prove a relation between optimal multiple-phase estimation procedures and the optimal cloning and phase conjugation maps. In

Section 7 we summarize the results presented in this paper. Some technical details of the derivations presented in the paper are explained in the Appendixes.

2. PHASE-COVARIANT DEVICES

In this paper we consider quantum devices, or channels (i.e., trace preserving completely positive maps[21]), from states on an input quantum system $\mathcal{H}_{\text{in}}$ to states on a generally different output quantum system $\mathcal{H}_{\text{out}}$, for which we assume that an underlying global symmetry under the action of the phase rotations group $\mathbb{U}(1)$ holds. More precisely, we will optimize the action of such devices on pure d-dimensional input states of the form

$$|\psi(\{\phi_j\})\rangle = \frac{1}{\sqrt{d}}(|0\rangle + e^{i\phi_1}|1\rangle + e^{i\phi_2}|2\rangle + \cdots + e^{i\phi_{d-1}}|d-1\rangle), \tag{1}$$

where $\{|0\rangle,\ldots,|d-1\rangle\}$ is a fixed orthonormal basis of a d-dimensional system $\mathcal{H}$, and the ϕ_j's are $(d-1)$ independent phases in the interval $[0,2\pi)$. Notice that the choice $\phi_0=0$ is not restrictive, since an overall phase is negligible. In the case of qubits, i.e., $d=2$, pure states as in Eq. (1) all lie on one equator of the Bloch sphere and they clearly form a set that is invariant under rotations around the fixed axis orthogonal to this equator. These rotations form a group that is isomorphic to the group $\mathbb{U}(1)$. For generic dimensions $d>2$, this geometrical picture is straightforwardly generalized by saying that pure states in Eq. (1) form a set of states that is invariant under the action of the unitary representation $U_{\{\phi_j\}}=|0\rangle\langle 0|+\Sigma_{j=1}^{d-1}|j\rangle\langle j|e^{i\phi_j}$ of the group $\mathbb{U}(1)^{\times(d-1)}$. In the following, with a little abuse of terminology, we will call states of the form of Eq. (1) as equatorial states, also in the case $d>2$. Notice that starting from a fixed state $|\psi_0\rangle=d^{-1/2}\Sigma_i|i\rangle$, usually called seed, it is possible to span the whole invariant family by applying the unitary operator $U_{\{\phi_j\}}$:

$$U_{\{\phi_j\}}|\psi_0\rangle = |\psi(\{\phi_j\})\rangle. \tag{2}$$

Since we are considering input states belonging to phase rotations and group-invariant families, the natural case for our analysis is then the framework of phase covariant channels, namely, channels $\mathcal{E}$ that automatically propagate to the output the action of the group on the input as follows:

$$\mathcal{E}(V_g\rho V_g^\dagger) = W_g\mathcal{E}(\rho)W_g^\dagger, \tag{3}$$

where V_g and W_g are unitary representations of $\mathbb{U}(1)^{\times(d-1)}$ on the input and output space, respectively. More explicitly, when the input consists of N copies of an unknown pure equatorial state, i.e., $|\psi(\{\phi_j\})\rangle^{\otimes N}$, we have $V_g=V_{\{\phi_j\}}=U_{\{\phi_j\}}^{\otimes N}$. The choice of the output representation W_g will depend on the task we want to optimize. For the moment, just notice that both V_g and W_g are different unitary representations of the same group $\mathbb{U}(1)^{\times(d-1)}$.

Since we are considering only pure input states of the form $|\psi\rangle^{\otimes N}$, we can restrict our attention to channels whose input states have support on the symmetric subspace $\mathcal{H}_+^{\otimes N}$ of $\mathcal{H}^{\otimes N}$, that is, $\mathcal{H}_{\text{in}}=\mathcal{H}_+^{\otimes N}$. Moreover, we also require that the output states have support on the symmetric subspace, namely, $\mathcal{H}_{\text{out}}=\mathcal{H}_+^{\otimes M}\subset\mathcal{H}^{\otimes M}$. In this way it is guaranteed that the output single-site density operators are the same. For the following, we choose an orthonormal basis in the symmetric subspace $\mathcal{H}_+^{\otimes N}$ of the form

$$|\{n_i\}\rangle_N = |n_0,n_1,n_2,\ldots,n_{d-1}\rangle_N = \frac{1}{\sqrt{N!}}\sum_{\{\pi\}}P_\pi^{(N)} \times|\underbrace{00\ldots0}_{n_0}\underbrace{11\ldots1}_{n_1}\ldots\underbrace{d-1\ldots d-1}_{n_{d-1}}\rangle, \tag{4}$$

where $P_\pi^{(N)}$ denotes a permutation operator of the N systems, and n_0 is the number of systems in state $|0\rangle$, n_1 in state $|1\rangle$, and so on, with the constraint $\Sigma_{i=0}^{d-1}n_i=N$. The notation $|\{m_i\}\rangle_M$, with $\Sigma_{i=0}^{d-1}m_i=M$, denotes the analogous symmetric state as in Eq. (4) for the output subspace $\mathcal{H}_+^{\otimes M}$. As a convention, in this paper we will consistently use n's for the input and m's for the output.

A convenient formalism to deal with covariant channels is the Choi–Jamiołkowski isomorphism[22,23] between completely positive maps $\mathcal{M}$ from states on $\mathcal{H}_{\text{in}}$ to states on $\mathcal{H}_{\text{out}}$ and positive operators $R_{\mathcal{M}}$ on $\mathcal{H}_{\text{out}}\otimes\mathcal{H}_{\text{in}}$:

$$\mathcal{M}\leftrightarrow R_{\mathcal{M}} = (\mathcal{M}\otimes\mathcal{I})|\Omega\rangle\langle\Omega|, \tag{5}$$

where $\mathcal{I}$ is the identity channel and $|\Omega\rangle=\Sigma_{k=1}^{d}|k\rangle\otimes|k\rangle$ is the (nonnormalized) maximally entangled vector in the Hilbert space $\mathcal{H}_{\text{in}}\otimes\mathcal{H}_{\text{in}}$. With the notation introduced in Eq. (4) we have

$$|\Omega\rangle = \sum_{\{n_i\}}|\{n_i\}\rangle_N\otimes|\{n_i\}\rangle_N. \tag{6}$$

The correspondence (5) is one to one, the inverse formula being

$$\mathcal{M}(\rho) = \text{Tr}_{\text{in}}[(\mathbb{I}_{\text{out}}\otimes\rho^*)R_{\mathcal{M}}], \tag{7}$$

where Tr_{in} denotes the trace over $\mathcal{H}_{\text{in}}$, $\mathbb{I}_{\text{out}}$ is the identity matrix over $\mathcal{H}_{\text{out}}$, and ρ^* is the complex conjugate of ρ with respect to the basis fixed by $|\Omega\rangle$ in Eq. (6). The trace preservation condition is then given by $\text{Tr}_{\text{out}}[R_{\mathcal{M}}]=\mathbb{I}_{\text{in}}$.

In terms of the Choi–Jamiołkowski operator, the covariance condition of Eq. (3) can be rewritten as a commutation relation[24]:

$$[R_{\mathcal{E}}, W_g\otimes V_g^*] = 0, \tag{8}$$

where $W_g\otimes V_g^*$ is a new unitary representation of $\mathbb{U}(1)^{\times(d-1)}$. Such a representation is generally reducible, where, by Schur's lemma, $R_{\mathcal{E}}$ splits into a direct sum:

$$R_{\mathcal{E}} = \bigoplus_\alpha R_{\mathcal{E}}^\alpha, \tag{9}$$

where the index α labels the equivalence classes of the one-dimensional[25] irreducible representations of $W_g\otimes V_g^*$. In Sections 4 and 5 we will specialize Eq. (8) to the cases of $N\to M$ cloning and $N\to M$ phase conjugation, for which $W_g=U_{\{\phi_j\}}^{\otimes M}$ and $W_g=(U_{\{\phi_j\}}^*)^{\otimes M}$, respectively.

3. ECONOMICAL MAPS

Let $\mathcal{M}$ be a completely positive, trace-preserving map from states on $\mathcal{H}_{\text{in}}$ to states on $\mathcal{H}_{\text{out}}$. From the Stinespring representation theorem,[26] it immediately follows that for

every completely positive trace-preserving map it is possible to find an auxiliary quantum system with Hilbert space $\mathcal{L}$ and an isometry V from $\mathcal{H}_{\rm in}$ to $\mathcal{H}_{\rm out}\otimes\mathcal{L}$, $V^\dagger V=\mathbb{I}_{\rm in}$, such that

$$\mathcal{M}(\rho)=\mathrm{Tr}_{\mathcal{L}}[V\rho V^\dagger]. \tag{10}$$

Starting from Eq. (10), it is always possible to construct a unitary interaction U realizing $\mathcal{M}$ (Refs. 27 and 28) as follows:

$$\mathcal{M}(\rho)=\mathrm{Tr}_{\mathcal{L}}[U(\rho\otimes|a\rangle\langle a|)U^\dagger], \tag{11}$$

where $|a\rangle$ is a fixed pure state of a second auxiliary quantum system, say $\mathcal{L}'$, such that $\mathcal{H}_{\rm in}\otimes\mathcal{L}'=\mathcal{H}_{\rm out}\otimes\mathcal{L}$. The Hilbert spaces $\mathcal{L}$ and $\mathcal{L}'$ are generally different, and actually play different physical roles.

We define a trace-preserving completely positive map $\mathcal{M}$ to be economical if and only if it admits a unitary form U as

$$\mathcal{M}(\rho)=U(\rho\otimes|a\rangle\langle a|)U^\dagger, \tag{12}$$

namely, if and only if the map can be physically realized without discarding, i.e., tracing out, any resources. We can simply prove that the only maps admitting an economical unitary implementation U as in Eq. (12) are those for which

$$\mathcal{M}(\rho)=V\rho V^\dagger \tag{13}$$

for an isometry $V, V^\dagger V=\mathbb{I}_{\rm in}$. In fact, since $(\mathbb{I}_{\rm in}\otimes\langle a|)U^\dagger U(\mathbb{I}_{\rm in}\otimes|a\rangle)=\mathbb{I}_{\rm in}, U(\mathbb{I}_{\rm in}\otimes|a\rangle)$ is an isometry from $\mathcal{H}_{\rm in}$ to $\mathcal{H}_{\rm out}\otimes\mathcal{L}$. On the other hand, starting from Eq. (13) and using the Gram–Schmidt method, one can extend any isometry V from $\mathcal{H}_{\rm in}$ to $\mathcal{H}_{\rm out}\otimes\mathcal{L}$ to a unitary U on the same output space, and write it in the form $V=U(\mathbb{I}_{\rm in}\otimes|a\rangle)$ for a unit vector $|a\rangle\in\mathcal{L}'$ with $\mathcal{H}_{\rm in}\otimes\mathcal{L}'=\mathcal{H}_{\rm out}\otimes\mathcal{L}$.

Considering classical resources as free, the most general definition of an economical map corresponds to having a random unitary realization of the form

$$\mathcal{M}(\rho)=\sum_i p_i U_i(\rho\otimes|a\rangle\langle a|)U_i^\dagger, \tag{14}$$

where $p_i\geq 0, \Sigma_i p_i=1$. Using the same fixed ancilla state $|a\rangle$ for all indices i is not a loss of generality, since in constructing the operators U_i's there is always freedom in the choice of the vector $|a\rangle$. According to this more general definition, all economical maps can always be written as a randomization of the form of Eq. (13) as follows:

$$\mathcal{M}(\rho)=\sum_i p_i V_i\rho V_i^\dagger. \tag{15}$$

4. PHASE-COVARIANT CLONING

In this section we derive the form of quantum channels $\mathcal{C}$ that best approximate the ideal cloning map:

$$|\psi(\{\phi_j\})\rangle^{\otimes N}\mapsto|\psi(\{\phi_j\})\rangle^{\otimes M}, \tag{16}$$

with $M>N$, for all possible values $\phi_j\in[0,2\pi)$. In this case the choice of the unitary representation on the output space is clearly $W_g=U_{\{\phi_j\}}^{\otimes M}$. The commutation relation of Eq. (8) can then be rewritten as

$$[R_{\mathcal{C}}, U_{\{\phi_j\}}^{\otimes M}\otimes(U_{\{\phi_j\}}^{*})^{\otimes N}]=0. \tag{17}$$

From Eq. (17) it follows that $R_{\mathcal{C}}$ splits into the block form

$$R_{\mathcal{C}}=\bigoplus_{\{m_j\}}R_{\{m_j\}}, \tag{18}$$

where each set of values $\{m_j\}$ identifies a unique class of equivalent irreducible representations of $U_{\{\phi_j\}}^{\otimes M}\otimes(U_{\{\phi_j\}}^{*})^{\otimes N}$. The equivalent representations within each class can be conveniently written, using the symmetrization convention as in Eq. (4), as

$$\{|m_0+n_0,m_1+n_1,m_2+n_2,\ldots,m_{d-1}+n_{d-1}\rangle_M \otimes|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_N\}_{\{n_i\}}, \tag{19}$$

with $\Sigma_{i=0}^{d-1}n_i=N$ and $\Sigma_{j=0}^{d-1}m_j=M-N$. The multiple index $\{n_i\}$ runs over all orthonormal vectors of the symmetrized basis for $\mathcal{H}_+^{\otimes N}$. With this notation, Eq. (18) becomes

$$R_{\mathcal{C}}=\sum_{\{m_j\}}\sum_{\{n_i'\},\{n_i''\}}r_{\{n_i'\},\{n_i''\}}^{\{m_j\}}|\{m_j\}+\{n_i'\}\rangle\langle\{m_j\}+\{n_i''\}|_M\otimes|\{n_i'\}\rangle \times\langle\{n_i''\}|_N. \tag{20}$$

We now have to adjust the parameters $\{r_{\{n_i'\},\{n_i''\}}^{\{m_j\}}\}$ describing a generic channel satisfying the commutation relation of Eq. (17) to shape $R_{\mathcal{C}}$ to optimally approximate the ideal map [relation (16)]. Such an optimal approximation reasonably maximizes the fidelity $F_{\mathcal{C}}$ between the ideal output, namely, $|\psi(\{\phi_i\})\rangle^{\otimes M}$, and the actual channel output $\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N})$. By exploiting the inverse formula of Eq. (7) and the commutation relation of Eq. (17), one has

$$F_{\mathcal{C}}=\mathrm{Tr}[|\psi_0\rangle\langle\psi_0|^{\otimes(N+M)}R_{\mathcal{C}}]. \tag{21}$$

Another commonly adopted figure of merit is the single-site fidelity $F_{\mathcal{C}}^1$ between the ideal output $|\psi(\{\phi_j\})\rangle$ and the actual single-site output $\mathrm{Tr}_{M-1}[\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N})]$, namely,

$$F_{\mathcal{C}}^1=\mathrm{Tr}[|\psi_0\rangle\langle\psi_0|\otimes\mathbb{I}^{\otimes(M-1)}\otimes|\psi_0\rangle\langle\psi_0|^{\otimes N}R_{\mathcal{C}}]. \tag{22}$$

We point out that a channel $\mathcal{C}$ maximizing $F_{\mathcal{C}}$ does not necessarily also maximize $F_{\mathcal{C}}^1$.[29,30]

When the output number of copies takes the form $M=kd+N$, with $k\in\mathbb{N}$ and d the dimension of $\mathcal{H}$, there exists a unique channel maximizing at the same time both $F_{\mathcal{C}}$ and $F_{\mathcal{C}}^1$.[31] Such a channel is described by the positive rank-one operator

$$R_{\mathcal{C}}=|r_{\{k\}}\rangle\langle r_{\{k\}}|, \tag{23}$$

where

$$|r_{\{k\}}\rangle=\sum_{\{n_j\}}|k+n_0,\ldots,k+n_i,\ldots\rangle_M\otimes|n_0,\ldots,n_i\ldots\rangle_N,$$

$$\sum_j n_j=N. \tag{24}$$

The corresponding single-site fidelity $F_{\mathcal{C}}^1$ takes the form

$$F_{\mathcal{C}}^{1}=\frac{1}{d}+\frac{1}{Md^{N+1}}\sum_{\{\bar{n}_j\}}\sum_{i\neq j}\frac{N!}{\bar{n}_0!\ldots\bar{n}_i!\ldots\bar{n}_j!\ldots}\times\sqrt{\frac{(\bar{n}_i+k+1)(\bar{n}_j+k+1)}{(\bar{n}_i+1)(\bar{n}_j+1)}},\quad M=kd+N,\quad(25)$$

where, for the sake of symmetry of the formula, we have chosen the multiple index $\bar{n}_j$ such that $\Sigma_j\bar{n}_j=N-1$. In the case $N=1$, Eq. (25) is simplified as

$$F_{\mathcal{C}}^{1}=\frac{1}{d}+\frac{(d-1)(M+d-1)}{Md^2},\quad M=kd+1,\qquad(26)$$

since $\Sigma_{i\neq j}(k+1)=kd(d-1)+d(d-1)=(d-1)(M+d-1)$. Notice that $F_{\mathcal{C}}^{1}$ is always strictly greater than the analogous optimal fidelity for the universal cloner,[29] that is, $F_{\mathrm{univ}}^{1}=(2M+d-1)/M(d+1)$. This is due to the fact that we are now imposing a covariance condition under the action of $\mathbb{U}(1)^{\times(d-1)}$ that is a much looser condition[32] than imposing covariance under the action of the whole universal group $\mathbb{SU}(d)$, and therefore there is more freedom in adjusting free parameters to obtain better performances.

As a final remark, notice that, since $R_{\mathcal{C}}$ is rank one, the channel $\mathcal{C}$ acts as [this can be simply checked by using the inverse formula of Eq. (7)]

$$\mathcal{C}(\rho^{\otimes N})=V\rho^{\otimes N}V^{\dagger},\qquad(27)$$

where V is the isometry defined as

$$V|n_0,n_1,\ldots,n_i,\ldots\rangle_N=|n_0+k,n_1+k,\ldots,n_i+k,\ldots\rangle_M.\qquad(28)$$

According to the definitions of Section 3, this implies that $\mathcal{C}$ is an economical map, and therefore it does not require additional resources other than the $(M-N)$ input blank copies to be unitarily realized. This is in contrast to what happens in the universal case, for which M additional systems must be provided[19,33] in addition to the N input copies.

5. PHASE CONJUGATION

Another basic device that is impossible to achieve in the framework of quantum mechanics is the NOT gate, where the Bloch vector of any input states is reversed, or equivalently the phase conjugation operation. In this section we will derive the form of the quantum channels $\mathcal{N}$ that optimally approximate the operation of phase conjugation:

$$|\psi(\{\phi_j\})\rangle^{\otimes N}\mapsto(|\psi(\{\phi_j\})\rangle^{*})^{\otimes M}=|\psi(\{-\phi_j\})\rangle^{\otimes M},\qquad(29)$$

with $M>N$, for all possible values $\phi_j\in[0,2\pi)$. The case $M=N=1$ has been thoroughly analyzed.[20] In the case of phase conjugation the output unitary representation of $\mathbb{U}(1)^{\times(d-1)}$ must be chosen as $W_g=(U_{\{\phi_j\}}^{*})^{\otimes M}$ and the commutation relation of Eq. (8) becomes

$$[R_{\mathcal{N}},(U_{\{\phi_j\}}^{*})^{\otimes(M+N)}]=0.\qquad(30)$$

As in the case of phase-covariant cloning, Eq. (30) implies a decomposition of $R_{\mathcal{N}}$ into the block form $R_{\mathcal{N}}=\oplus_{\{m_j\}}R_{\{m_j\}}$, where each set of values $\{m_j\}$ identifies a unique class of equivalent irreducible representations of $(U_{\{\phi_j\}}^{*})^{\otimes(M+N)}$. The equivalent representations within each class can be conveniently written as

$$\{|m_0-n_0,m_1-n_1,m_2-n_2,\ldots,m_{d-1}-n_{d-1}\rangle_M\otimes|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_N\}_{\{n_i\}},\qquad(31)$$

with $\Sigma_{i=0}^{d-1}n_i=N$ and $\Sigma_{j=0}^{d-1}m_j=M+N$. It is clear that expression (31) is well defined only when $m_i\geq n_i$, for all i. In the following we will see that, when the analytical optimization is possible, such a condition is always satisfied.

The figure of merit that we will consider to approximate the phase conjugation channel is the single-site fidelity

$$F_{\mathcal{N}}^{1}=\mathrm{Tr}[|\psi_0\rangle\langle\psi_0|\otimes\mathbb{I}^{\otimes(M-1)}\otimes|\psi_0\rangle\langle\psi_0|^{\otimes N}R_{\mathcal{N}}],\qquad(32)$$

where

$$R_{\mathcal{N}}=\sum_{\{m_j\}}\sum_{\{n_i'\},\{n_i''\}}r_{\{n_i'\},\{n_i''\}}^{\{m_j\}}|\{m_j\}+\{n_i'\}\rangle\langle\{m_j\}+\{n_i''\}|_M\otimes|\{n_i'\}\rangle\times\langle\{n_i''\}|_N.\qquad(33)$$

Exploiting cumbersome combinatorial calculations similar to those reported in previous work,[31] it can be shown that, in the case $M=kd-N$, with $k\in\mathcal{N}\geq N$ and d the dimension of $\mathcal{H}$, there exists a unique channel maximizing $F_{\mathcal{C}}^{1}$. Such a channel is described by the positive rank-one operator

$$R_{\mathcal{N}}=|r_{\{k\}}\rangle\langle r_{\{k\}}|,\qquad(34)$$

where

$$|r_{\{k\}}\rangle=\sum_{\{n_j\}}|k-n_0,\ldots,k-n_i,\ldots\rangle_M\otimes|n_0,\ldots,n_i\ldots\rangle_N,\quad\sum_j n_j=N,\qquad(35)$$

and it acts as an isometrical embedding

$$\mathcal{N}(\rho^{\otimes N})=V\rho^{\otimes N}V^{\dagger},\qquad(36)$$

where the isometry V is defined as

$$V|n_0,n_1,\ldots,n_i,\ldots\rangle_N=|k-n_0,k-n_1,\ldots,k-n_i,\ldots\rangle_M.\qquad(37)$$

Therefore, the optimal phase conjugation map for the output number of copies $M=kd-N$ can also be realized economically. Its single-site fidelity $F_{\mathcal{N}}^{1}$ is given by

$$F_{\mathcal{N}}^{1}=\frac{1}{d}+\frac{1}{Md^{N+1}}\sum_{\{\bar{n}_j\}}\sum_{i\neq j}\frac{N!}{\bar{n}_0!\ldots\bar{n}_i!\ldots\bar{n}_j!\ldots}\times\sqrt{\frac{(k-\bar{n}_i)(k-\bar{n}_j)}{(\bar{n}_i+1)(\bar{n}_j+1)}},\quad M=kd-N,\qquad(38)$$

where $\Sigma_j\bar{n}_j=N-1$. Since $\Sigma_{i\neq j}k=kd(d-1)=(d-1)(M+1)$ in the case $N=1$, the above expression is simplified as

$$F_{\mathcal{N}}^{1}=\frac{1}{d}+\frac{(d-1)(M+1)}{Md^2},\quad M=kd-1.\qquad(39)$$

Notice that for qubits, $F_{\mathcal{N}}^{1}=F_{\mathcal{C}}^{1}$. This is due to the fact that, for equatorial qubits, perfect phase conjugation can be

achieved unitarily by a π rotation along the x axis.[18,20] Optimal phase conjugation therefore is equivalent to optimal phase-covariant cloning followed by such a rotation, which does not decrease the cloning fidelity. In all the other cases with $d>2, F_{\mathcal{N}}^1$ is always strictly smaller than $F_{\mathcal{C}}^1$. Actually, in these cases phase conjugation can be performed only approximately and therefore the global transformation corresponding to a generation of many phase-conjugated copies is worse than just cloning them. However, in the limit of a large number of output copies, i.e., $M\to\infty$, they both tend to the same limit, as we will show in Section 6.

6. RELATIONS WITH OPTIMAL PHASE ESTIMATION

Both the cloning fidelity $F_{\mathcal{C}}^1$ in Eq. (25) and the phase conjugation fidelity $F_{\mathcal{N}}^1$ in Eq. (38), in the limit $M\to\infty$, that is, $k\to\infty$ with $M\approx kd$, take the form

$$F^1=\frac{1}{d}+\frac{1}{d^{N+2}}\sum_{\{\bar{n}_i\}}\sum_{i\neq j}\frac{N!}{\bar{n}_0!\cdots\sqrt{(\bar{n}_i+1)(\bar{n}_j+1)}},$$
$$\times\sum_i \bar{n}_i=N-1. \tag{40}$$

Equation (40) coincides with the single-site fidelity $F_{\mathcal{P}}^1$ of optimal phase estimation on N copies of equatorial states.[34] For all possible values of N and M, the following relations then hold:

$$F_{\mathcal{C}}^1\geq F_{\mathcal{N}}^1\geq F_{\mathcal{P}}^1,\quad \lim_{M\to\infty}F_{\mathcal{C}}^1=\lim_{M\to\infty}F_{\mathcal{N}}^1=F_{\mathcal{P}}^1. \tag{41}$$

Inequalities (41) are illustrated in Fig. 1, where the optimal fidelities of phase-covariant cloning and phase conjugation are reported for equatorial states with $d=5$ and $N=1$. First, let us notice that phase-covariant conjugation, contrary to the case of universal transposition[19] for which it is known that the optimal strategy trivially consists of an estimation followed by a suitable preparation, achieves a fidelity $F_{\mathcal{N}}^1$ that is always greater than the fidelity $F_{\mathcal{P}}^1$ achievable by means of a measure-and-prepare scheme. Moreover, inequalities (41) confirm the general fact that cloning fidelity, in the limit of an infinite number of output copies, tends to state estimation fidelity, and shows that this also holds for other symmetrical covariant

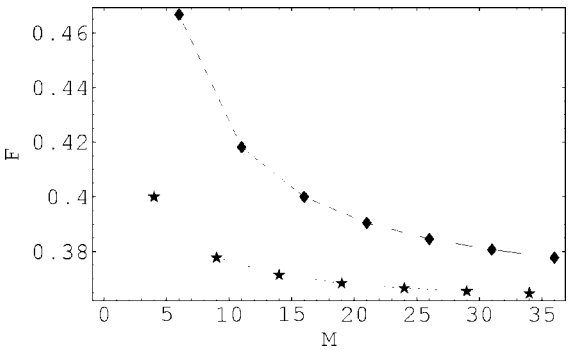

Fig. 1. Comparison between single-site fidelities of phase covariant $1\to M$ optimal cloning (solid curve) and phase conjugation (dotted curve) for $d=5$. Both curves tend to the limit of $9/25=0.36$, that is, the fidelity of optimal phase estimation.

devices, such as phase conjugation.

Here we prove that not only the fidelities $F_{\mathcal{C}}^1$ and $F_{\mathcal{N}}^1$ tend to the phase estimation fidelity $F_{\mathcal{P}}^1$, but also that optimal phase-covariant cloning $\mathcal{C}$ and phase conjugation $\mathcal{N}$ maps tend, in the limit, to the phase estimation map $\mathcal{P}$ [which estimates the phases $\{\overline{\phi_j}\}$ and reprepares the state $|\psi(\{\overline{\phi_j}\})\rangle$]. This is clearly a much stronger statement than that concerning just fidelities.[35,36] The main ingredient we need for the proof is that the single-site output state coming from the channel $\mathcal{C}$ can be parametrized by a shrinking parameter $\eta_{\mathcal{C}}$ as

$$\mathrm{Tr}_{M-1}[\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\}|)^{\otimes N})]$$
$$=\eta_{\mathcal{C}}|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\}|)+(1-\eta_{\mathcal{C}})\frac{\mathbb{I}}{d}, \tag{42}$$

with $\eta_{\mathcal{C}}=(dF_{\mathcal{C}}^1-1)/(d-1)$. Analogous formulas hold for phase conjugation $\mathcal{N}$ and phase estimation $\mathcal{P}$, as a consequence of the phase-covariant property of the maps (for the explicit calculations, see Appendixes A and B).

The proof then goes through a concatenation argument. Imagine performing an optimal phase estimation[34] over N copies of the unknown state $|\psi(\{\phi_j\})\rangle$. After obtaining the optimal estimated value $\{\overline{\phi_j}\}$ of the phases, it is possible to prepare M copies of the state $|\psi(\{\overline{\phi_j}\})\rangle$. This procedure is, by definition, a suboptimal phase-covariant $N\to M$ cloning: The fidelity of such M copies must be smaller than (or at most equal to) the fidelity of the output of an optimal phase-covariant cloner, that is,

$$F_{\mathcal{P}}^1(N)\leq F_{\mathcal{C}}^1(N,M),\quad \forall N,M. \tag{43}$$

(We put in parentheses the dependence of the fidelities on the input number of copies N and the output number M.)

The opposite direction can be proved by concatenating the optimal $N\to M$ phase-covariant cloner with the optimal state estimation described in Refs. 37 and 38. Since a state estimation implies a phase estimation, it is possible to interpret the whole procedure as a suboptimal phase estimation: The single-site fidelity $\bar{F}^1(N,M)$ obtained in this suboptimal way must be smaller than or equal to the optimal phase estimation fidelity $F_{\mathcal{P}}^1(N)$ for all possible values of M. The state estimation map $\mathcal{S}$ works as follows[38]:

$$\mathcal{S}(\rho^{\otimes M})=\eta_{\mathcal{S}}\rho+(1-\eta_{\mathcal{S}})\frac{\mathbb{I}}{d}. \tag{44}$$

Applying $\mathcal{S}$ to the output of the phase-covariant $N\to M$ cloner, we get

$$\mathcal{S}(\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N}))=\eta_{\mathcal{S}}\mathrm{Tr}_{M-1}[\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N})]$$
$$+(1-\eta_{\mathcal{S}})\frac{\mathbb{I}}{d}. \tag{45}$$

Since we assumed that the output state ρ_M of a phase-covariant cloner has support on the symmetric subspace, it can be linearly decomposed as $\rho_M=\Sigma_i\lambda_i|\psi_i\rangle\langle\psi_i|^{\otimes M}$ with $\Sigma_i\lambda_i=1$.[39,40] Therefore the above expression can be written as

$$\mathcal{S}(\mathcal{C}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N})) = \eta_S\eta_{\mathcal{C}}|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})| + (\eta_S(1-\eta_{\mathcal{C}}) + (1-\eta_S))\frac{\mathbb{I}}{d}. \quad (46)$$

Noticing that the shrinking factor $\eta_S = M/(M+d)$ (Ref. 38) approaches unit for $M \to \infty$, Eq. (46) implies that

$$\lim_{M\to\infty} \bar{F}(N,M) = \lim_{M\to\infty} F_{\mathcal{C}}(N,M); \quad (47)$$

and according to the previous remark about the suboptimality of this phase estimation procedure, one has

$$\lim_{M\to\infty} F_{\mathcal{C}}(N,M) \le F_{\mathcal{P}}(N), \quad \forall N. \quad (48)$$

Inequality (48) together with inequality (43) prove inequalities (41).

The above argument can also be applied to the case of phase conjugation. Actually, a suboptimal phase-covariant conjugation map can be achieved by first performing an optimal phase estimation on the input equatorial states, which gives the estimated values $\{\overline{\phi_j}\}$ for the phases, and then preparing M copies of the state $|\psi(\{-\overline{\phi_j}\})\rangle$. Moreover, a suboptimal phase estimation can be realized by first applying an optimal $N \to M$ phase-covariant conjugation device and then performing optimal state estimation on the M output states. In this way we would be able to estimate the $(d-1)$ phase values of the M output states and we would have an estimate of the phases of the N input states just by changing the signs. The comparison of the above two procedures allows us to establish the equivalence of optimal phase estimation and optimal phase-covariant transposition in the limit of an infinite number of output copies.

7. CONCLUSIONS

In this paper we have studied the efficiency of phase-covariant multiuser channels in an arbitrary finite dimension. In particular, we have derived the form of the channels that optimally approach quantum cloning and phase conjugation for multiphase equatorial states. We have shown that for certain relations between the input and output number of copies, the optimal transformations can be achieved economically. We have derived a relation between the above-mentioned transformations and optimal multiphase estimation procedures. In the case of phase conjugation we have shown that, in contrast to the customary case of the universal-NOT on qubits (or the universal conjugation in arbitrary dimension), the optimal phase-covariant transformation for equatorial states is a nonclassical channel, which cannot be achieved by a measurement or preparation procedure.

APPENDIX A: SINGLE-SITE REDUCED OUTPUT STATE OF OPTIMAL PHASE ESTIMATION

The phase estimation channel $\mathcal{P}$ working over N copies of the input state $|\psi(\{\phi_j\})\rangle$ can be regarded as a machine preparing the state $|\psi(\{\overline{\phi_j}\})\rangle$ according to the estimated phase values $\{\overline{\phi_j}\}$. The output state $|\psi(\{\overline{\phi_j}\})\rangle$ is prepared with probability density:

$$p(\{\overline{\phi_j}\}) = |\langle\psi(\{\phi_j\})^{\otimes N}|e(\{\overline{\phi_j}\})\rangle|^2, \quad (A1)$$

where

$$|e(\{\overline{\phi_j}\})\rangle = U^{\otimes N}_{\{\overline{\phi_j}\}} \sum_{\{n_i\}} |\{n_i\}\rangle_N, \quad \sum_i n_i = N, \quad (A2)$$

namely, a generalized Susskind–Glogower state,[41] and $|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})|$ be the positive operator valued measure density of the optimal (multiple-) phase estimation[34] over N copies. Using the formalism of quantum operations, the single-site reduced output state of such an apparatus can be simply written as

$$\mathcal{P}(|\psi(\{\phi_j\})\rangle\langle\psi(\{\phi_j\})|^{\otimes N}) = \int \frac{\mathrm{d}\{\overline{\phi_j}\}}{(2\pi)^{d-1}} p(\{\overline{\phi_j}\})|\psi(\{\overline{\phi_j}\})\rangle\langle\psi(\{\overline{\phi_j}\})|. \quad (A3)$$

By covariance, we can exploit the calculations only for the input $|\psi_0\rangle$ and then generalize trivially to all possible input states $|\psi(\{\phi_j\})\rangle$ considered here. From Eqs. (A1) and (A3), the starting point is

$$\begin{aligned}\mathcal{P}\langle\psi_0|\langle\psi_0|^{\otimes N} &= \int \frac{\mathrm{d}\{\overline{\phi_j}\}}{(2\pi)^{d-1}} \mathrm{Tr}[\langle\psi_0||\psi_0\rangle^{\otimes N}|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})|] \\ &\quad \times|\psi(\{\overline{\phi_j}\})\rangle\langle\psi(\{\overline{\phi_j}\})| \\ &= \mathrm{Tr}_N\Bigg[\mathbb{I}\otimes|\psi_0\rangle\langle\psi_0|^{\otimes N}\int\frac{\mathrm{d}\{\overline{\phi_j}\}}{(2\pi)^{d-1}}|\psi(\{\overline{\phi_j}\})\rangle \\ &\quad \times\langle\psi(\{\overline{\phi_j}\})|\otimes|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})|\Bigg]. \end{aligned} \quad (A4)$$

Recalling the orthogonality relation

$$\int \frac{\mathrm{d}\gamma}{2\pi}\exp[i(m-n)\gamma] = \delta_{mn}, \quad \forall m,n \in \mathbb{Z}, \quad (A5)$$

and the explicit expression for $|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})|$,

$$|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})| = U(\{\overline{\phi_j}\})^{\otimes N}\Bigg[\sum_{\{n_i'\},\{n_j''\}}|\{n_i'\}\rangle\langle\{n_j''\}|\Bigg]U^\dagger(\{\overline{\phi_j}\})^{\otimes N}, \quad (A6)$$

we have

$$\int \frac{\mathrm{d}\{\overline{\phi_j}\}}{(2\pi)^{d-1}}|\psi(\{\overline{\phi_j}\})\rangle\langle\psi(\{\overline{\phi_j}\})|\otimes|e(\{\overline{\phi_j}\})\rangle\langle e(\{\overline{\phi_j}\})| = \sum_{\{n_i\}}\sum_{i,j}\frac{|i\rangle\langle j|}{d}\otimes|\{n_i\}\rangle\langle n_0,\ldots,n_i-1,\ldots,n_j+1,\ldots|. \quad (A7)$$

Substituting Eq. (A7) into Eq. (A4), we get the formula we were looking for, namely,

$$\mathcal{P}(|\psi_0\rangle|\psi_0|) = \frac{\mathbb{I}}{d} + \frac{1}{d^{N+1}} \sum_{\{\pi_i\}} \sum_{i\neq j} \frac{N!}{\bar{n}_0! \dots} \frac{1}{\sqrt{(\bar{n}_i+1)(\bar{n}_j+1)}} |i\rangle\langle j|, \quad \times \sum_j \bar{n}_j = N-1, \tag{A8}$$

hence the single-site fidelity of Eq. (40) of multiphase estimation.

APPENDIX B: SINGLE-SITE REDUCED OUTPUT STATE OF OPTIMAL PHASE-COVARIANT CLONING AND OPTIMAL PHASE CONJUGATION

Here we explicitly derive the general form of the reduced output state of the phase-covariant $N\to M$ cloner in Eq. (42). (The phase conjugation case is completely analogous.) From Eqs. (7) and (23),

$$\begin{aligned}
&\mathrm{Tr}_{M-1}[\mathcal{C}(|\psi_0\rangle\langle\psi_0|^{\otimes N})] \\
&= \mathrm{Tr}_{M-1,N}\Bigg[\mathbb{I}^{\otimes M} \otimes |\psi_0\rangle\langle\psi_0|^{\otimes N} \sum_{\{n_i'\},\{n_j''\}} |n_0'+k, \dots\rangle\langle n_0''+k, \dots|_M \\
&\quad \otimes |n_0', \dots\rangle\langle n_0'', \dots|_N\Bigg] = \frac{1}{d^N} \sum_{\{n_i'\},\{n_j''\}} \Bigg[\binom{N}{n_0';n_1';\dots} \\
&\quad \times \binom{N}{n_0'';n_1'';\dots}\Bigg]^{1/2} \\
&\quad \times \mathrm{Tr}_{M-1}[|n_0'+k, \dots\rangle\langle n_0''+k, \dots|_M] \\
&= \frac{1}{d^N} \sum_{\{n_i'\},\{n_j''\}} \Bigg[\binom{N}{n_0';n_1';\dots}\binom{N}{n_0'';n_1'';\dots}\Bigg]^{1/2} \Bigg[\binom{M}{n_0'+k;\dots} \\
&\quad \times \binom{M}{n_0''+k;\dots}\Bigg]^{-1/2} \mathrm{Tr}_{M-1}[|\widetilde{n_0'+k}, \dots\rangle\langle\widetilde{n_0''+k}, \dots|_M] \\
&= T_{\mathrm{diag}} + T_{\text{off-diag}},
\end{aligned} \tag{B1}$$

where

$$|\widetilde{n_0+k}, \dots\rangle_M = \sum_{\{\pi\}} P_\pi^{(M)} |\underbrace{00\dots0}_{n_0+k}\underbrace{11\dots1}_{n_1+k}\dots\underbrace{d-1\dots d-1}_{n_{d-1}+k}\rangle \tag{B2}$$

is a nonnormalized vector, with the notation of Eq. (4). To make the calculation clearer, we split Eq. (B1) in its diagonal part,

$$\begin{aligned}
T_{\mathrm{diag}} &= \frac{1}{d^N} \sum_{\{n_i'\},\{n_j''\}} \sum_i \Bigg[\binom{N}{n_0';n_1';\dots}\binom{N}{n_0'';n_1'';\dots}\Bigg]^{1/2} \\
&\quad \times \Bigg[\binom{M}{n_0'+k;\dots}\binom{M}{n_0''+k;\dots}\Bigg]^{-1/2} \\
&\quad \times \mathrm{Tr}_{M-1}[|i\rangle\langle i| \otimes |n_0'+k, \dots, n_i'+k-1, \dots\rangle\langle n_0'' \\
&\quad + k, \dots n_i''+k-1, \dots|] \\
&\quad \times \Bigg[\binom{M-1}{n_0'+k; \dots; n_i'+k-1;\dots} \\
&\quad \times \binom{M-1}{n_0''+k; \dots; n_i''+k-1;\dots}\Bigg]^{1/2} \\
&= \frac{1}{Md^N} \sum_{\{n_i\}} \frac{N!}{n_0!\, n_1! \dots} \sum_i (n_i+k)|i\rangle\langle i|,
\end{aligned} \tag{B3}$$

and its off-diagonal part,

$$\begin{aligned}
T_{\text{off-diag}} &= \frac{1}{Md^N} \sum_{\{n_i\}} \sum_{i\neq j} \frac{N!}{n_0! \dots (n_i-1)! \dots n_j! \dots} \\
&\quad \times \sqrt{\frac{(n_i+k)(n_j+k+1)}{n_i(n_j+1)}} |i\rangle\langle j| \\
&= \frac{1}{Md^N} \sum_{\{\bar{n}_i\}} \sum_{i\neq j} \frac{N!}{\bar{n}_0! \dots \bar{n}_i! \dots \bar{n}_j! \dots} \\
&\quad \times \sqrt{\frac{(\bar{n}_i+k+1)(\bar{n}_j+k+1)}{(\bar{n}_{i+1})(\bar{n}_j+1)}} |i\rangle\langle j|,
\end{aligned} \tag{B4}$$

with the constraints $\Sigma_j n_j = N$ and $\Sigma_j \bar{n}_j = N-1$.

First, notice that the reduced state is correctly normalized since $\Sigma_{\{n_i\}} N!/(n_0!\dots) = d^N$ and $\Sigma_i (n_i+k) = M$, and that the fidelity with respect to $|\psi_0\rangle$ is precisely $F_{\mathcal{C}}^1(N,M)$ in Eq. (25), since

$$\mathrm{Tr}\Bigg[|\psi_0\rangle\langle\psi_0| \sum_i \frac{n_i+k}{M} |i\rangle\langle i|\Bigg] = \frac{1}{d}, \tag{B5}$$

$$\mathrm{Tr}\Bigg[|\psi_0\rangle\langle\psi_0| \sum_{i\neq j} \sqrt{\frac{(\bar{n}_i+k+1)(\bar{n}_j+k+1)}{(\bar{n}_i+1)(\bar{n}_j+1)}} |i\rangle\langle j|\Bigg] = \frac{1}{d} \sum_{i\neq j} \sqrt{\frac{(\bar{n}_i+k+1)(\bar{n}_j+k+1)}{(\bar{n}_i+1)(\bar{n}_j+1)}}. \tag{B6}$$

Moreover, looking at the expressions of T_{diag} and $T_{\text{off-diag}}$ involving a sum over all possible multiple indices $\{n_i\}$, one can recognize that the diagonal entries are all multiplied by the same coefficient, as well as the off-diagonal ones. The reduced output state can then be written as

$$\mathrm{Tr}_{M-1}[\mathcal{C}(|\psi_0\rangle\langle\psi_0|^{\otimes N})] = \eta_{\mathcal{C}}(N,M)|\psi_0\rangle\langle\psi_0| + (1-\eta_{\mathcal{C}}(N,M))\frac{\mathbb{I}}{d}. \tag{B7}$$

ACKNOWLEDGMENTS

This work has been supported in part by the European Commission under the project Development of a Global Network to Secure Communication based on Quantum Cryptography (contract IST-2003-506813) and by the Italian Minístero dell'Università e della Ricerca under Programmi di Ricerca di Interesse Nazionale 2005.

Corresponding author F. Buscemi's e-mail address is buscemi@qci.jst.go.jp.

REFERENCES AND NOTES

1. H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with 3-state systems," Phys. Rev. Lett. **85**, 3313–3316 (2000).
2. D. Bruß and C. Macchiavello, "Optimal eavesdropping in cryptography with three-dimensional quantum states," Phys. Rev. Lett. **88**, 127901 (2002).
3. N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett. **88**, 127902 (2002).
4. M. Fitzi, N. Gisin, and U. Maurer, "Quantum solution to the Byzantine agreement problem," Phys. Rev. Lett. **87**, 217901 (2002).
5. G. Molina-Terriza, A. Vaziri, J. Rehacek, Z. Hradila, and A. Zeilinger, "Triggered qutrits for quantum communication protocols," Phys. Rev. Lett. **92**, 167903 (2004).
6. R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, "Bell-type test of energy-time entangled qutrits," Phys. Rev. Lett. **93**, 010503 (2004).
7. R. Das, A. Mitra, V. Kumar, and A. Kumar, "Quantum information processing by NMR: preparation of pseudopure states and implementation of unitary operations in a single-qutrit system," http:arxiv.orglabs/quant-ph/0307240.
8. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," Proc. R. Soc. London, Ser. A **454**, 339–354 (1998).
9. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
10. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, 1984), pp. 175–179.
11. A. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
12. For a review, see, for example, V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, "Quantum cloning," Rev. Mod. Phys. **77**, 1225–1256 (2005).
13. D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, "Phase-covariant quantum cloning," Phys. Rev. A **62**, 012302 (2000).
14. F. Caruso, H. Bechmann Pasquinucci, and C. Macchiavello, "Robustness of a quantum key distribution with two and three mutually unbiased bases," Phys. Rev. A **72**, 032340 (2005).
15. V. Scarani and N. Gisin, "Spectral decomposition of Bell's operators for qubits," J. Phys. A **34**, 6043–6053 (2001).
16. A. Peres, "Separability criterion for density matrices," Phys. Rev. Lett. **77**, 1413–1415 (1996).
17. P. Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," Phys. Lett. A **232**, 333–339 (1997).
18. V. Bužek, M. Hillery, and R. F. Werner, "Optimal manipulations with qubits: universal-NOT gate," Phys. Rev. A **60**, R2626–R2629 (1999).
19. F. Buscemi, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, "Optimal realization of the transposition maps," Phys. Lett. A **314**, 374–379 (2003).
20. F. Buscemi, G. M. D'Ariano, and C. Macchiavello, "Optimal time-reversal of multi-phase equatorial states," Phys. Rev. A **72**, 062311 (2005).
21. K. Kraus, *States, Effects, and Operations: Fundamental Notions in Quantum Theory*, Lecture Notes in Physics (Springer-Verlag, 1983), Vol. 190.
22. A. Jamiołkowski, "Linear transformations which preserve trace and positive semidefiniteness of operators," Rep. Math. Phys. **3**, 275–278 (1972).
23. M.-D. Choi, "Completely positive linear maps on complex matrices," Linear Algebr. Appl. **10**, 285–290 (1975).
24. G. M. D'Ariano and P. Lo Presti, "Optimal nonuniversally covariant cloning," Phys. Rev. A **64**, 042308 (2001).
25. The group $\mathrm{U}(1)^{\times(d-1)}$ is commutative, hence its irreducible representations are all one dimensional.
26. W. F. Stinespring, "Positive functions on C^*-algebras," Proc. Am. Math. Soc. **6**, 211–216 (1955).
27. M. Ozawa, "Quantum measuring processes of continuous observables," J. Math. Phys. **25**, 79–87 (1984).
28. F. Buscemi, G. M. D'Ariano, and M. F. Sacchi, "Physical realizations of quantum operations," Phys. Rev. A **68**, 042113 (2003).
29. M. Keyl and R. F. Werner, "Optimal cloning of pure states, judging single clones," J. Math. Phys. **40**, 3283–3299 (1999).
30. G. M. D'Ariano and C. Macchiavello, "Optimal phase-covariant cloning for qubits and qutrits," Phys. Rev. A **67**, 042306 (2003).
31. F. Buscemi, G. M. D'Ariano, and C. Macchiavello, "Economical phase-covariant cloning of qudits," Phys. Rev. A **71**, 042327 (2005).
32. Actually, $\mathrm{U}(1)^{\times(d-1)}$ is a proper subgroup of $\mathrm{SU}(d)$.
33. T. Durt, J. Fiurasek, and N. J. Cerf, "Economical quantum cloning in any dimension," Phys. Rev. A **72**, 052322 (2005).
34. C. Macchiavello, "Optimal estimation of multiple phases," Phys. Rev. A **67**, 062302 (2003).
35. Recently, it has been proved that cloning channels, in the limit of infinite output copies, tend to measure-and-prepare channels. Here, we are able to explicitly show how fast this limit is reached, for every finite M.
36. J. Bae and A. Acín, "Asymptotic quantum cloning is state estimation," http://arxiv.orglabs/quant-ph/0603078.
37. R. Derka, V. Bužek, and A. K. Ekert, "Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement," Phys. Rev. Lett. **80**, 1571–1575 (1998).
38. D. Bruß and C. Macchiavello, "Optimal state estimation for d-dimensional quantum systems," Phys. Lett. A **253**, 249–251 (1999).
39. This holds by linearity, since every symmetric operator O can be written as a linear combination of N-fold tensor product pure states, namely, $O=\Sigma_i \lambda_i |\psi_i\rangle\langle\psi_i|^{\otimes N}$.
40. G. M. D'Ariano, V. Giovannetti, and P. Perinotti, "Optimal estimation of quantum observables," J. Math. Phys. **47**, 022102 (2006).
41. L. Susskind and J. Glogower, "Quantum mechanical phase and time operator," Physics (Long Island City, N.Y.) **1**, 49–61 (1964).