Economical quantum cloning in any dimension

Thomas Durt,[1] Jaromír Fiurášek,[2,3] and Nicolas J. Cerf[2]
[1]*TONA-TENA, Free University of Brussels, Pleinlaan 2, 1050 Brussels, Belgium*
[2]*QUIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[3]*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*
(Received 11 January 2005; published 21 November 2005)

The possibility of cloning a d-dimensional quantum system without an ancilla is explored, extending on the economical phase-covariant cloning machine for qubits found in Phys. Rev. A **60**, 2764 (1999). We prove the impossibility of constructing an economical version of the optimal universal $1\rightarrow 2$ cloning machine in any dimension. We also show, using an ansatz on the generic form of cloning machines, that the d-dimensional $1\rightarrow 2$ phase-covariant cloner, which optimally clones all balanced superpositions with arbitrary phases, can be realized economically only in dimension $d=2$. The used ansatz is supported by numerical evidence up to $d=7$. An economical phase-covariant cloner can nevertheless be constructed for $d>2$, albeit with a slightly lower fidelity than that of the optimal cloner requiring an ancilla. Finally, using again an ansatz on cloning machines, we show that an economical version of the $1\rightarrow 2$ Fourier-covariant cloner, which optimally clones the computational basis and its Fourier transform, is also possible only in dimension $d=2$.

DOI: 10.1103/PhysRevA.72.052322 PACS number(s): 03.67.−a, 42.50.−p, 89.70.+c

I. INTRODUCTION

During the last decade, many promising applications of ideas developed within the framework of quantum information theory, such as quantum cryptography, quantum computing, quantum cloning, and quantum teleportation were implemented experimentally [1–4]. Although it is not certain whether these spectacular progresses will lead to a practical quantum computer [5] because of the difficulties related to decoherence, quantum cryptography is already a well established and mature technology [1,6]. Traditionally, quantum key distribution is implemented with two-level quantum systems, usually referred to as qubits. The security of the quantum key distribution (QKD) protocols such as the Bennett-Brassard 1984 (BB84) protocol [7] is guaranteed by the no-cloning theorem [8,9], which states that the perfect copying (or cloning) of a set of states that contains at least two non-orthogonal states is impossible. It is, however, possible to realize an approximate quantum cloning, a concept introduced in a seminal paper by Bužek and Hillery [10], where a universal (or state-independent) and symmetric one-to-two cloning transformation was introduced for qubits.

Cloning machines can be used as a very efficient means of eavesdropping on the QKD protocols. In this context, it is important to study machines which optimally clone a particular subset of states of the Hilbert space, for example the Fourier-covariant cloning machine, which optimally copies two mutually unbiased bases under a Fourier transform [11], or the phase-covariant cloning machine, which optimally clones all balanced superpositions of the computational basis states with arbitrary phases [12–17]. In particular, the optimal Fourier-covariant cloner in two dimensions, is known to provide the most dangerous eavesdropping strategy against the BB84 quantum cryptographic protocol [18,19], while the phase-covariant cloner was shown in Refs. [20,21] to play the same role relatively to the Ekert protocol [22].

In the present paper, we shall concentrate on the one-to-two cloning machines, which produce two copies of a single d-dimensional system (a qudit). In an eavesdropping scenario, one copy is sent to the legitimate receiver while the other is kept by the eavesdropper. The $1\rightarrow 2$ cloning transformation for qudits can typically be expressed as a unitary operation on the Hilbert space of three qudits—the input, a blank copy, and an ancilla. The presence of an ancilla significantly affects the experimental implementation of the cloning operation, which becomes more complicated and sensitive to decoherence as it has been shown in a recent NMR realization of the optimal universal qubit cloner [2]. This problem, which may drastically reduce the achieved cloning fidelity, can be circumvented if an *economical* approach is followed, which avoids the ancilla. The cloning is then realized as a unitary operation on two qudits only: the input and the blank copy. This transformation is obviously simpler to implement as it requires less qudits and two-qudit gates, and also only demands to control the entanglement of a pair of qudits. It is thus likely to be much less sensitive to noise and decoherence than its three qudit counterpart, a fact that was recently confirmed experimentally [23]. To date, the only $1\rightarrow 2$ cloning machine for which an economical realization is known is the phase-covariant qubit cloner due to Niu and Griffiths [24].

This (asymmetric) phase-covariant qubit cloning machine works as follows. During the process, the qubit to be cloned, initially in state $|\psi\rangle_B$, is coupled to another qubit which becomes the second copy and is initially prepared in state $|0\rangle_E$ (the labels B and E refer to the tradition in quantum cryptography according to which the receiver of the key is called Bob and the eavesdropper Eve). Then, the state $|\psi\rangle_B|0\rangle_E$ undergoes a unitary transformation U_{BE} such that

$$U_{BE}|0\rangle_B|0\rangle_E=|0\rangle_B|0\rangle_E,$$

$$U_{BE}|1\rangle_B|0\rangle_E=\cos\alpha|1\rangle_B|0\rangle_E+\sin\alpha|0\rangle_B|1\rangle_E. \quad (1)$$

It can be shown that when the input qubit is in an equatorial state,

$$|\psi\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + e^{i\phi}|1\rangle_B) \tag{2}$$

the fidelities of Bob's and Eve's clones give

$$F_B = \langle\psi|_B \mathrm{Tr}_E(\rho)|\psi\rangle_B = \frac{1+\cos\alpha}{2},$$

$$F_E = \langle\psi|_E \mathrm{Tr}_B(\rho)|\psi\rangle_E = \frac{1+\sin\alpha}{2}, \tag{3}$$

where $\rho=|\Phi_{BE}\rangle\langle\Phi_{BE}|$ and $|\Phi_{BE}\rangle=U_{BE}|\psi\rangle_B|0\rangle_E$. These fidelities do not depend on the azimuthal angle ϕ, so that these cloners are called phase-covariant. The special case $\alpha=\pi/4$ corresponds to the symmetric phase-covariant cloner, which provides two clones of equal fidelity $F_B=F_E=(2+\sqrt{2})/4\approx 0.8536$.

It is worth emphasizing that, except for the two qubits which are used to carry the two copies, this transformation does not require any extra qubit (ancilla), and is thus an economical cloning process. In a recent paper, a general, necessary and sufficient, criterion was derived in order to characterize the reducibility of three-qubit cloners to two-qubit cloners, and it was concluded that the phase-covariant cloner is the only cloner in dimension $d=2$ that admits an economical realization [25]. It was also shown recently that the optimal $N\rightarrow M$ phase-covariant cloning of qudits can be implemented in an economical way (without an ancilla) provided that $M=kd+N$, where k is an integer [26].

The goal of the present paper is to further extend the study carried out in Ref. [25] and to investigate whether a two-qudit realization exists for various d-dimensional $1\rightarrow 2$ cloning machines. In contrast to Ref. [26], where only phase-covariant cloning was considered, we shall investigate the possibility of an economical implementation of universal, phase-covariant, as well as Fourier-covariant cloning machines. More generally, we aim at elucidating the connections that exist between the cloners with or without ancillas. We prove a series of no-go theorems for economical $1\rightarrow 2$ cloning. In particular, we show that, without an ancilla, it is impossible to realize the (deterministic) optimal universal cloning machine in any dimension d (Sec. II), and that an economical implementation of optimal phase-covariant cloners does not exist for dimensions $d>2$ (Sec. III). This latter result relies on some ansatz on the cloning transformation, which is made very plausible by a numerical check up to $d=7$. As a side-result, we also consider the best economical phase-covariant cloner in d dimensions, which achieves a high fidelity although it does not perform as well as the optimal phase-covariant cloner with an ancilla (Sec. IV). Moreover, we provide a strong evidence that the optimal cloning of a pair of mutually unbiased bases, or Fourier-covariant cloning, requires an ancilla if $d>2$ (Sec. V). All these results strongly suggest that the Niu-Griffiths phase-covariant qubit cloner [24], which does not require an ancilla, is quite unique among the $1\rightarrow 2$ cloning machines in all dimensions.

II. UNIVERSAL CLONING MACHINES

Let us begin by introducing an isomorphism between completely positive maps $\mathcal{S}$ and positive semidefinite operators $S\geqslant 0$ on the tensor product of input and output Hilbert spaces $\mathcal{H}_{\mathrm{in}}\otimes\mathcal{H}_{\mathrm{out}}$ [27,28]. Consider a maximally entangled state on $\mathcal{H}_{\mathrm{in}}^{\otimes 2}$,

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d}|j\rangle_1|j\rangle_2, \tag{4}$$

where $d=\dim(\mathcal{H}_{\mathrm{in}})$. The map $\mathcal{S}$ is applied to the subsystem 2, while nothing happens with subsystem 1. The resulting (generally mixed) quantum state is isomorphic to $\mathcal{S}$ and reads

$$S = \mathcal{I}_1\otimes\mathcal{S}_2(d|\Phi^+\rangle\langle\Phi^+|). \tag{5}$$

The prefactor d is introduced for normalization purposes. A trace preserving map satisfies the condition

$$\mathrm{Tr}_{\mathrm{out}}[S] = \mathbb{1}_{\mathrm{in}}. \tag{6}$$

The CP map $\rho_{\mathrm{out}}=\mathcal{S}(\rho_{\mathrm{in}})$ can be expressed in terms of S as follows [29]:

$$\rho_{\mathrm{out}} = \mathrm{Tr}_{\mathrm{in}}[\rho_{\mathrm{in}}^T\otimes\mathbb{1}_{\mathrm{out}}S], \tag{7}$$

where T denotes the transposition in the computational basis.

Let us now assume that S describes the $1\rightarrow 2$ cloning transformation of qudits. The output Hilbert space is endowed with tensor product structure, $\mathcal{H}_{\mathrm{out}}=\mathcal{H}_B\otimes\mathcal{H}_E$, where the subscripts B and E label the two clones [in the framework of quantum cryptography, they label the authorized user's (Bob's) copy and the spy's (Eve's) copy]. For each particular input state $|\psi\rangle$, we can calculate the fidelity of each clone as follows:

$$F_B(\psi) = \mathrm{Tr}(\psi_{\mathrm{in}}^T\otimes\psi_B\otimes\mathbb{1}_E S),$$

$$F_E(\psi) = \mathrm{Tr}(\psi_{\mathrm{in}}^T\otimes\mathbb{1}_B\otimes\psi_E S), \tag{8}$$

where the subscript "in" labels the input and $\psi\equiv|\psi\rangle\langle\psi|$ is a short hand notation for a density matrix of a pure state. We are usually interested in the average performance of the cloning machine, which can be quantified by the mean fidelities

$$F_B = \int_\psi F_B(\psi)d\psi, \quad F_E = \int_\psi F_E(\psi)d\psi, \tag{9}$$

where the measure $d\psi$ determines the kind of the cloning machines we are dealing with. Universal cloning machines correspond to choosing $d\psi$ to be the invariant measure on the factor space $\mathrm{SU}(d)/\mathrm{SU}(d-1)$ induced by the Haar measure on the group $\mathrm{SU}(d)$. The fidelities (9) are linear functions of the operator S,

$$F_B = \mathrm{Tr}[SR_B], \quad F_E = \mathrm{Tr}[SR_E], \tag{10}$$

where the positive semidefinite operators R_j are given by

$$R_B = \int_\psi \psi_{\text{in}}^T \otimes \psi_B \otimes \mathbb{1}_E d\psi, \quad R_E = \int_\psi \psi_{\text{in}}^T \otimes \mathbb{1}_B \otimes \psi_E d\psi. \tag{11}$$

In the case of universal cloning, the integral over $d\psi$ can be easily calculated with the help of Schur's lemma, and we get, for instance,

$$\int_\psi \psi_{\text{in}}^T \otimes \psi_B d\psi = \frac{2}{d(d+1)}(\Pi^+_{\text{in},B})^{T_{\text{in}}} = \frac{1}{d(d+1)}[\mathbb{1}_{\text{in}} \otimes \mathbb{1}_B + d\Phi^+_{\text{in},B}].$$

Here, Π^+ denotes a projector onto symmetric subspace of two qudits, $d(d+1)/2$ is the dimension of this subspace, and T_{in} stands for transposition with respect to the subsystem "in".

The optimal symmetric cloning machine S should maximize the average of mean fidelities F_B and F_E [30],

$$F = \frac{1}{2}(F_B + F_E) = \text{Tr}[SR], \tag{12}$$

where $R=(R_B+R_E)/2$. The maximum achievable F is upper bounded by the maximum eigenvalue $r_{\max}$ of the operator R. Taking into account the trace-preservation condition (6), we have [29]

$$F \leqslant d r_{\max}. \tag{13}$$

In the case of the universal and phase-covariant $1\to 2$ cloning machines considered in the present paper this bound is saturated if we use an ancilla as we shall see below.

We have to calculate the eigenvalues of an operator

$$R = \frac{1}{2d(d+1)}(2\mathbb{1}_{\text{in},BE} + d\Phi^+_{\text{in},B} \otimes \mathbb{1}_E + d\Phi^+_{\text{in},E} \otimes \mathbb{1}_B). \tag{14}$$

Due to the high symmetry, the operator R has only three different eigenvalues. One eigenvalue reads $1/[d(d+1)]$ and is (d^3-2d)-fold degenerate. The other two eigenvalues are each d-fold degenerate and read

$$r_{\max} = \frac{d+3}{2d(d+1)}, \quad r_3 = \frac{1}{2d}.$$

The corresponding eigenstates lie in the $2d$-dimensional subspace spanned by $|\Phi^+\rangle_{\text{in},B}|k\rangle_E$ and $|\Phi^+\rangle_{\text{in},E}|k\rangle_B$, with $k=1,\ldots,d$. The d eigenstates corresponding to the maximum eigenvalue $r_{\max}$ can be expressed as

$$|r_{\max};k\rangle = \sqrt{\frac{d}{2(d+1)}}(|k\rangle_B|\Phi^+\rangle_{\text{in},E} + |k\rangle_E|\Phi^+\rangle_{\text{in},B}), \tag{15}$$

where $k=1,\ldots,d$. Note that $dr_{\max}=(d+3)/[2(d+1)]$ which is the fidelity of the optimal d-dimensional universal cloner [31–33]; hence the inequality (13) is saturated. It is then clear that the support of any admissible optimal cloning CP map S must be the d-dimensional space spanned by the eigenstates $|r_{\max};k\rangle$. This will be exploited in what follows to prove that it is not possible to implement the cloning transformation in an economic way, i.e., without an ancilla, just by applying (randomly, with probability p_l) a two-qudit unitary transformation U_l to the original state and a blank copy.

Indeed, if this convex mixture of unitaries implements an optimal cloning transformation which maximizes the fidelity F, then, by convexity, each unitary U_l is optimal in a sense that it yields the maximal mean fidelity. Consider one such unitary U. The corresponding operator S_U represents a pure state, since S_U is obtained by applying U to a pure state $|\Phi^+\rangle$. The question is thus whether there exists a state

$$|S_U\rangle = \sum_{k=1}^{d} c_k |r_{\max};k\rangle \tag{16}$$

such that $S_U=|S_U\rangle\langle S_U|$ satisfies the trace-preservation condition (6). After a simple algebra, the condition $\text{Tr}_{BE}[S_U]=\mathbb{1}_{\text{in}}$ turns out to be equivalent to

$$\frac{1}{d+1}\sum_{k=1}^{d} |c_k|^2 \mathbb{1} + \frac{1}{d+1}\sum_{k,l} c_k c_l^* |l\rangle\langle k| = \mathbb{1}. \tag{17}$$

This condition is equivalent to the requirement that the rank-one projector $|c^*\rangle\langle c^*|$ is proportional to the identity operator, which is clearly impossible for any dimension $d \geqslant 2$. This concludes our proof that the universal $1\to 2$ economical cloning is impossible.

III. PHASE-COVARIANT CLONING MACHINES

Let us now investigate the possibility of the economical implementation of phase-covariant cloning machines which clone equally well all balanced superpositions of computational basis states

$$|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d} e^{i\phi_j}|j\rangle.$$

We will proceed similarly as before and first determine the operators R_B^{PC} and R_E^{PC}, where the superscript "pc" indicates states and operators related to phase-covariant cloning. The integration in Eq. (11) is over the d phases ϕ_j, and we have to evaluate the integral

$$\prod_{j=1}^{d}\int_0^{2\pi}\frac{d\phi_j}{2\pi}\psi_{\text{in}}^T \otimes \psi_B = \frac{1}{d}\Phi^+_{\text{in},B} + \frac{1}{d^2}\mathbb{1}_{\text{in}} \otimes \mathbb{1}_B - \frac{1}{d^2}\sum_{j=1}^{d}(|jj\rangle\langle jj|)_{\text{in},B}.$$

In order to determine the subspace that is the support of all possible optimal cloning transformations S^{PC}, we have to determine the maximum eigenvalue of the operator $R^{\text{PC}}=(R_B^{\text{PC}}+R_E^{\text{PC}})/2$ and the corresponding eigenstates. We have

$$R^{\rm PC} = \frac{1}{d^2}\mathbb{1}_{\rm in} \otimes \mathbb{1}_B \otimes \mathbb{1}_E + \frac{1}{2d}(\Phi^+_{{\rm in},B} \otimes \mathbb{1}_E + \Phi^+_{{\rm in},E} \otimes \mathbb{1}_B) - \frac{1}{2d^2}\sum_{j=1}^{d} [(|jj\rangle\langle jj|)_{{\rm in},B} \otimes \mathbb{1}_E + (|jj\rangle\langle jj|)_{{\rm in},E} \otimes \mathbb{1}_B]. \tag{18}$$

Taking into account the symmetry properties of the operator $R^{\rm PC}$, we can easily construct the eigenstates of $R^{\rm PC}$ which correspond to the eigenvalue

$$r^{\rm PC}_{\rm max} = \frac{1}{4d^2}(d + 2 + \sqrt{d^2 + 4d - 4})$$

and we have

$$|r^{\rm PC}_{\rm max};k\rangle = \alpha(|\Phi^+\rangle_{{\rm in},B}|k\rangle_E + |\Phi^+\rangle_{{\rm in},E}|k\rangle_B) + \beta|kkk\rangle_{{\rm in},BE}, \tag{19}$$

where $k=1,\ldots,d$, and

$$\frac{\alpha}{\beta} = -d^{5/2}r^{\rm PC}_{\rm max}. \tag{20}$$

However, it is very difficult to generally prove that $r^{\rm PC}_{\rm max}$ is the highest eigenvalue of $R^{\rm PC}$ and that the d states (19) are the *only* eigenstates with this eigenvalue. While we have not been able to prove this analytically for arbitrary d, we have checked numerically that this is indeed the case for $d=2,3,\ldots,7$ and we conjecture that this holds for any d. Again, we find that $dr^{\rm PC}_{\rm max}$ is equal to the fidelity of the optimal d-dimensional phase-covariant cloner [15–17], so the inequality (13) is saturated.

We can now prove that for $d>2$ it is not possible to design an economical $1\rightarrow 2$ phase-covariant cloning machine which does not require an ancilla. If such a machine would exist, then there would be a state

$$|S^{\rm PC}\rangle = \sum_{k=1}^{d} c_k|r^{\rm PC}_{\rm max};k\rangle, \tag{21}$$

which would satisfy the trace-preservation condition (6). On inserting Eq. (19) into Eq. (21) we obtain

$${\rm Tr}_{BE}(|S^{\rm PC}\rangle\langle S^{\rm PC}|) = 2d^{-1}\sum_k |c_k|^2\mathbb{1} + \gamma\sum_k |c_k|^2|k\rangle\langle k| + 2\frac{\alpha^2}{d}\sum_{j\neq k} c_k c_j^*|j\rangle\langle k|, \tag{22}$$

where

$$\gamma = \beta^2 + \frac{4\alpha\beta}{\sqrt{d}} + \frac{2\alpha^2}{d}.$$

We have to distinguish two cases. If $\gamma=0$ then the trace-preservation condition (6) can be satisfied by setting $c_k=0$ if $k\neq l$ and $c_l=\sqrt{d/2}$ for some $l\in\{1,\ldots,d\}$. From $\gamma=0$ we obtain $\alpha/\beta=-\sqrt{d}(4\pm 2\sqrt{2})/4$. By comparing this expression with Eq. (20) we obtain an equation for d which has only one positive integer solution $d=2$. In this particular case, the pure state $|r^{\rm PC}_{\rm max};k\rangle$ describes the symmetric Niu-Griffiths phase-covariant cloning machine for qubits [24] and we have, in accordance with Eqs. (1) and (5),

$$|S^{\rm PC}\rangle = |0\rangle_{\rm in}|00\rangle_{BE} + \frac{1}{\sqrt{2}}|1\rangle_{\rm in}(|01\rangle + |10\rangle)_{BE}.$$

For $d>2$ it holds that $\gamma\neq 0$ and the trace-preservation condition thus implies $c_k c_j^* = C\delta_{jk}$, where $C>0$ is some constant. It is clear that this latter constraint does not admit any solution, hence we conclude that for $d>2$ the economical phase-covariant cloning machine does not exist. Strictly speaking, our proof holds only for $d=3,\ldots,7$ where we numerically verified that the eigenstates (19) are the only ones corresponding to the maximal eigenvalue of $R^{\rm PC}$. However, we expect that it holds for any $d>2$.

IV. SUBOPTIMAL ECONOMICAL PHASE-COVARIANT CLONING MACHINES

Since the optimal phase-covariant cloning cannot be realized without an ancilla, we can ask what is the best economical approximation to the optimal cloner, i.e., which unitary operation on the Hilbert space of two qudits, an input and a blank copy, achieves the maximum cloning fidelity. In our formalism, the unitary operation is represented by a rank one operator $S_U=|S_U\rangle\langle S_U|$ which satisfies ${\rm Tr}_{EB}[|S_U\rangle\langle S_U|]=\mathbb{1}_{\rm in}$. The optimal U can be easily determined if we impose some natural constraints on the cloning transformation. First of all, we require that it should be invariant with respect to swapping the two clones E and B, which implies that the output Hilbert space of S_U should be the symmetric subspace of the two qudits, spanned by the states $|kl^+\rangle$ defined as $|kl^+\rangle=(|kl\rangle+|lk\rangle)/\sqrt{2}$, $k\neq l$, and $|kk^+\rangle=|kk\rangle$. The second condition is that the cloning should be phase covariant, i.e., the map S_U should be invariant with respect to an arbitrary phase shift applied to the input qubit, followed by the inverse phase shifts on the two clones. Mathematically, this condition can be expressed as

$$[V_{\rm in}(\phi) \otimes V_B^\dagger(\phi) \otimes V_E^\dagger(\phi)]|S_U\rangle = e^{i\phi}|S_U\rangle, \tag{23}$$

where ϕ is some overall phase factor

$$V(\phi) = \sum_{k=1}^{d} e^{i\phi_k}|k\rangle\langle k|,$$

and the phases ϕ_k can be arbitrary. In order to satisfy the condition (23), the state $|S_U\rangle$ must have one of the following forms:

$$|S_U\rangle = |k\rangle_{\rm in}|lm^+\rangle_{BE}, \quad k\neq l\neq m,$$

$$|S_U\rangle = |k\rangle_{\rm in}|ll^+\rangle_{BE}, \quad k\neq l,$$

$$|S_U\rangle = \sum_{k=1}^{d} s_k|k\rangle_{\rm in}|kl^+\rangle_{BE}.$$

It is clear that the trace preservation condition can be satisfied only by the third option, provided that $s_k=e^{i\theta_k}$. The fidelity of the clones produced by this map is given by

TABLE I. Comparison of the fidelities of the optimal and economical phase-covariant cloners for several d.

d	2	3	4	5	10	20	200
$F_{\rm econ}^{\rm PC}$	0.854	0.759	0.702	0.666	0.587	0.544	0.505
$F_{\rm opt}^{\rm PC}$	0.854	0.760	0.706	0.670	0.591	0.548	0.505

$$F=\frac{1}{2d^2}\left(d-1+\left|\sum_{k\neq l}e^{i\theta_k}+\sqrt{2}e^{i\theta_l}\right|^2\right)$$

and is maximized when $\theta_k=0$, $k=1,\ldots,d$. The optimal economical phase-covariant cloning transformation which is invariant with respect to the swapping of the two clones and is also phase covariant can be thus expressed as

$$|k\rangle\rightarrow|kl^+\rangle, \tag{24}$$

where $l\in\{1,\ldots,d,\}$ is arbitrary, and the corresponding fidelity reads

$$F_{\rm econ}^{\rm PC}(d)=\frac{1}{2d^2}[d-1+(d-1+\sqrt{2})^2]. \tag{25}$$

It is interesting to compare the fidelity of this economical suboptimal cloner with the fidelity of the optimal d-dimensional phase-covariant cloner [15–17],

$$F_{\rm opt}^{\rm PC}(d)=\frac{1}{4d}(d+2+\sqrt{d^2+4d-4}). \tag{26}$$

The values of the fidelities $F_{\rm econ}^{\rm PC}$ and $F_{\rm opt}^{\rm PC}$ are displayed in Table I for several dimensions d. We see that the economical cloner exhibits very good performances and that its fidelity is only very slightly lower than that of the optimal cloner. More quantitatively, numerical calculations confirm that $F_{\rm opt}^{\rm PC}(d)-F_{\rm econ}^{\rm PC}(d)\leqslant 0.0045$ for all d.

V. FOURIER-COVARIANT CLONING MACHINES

A. Ansatz on the cloning transformation

Although it is not always easy to prove analytically that certain cloning machines optimize given quantities such as Bob or Eve's fidelities, an educated guess is often possible. For instance, one can show that the overwhelming majority of optimal $1\rightarrow 2$ cloning machines that can be found in the literature obeys the ansatz given in Refs. [33,34] based on "double-Bell" states [35]. According to this ansatz, the cloning transformation is represented by a pure state in a d^4-dimensional Hilbert space for the qudits conventionally labeled by A, B, E, and M, where A represents Alice's qudit and is formally equivalent to the label "in" introduced in the previous section, B and E represent Bob's and Eve's qudits as before, while M represents an external ancilla. Moreover, the cloning state is assumed to be biorthogonal in the Bell bases, where the d^2 Bell states for qudits are defined as follows:

$$|B_{m,n}\rangle_{1,2}=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\gamma^{kn}|k\rangle_1|k+m\rangle_2, \tag{27}$$

where $m,n\in\{0,1,\ldots,d-1\}$, $\gamma=e^{i2\pi/d}$ is the dth root of unity, and $|j\rangle_{1(2)}$ represents a state of the qudit system 1 (2) chosen in the computational basis. They are maximally entangled states and form an orthonormal basis of the d^2-dimensional Hilbert space of qudits 1 and 2. Because the cloning state is bi-orthogonal in the Bell bases, it can be expressed as follows:

$$|\Psi\rangle_{A,B,E,M}=\sum_{m,n=0}^{d-1}a_{m,n}|B_{m,n}\rangle_{A,B}|B_{m,-n}\rangle_{E,M}. \tag{28}$$

Here $a_{m,n}$ is a (normalized) $d\times d$ matrix. The specification of the d^2 amplitudes $a_{m,n}$ defines the cloning transformation. We now give several examples.

The optimal universal (generally asymmetric) cloning machine is defined by the following amplitude matrix:

$$a_{m,n}^U=x_1\delta_{m,0}\delta_{n,0}+x_3/d. \tag{29}$$

The optimal *symmetric* universal d-dimensional cloner (the one for which Eve's fidelity is maximal, under the constraint that Bob's fidelity is equal to Eve's fidelity) is obtained by choosing $x_1^2=x_3^2=d/[2(d+1)]$. It copies all states with the same fidelity. The qubit phase-covariant cloner copies equally well two mutually unbiased qubit bases (such that any basis state in one basis has equal squared amplitudes when expressed in the other basis). It possesses two interesting generalizations in higher dimension: (a) the phase-covariant cloner and (b) the Fourier-covariant cloner.

(a) The phase-covariant cloner has already been defined in Sec. III. It clones equally well all balanced superpositions of computational basis states, $|\psi\rangle=(1/\sqrt{d})\sum_{j=1}^{d}e^{i\phi_j}|j\rangle$. The asymmetric phase-covariant cloning machine is described (for arbitrary dimension) in Refs. [16,17]. It is defined by the following amplitude matrix:

$$a_{m,n}^{\rm PC}=x_1\delta_{m,0}\delta_{n,0}+x_2\delta_{m,0}+x_3, \tag{30}$$

where x_1, x_2 and x_3 are real positive parameters.

(b) The Fourier-covariant cloner clones equally well two mutually unbiased bases that are discrete Fourier transforms of each other. It is characterized by the following amplitude matrix [11]

$$a_{m,n}^F=x_1\delta_{m,0}\delta_{n,0}+x_2(\delta_{m,0}+\delta_{n,0})+x_3, \tag{31}$$

where x_1, x_2, and x_3 are real positive parameters.

B. Conditions for economical cloning

Let us investigate whether or not an economic realization of such optimal cloning machines is possible, that is, whether it is possible to reach the same fidelity without making use of the ancilla. Our analysis relies on the above ansatz on the form of the cloning transformation, but it is general in that it applies to all types of cloning machines (universal, phase covariant, and Fourier covariant, which is the case we are mostly interested in here). Concretely, cloning economically means that it is possible to find $l_{\max}$ probabilities p_l and $l_{\max}$ unitary transformations U^l_{BE} that act on the qudits B and E such that

$$S_{ABE} = \mathrm{Tr}_M \Psi^{\mathrm{opt}}_{A,B,E,M} = \sum_{l=1,\ldots,l_{\max}} p_l \Phi^l_{A,B,E}, \tag{32}$$

where $\Psi = |\Psi\rangle\langle\Psi|$ and $\Phi = |\Phi\rangle\langle\Phi|$ are short-hand notations for density matrices of pure states, and

$$|\Phi\rangle^l_{A,B,E} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A U^l_{BE} |k\rangle_B |\psi_0\rangle_E. \tag{33}$$

As a consequence of the convexity of the average fidelity of cloning, if the CP map S_{ABE} represents an optimal cloning transformation then each unitary transformation $\Phi^l_{A,B,E}$ is also optimal in a sense that it maximizes the average cloning fidelity. The support of the CP map S associated with the cloning machines that fulfill the ansatz (28) is spanned by the d states

$$|r_p\rangle = {}_M\langle p| \sum_{m,n=0}^{d-1} a_{m,n} |B_{m,n}\rangle_{A,B} |B_{m,-n}\rangle_{E,M}, \tag{34}$$

where $p \in \{0,1,\ldots,d-1\}$. In what follows we assume that the states $|r_p\rangle$ are eigenstates with maximum eigenvalue $r_{\max}$ of an operator R which appears in the formula for the cloning fidelity, $F = \mathrm{Tr}[RS_{ABE}]$. Moreover, we assume that the states $|r_p\rangle$ are the complete set of eigenstates with the eigenvalue $r_{\max}$. The results we obtained in the Secs. II and III revealed that this is true for a symmetric universal cloning machine for any d and for a phase-covariant cloning machine with $d=2,\ldots,7$. Here, we conjecture that this also holds for phase-covariant and Fourier-covariant cloning machines for arbitrary d.

If economical optimal cloning is possible, we must be able to construct the pure states $|\Phi\rangle^l_{A,B,E}$ which appear in Eqs. (32) and (33) as linear combinations of the states $|r_p\rangle$. This means that there must exist $dl_{\max}$ amplitudes α^l_k (with $\sum_{k=0}^{d-1} |\alpha^l_k|^2 = 1$) such that

$$U^l_{BE} |k\rangle_B |\psi_0\rangle_E = \sum_{m,n,j=0}^{d-1} \alpha^l_{j+m} a_{m,n} \gamma^{n(k-j)} |k+m\rangle_B |j\rangle_E, \tag{35}$$

for $l=1,\ldots,l_{\max}$. The constraints (35) are a necessary condition for the existence of economical cloning, whenever the support of the admissible CP maps S^l associated with the economical cloning transformations U^l is spanned by the d states $|r_p\rangle$.

Let us assume that the optimal cloning state is given by Eq. (28) with the amplitude matrix (31), which includes the class of (symmetric and asymmetric) universal and Fourier-covariant cloning machines. If an economical realization of such cloners exists, then there must exist d amplitudes α_k and a unitary transformation U_{BE} which satisfy Eq. (35). On inserting the explicit formula (31) for the amplitude matrix $a_{m,n}$ into Eq. (35) we obtain

$$U_{BE} |k\rangle_B |\psi_0\rangle_E = \sum_{j,m=0}^{d-1} \alpha_{m+j} [x_1 \delta_{m,0} + d x_3 \delta_{j,k} + x_2 (d \delta_{m,0} \delta_{j,k} + 1)] \times |m+k\rangle_B |j\rangle_E. \tag{36}$$

Unitarity [or equivalently trace preservation (6)] imposes the following condition:

$${}_B\langle k'|_E\langle \psi_0| U^\dagger_{BE} U_{BE} |k\rangle_B |\psi_0\rangle_E = \delta_{k,k'}. \tag{37}$$

Taking $k=k'$ in Eqs. (36) and (37) we get after some algebra

$$\sum_j |\alpha_j|^2 f_d(x_1,x_2,x_3) + |\alpha_k|^2 g_d(x_1,x_2,x_3) = 1, \quad \forall\, k, \tag{38}$$

where f_d and g_d are second order polynomials in x_j,

$$f_d = x_1^2 + d x_2^2 + d^2 x_3^2 + 2 x_1 x_2 + 2 d x_2 x_3,$$

$$g_d = (d^2 + 2d) x_2^2 + 2 d x_1 x_2 + 2 d x_1 x_3 + 2 d^2 x_2 x_3. \tag{39}$$

If we now consider the case $k \neq k'$ in Eq. (37) we obtain

$$(d x_2^2 + 2 x_1 x_2 + 2 d x_2 x_3) \sum_j \alpha_j \alpha^*_{j+k-k'} + d x_2^2 (\alpha_k \alpha^*_{2k-k'} + \alpha_{2k'-k} \alpha^*_{k'}) + 2 d x_1 x_3 \alpha_{k'} \alpha^*_k = 0. \tag{40}$$

Normalization of the cloning state (28) imposes that $f_d + g_d/d = 1$. In virtue of Eq. (38), either $|\alpha_k|^2 = 1/d$, $\forall k$ or $g_d = 0$. The latter constraint is neither satisfied by the universal nor by the Fourier-covariant cloners so that in order that such cloners admit an economical realization $|\alpha_k|^2 = 1/d$ and the norms of all the d a priori unknown parameters α_k must be equal. In order to ensure unitarity, it is still necessary to fulfill the condition (40). It is worth noting that in Eq. (40) only products of α^*_i and α_j appear of which the indices differ by the same quantity $i-j=k-k'$. Hence, if we make the substitution $k'=k-m$ in Eq. (40) and then sum over $m=0,\cdots,d-1$, we get the following constraint:

$$g_d(x_1,x_2,x_3) \sum_j \alpha_j \alpha^*_{j+m} = 0, \quad m \neq 0.$$

Since $g_d=0$ is never satisfied by the optimal universal or Fourier-covariant cloners, we find that $\sum_j \alpha_j \alpha^*_{j+m} = 0$, $m \neq 0$. As a consequence, the satisfaction of condition (40) also implies

$$x_2^2 (\alpha_k \alpha^*_{2k-k'} + \alpha_{2k'-k} \alpha^*_{k'}) + 2 x_1 x_3 \alpha_{k'} \alpha^*_k = 0. \tag{41}$$

In the case of the universal cloner, $x_2=0$ and $x_1 x_3 \neq 0$, so it is clear that no solution exists for this system of equations for any $d \geqslant 2$, confirming Sec. II. In the case of the Fourier-covariant cloner, we shall show that this system of equations admits a solution only in dimension $d=2$. The solution then corresponds to the Niu-Griffiths economical realization of the qubit phase-covariant cloner already mentioned in previous sections. The asymmetric economical realization of this cloner was studied in detail in Ref. [25].

For the optimal Fourier-covariant cloner, it can be shown that the ancilla does not bring extra information about the state under copy, which is expressed by the relation

$x_2^2=x_1x_3$. The amplitudes α_j must then obey the relations

$$\alpha_k\alpha^*_{2k-k'}+\alpha_{2k'-k}\alpha^*_{k'}+2\alpha_{k'}\alpha^*_k=0, \quad \forall\, k\neq k'. \tag{42}$$

Since all the amplitudes α_j have the same norm, the triangular inequality together with Eq. (42) implies that

$$\alpha_k\alpha^*_{k+m}=\alpha_{k-2m}\alpha^*_{k-m}=-\alpha_{k-m}\alpha^*_k. \tag{43}$$

It is convenient to consider normalized amplitudes $\tilde{\alpha}_j=\sqrt{d}\alpha_j$, $|\tilde{\alpha}_j|=1$. Taking $m=1$ we obtain from Eq. (43) the recurrence formula $\tilde{\alpha}_{k+1}=-\tilde{\alpha}_k^2\tilde{\alpha}^*_{k-1}$. Without loss of generality, we can assume $\tilde{\alpha}_0=1$ and express all $\tilde{\alpha}_j$ in terms of $\tilde{\alpha}_1$ as follows: $\tilde{\alpha}_{2n}=(-1)^n\tilde{\alpha}_1^{2n}$ and $\tilde{\alpha}_{2n+1}=(-1)^n\tilde{\alpha}_1^{2n+1}$. Substituting these expressions in the constraint $\Sigma_{l=0}^{d-1}\alpha_j\alpha^*_{j+m}=0$ with $m=2$ leads to $\tilde{\alpha}_1^2=0$, which contradicts the fact that $|\tilde{\alpha}_1|=1$. It is only in dimension 2 that the contradiction can be avoided because $m=2=0$ modulo d in dimension 2.

C. Suboptimal economical Fourier-covariant cloner

Since the optimal Fourier-covariant cloner seems to require an ancilla for $d>2$, we can again seek an approximate economical version of this cloner. It turns out that the economical phase-covariant cloner discussed in Sec. IV can readily be used also for the economical Fourier-covariant cloning. As a matter of fact, this is the best economical Fourier-covariant cloner that we could find, although we have no proof that a better such cloner does not exist. In order to employ the economical phase-covariant cloner, Eq. (24), we need to work in a basis B where both the computational basis states and Fourier basis states are expressed as balanced superpositions of the states of the basis B.

This is possible due to the property that in each dimension there exist three mutually unbiased bases which may be expressed as eigenstates of the operators X_d, Z_d, and X_dZ_d, where X_d and Z_d are d-dimensional generalizations of the Pauli matrices σ_X and σ_Z, $Z_d|n\rangle=\exp(i2\pi n/d)|n\rangle$ and $X_d|n\rangle=|n+1\rangle$. This follows from the theorem 2.1 of Ref. [36]. The eigenstates of Z_d form the computational basis, the eigenstates of X_d represent the Fourier basis, and the eigenstates of X_dZ_d provide the basis where all the states we want to clone become balanced superpositions of the basis states. Therefore the economical phase-covariant cloner of Sec. IV could be used to clone these states. The fidelity of this cloner is of course still given by Eq. (25). When we compare it with the fidelity of the optimal d-dimensional Fourier-covariant cloner [11]

$$F^{\text{Fourier}}_{\text{opt}}=\frac{1}{2}\left(1+\frac{1}{\sqrt{d}}\right),$$

we find that the difference between the optimal and economical fidelities can be rather large, up to 0.07. Thus, this economical version of the Fourier-covariant cloner performs rather badly compared to the economical version of the phase-covariant cloner. This is expected since it clones with the same fidelity a larger class of states than needed.

D. Economical phase-covariant cloner

Although the possibility for economical phase-covariant cloner was already discussed in Sec. III, we treat it here (in the symmetric or asymmetric version) with the parametrization used above in the present section as it presents many similarities with the Fourier-covariant case. When the constraints (30) and (35) are satisfied, it is easy to derive the following system of equations:

$$x_1^2+d^2x_3^2+|\alpha_k|^2(g_d-2dx_2^2)=1, \quad \forall\, k,$$

$$2dx_1x_3\alpha^*_{-k'}\alpha_k=0, \quad \forall\, k\neq k'. \tag{44}$$

The solution of the second constraint is $\alpha_k=\delta_{k,l}$. Inserting in the first constraint, we get the equation $x_1^2+d^2x_3^2=1$ which is fulfilled in dimension $d=2$ only, in virtue of the identity $x_3^2=(x_1+x_2+x_3)(x_2+x_3)$, and of the normalization of the cloning state $x_1^2+d^2x_3^2+dx_2^2+2x_1x_2+2x_1x_3+2d.x_2x_3=1$, in which case we recover the Fourier-covariant cloner and its Niu-Griffiths economical realization. Note that this proof provides strong evidence of the impossibility of economical $1\to 2$ phase-covariant cloning in any finite dimension different from 2, extending the strict proof of Sec. III for dimensions 3 to 7. Note also that the two-dimensional realization of the phase-covariant cloner (30) differs, in our parametrization, from the two-dimensional Fourier covariant cloner (31), but they can be shown to be equivalent up to a change of basis and a relabeling of the x parameters.

VI. CONCLUSIONS

In this paper, we have focused on $1\to 2$ cloning machines in arbitrary dimensions, and have investigated the connections between the cloners with and without ancilla. We have established a series of no-go theorems for economical cloning, some of them being firm (universal cloner), others relying on an ansatz which was only tested numerically (phase-covariant and Fourier-covariant cloners). In short, no economical universal cloner exists in any dimension, while we need $d=2$ to find an economical version of the phase-covariant and Fourier-covariant cloners (in which case they coincide).

Note that, in our approach, the figure of merit is the cloning fidelity, but it seems that the cloners that optimize Eve's information also fulfill the ansatz (28). In this case, the CP map approach is not very well adapted because of the nonlinearity of the information measure. Nevertheless, we were able to establish the validity of the condition (32) in an independent manner, under the assumption of optimality of the ansatz only.

Our results strongly suggest that the Niu-Griffiths economical phase-covariant cloning machine for qubits is quite unique among the optimal $1\to 2$ cloning machines. This conclusion is of importance in connection with the security of quantum cryptographic protocols because it shows that the realization of cloning attacks on quantum cryptographic protocols that exploit higher-dimensional Hilbert spaces would require the mastering and control of three-qudit transformations, which constitutes a serious technological challenge. Another possibility would be of course to implement a suboptimal economical phase-covariant cloner, as presented in Sec. IV, but the resulting attack would be weaker.

To be complete, it is worth noting that in the limit of an infinite dimension, the optimal phase-covariant, Fourier-covariant, and universal cloners tend all to a fidelity of $1/2$, for which an economical realization exists: the original qudit is replaced by noise and directed to Eve with probability $1/2$, or resent to Bob without disturbance while Eve receives the noise with probability $1/2$. In this rather trivial limit, economical cloning is thus always possible, and extremely cheap.

In a future work, it would be interesting to study the possibility of economical $1 \rightarrow N$ cloning, where it seems that the limitations are less drastic than in the $1 \rightarrow 2$ case. For instance, the $1 \rightarrow 3$ and $1 \rightarrow N$ cloners studied in Refs. [26,37,38] also admit an economical realization.

ACKNOWLEDGMENTS

Special thanks to Helle Bechmann-Pasquinucci (QUIT group, University of Pavia), who is partially at the origin of this work, and to the other members of the QUIT group for stimulating discussions. These discussions have led independently to the present paper and to Ref. [26]. T.D. thanks the Fonds voor Wetenschappelijke Onderzoek-Vlaanderen for financial support. This research was supported by the Belgian Office for Scientific, Technical and Cultural Affairs in the framework of the Inter-University Attraction Pole Program of the Belgian government under grant V-18, the Fund for Scientific Research-Flanders (FWO-V), the Concerted Research Action "Photonics in Computing," the Solvay Institutes for Physics and Chemistry, and the research council (OZR) of the VUB. N.J.C. and J.F. acknowledge financial support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, and from the European Union under projects Nos. RESQ (IST-2001-37559) and SECOQC (IST-2002-506813). J.F. also acknowledges support from the Grant No. MSM 6198959213 of the Czech Ministry of Education.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] H.-K. Cummins, C. Jones, A. Furze, N-F Soffe, M. Mosca, J. M. Peach, and J-A Jones, Phys. Rev. Lett. **88**, 187901 (2002).
[3] N. Gisin, I. Marcikic, H. de Riedmatten, W. Tittel, and H. Zbinden, Nature (London) **421**, 509 (2003).
[4] S. Gulde, M. Riebe, G. P-T Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) **421**, 48 (2003).
[5] J. Jones, Nature (London) **421**, 29 (2003).
[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[7] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.
[8] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[9] D. Dieks, Phys. Lett. **92**, 271 (1982).
[10] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[11] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002); M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, J. Phys. A **35**, 10065 (2002).
[12] D. Bruss, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
[13] N. J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002).
[14] H. Fan, K. Matsumoto, X.-B. Wang, and M. Wadati, Phys. Rev. A **65**, 012304 (2002).
[15] H. Fan, H. Imai, K. Matsumoto, and X. B. Wang, Phys. Rev. A **67**, 022317 (2003).
[16] A. T. Rezakhani, S. Siadatnejad, and A. H. Ghaderi, Phys. Lett. A **336**, 278 (2005).
[17] L.-P. Lamoureux and N. J. Cerf, Quantum Inf. Comput. **5**, 32 (2005).
[18] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[19] R. B. Griffiths and C.-S. Niu, Phys. Rev. A **56**, 1173 (1997).
[20] T. Durt, N. J. Cerf, N. Gisin, M. Zukowski, Phys. Rev. A **67**, 012311 (2003).
[21] T. Durt, D. Kaszlikowski, J-L Chen, and L-C Kwek, Phys. Rev. A **69**, 032313 (2004).
[22] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[23] J. Du, T. Durt, P. Zou, L. C. Kwek, C. H. Lai, C. H. Oh, and A. Ekert, Phys. Rev. Lett. **94**, 040505 (2005).
[24] C-S. Niu and R. B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
[25] T. Durt and J. Du, Phys. Rev. A **69**, 062316 (2004).
[26] F. Buscemi, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).
[27] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[28] M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975).
[29] J. Fiurášek, Phys. Rev. A **64**, 062310 (2001).
[30] J. Fiurášek, Phys. Rev. A **67**, 052314 (2003).
[31] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[32] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[33] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); J. Mod. Opt. **47**, 187 (2000).
[34] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[35] The deep reason for the appearance of Bell states in the formalism of cloning machines is the invariance with respect to the discrete Weyl-Heisenberg group (see G. Chiribella, G. M. D'Ariano, P. Perinotti, and N. J. Cerf, quant-ph/0507130). In a paper in preparation, the role of a cyclic subgroup of this group will be analyzed in details. It will be shown that some restrictive assumptions must be made about the optimality of the cloner (see also Ref. [21]).
[36] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[37] V. Bužek, S. L. Braunstein, M. Hillery, and D. Bruss, Phys. Rev. A **56**, 3446 (1997).
[38] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).