Optimal probabilistic cloning and purification of quantum states

Jaromír Fiurášek[1,2]
[1]*QUIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[2]*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*

(Received 25 March 2004; published 10 September 2004)

We investigate the probabilistic cloning and purification of quantum states. The performance of these probabilistic operations is quantified by the average fidelity between the ideal and actual output states. We provide a simple formula for the maximal achievable average fidelity and we explicitly show how to construct a probabilistic operation that achieves this fidelity. We illustrate our method on several examples such as the phase covariant cloning of qubits, cloning of coherent states, and purification of qubits transmitted via depolarizing channel and amplitude damping channel. Our examples reveal that the probabilistic cloner may yield higher fidelity than the best deterministic cloner even when the states that should be cloned are linearly dependent and are drawn from a continuous set.

DOI: 10.1103/PhysRevA.70.032308 PACS number(s): 03.67.Pp, 03.65.−w

I. INTRODUCTION

The recent spectacular development of the quantum information theory has revealed that information processing based on the laws of quantum mechanics enables implementation of tasks that are impossible or very hard to accomplish classically. The prime examples are the quantum cryptography which allows unconditionally secure distribution of a secret key [1] and the exponential speedup of certain computational tasks, such as the factoring of integers [2]. On the other hand, the linearity of quantum mechanics also imposes certain constraints on the processing of quantum information that have no classical counterpart. Perhaps the most famous example is the no-cloning theorem which states that an unknown quantum state cannot be copied [3]. However, this restriction provides, in fact, a valuable resource explored in the quantum key distribution protocols, because it forbids an eavesdropper to gain information on the distributed secret key without introducing errors.

Since exact copying is forbidden, a natural problem arises what is the optimal approximate cloning transformation. This question was first asked by Bužek and Hillery in their seminal paper [4] and since then it has been addressed by numerous authors who considered various cloning scenarios, such as cloning of qubits [5,6], cloning of d-dimensional systems (qudits) [7–11] and cloning of continuous variables [12–14]. Much attention has been recently paid also to the cloning of subsets of Hilbert space, such as the phase covariant cloning machine for equatorial qubits [15–18] and cloning of real states [19] or maximally entangled states [20]. Remarkably, the cloning machines turned out to be very efficient or even optimal eavesdropping attacks on many quantum cryptographic protocols [21–24] and their investigation is largely motivated by these practical aspects.

Typically, the cloner is assumed to be a deterministic machine that always produces an output. Nevertheless, one can consider also probabilistic cloning machines that sometimes fail and do not provide any outcome. The probabilistic cloners have been discussed in the literature in the context of cloning of a discrete finite set of quantum states and it was shown that an exact probabilistic cloning is possible if and only if the set consists of linearly independent states [25,26].

However, one may hope that the probabilistic machines may yield better results also for the sets of linearly dependent quantum states and even for infinite (continuous) sets. Here, we investigate the probabilistic cloning of linearly dependent states and we establish a general theory of the optimal probabilistic cloning machines. We provide a simple formula for the maximal average fidelity of the probabilistic machine and we also show how to construct the optimal cloning transformations.

In fact, our formalism is very general and it concerns optimal probabilistic implementations of arbitrary transformations whose outputs should ideally be pure states. Besides cloning, this includes also universal NOT gate for qubits [27,28], and, perhaps even more importantly, probabilistic purification of mixed quantum states [29–31]. In what follows we first establish the general formalism and then we work out several explicit examples that will illustrate our method.

II. OPTIMAL PROBABILISTIC TRANSFORMATIONS

The probabilistic machines investigated in the present paper optimally (in a sense defined below) approximate the map from a set S_{in} of input (generally mixed) states ρ_{in} to the set S_{out} of the output pure states $|\psi_{\mathrm{out}}\rangle$,

$$\rho_{\mathrm{in}} \rightarrow \psi_{\mathrm{out}}(\rho_{\mathrm{in}}), \tag{1}$$

where $\psi_{\mathrm{out}} \equiv |\psi_{\mathrm{out}}\rangle\langle\psi_{\mathrm{out}}|$ is a short-hand notation for the density matrix of a pure state. If S_{in} is a set of pure states (such as in the case of cloning) then we replace ρ_{in} with ψ_{in}. The most general probabilistic transformation in quantum mechanics is a linear trace decreasing completely positive (CP) map [32] that transforms operators on the input Hilbert space $\mathcal{H}_{\mathrm{in}}$ onto the operators on the output Hilbert space $\mathcal{H}_{\mathrm{out}}$. In what follows we will exploit the isomorphism between a CP map $\rho_{\mathrm{out}} = \mathcal{E}(\rho_{\mathrm{in}})$ and a positive semidefinite operator E on the Hilbert space $\mathcal{H} = \mathcal{H}_{\mathrm{in}} \otimes \mathcal{H}_{\mathrm{out}}$ [33,34]. Let $|j\rangle$ denote a basis in a d-dimensional Hilbert space $\mathcal{H}_{\mathrm{in}}$. The operator E can be obtained from the maximally entangled state on $\mathcal{H}_{\mathrm{in}} \otimes \mathcal{H}_{\mathrm{in}}$,

1050-2947/2004/70(3)/032308(9)/$22.50

$|\Phi\rangle=\Sigma_{j=1}^{d}\,|j\rangle_A|j\rangle_B$, if we apply the map $\mathcal{E}$ to one part of $|\Phi\rangle$. We have $E=\mathcal{I}_A\otimes\mathcal{E}_B(\Phi)$ where $\mathcal{I}$ denotes the identity map.

The transformation $\rho_{\mathrm{out}}=\mathcal{E}(\rho_{\mathrm{in}})$ can be rewritten in terms of E as follows:

$$\rho_{\mathrm{out}}=\mathrm{Tr}_{\mathrm{in}}[E\rho_{\mathrm{in}}^{T}\otimes\mathbb{1}_{\mathrm{out}}],\tag{2}$$

where $\mathrm{Tr}_{\mathrm{in}}$ denotes the partial trace over the input Hilbert space and T stands for the transposition in the basis $|j\rangle$. The map must be trace decreasing which means that $\mathrm{Tr}[\rho_{\mathrm{out}}]\leqslant\mathrm{Tr}(\rho_{\mathrm{in}})$ for all $\rho_{\mathrm{in}}\geqslant 0$. This implies that E must satisfy the inequality

$$\mathrm{Tr}_{\mathrm{out}}(E)\leqslant\mathbb{1}_{\mathrm{in}},\tag{3}$$

where $\mathbb{1}$ denotes the identity operator and the equality in (3) is achieved by deterministic (trace preserving) CP maps.

Consider a particular input ρ_{in}. The normalized output state $\tilde{\rho}_{\mathrm{out}}$ is given by $\tilde{\rho}_{\mathrm{out}}=\rho_{\mathrm{out}}/P(\rho_{\mathrm{in}})$ where

$$P(\rho_{\mathrm{in}})=\mathrm{Tr}[E\rho_{\mathrm{in}}^{T}\otimes\mathbb{1}_{\mathrm{out}}]\tag{4}$$

is the probability of successful application of the map $\mathcal{E}$ to ρ_{in}. The performance of the map $\mathcal{E}$ for the particular input ρ_{in} can be conveniently quantified by the fidelity between the actual and the ideal outputs

$$F(\rho_{\mathrm{in}})=\langle\psi_{\mathrm{out}}|\tilde{\rho}_{\mathrm{out}}|\psi_{\mathrm{out}}\rangle.\tag{5}$$

Expressed in terms of E we have

$$F(\rho_{\mathrm{in}})=\frac{1}{P(\rho_{\mathrm{in}})}\mathrm{Tr}(E\ \rho_{\mathrm{in}}^{T}\otimes\psi_{\mathrm{out}}).\tag{6}$$

We assume that the set S_{in} is endowed with an *a priori* probability distribution $d\rho_{\mathrm{in}}$ such that $\int_{S_{\mathrm{in}}}d\rho_{\mathrm{in}}=1$. Here and in what follows we assume that the set S_{in} is continuous. Of course, all formulas remain valid also for discrete sets, one simply must replace the integrals with corresponding summations over the elements of S_{in}.

The average probability of success is defined as

$$\overline{P}=\int_{S_{\mathrm{in}}}P(\rho_{\mathrm{in}})d\rho_{\mathrm{in}}=\mathrm{Tr}[EA],\tag{7}$$

where

$$A=\int_{S_{\mathrm{in}}}\rho_{\mathrm{in}}^{T}\otimes\mathbb{1}_{\mathrm{out}}d\rho_{\mathrm{in}}.\tag{8}$$

We now introduce the mean fidelity F of the transformation $\mathcal{E}$ as the average of the fidelities $F(\rho_{\mathrm{in}})$, with proper weights $P(\rho_{\mathrm{in}})d\rho_{\mathrm{in}}/\overline{P}$,

$$F=\int_{S_{\mathrm{in}}}F(\rho_{\mathrm{in}})\frac{P(\rho_{\mathrm{in}})}{\overline{P}}d\rho_{\mathrm{in}}.\tag{9}$$

The mean fidelity is the figure of merit considered in the present paper and in what follows we shall look for the optimal map $\mathcal{E}$ that maximizes F.

If we insert the expression (6) into Eq. (9) we obtain $F=\overline{F}/\overline{P}$ where $\overline{F}=\mathrm{Tr}[ER]$ and

$$R=\int_{S_{\mathrm{in}}}\rho_{\mathrm{in}}^{T}\otimes\psi_{\mathrm{out}}\,d\rho_{\mathrm{in}}.\tag{10}$$

Taking everything together, we want to find E that maximizes the mean fidelity

$$F=\frac{\mathrm{Tr}(ER)}{\mathrm{Tr}(EA)},\tag{11}$$

where $R\geqslant 0$ and $A>0$ are defined above. The positive semidefinite operator E representing a trace-decreasing CP map must satisfy the constraint (3). However, this constraint is irrelevant as far as the mean fidelity (11) is concerned because the value of F does not change under the renormalization,

$$E\to E'=e_{\max}^{-1}E,\tag{12}$$

where $e_{\max}=\max[\mathrm{eig}(\mathrm{Tr}_{\mathrm{out}}E)]$, $\mathrm{eig}(X)$ denotes the set of eigenvalues of X, and E' satisfies the inequality (3) by construction. This fact greatly simplifies the analysis. Strictly speaking, these arguments are valid only for finite dimensional Hilbert spaces where $e_{\max}$ is always finite and $\overline{P'}=\mathrm{Tr}[E'A]>0$ since $A>0$. As we will see in the next section, a little extra care is needed when dealing with infinite dimensional systems.

The above argumentation shows that we have to maximize the fidelity (11) under the constraint $E\geqslant 0$. We now show that the optimal E can always be assumed to be a rank one operator (a pure state). Suppose that E represents the optimal CP map. Since $E\geqslant 0$ we can express it as a convex mixture of rank one operators, $E=\Sigma_j\ e_j|E_j\rangle\langle E_j|$ with $e_j>0$. Let $F_j=\mathrm{Tr}(E_jR)/\mathrm{Tr}(E_jA)$ denote the mean fidelity corresponding to the map $E_j\equiv|E_j\rangle\langle E_j|$. On inserting the expansion of E into Eq. (11) we obtain

$$F=\frac{\sum_j\ p_jF_j}{\sum_k\ p_k}\leqslant\max_j(F_j),\tag{13}$$

where $p_j=e_j\ \mathrm{Tr}(E_jA)>0$. If E is optimal map, then Eq. (13) implies that all the fidelities $F_j=F$ and, consequently, the maximum mean fidelity F is achieved by each rank-one operator E_j. We can thus assume $E=|E\rangle\langle E|$ and we introduce new state $|\tilde{E}\rangle=A^{1/2}|E\rangle$ and rewrite (11) as follows:

$$F=\frac{\langle\tilde{E}|A^{-1/2}RA^{-1/2}|\tilde{E}\rangle}{\langle\tilde{E}|\tilde{E}\rangle}.\tag{14}$$

It follows that the optimal vector $|\tilde{E}\rangle$ is the eigenvector $|\mu_{\max}\rangle$ of $M=A^{-1/2}RA^{-1/2}$ that corresponds to the maximal eigenvalue $\mu_{\max}$ of M. The maximal achievable mean fidelity is equal to the maximal eigenvalue,

$$F_{\max}=\max[\mathrm{eig}(A^{-1/2}RA^{-1/2})].\tag{15}$$

This formula is one of the the main results of the present paper. The transformation that achieves $F_{\max}$ is explicitly given by

$$E = e_{\max}^{-1} A^{-1/2} |\mu_{\max}\rangle\langle\mu_{\max}| A^{-1/2}, \tag{16}$$

where we have normalized according to (12) so that E is a trace-decreasing map. If the largest eigenvalue $\mu_{\max}$ is nondegenerate, then this is the unique optimal E and the problem is thus completely solved. However, if the eigenvalue $\mu_{\max}$ is n-fold degenerate, with $|\mu_{\max,j}\rangle$, $j=1,\ldots,n$ being the n eigenvectors, then there exist many different transformations that saturate the fidelity bound (15). It can be proved by direct substitution into Eq. (11) that any operator

$$E = \sum_{j,k=1}^{n} E_{jk} A^{-1/2} |\mu_{\max,j}\rangle\langle\mu_{\max,k}| A^{-1/2} \tag{17}$$

yields the maximal fidelity $F=\mu_{\max}$. Let $\mathcal{K}$ be the Hilbert space spanned by the vectors $A^{-1/2}|\mu_{\max,j}\rangle$. Then E can be any positive semidefinite operator on $\mathcal{K}$ that satisfies (3). In this case, we would like to find the map E that maximizes the average probability of success $\overline{P}$ while reaching the fidelity $F_{\max}$. The optimization problem that must be solved can be formulated as follows:

$$\text{maximize} \quad \overline{P} = \mathrm{Tr}[EA] \quad \text{under the constraints}$$

$$E \geqslant 0, \quad E \in B(\mathcal{K}), \quad \mathrm{Tr}_{\mathrm{out}}[E] \leqslant \mathbb{1}, \tag{18}$$

where $B(\mathcal{K})$ denotes the set of linear bounded operators on $\mathcal{K}$. This is an instance of the so-called semidefinite program (SDP) that can be very efficiently solved numerically and by means of the duality lemma one can easily check that the global maximum was found [35]. In this context it is worth noting that many optimization problems in quantum information theory can be formulated as semidefinite programs. This includes several separability criteria [36,37], calculation of distillable entanglement [38], optimization of the teleportation protocols with mixed entangled states [39], determination of optimal POVM for discrimination of quantum states [40,41], derivation of optimal trace-preserving CP maps for cloning [42,43], construction of local hidden variable theories [44], etc.

Generally, the fidelity $F(\rho_{\mathrm{in}})$ will depend on ρ_{in}. However, there is an important class of sets of input states S_{in} and transformations (1) such that the optimal CP map is universal. By universality we mean that the probability of success $P(\rho_{\mathrm{in}})$ as well as the fidelity $F(\rho_{\mathrm{in}})$ is independent of ρ_{in}. This occurs whenever the set of the input and output states can be obtained as orbits of some group G. Consider a compact group G with elements g. Let $U(g)$ and $V(g)$ denote unitary representations of G on $\mathcal{H}_{\mathrm{in}}$ and $\mathcal{H}_{\mathrm{out}}$, respectively. The unitary $U(g)$ generates the set of input states,

$$\rho_{\mathrm{in}}(g) = U(g)\rho_{\mathrm{in}}(g_0)U^{\dagger}(g), \tag{19}$$

where g_0 is the identity element of the group and $U(g_0)=\mathbb{1}$. We also assume that the set of output states can be obtained from $\psi_{\mathrm{out}}(g_0)$ as follows:

$$\psi_{\mathrm{out}}(g) = V(g)\psi_{\mathrm{out}}(g_0)V^{\dagger}(g) \tag{20}$$

and $V(g_0)=\mathbb{1}$. The final assumption is that the distribution of the inputs coincides with the invariant measure on the group G, $d\rho_{\mathrm{in}}=dg$. Under these assumptions, it is possible to convert any optimal map $\mathcal{E}$ into a universal map $\widetilde{\mathcal{E}}$ that achieves the same fidelity as $\mathcal{E}$ by the twirling operation. One first applies randomly a unitary $U(h)$ to the input and then this is undone by applying $V^{-1}(h)$ to the output. The composition of the twirling operation with the map $\mathcal{E}$ yields

$$\rho_{\mathrm{out}}(g) = \int_G V^{\dagger}(h)\mathrm{Tr}_{\mathrm{in}}[E\rho_{\mathrm{in}}^{T}(hg) \otimes \mathbb{1}_{\mathrm{out}}]V(h)dh, \tag{21}$$

and the probability of success reads

$$P'[\rho_{\mathrm{in}}(g)] = \int_G \mathrm{Tr}[E\rho_{\mathrm{in}}^{T}(hg) \otimes \mathbb{1}_{\mathrm{out}}]dh = \overline{P}. \tag{22}$$

Here, we used the group composition law $U(h)U(g)=U(hg)$ to obtain $U(h)\rho_{\mathrm{in}}(g)U^{\dagger}(h)=\rho_{\mathrm{in}}(hg)$, and the substitution $q=hg$, $dq=dh$. Similarly, we find that

$$F'(\rho_{\mathrm{in}}) = \frac{1}{\overline{P}}\int_G \mathrm{Tr}[E\rho_{\mathrm{in}}^{T}(hg) \otimes \psi_{\mathrm{out}}(hg)]dh = F, \tag{23}$$

which confirms that the twirling operation results in a universal machine that works equally well for all possible input states.

III. PROBABILISTIC CLONING

Having established the general formalism, we now turn our attention to the explicit examples of application. Let us first consider the universal symmetric $1\rightarrow M$ cloning machine for qubits. Here, the input state is a single qubit $|\psi\rangle=\cos(\vartheta/2)|0\rangle+e^{i\phi}\sin(\vartheta/2)|1\rangle$, uniformly distributed over the surface of the Bloch sphere, $d\psi_{\mathrm{in}}=(1/4\pi)\sin\vartheta\, d\vartheta\, d\phi$. The cloning machine should produce M identical clones, hence $\psi_{\mathrm{out}}=\psi_{\mathrm{in}}^{\otimes M}$ and $\mathcal{H}_{\mathrm{out}}$ is the fully symmetric subspace of M qubits. The operators R and A can be easily determined with the help of Schur's lemma which states that an operator which commutes with all elements of an irreducible representation of a group is proportional to the identity operator. It can be shown that the integration over the surface of the Bloch sphere yields the same result as the integration over the whole group SU(2) with the invariant Haar measure dg. Consider the operator $X=\int_{\mathrm{SU}(2)}[\psi(g)]^{\otimes K}\, dg$, where $|\psi(g)\rangle=U(g)|0\rangle$ and $g\in\mathrm{SU}(2)$. The support of X is the fully symmetric subspace of K qubits and let $\Pi_{+,K}$ denote the projector onto this subspace. The representation $V(g)=\Pi_{+,K}[U(g)]^{\otimes K}\Pi_{+,K}$ of the group SU(2) on the fully symmetric subspace of K qubits is irreducible and the operator X commutes with all unitaries $V(g)$ (this follows from the invariance of the Haar measure). Schur's lemma then implies that $X=\Pi_{+,K}/(K+1)$, where the normalization prefactor was determined from $\mathrm{Tr}(X)=1$. Using this result, we obtain

$$R = \frac{1}{M+2}(\Pi_{+,M+1})^{T_1}, \quad A = \tfrac{1}{2}\mathbb{1}_{\mathrm{in}} \otimes \mathbb{1}_{\mathrm{out}}, \tag{24}$$

where T_1 indicates partial transposition with respect to the first (input) qubit. On inserting the operators (24) into Eq.

(15) we find that $F_{\max}=2/(M+1)$. As shown in Ref. [7] the optimal deterministic cloning machine saturates this bound, hence it is impossible to improve the fidelity via probabilistic cloning.

Let us now consider the transposition operation for qudits, i.e., a map that produces a transposed qudit state ψ^T (in some fixed basis) from N copies of ψ, $\psi^{\otimes N}\rightarrow\psi^T$. For qubits, this map is unitarily equivalent to the universal NOT gate $\psi^{\otimes N}\rightarrow\psi_{\perp}$ [27,28]. The Hilbert space $\mathcal{H}_{\text{in}}$ is the fully symmetric subspace of the Hilbert space of N qudits and $\mathcal{H}_{\text{out}}$ is the Hilbert space of a single qudit. In the formulas (8) and (10) for A and R we average over all ψ_{in} that are represented as orbits of the group SU(d) according to Eq. (19). The probability density $d\psi_{\text{in}}\equiv dg$, where dg is the invariant Haar measure on the group SU(d). With the help of Schur's lemma one easily finds

$$A=\frac{1}{D(N,d)}\mathbb{1}_{\text{in}}\otimes\mathbb{1}_{\text{out}},\quad R=\frac{1}{D(N+1,d)}\Pi^{(d)}_{+,N+1},\tag{25}$$

where $\Pi^{(d)}_{+,N+1}$ is the projector onto symmetric subspace of $N+1$ qudits and $D(N+1,d)=\binom{N+d}{d-1}$ is the dimension of this subspace. The optimal fidelity obtained from Eq. (15) reads $F_{\max}=(N+1)/(N+d)$, which is exactly the fidelity of the optimal *deterministic* estimation of the qudit state from N copies [45]. Hence the optimal approximate transposition map simply consists of the optimal estimation of ψ followed by the preparation of the transposed estimated state. Note also that the fidelity $F_{\max}=2/(d+1)$ of the optimal deterministic transposition map for $N=1$ was recently derived in Ref. [46].

In all the above examples the optimal probabilistic machine could not outperform the deterministic machines. This can be attributed to the very high symmetry present in all the above considered examples. The question is whether there are interesting cases when S_{in} is a continuous set of linearly dependent states and the probabilistic machine achieves higher fidelity than the deterministic one. Below we answer this question in affirmative by providing explicit examples. We will focus on phase covariant cloning machines, where the underlying group is the Abelian group U(1). Specifically, we shall first consider probabilistic $N\rightarrow M$ phase covariant cloning of qubits [15,17]. Here, the input state $|\psi\rangle=(|0\rangle+e^{i\phi}|1\rangle)/\sqrt{2}$ lies on the equator of the Bloch sphere and is characterized by a single parameter, the phase ϕ. Moreover, $\int dg=\int_0^{2\pi}d\phi/(2\pi)$. The input and output states are given by

$$\psi_{\text{in}}=\psi^{\otimes N},\quad \psi_{\text{out}}=\psi^{\otimes M}.\tag{26}$$

The integration appearing in the expression (10) can easily be carried out and one arrives at

$$R=\frac{1}{2^{M+N}}\sum_{y=-N}^{M}|\Phi_{M,N,y}\rangle\langle\Phi_{M,N,y}|,\tag{27}$$

where

$$|\Phi_{M,N,y}\rangle=\sum_{k=\max(0,-y)}^{\min(N,M-y)}\sqrt{\binom{N}{k}\binom{M}{k+y}}|N,k\rangle_{\text{in}}|M,y+k\rangle_{\text{out}},\tag{28}$$

and $|N,k\rangle$ denotes a totally symmetric state of N qubits with k qubits in the state $|1\rangle$ and $N-k$ qubits in the state $|0\rangle$. Similarly, one gets

$$A=\frac{1}{2^N}\sum_{k=0}^{N}\binom{N}{k}|N,k\rangle\langle N,k|\otimes\mathbb{1}_{\text{out}}.\tag{29}$$

Since the states $|\Phi_{M,N,y}\rangle$ are mutually orthogonal, the matrix R is diagonal and, consequently, also $M=A^{-1/2}RA^{-1/2}$ is diagonal. The maximal eigenvalue can thus be easily determined and the maximal fidelity is given by

$$F_{\max}(N,M)=\frac{1}{2^M}\sum_{k=0}^{N}\binom{M}{k+\left[\frac{M-N}{2}\right]},\tag{30}$$

where $[x]$ denotes the integer part of x. For $N>1$, the fidelity (30) is higher than the fidelity of the optimal deterministic phase covariant cloner that was given in Ref. [17]. The maximal improvement of the fidelity is of the order of 1%.

The optimal probabilistic cloning transformation can be written as

$$|N,k\rangle\rightarrow\frac{1}{\mathcal{N}}\sqrt{\binom{M}{k+\Delta_{MN}}\binom{N}{k}^{-1}}|M,\Delta_{MN}+k\rangle,\tag{31}$$

where $\Delta_{MN}=[(M-N)/2]$ and

$$\mathcal{N}=\max_k\sqrt{\binom{M}{k+\Delta_{MN}}\binom{N}{k}^{-1}}\tag{32}$$

is a normalization prefactor. If $M-N$ is even, then Eq. (31) is the unique optimal phase-covariant probabilistic cloning transformation that optimally matches the input state $|\psi\rangle^{\otimes N}$ onto the ideal output $|\psi\rangle^{\otimes M}$. For odd $M-N$, however, we can obtain another optimal operation by replacing Δ_{MN} with $\Delta_{MN}+1$ in Eqs. (31) and (32). This implies that the support $\mathcal{K}$ of the optimal operator E is two dimensional and the optimal map that maximizes the success probability must be calculated by solving the semidefinite program (18).

A second example where the probabilistic cloner outperforms the deterministic one is the $1\rightarrow M$ copying of coherent states $|\alpha\rangle$ on a circle. Recall that $|\alpha\rangle=e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\alpha^N/\sqrt{n!}|n\rangle$, where $|n\rangle$ is the n-photon Fock state. Since we assume that $|\alpha\rangle$ lie on a circle, the amplitude $r=|\alpha|$ is fixed while the phase $\phi=\arg(\alpha)$ is arbitrary. First of all, we observe that the perfect cloning is equivalent to noiseless amplification, because the output state $|\alpha\rangle^{\otimes M}$ can be unitarily mapped onto the state $|\sqrt{M}\alpha\rangle\otimes|0\rangle^{\otimes M-1}$ by an array of $M-1$ beam splitters [14]. Thus the cloning is equivalent to $|\alpha\rangle\rightarrow|\sqrt{M}\alpha\rangle$. The operators A and R are calculated as averages over the phase ϕ and one finds that the maximum eigenvalue of M is $\mu_{\max}=1$ which indicates that an exact probabilistic cloning is possible. However, we must be careful because we deal with infinite dimensional Hilbert space and it turns out that the fidelity $F=1$ can be achieved only in the limit of zero probability of success $P \to 0$. Nevertheless, arbitrarily high fidelity can be reached with finite success probability if we first project the input state onto the subspace spanned by the first $N+1$ Fock states $|0\rangle, \ldots, |N\rangle$ and then apply a diagonal filter that approximates the noiseless amplification, $|n\rangle \to M^{(n-N)/2}|n\rangle$, $n=0,\ldots,N$. The fidelity

$$F = e^{-M|\alpha|^2} \sum_{n=0}^{N} \frac{M^n|\alpha|^{2n}}{n!} \tag{33}$$

can be arbitrarily close to 1 as $N \to \infty$. Clearly, this probabilistic cloning achieves even higher fidelity for the coherent states inside the circle, where $|\alpha| < r$.

IV. PURIFICATION OF MIXED STATES

Another important application of the optimization technique developed in Sec. II consists in the design of the optimal protocols for purification of mixed quantum states. Suppose that Alice and Bob can communicate via a noisy quantum channel $\mathcal{C}$. Alice wants to send to Bob a quantum state ψ from some set S_{in}. However, since the channel is noisy, Bob receives mixed state $\rho=\mathcal{C}(\psi)$. To partially compensate for the effects of the noisy channel, Alice sends N copies of the state ψ to Bob who subsequently attempts to extract ψ from the state $\rho^{\otimes N}$. The purification of qubits transmitted through the depolarizing channel, $\rho=\eta\psi+\frac{1}{2}(1-\eta)\mathbb{1}$, has been analyzed in detail in Refs. [29,30]. Very recently, the optimal purification protocol for two copies of the qubit has been demonstrated experimentally for the polarization states of single photons by exploiting the interference of two photons on a balanced beam splitter [31]. Applications of the purification procedure to the quantum state estimation and transmission have been discussed in Refs. [47,48]. Here, we demonstrate that the present optimization procedure can be used to straightforwardly determine the optimal probabilistic purification protocol. Then we will consider the same problem for the amplitude damping channel.

A. Depolarizing channel

For the sake of simplicity we illustrate the method on the case when Alice sends two copies of the state $|\psi\rangle$ to Bob, hence Bob's input mixed state reads $\rho_{\text{in}}=[\eta\psi+\frac{1}{2}(1-\eta)\mathbb{1}]^{\otimes 2}$. The ideal output is a single-qubit pure state ψ. Assuming uniform distribution of ψ over the surface of the Bloch sphere, one obtains the following expressions for the operators A and R:

$$A = \left(\frac{1}{3}\eta^2\Pi_{+,12} + \frac{1-\eta^2}{4}\mathbb{1}_1 \otimes \mathbb{1}_2\right) \otimes \mathbb{1}_3,$$

$$R^{T_3} = \frac{\eta^2}{4}\Pi_{+,123} + \frac{(1-\eta)^2}{8}\mathbb{1}_{123} + \frac{\eta}{6}(1-\eta)(\mathbb{1}_1 \otimes \Pi_{+,23} + \mathbb{1}_2 \otimes \Pi_{+,13}), \tag{34}$$

where 1 and 2 label the input qubits while 3 labels the output qubit, $\Pi_{+,jk}$ and $\Pi_{+,ijk}$ are projectors on the symmetric subspace of two qubits j,k or three qubits i,j,k, respectively, and T_3 stands for the partial transposition with respect to the third qubit. From Eq. (15) we obtain the maximal achievable purification fidelity,

$$F = \frac{3+4\eta+\eta^2}{2(3+\eta^2)}, \tag{35}$$

which is larger than the original fidelity $F_0=\langle\psi|\rho|\psi\rangle=(1+\eta)/2$, for all $0<\eta<1$. As shown in Refs. [29–31], the optimal purification strategy is to project the two-qubit state $\rho^{\otimes 2}$ onto the symmetric subspace and then throw away one of the qubits. This procedure achieves the optimal fidelity (35). Let us now demonstrate that this protocol can be derived by solving the semidefinite program (18). The maximal eigenvalue of the matrix M is doubly degenerate and the basis states that span the two-dimensional Hilbert space $\mathcal{K}$ are given by

$$|e_1\rangle = \frac{1}{\sqrt{6}}(\sqrt{2}|\Psi_+\rangle|0\rangle + 2|11\rangle|1\rangle),$$

$$|e_2\rangle = \frac{1}{\sqrt{6}}(\sqrt{2}|\Psi_+\rangle|1\rangle + 2|00\rangle|0\rangle), \tag{36}$$

where $|\Psi_+\rangle=(|01\rangle+|10\rangle)/\sqrt{2}$. From Eq. (7) and the definition of A we find that $\overline{P}=\text{Tr}_{\text{in}}[\lambda X]$, where $\lambda=\int_{S_{\text{in}}}\rho_{\text{in}}^T\, d\rho_{\text{in}}$ and $X=\text{Tr}_{\text{out}}(E)$. Since $E=\Sigma_{j=1,2}\, c_{jk}|e_j\rangle\langle e_k|$ it follows that the support of X is the symmetric subspace of two qubits. From Eq. (3) we thus have $X \leqslant \Pi_{+,12}$. The maximum $\overline{P}$ is obtained when $X=\Pi_{+,12}$, which can be achieved by the following choice of E:

$$E = \tfrac{3}{2}(|e_1\rangle\langle e_1| + |e_2\rangle\langle e_2|).$$

It is easy to check that this trace-decreasing CP map indeed describes the projection of two qubits onto the symmetric subspace followed by tracing over the second qubit.

The strategy to send the state $|\psi\psi\rangle$ is not the only possible option how Alice can encode the state $|\psi\rangle$ into the two qubits that she sends to Bob via depolarizing channel. For instance, she can send him the state $|\psi\rangle|\psi_\perp\rangle$, where $\langle\psi|\psi_\perp\rangle=0$. As shown by Gisin and Popescu [27], the state $|\psi\rangle$ can be estimated with higher fidelity from a single copy of the state $|\psi\psi_\perp\rangle$ than from a single copy of $|\psi\psi\rangle$. We cannot therefore *a priori* rule out that sending the state $|\psi\psi_\perp\rangle$ can be advantageous also in the present context. If Alice sends $|\psi\psi_\perp\rangle$ then Bob's input mixed state reads

$$\rho_{\text{in}} = \left(\eta\psi + \frac{1-\eta}{2}\mathbb{1}\right) \otimes \left(\eta\psi_\perp + \frac{1-\eta}{2}\mathbb{1}\right).$$

The calculation of the optimal purification fidelity is completely similar to the case of sending $|\psi\psi\rangle$. The integrals (8) and (10) yielding the relevant operators $A_\perp$ and $R_\perp$ can be easily evaluated with the help of the substitution $\psi_\perp=\mathbb{1}-\psi$ and we obtain

$$A_\perp = \left(\frac{1+\eta^2}{4}\mathbb{1}_1 \otimes \mathbb{1}_2 - \frac{1}{3}\eta^2\Pi_{+,12}\right) \otimes \mathbb{1}_3,$$

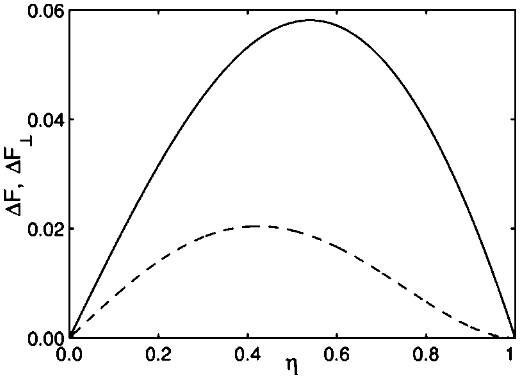

FIG. 1. The maximal possible improvements of fidelity $\Delta F(\eta)$ (solid line) and $\Delta F_\perp(\eta)$ (dashed line) that can be achieved by purification when the two-qubit state $|\psi\psi\rangle$ or $|\psi\psi_\perp\rangle$, respectively, is sent through the depolarizing channel with parameter η.

$$R_\perp^{T_3} = -\frac{\eta^2}{4}\Pi_{+,123} + \frac{1-\eta^2}{8}\mathbb{1}_{123} + \frac{\eta}{6}(1+\eta)\mathbb{1}_2 \otimes \Pi_{+,13} - \frac{\eta}{6}(1-\eta)\mathbb{1}_1 \otimes \Pi_{+,23}. \qquad (37)$$

The maximal fidelity $F_\perp$ is determined as the maximum eigenvalue of the operator $A_\perp^{-1/2}R_\perp A_\perp^{-1/2}$.

The results of numerical calculations are given in Fig. 1. For comparison we plot on this figure the gains in fidelity $\Delta F_\perp = F_\perp(\eta) - F_0(\eta)$ and $\Delta F = F(\eta) - F_0(\eta)$ achieved when Alice sends the state $|\psi\psi_\perp\rangle$ or $|\psi\psi\rangle$, respectively. We can see that as far as the purification is concerned, it is strictly better for any $0<\eta<1$ to send the state $|\psi\psi\rangle$ than $|\psi\psi_\perp\rangle$. The nonzero values of $\Delta F_\perp(\eta)$ clearly show that purification is possible also when Alice sends the state $|\psi\psi_\perp\rangle$ but the fidelity improvement is much smaller than when sending the state $|\psi\psi\rangle$.

B. Amplitude damping channel

To further illustrate the utility and universality of our optimization method, let us now consider a different class of noisy channels, namely, an amplitude-damping channel that maps a pure state ψ onto a mixed state

$$\rho_{AD}(\vartheta,\phi) = \begin{pmatrix} \eta^2\cos^2\dfrac{\vartheta}{2} & \dfrac{\eta}{2}\sin\vartheta\, e^{-i\phi} \\ \dfrac{\eta}{2}\sin\vartheta\, e^{i\phi} & 1-\eta^2\cos^2\dfrac{\vartheta}{2} \end{pmatrix}. \qquad (38)$$

This channel may arise, for instance, when the qubit is represented by the ground and excited atomic states $|g\rangle$ and $|e\rangle$ where $|e\rangle$ can decay to $|g\rangle$ via spontaneous emission. In order to preserve the covariance (19) that guarantees the universality of the optimal purification protocol, we shall assume that Alice is sending to Bob N copies of a state $|\psi(\phi)\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ that lies on the equator of the Bloch sphere, i.e., the set S_{in} consists of the states $\rho_{\text{BOB}}^{\otimes N}(\phi) = \rho_{AD}^{\otimes N}(\pi/2,\phi)$.

The operators R_{AD} and A_{AD} are obtained by integrating over the phase ϕ,

$$A_{AD} = \frac{1}{2\pi}\int_0^{2\pi} \rho_{\text{BOB}}^{\otimes N}(-\phi) \otimes \mathbb{1}_{\text{out}}\, d\phi,$$

$$R_{AD} = \frac{1}{2\pi}\int_0^{2\pi} \rho_{\text{BOB}}^{\otimes N}(-\phi) \otimes \psi(\phi) d\phi. \qquad (39)$$

We now prove that when determining the maximum achievable purification fidelity, we can assume that the optimal map $\mathcal{E}$ is a composition of two maps, $\mathcal{E} = \tilde{\mathcal{E}} \circ \mathcal{P}_N$, where the map $\mathcal{P}_N$ projects the input state $\rho_{\text{BOB}}^{\otimes N}$ onto the symmetric subspace of N qubits $\mathcal{H}_{+,N}$ and $\tilde{\mathcal{E}}$ maps operators on $\mathcal{H}_{+,N}$ onto operators on the Hilbert space of single output qubit. By definition, the operators A_{AD} and R_{AD} commute with arbitrary permutation operator Π_j that changes the order of the N input qubits. Suppose that $E = |e\rangle\langle e|$ is an optimal map yielding maximal fidelity $F_{\max}$ which is equal to the maximum eigenvalue of matrix $M_{AD} = A_{AD}^{-1/2}R_{AD}A_{AD}^{-1/2}$. As shown in Sec. II, the corresponding optimal eigenvector $|\mu\rangle$ of M is related to $|e\rangle$ as follows: $|\mu\rangle = A_{AD}^{1/2}|e\rangle$. Let us now consider a symmetrized state $|x\rangle$ that we obtain from $|e\rangle$ by making a linear superposition of all $N!$ permutations of N input qubits,

$$|x\rangle = \sum_j \Pi_j \otimes \mathbb{1}_{\text{out}}|e\rangle. \qquad (40)$$

It is easy to show that $A_{AD}^{1/2}|x\rangle$ is an eigenstate of M_{AD} with eigenvalue $F_{\max}$. We have

$$\begin{aligned} M_{AD}A_{AD}^{1/2}|x\rangle &= A_{AD}^{1/2}A_{AD}^{-1}R_{AD}\sum_j \Pi_j A_{AD}^{-1/2}|\mu\rangle \\ &= A_{AD}^{1/2}\sum_j \Pi_j A_{AD}^{-1/2}F_{\max}|\mu\rangle \\ &= F_{\max}A_{AD}^{1/2}|x\rangle, \end{aligned} \qquad (41)$$

where we have used that both A_{AD} and R_{AD} commute with Π_j. Thus the map $X = |x\rangle\langle x|$ achieves the maximal fidelity $F_{\max}$. It holds that $\text{Tr}_{\text{out}}(X) \in B(\mathcal{H}_{+,N})$ which proves that we can restrict our attention to the maps $\tilde{\mathcal{E}}$ when calculating the maximal fidelity of purified state.

The calculations can be further considerably simplified by the observation that the optimal map $\tilde{\mathcal{E}}$ can be made phase-covariant [16,17], that is, invariant under the twirling operation,

$$\tilde{E} = \int_0^{2\pi} \frac{d\phi}{2\pi} U^T(\phi) \otimes V^\dagger(\phi)\tilde{E}U^*(\phi) \otimes V(\phi), \qquad (42)$$

where $U(\phi)|N,k\rangle = e^{ik\phi}|N,k\rangle$, $k=0,\ldots,N$ and $V(\phi)|j\rangle = e^{ij\phi}|j\rangle$, $j=0,1$. This implies that the operator $\tilde{E}$ can be expressed as a direct sum,

$$\tilde{E} = \bigoplus_{k=-1}^{N} \tilde{E}_k, \qquad (43)$$

where the support of the operator $\tilde{E}_k$ is a two-dimensional Hilbert space $\mathcal{H}_k$, $k=0,\ldots,N-1$ spanned by $|N,k\rangle|0\rangle$ and $|N,k+1\rangle|1\rangle$ and

$$\tilde{E}_{-1} = e_{-1}|N,0\rangle\langle N,0| \otimes |1\rangle\langle 1|,$$

$$\tilde{E}_N = e_N|N,N\rangle\langle N,N| \otimes |0\rangle\langle 0|. \tag{44}$$

The decomposition (43) implies that we can perform the optimization of each CP map $\tilde{E}_k$ separately and then choose the k that yields the highest fidelity. It is easy to see that the trace decreasing CP maps $\tilde{E}_{-1}$ and $\tilde{E}_N$ lead to very low purification fidelity $\frac{1}{2}$ so it is optimal for all N to set $e_{-1}=e_N=0$. Without loss of generality, we can assume that the optimal $\tilde{E}_k$ is a rank-one operator, $\tilde{E}_k=|\tilde{E}_k\rangle\langle\tilde{E}_k|$, where

$$|\tilde{E}_k\rangle = |N,k\rangle|0\rangle + \alpha_{N,k}(\eta)|N,k+1\rangle|1\rangle. \tag{45}$$

The action of this operation can be understood as follows. First the N-qubit state is projected onto two-dimensional subspace of $\mathcal{H}_{+,N}$ spanned by $|N,k\rangle$ and $|N,k+1\rangle$ and then the following transformation is carried out:

$$|N,k\rangle \to |0\rangle, \quad |N,k+1\rangle \to \alpha_{N,k}(\eta)|1\rangle. \tag{46}$$

The unnormalized density matrix of the purified qubit obtained by applying the map (46) reads

$$\rho_{\text{out}} = \begin{pmatrix} \sigma_{k,k}^{(N)} & \alpha_{N,k}^{*}\sigma_{k,k+1}^{(N)}e^{-i\phi} \\ \alpha_{N,k}\sigma_{k,k+1}^{(N)}e^{i\phi} & |\alpha_{N,k}|^2\sigma_{k+1,k+1}^{(N)} \end{pmatrix}. \tag{47}$$

The relevant matrix elements

$$\sigma_{j,k}^{(N)} = \langle N,j|\rho_{AD}^{\otimes N}(\pi/2,0)|N,k\rangle$$

can be expressed in terms of a finite series,

$$\sigma_{k,k}^{(N)} = 2^{-N}\eta^{2N-2k}\sum_{l=0}^{k}\binom{k}{l}\binom{N-k}{k-l}(2-\eta^2)^l,$$

$$\sigma_{k,k+1}^{(N)} = 2^{-N}\eta^{2N-2k-1}\sqrt{\frac{k+1}{N-k}} \times \sum_{l=0}^{k}\binom{k}{l}\binom{N-k}{k+1-l}(2-\eta^2)^l.$$

The optimal $\alpha_{N,k}(\eta)$ that maximizes the fidelity of the purified state (47) with respect to the original pure state $(|0\rangle+e^{i\phi}|1\rangle)/\sqrt{2}$ is given by $\alpha_{N,k}=\sqrt{\sigma_{k,k}^{(N)}/\sigma_{k+1,k+1}^{(N)}}$ and the fidelity of purified qubit reads

$$F_{N,k} = \frac{1}{2}\left(1 + \frac{\sigma_{k,k+1}^{(N)}}{\sqrt{\sigma_{k,k}^{(N)}\sigma_{k+1,k+1}^{(N)}}}\right). \tag{48}$$

The maximum achievable fidelity can be found as a maximum over all k, $F_{N,\max}=\max_k F_{N,k}$. Based on numerical calculations we conjecture that for odd N the best fidelity is reached for $k=(N-1)/2$ while for even N there are two alternatives leading to the same optimal F, namely $k=N/2-1$ and $k=N/2$. For $N\leqslant 10$ we have checked that these choices of k are optimal which supports this conjecture.

We shall now present explicit results for $N=1,2,3$. Besides the maximal fidelity, we are interested also in the maximal probability $\overline{P}$ of optimal purification. We have therefore carried out full calculations of the operators A_{AD} and R_{AD} for $N=1,2,3$ and determined the degeneracy of the maximal eigenvalue of matrix M. These calculations reveal that the optimal eigenvectors $A_{AD}^{1/2}|e\rangle$ of M all satisfy the relation $\text{Tr}_{\text{out}}[e] \in B(\mathcal{H}_{+,N})$ so we can in fact consider only the maps of the form (45) without any loss of generality.

If only a single qubit is sent to Bob, then the only option is $k=0$ and the best filter is obtained by setting $\alpha_{1,0}=\eta/\sqrt{2-\eta^2}$ which achieves a fidelity $F_1=\frac{1}{2}(1+1/\sqrt{2-\eta^2})$. The purification succeeds with probability $P_1=\eta^2$.

For $N=2$ the maximum fidelity F_2 is given by

$$F_2 = \frac{1}{2}\left(1 + \sqrt{\frac{2}{3-\eta^2}}\right). \tag{49}$$

One option how to achieve F_2 is to choose $k=0$ and $\alpha_{2,0}=\eta/\sqrt{3-\eta^2}$. The second alternative is $k=1$ and $\alpha_{2,1}=\eta\sqrt{3-\eta^2}/(2-\eta^2)$. The Hilbert space $\mathcal{K}$ of the admissible optimal operations E is thus two dimensional and spanned by basis states,

$$|e_1\rangle = |00\rangle|0\rangle + \alpha_{2,0}|\Psi_+\rangle|1\rangle,$$

$$|e_2\rangle = |\Psi_+\rangle|0\rangle + \alpha_{2,1}|11\rangle|1\rangle. \tag{50}$$

To find E that maximizes $\overline{P}$ we must solve (18).

It follows from (42) and (43) that the optimal E is diagonal in basis $|e_1\rangle,|e_2\rangle$, $E=p_1e_1+p_2e_2$. Consequently, the semidefinite program (18) reduces to a linear program and we have to maximize

$$\overline{P} = \tfrac{1}{2}p_1\eta^4 + \tfrac{1}{2}p_2\eta^2(3-\eta^2)$$

under the constraints

$$0 \leqslant p_1 \leqslant 1, \quad 0 \leqslant p_2 \leqslant \alpha_{2,1}^{-2}, \quad 0 \leqslant p_1\alpha_{2,0}^2 + p_2 \leqslant 1.$$

For $\eta \leqslant \eta_{th} \equiv (7-\sqrt{17})^{1/2}/2$ the optimal coefficients read $p_1=0$, $p_2=1$ while for $\eta > \eta_{\text{th}}$ we have $p_1=(\alpha_{2,1}^2-1)/(\alpha_{2,0}^2\alpha_{2,1}^2)$ and $p_2=\alpha_{2,1}^{-2}$. For all $0<\eta\leqslant 1$ the optimal probability is given by a simple formula

$$P_2 = \tfrac{1}{2}\eta^2(3-\eta^2). \tag{51}$$

Finally, when Alice sends three qubits to Bob ($N=3$), then the optimal fidelity of Bob's purified qubit is given by

$$F_3 = \frac{1}{2}\left[1 + \frac{5-2\eta^2}{(4-\eta^2)\sqrt{2-\eta^2}}\right], \tag{52}$$

and the only way to reach F_3 is to choose $k=1$ and $\alpha_{3,1}=\eta/\sqrt{2-\eta^2}$. The purification succeeds with probability $P_3=\eta^4-\eta^6/4$.

The dependence of the optimal fidelities on η is plotted in Fig. 2(a) which clearly illustrates that the purification results in a significant improvement of the fidelity. The relative improvement is maximal when $\eta\to 0$ but this is reached at the expense of very low probability of success, see Fig. 2(b). Note also that $\lim_{\eta\to 1}P_3=3/4$. If Bob possesses three noisy qubits and tries to extract one qubit, then his optimal probabilistic strategy will have a finite probability of failure for arbitrarily low damping.

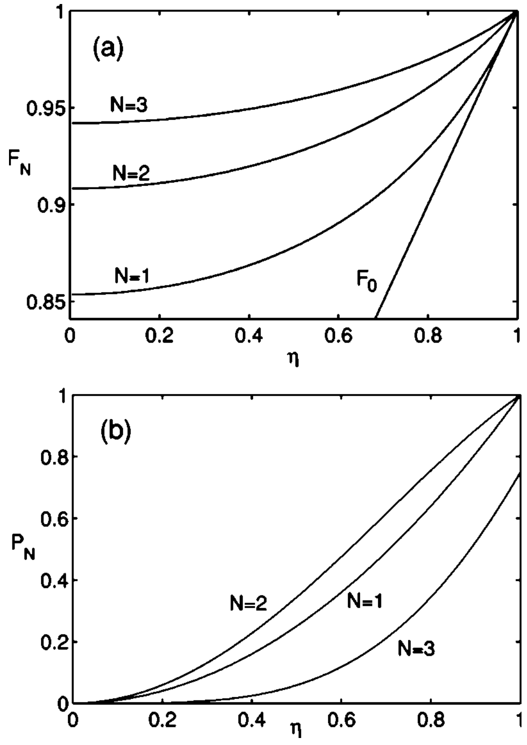

FIG. 2. (a) Maximal fidelity of the purified qubit when Alice sends N copies of the qubit via amplitude damping channel parametrized by η. For comparison, the curve labeled F_0 displays the fidelity of the single qubit after passing through the channel, $F_0 = (1+\eta)/2$. (b) The corresponding maximal probability of successful purification.

V. CONCLUSIONS

In this paper we have investigated the optimal *probabilistic* realizations of several important quantum-information-processing tasks such as the optimal cloning of quantum states and purification of mixed quantum states. We have derived a simple formula for the maximum achievable average fidelity and we have provided an explicit prescription how to construct a trace-decreasing CP map that reaches the fidelity $F_{\max}$. We have demonstrated that the fidelity of probabilistic cloning can be strictly higher than the maximal fidelity of deterministic cloning even if the set of the cloned states is linearly dependent and continuous. However, it should be stressed that this improvement in fidelity is achieved at the expense of a certain fraction of unsuccessful events when the probabilistic transformation fails and does not produce any output state.

The optimal probabilistic maps may find a variety of applications. For instance, the phase covariant cloning is an efficient attack on several quantum key distribution protocols. In particular, the 2 → 3 phase-covariant cloning is explored for eavesdropping purposes in Ref. [24]. Thus, the probabilistic phase-covariant cloning discussed in the present paper may be possibly used as a new eavesdropping attack. Moreover, the general theory of optimal probabilistic transformations developed in the present paper has much broader range of applications than just cloning. In particular, it provides a method to engineer optimal protocols for purification of mixed quantum states.

We have seen on the example of the amplitude damping channel that the optimal probabilistic purification may result in a dramatic improvement of the fidelity of the final Bob's state with respect to the original state that was sent to him by Alice via a noisy channel. However, the large improvement of the fidelity is typically accompanied by a very low probability of success. It is therefore highly desirable to optimize the probabilistic transformation also with respect to the average success probability which leads to a semidefinite program that can be very efficiently solved numerically. For the particular cases of purification of mixed states investigated in the present paper, we have been able to solve the resulting SDP analytically, by exploiting the symmetries inherent to the problem.

The protocol considered in the present paper can be even further generalized as follows. One can imagine a scenario where the average fidelity F of the operation is maximized for a fixed chosen average probability of success $\overline{P}$, or vice versa, these two alternatives are clearly equivalent. Generally, there will always be a trade-off between $\overline{P}$ and F and the optimal fidelity will be some function of $\overline{P}$. One can then choose the working point on the $F(\overline{P})$ curve that is most fitting for the particular task at hand. The determination of maximal F obtainable for some fixed $\overline{P}$ can be formulated as a semidefinite program similar to that given by Eq. (18). The deterministic machines and the probabilistic machines that achieve the maximum possible fidelity represent two extreme regimes of such a more general scenario.

ACKNOWLEDGMENTS

The author would like to thank Nicolas J. Cerf for many stimulating discussions. Financial support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, from the IUAP program of the Belgian Government under Grant No. V-18, from the EU under project CHIC (IST-2001-33578), and from Grant No. LN00A015 of the Czech Ministry of Education, is acknowledged.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, New York, 1994), p. 124.
[3] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[4] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[5] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[6] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**,

2598 (1998).
[7] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[8] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[9] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).
[10] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[11] S. L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[12] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[13] S. L. Braunstein *et al.*, Phys. Rev. Lett. **86**, 4938 (2001).
[14] J. Fiurášek, Phys. Rev. Lett. **86**, 4942 (2001).
[15] D. Bruss *et al.*, Phys. Rev. A **62**, 012302 (2000).
[16] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[17] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).
[18] J. Fiurášek, Phys. Rev. A **67**, 052314 (2003).
[19] P. Navez and N. J. Cerf, Phys. Rev. A **68**, 032313 (2003).
[20] L.- P. Lamoureux, P. Navez, J. Fiurášek, and N. J. Cerf, Phys. Rev. A **69**, 040301 (2004).
[21] C. A. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997).
[22] C.- S. Niu and R. B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
[23] N. J. Cerf *et al.*, Phys. Rev. Lett. **88**, 127902 (2002).
[24] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[25] L. M. Duan and G. C. Guo, Phys. Lett. A **243**, 261 (1998); Phys. Rev. Lett. **80**, 4999 (1998).
[26] A. Chefles and S. M. Barnett, J. Phys. A **31**, 10097 (1998); Phys. Rev. A **60**, 136 (1999).
[27] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).
[28] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2626 (1999).
[29] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. **82**, 4344 (1999).
[30] M. Keyl and R. F. Werner, Ann. Inst. Henri Poincare, Anal. Non Lineaire **2**, 1 (2001).
[31] M. Ricci, F. De Martini, N. J. Cerf, R. Filip, J. Fiurášek, and C. Macchiavello, e-print quant-ph/0403118.
[32] We assume that there is no correlation between the device that prepares the input states ρ_{in} and the degrees of freedom that subsequently interact with ρ_{in}.
[33] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[34] M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975).
[35] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
[36] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[37] H. J. Woerdeman, Phys. Rev. A **67**, 010303 (2003).
[38] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).
[39] F. Verstraete and H. Verschelde, Phys. Rev. A **66**, 022307 (2002); Phys. Rev. Lett. **90**, 097901 (2003).
[40] M. Ježek, J. Řeháček, and J. Fiurášek, Phys. Rev. A **65**, 060301(R) (2002).
[41] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **49**, 1007 (2003).
[42] K. Audenaert and B. De Moor, Phys. Rev. A **65**, 030302(R) (2002).
[43] J. Fiurášek, S. Iblisdir, S. Massar, and N. J. Cerf, Phys. Rev. A **65**, 040302 (2002).
[44] B. M. Terhal, A. C. Doherty, and D. Schwab, Phys. Rev. Lett. **90**, 157903 (2003).
[45] D. Bruss and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).
[46] F. Buscemi, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Lett. A **314**, 374 (2003).
[47] H. Mack, D. G. Fischer, and M. Freyberger, Phys. Rev. A **62**, 042301 (2001).
[48] D. G. Fischer, H. Mack, and M. Freyberger, Phys. Rev. A **63**, 042305 (2001).