Physical purification of quantum states

M. Kleinmann,* H. Kampermann, T. Meyer, and D. Bruß Institut für Theoretische Physik, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany (Received 16 September 2005; revised manuscript received 10 March 2006; published 8 June 2006)

We introduce the concept of a physical process that purifies a mixed quantum state, taken from a set of states, and investigate the conditions under which such a purification map exists. Here, a purification of a mixed quantum state is a pure state in a higher-dimensional Hilbert space, the reduced density matrix of which is identical to the original state. We characterize all sets of mixed quantum states, for which perfect purification is possible. Surprisingly, some sets of two noncommuting states are among them. Furthermore, we investigate the possibility of performing an imperfect purification.

DOI: 10.1103/PhysRevA.73.062309 PACS number(s): 03.67.-a, 03.65.-w

I. INTRODUCTION

A fundamental entity in quantum mechanics and quantum information is a mixed quantum state. A mixed quantum state can be either understood as a statistical mixture of pure quantum states, or as being part of a higher-dimensional, pure state—a purification of the mixed state. Formally, given the decomposition $\rho = \sum_i p_i |\chi_i\rangle\langle\chi_i|$, where $p_i \ge 0$ and $\sum_i p_i = 1$, an example for a purification of ρ is given by $|\psi\rangle = \sum_i \sqrt{p_i} |\chi_i\rangle\langle a_i\rangle$, with the auxiliary states $|a_i\rangle$ being mutually orthogonal. This abstract point of view was, so far, the main impetus for discussing purifications of a single, known quantum state [1,2].

In this paper, we consider the purification of an *unknown* quantum state. More precisely, we introduce the fundamental question whether there exists a *physical process* (i.e., a completely positive map) that takes any state of a given set to one of its purifications. (We remind the reader for clarity that there exists a different notion of "purification" in the literature, referring to the process of performing operations on several identical copies of a given state, such that the purity of some of them is increased; a typical application is entanglement distillation.) Our aim is to characterize all sets of states for which a purifying map exists. The existence of such a process implies a nontrivial physical equivalence between certain sets of mixed and pure quantum states.

Let us introduce our concepts and outline the structure of this paper. As already pointed out above, a purification of a mixed state has to satisfy two characteristic properties: first, it has to be pure, and second, tracing out the auxiliary system has to yield back the original state. We call the second property *faithfulness* and name a process a *perfect purifier* for a mixed state, when the output achieves both properties. It is straightforward to prove that the linearity of quantum mechanics does not allow the existence of a perfect purifier for a completely unknown quantum state, i.e., a state taken from the set of *all* states. However, will dropping the condition of faithfulness *or* the one of purity allow nontrivial purification processes for an unknown quantum state? It will be shown in Theorem 1 that this is not the case. Consequently, in Sec. III we will restrict the set of possible input states, and investi-

*Electronic address: kleinmann@thphy.uni-duesseldorf.de

gate the properties of purifying maps acting on the most simple nontrivial set, namely a set of only two mixed states. While keeping the condition of purity, we will find that the deviation from perfect faithfulness depends on a purely geometric quantity of the two inputs. This result will allow us to derive lower and upper bounds on the achievable faithfulness. Since these bounds do not exclude perfect faithfulness for certain pairs of states, we then, in Sec. IV proceed to investigate the existence of a perfect purifier in general. Theorem 2 completely characterizes all sets of states that can be purified perfectly. Finally, we will provide an operational test for a given pair of states that allows to check whether a physical purification is possible.

II. THE GENERAL PURIFICATION TASK

In the following we will denote by \mathcal{M} a given set of mixed states, represented by density operators that act on a finite-dimensional Hilbert space \mathcal{H} . The elements $\rho_i \in \mathcal{M}$ are allowed to have unbalanced a priori probabilities $\eta_i > 0$, satisfying $\Sigma_i \eta_i = 1$. We consider deterministic physical processes represented by completely positive and trace preserving [14] linear maps Λ that take any density operator acting on \mathcal{H} to a density operator acting on $\mathcal{H} \otimes \mathcal{H}_{aux}$, where \mathcal{H}_{aux} denotes an auxiliary space of unspecified dimension. We refer to such a physical process as a perfect purifier if for each $\rho_i \in \mathcal{M}$, the output $\Lambda[\rho_i]$ is pure as well as faithful, i.e., $\operatorname{tr}_{\operatorname{aux}} \Lambda[\rho_i] = \rho_i$. If these conditions are not met, we will measure the average output purity by $p = \sum_i \eta_i \operatorname{tr} \Lambda [\rho_i]^2$ and the average faithfulness by $f=1-\sum_i \eta_i \|\rho_i - \operatorname{tr}_{\operatorname{aux}} \Lambda[\rho_i]\|$. Here, $\|\rho - \sigma\| = \frac{1}{2} \operatorname{tr} |\rho - \sigma|$ denotes the trace distance, where |A| $=\sqrt{A^{\dagger}A}$. The trace distance is a good measure for the distinguishability of two states as it vanishes for identical states and is equal to one for orthogonal states. In particular, the success probability for the minimum error discrimination procedure [3,4] of two states having equal a priori probability depends linearly on the trace distance of the states. We call any deterministic process a purifier of \mathcal{M} , if it does not decrease the average purity of \mathcal{M} .

For the universal case where the set \mathcal{M} contains all possible density operators acting on a given Hilbert space, neither relaxing the condition of purity nor relaxing the condition of faithfulness allows nontrivial purifiers.

Theorem 1. (i) Any universal purifier with perfect output

purity is a constant map. (ii) A universal purifier with perfect faithfulness does not increase the purity of any state.

Proof. We prove (i) by contradiction. Suppose there exists a purifier Λ such that $\Lambda[\rho]$ is pure for any state ρ , and with the property that at least for two states ρ_1 and ρ_2 , $\Lambda[\rho_1] \neq \Lambda[\rho_2]$ holds. But for the state $\rho_3 = (\rho_1 + \rho_2)/2$, the purity of $\Lambda[\rho_3] = (\Lambda[\rho_1] + \Lambda[\rho_2])/2$ requires $\Lambda[\rho_1] = \Lambda[\rho_2]$.

Proof of statement (ii): perfect faithfulness of a universal purifier requires that any pure state $|\phi\rangle\langle\phi|$ is mapped onto the state $|\phi\rangle\langle\phi|\otimes\sigma_{\phi}$ for some state σ_{ϕ} acting on \mathcal{H}_{aux} . For any state ρ we find with the spectral decomposition $\rho=\Sigma p_i|\lambda_i\rangle\langle\lambda_i|$ that due to linearity $\mathrm{tr}\ \Lambda[\rho]^2=\mathrm{tr}(\Sigma_ip_i|\lambda_i\rangle\langle\lambda_i|\otimes\sigma_{\lambda_i})^2=\Sigma_ip_i^2\mathrm{tr}\ \sigma_{\lambda_i}^2\leq\Sigma_ip_i^2=\mathrm{tr}\ \rho^2,$ i.e., no state can become purer by the action of Λ .

Let us mention that there is some similarity of the arguments given in the proof above with the no-cloning theorem [5–7]. In both scenarios, linearity of quantum mechanics forbids the existence of some physical process, when the input set contains *all* states. Even when the set of input states is restricted to two pure states, perfect quantum cloning is impossible, as follows from unitarity. It was furthermore shown that broadcasting (a natural generalization of quantum cloning to mixed input states) is possible for a set of two mixed states, if and only if the states commute [8]. The same criterion does *not* apply for purification maps: a pair of orthogonal or identical states can, of course, be purified perfectly—but in any other case of commuting states we will show that perfect purification is impossible. Yet for some noncommuting states, a perfect purification process exists.

III. TWO-STATE PURIFIERS WITH PURE OUTPUT

In this section we will focus on the case of two input states and perfect output purity, i.e., a deterministic process which takes any state from the set $\mathcal{M} = \{\rho, \rho'\}$ to a pure state. A characteristic quantity for purification will turn out to be the *worst-case distinguishability* $\mathcal{D}(\rho, \rho')$, which denotes the trace distance of the two closest states that may appear physically in the ensembles of ρ and ρ' , i.e.,

$$\mathcal{D}(\rho, \rho') = \min_{|\chi\rangle, |\chi'\rangle} ||\chi\rangle\langle\chi| - |\chi'\rangle\langle\chi'||, \tag{1}$$

where $|\chi\rangle$ and $|\chi'\rangle$ are normalized vectors in the range of ρ and ρ' , respectively. (We point out that this quantity can be calculated by taking the sine of the smallest canonical angle [9] between the range of ρ and the range of ρ' .) The notion of distinguishability here refers to the success probability of a minimum error discrimination, as explained above.

Although at first sight the worst-case distinguishability resembles a distance, mathematically speaking it is none: The triangular inequality does not hold, and $\mathcal{D}(\rho, \rho') = 0$ is true for some $\rho \neq \rho'$. Note that any two states with overlapping ranges have, in fact, a vanishing worst-case distinguishability. On the other hand, $\mathcal{D}(\rho, \rho') = 1$ is equivalent to ρ and ρ' being orthogonal, i.e., $\|\rho - \rho'\| = 1$. Thus commuting states are either orthogonal or have a vanishing worst-case distinguishability.

A. Characterization of two-state purifiers

We are now in the position to study the general consequences of perfect output purity. Suppose that Λ is a purifier of ρ and ρ' with perfect output purity. As a defining property of any normalized vector $|\chi\rangle$ in the range of ρ one can write $\rho = \alpha |\chi\rangle\langle\chi| + \beta \tilde{\rho}$ with positive numbers α and β , and positive semidefinite $\tilde{\rho}$. Using the same convexity argument as in the proof of Theorem 1 (i), it follows that $\Lambda[|\chi\rangle\langle\chi|] = \Lambda[\rho]$. An analogous argument holds for all vectors $|\chi'\rangle$ in the range of ρ' . Thus we have $\|\Lambda[\rho] - \Lambda[\rho']\| = \|\Lambda[|\chi\rangle\langle\chi|] - \Lambda[|\chi'\rangle\langle\chi'|]\| \le \||\chi\rangle\langle\chi| - |\chi'\rangle\langle\chi'|\|$, where in the inequality we used that a deterministic physical process Λ cannot increase the trace distance between two states [10]. By choosing for $|\chi\rangle\langle\chi|$ and $|\chi'\rangle\langle\chi'|$ the states with minimal distance [cf. definition in Eq. (1)], we have shown that for maps Λ where $\Lambda[\rho]$ as well as $\Lambda[\rho']$ are pure,

$$\mathcal{D}(\rho, \rho') \ge \|\Lambda[\rho] - \Lambda[\rho']\| \tag{2}$$

must hold.

It is important that there always exists a map which reaches equality in Eq. (2). In order to see this, one constructs a canonical basis [9] of the ranges of both states, i.e., an orthonormal basis $\{|\chi_i\rangle\}$ of the range of ρ and $\{|\chi'_i\rangle\}$ of the range of ρ' , such that in addition $\langle \chi_i | \chi_i' \rangle = 0$ holds for all i $\neq j$. One can show that there always exists a map, which decreases the distance of two pure states by an arbitrary value. Such a map is now applied in each of the orthogonal subspaces spanned by $\{|\chi_i\rangle, |\chi_i'\rangle\}$, such that the distance $\||\chi_i\rangle\langle\chi_i|-|\chi_i'\rangle\langle\chi_i'\|$ decreases to be $\mathcal{D}(\rho,\rho')$. The composed map has the property, that if applied to ρ and ρ' , an orthonormal eigenbasis for both output states exists, such that all nonorthogonal eigenvectors (one of the output of ρ and one of ρ') have a distance $\mathcal{D}(\rho, \rho')$. Now a map can readily be found, which maps the output states to pure states having a distance $\mathcal{D}(\rho, \rho')$. The fact that one can always reach the equality in Eq. (2) completes the characterization of the output of a general process, which maps two input states ρ and ρ' to two pure states.

B. Bounds on two-state purifiers

As an application of the result in Sec. III A we now estimate the faithfulness of a purifier with perfect output in the case of two input states. For this purpose we assume that the state ρ (ρ') occurs with *a priori* probability η (η'), where $\eta' \geq \eta$ without loss of generality. We denote the deviation from perfect faithfulness by δ , i.e.,

$$\delta = \eta \| \rho - \operatorname{tr}_{\text{aux}} \Lambda[\rho] \| + \eta' \| \rho' - \operatorname{tr}_{\text{aux}} \Lambda[\rho'] \|. \tag{3}$$

Using the triangular inequality for the trace distance,

$$\begin{aligned} \|\rho - \rho'\| &\leq \|\rho - \mathrm{tr}_{\mathrm{aux}} \Lambda[\rho]\| + \|\mathrm{tr}_{\mathrm{aux}} \Lambda[\rho] - \mathrm{tr}_{\mathrm{aux}} \Lambda[\rho']\| \\ &+ \|\mathrm{tr}_{\mathrm{aux}} \Lambda[\rho'] - \rho'\| \end{aligned}$$

holds, and we obtain due to Eq. (2) the lower bound

$$\delta \ge \eta \lceil \|\rho - \rho'\| - \mathcal{D}(\rho, \rho') \rceil. \tag{4}$$

A straightforward upper bound on δ for the optimal process (i.e., minimal δ) can be obtained by considering a con-

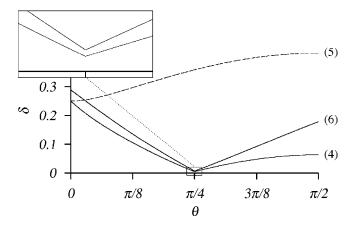


FIG. 1. Example for lower and upper bounds on the optimal deviation from perfect faithfulness δ of a two-state purifier with pure output. See main text for explanation.

stant purifier that produces a perfect purification of ρ' . This leads to the first upper bound

$$\delta_{\text{opt}} \le \eta \| \rho - \rho' \|. \tag{5}$$

A more sophisticated upper bound on δ is given by using the map which reaches the equality in Eq. (2). One chooses the output of ρ' to be a purification of ρ' and the output of ρ to be a pure state, which is as close as possible—according to Eq. (2)—to a purification of ρ . Since the maximal overlap of all purifications for two states ρ and ρ' is given by the Uhlmann fidelity $F(\rho, \rho') = \text{tr} \sqrt{\sqrt{\rho} \rho' \sqrt{\rho}}$ [11,12], we find with $\sin \alpha = \mathcal{D}(\rho, \rho')$ and $\cos \beta = F(\rho, \rho')$ the second upper bound

$$\delta_{\text{opt}} \le \eta \sin(\beta - \alpha).$$
 (6)

Let us give an explicit example for these bounds. We consider the states $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes |0\rangle\langle 0|$ and $\rho' = \frac{2}{3}|0\rangle\langle 0| \otimes |+\rangle\langle +|+\frac{1}{3}|1\rangle\langle 1| \otimes |\theta\rangle\langle \theta|$, which appear with equal *a priori* probability, where $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. In Fig. 1 the bounds for the optimal deviation from faithfulness δ are shown: the lower bound as given in Eq. (4), the first (dashed line) and second upper bound, cf. Eq. (5) and (6). At $\theta = 0$ the ranges of both states share the vector $|1\rangle \otimes |0\rangle$ and thus the worst-case distinguishability vanishes and the optimal faithfulness is given by the upper bound in Eq. (5). The second upper bound and the lower bound almost coincide at $\theta = \pi/4$ with $0.0050 < \delta < 0.0072$. Note that the upper bounds cross each other, i.e., depending on the input state, either the first or the second upper bound is tighter.

An interesting question in this context is the following: given two quantum states, does a better distinguishability (in the sense of minimum error discrimination) imply a better faithfulness? The surprising answer is no: in the example given above, the trace distance of the two states monotonically increases from θ =0 to θ = π /2, while the deviation from faithfulness has its minimum at θ = π /4. The examples illustrates that the worst-case distinguishability is indeed an important quantity for purifying processes. This is remarkable, as the worst-case distinguishability is purely determined by the geometric features of the states, whereas the

statistical weights in the ensembles do not play any role. Note that a related, but not purely geometric quantity $F_1^+(\rho, \rho')$ was introduced in [13].

IV. SETS THAT CAN BE PURIFIED PERFECTLY

Finally, our focus turns to the general analysis of perfect purifiers. The existence of a perfect purifier for a set \mathcal{M} has far-reaching implications, as it is possible to convert all states in \mathcal{M} to pure states in a reversible way. An investigation of the property of reversibility indeed turns out to be the key for understanding perfect purification: Suppose that we have a purifier Λ of a set \mathcal{M} with perfect output purity (but not necessarily perfect faithfulness), and some completely positive and trace preserving map Λ' , such that for any ρ_i $\in \mathcal{M}$ this map is the reverse map of Λ , i.e., $\Lambda'[\Lambda[\rho_i]] = \rho_i$. The action of any completely positive and trace preserving map can always be formulated as appending a (pure) ancilla state, performing a unitary rotation and finally tracing out an appropriate subsystem. We write Λ' in this manner and apply everything, apart from tracing out, to the output of Λ . For this composed map we write the shorthand notation $\tilde{\Lambda}$. The output of $\tilde{\Lambda}$ is still pure for any state in \mathcal{M} and the remaining step of the map Λ' , namely the trace over the subsystem, yields back the original state, thus $\tilde{\Lambda}$ is a *perfect* purifier of \mathcal{M} .

In order to further approach the characterization of sets that can be purified perfectly, we call a set of states *essentially pure*, if every state from the set can be globally rotated into a tensor product of a pure state and a common mixed contribution, or in more technical terms: A set of states \mathcal{M} is called essentially pure, if one can find states ω_{aux} and σ_{B} , a unitary transformation U, and a set of *pure* states \mathcal{P}_{A} , such that for all $\rho_i \in \mathcal{M}$ there is a corresponding pure state $|\phi_i\rangle\langle\phi_i| \in \mathcal{P}_{\text{A}}$ with

$$\rho_i \otimes \omega_{\text{aux}} = U(|\phi_i\rangle\langle\phi_i| \otimes \sigma_{\text{B}})U^{\dagger}. \tag{7}$$

Note that the tensor product symbol on the two sides of this equation, in general, denotes *different* splits of the composite system: on the left-hand side one sees the composition of the original system and an auxiliary system, while on the right-hand side the composition refers to some system A and some system B. Essentially pure sets can be purified perfectly: A process which appends ω_{aux} to ρ_i , performs U^{\dagger} and traces out system B produces a pure state for any state in \mathcal{M} . On the other hand a process, which appends σ_B to $|\phi_i\rangle\langle\phi_i|$, performs U and traces out the auxiliary system, undoes the action of the purifying map. Thus, a perfect purifier of \mathcal{M} exists. Of course, a union of essentially pure sets, where any two states taken from different sets are orthogonal, can also be purified perfectly. We call such a union an *orthogonal union* of essentially pure sets.

Theorem 2. For a set of states \mathcal{M} , the following statements are equivalent: (i) A perfect purifier of \mathcal{M} exists. (ii) There exists a completely positive and trace preserving map, which maps any state in \mathcal{M} to a pure state and does not change the trace distance of any two states in \mathcal{M} . (iii) \mathcal{M} is an orthogonal union of essentially pure sets.

Proof. Our motivation for the definition of orthogonal unions of essentially pure sets was indeed that this property implies the existence of a perfect purifier. Thus, we have already shown that (iii) implies (i). Furthermore, from the fact that no process can increase the trace distance, together with the existence of a reversible map, (ii) is a direct consequence of (i). Thus it only remains to show that (ii) implies (iii): If (ii) holds for an \mathcal{M} that is a union of mutually orthogonal subsets, there exist maps that satisfy (ii) for each subset. Therefore, we can assume without loss of generality that one cannot split the set \mathcal{M} into orthogonal parts. With $|a\rangle\langle a|$ being a pure auxiliary state and U^{\dagger} a unitary transformation, we can write the action of Λ as $\rho \mapsto \operatorname{tr}_{\mathbf{R}} U^{\dagger}(\rho \otimes |a\rangle\langle a|)U$, where B denotes an appropriate

subsystem. Since the output of Λ for a state $\rho_i \in \mathcal{M}$ is a pure state (represented by a projector Φ_i), we have $U^{\dagger}(\rho_i \otimes |a\rangle\langle a|)U = \Phi_i \otimes \sigma_i$, with σ_i a state in subsystem B. The final step is now to show that $\sigma_i = \sigma_j$ holds. For any two states $\rho_i, \rho_i \in \mathcal{M}$, due to the assumption (ii),

$$\|\Phi_i - \Phi_i\| = \|\rho_i - \rho_i\| = \|\Phi_i \otimes \sigma_i - \Phi_i \otimes \sigma_i\|$$
 (8)

holds. A minimum error discrimination [3,4] in subsystem B on the right-hand side can be written as $\sigma_i \rightarrow q_i |0\rangle\langle 0| + (1-q_i)|1\rangle\langle 1|$ and $\sigma_j \rightarrow (1-q_j)|0\rangle\langle 0| + q_j|1\rangle\langle 1|$, where $(q_i+q_j)/2 = (1+\|\sigma_i-\sigma_j\|)/2$ is the success probability for the optimal discrimination measurement. We find

$$\|\Phi_{i} \otimes \sigma_{i} - \Phi_{i} \otimes \sigma_{i}\|^{2} \ge [\|q_{i}\Phi_{i} - (1 - q_{i})\Phi_{i}\| + \|(1 - q_{i})\Phi_{i} - q_{i}\Phi_{i}\|]^{2} \ge \|\Phi_{i} - \Phi_{i}\|^{2} + \|\sigma_{i} - \sigma_{i}\|^{2} tr(\Phi_{i}\Phi_{i}), \tag{9}$$

where in the first step we used, that the discrimination procedure cannot increase the trace distance. The second inequality follows from a lengthy but straightforward calculation. From a comparison with Eq. (8) either $\sigma_i = \sigma_j$ or $\operatorname{tr}(\Phi_i \Phi_j) = 0$ (or both) must hold. The latter case implies ρ_i to be orthogonal to ρ_j , i.e., if $\sigma_i \neq \sigma_j$ for two states, then one can split $\mathcal M$ into two orthogonal sets, in contrast to our assumption.

This Theorem completely characterizes all sets of states that can be purified perfectly, cf. also Eq. (7). It is surprising that one can even purify a set of *continuous* states, meaning that the set may contain infinitesimally close neighbors. It is also worth mentioning that all states in an essentially pure set share the same spectrum and pairwise have a completely degenerate set of canonical angles [9]. What is the lowest dimension, in which perfect purification is possible for non-orthogonal mixed states? This cannot happen unless the dimension of the Hilbert space is at least four: In two and three dimensions, only pure states can have identical spectra without having an overlapping range.

Although essentially pure sets can be characterized in a explicit manner and have a lot of straightforward features, there is no obvious method to verify whether a given set is of the structure as specified in Eq. (7). However, for the case, where \mathcal{M} consists of only two states, there exists a computable test: From the lower bound on δ derived in Eq. (4) it follows that $\|\rho-\rho'\|=\mathcal{D}(\rho,\rho')$ is a necessary condition for the existence of a perfect two-state purifier. It is also a sufficient condition: For any two states ρ and ρ' there is a map Λ such that $\|\Lambda[\rho]-\Lambda[\rho']\|=\mathcal{D}(\rho,\rho')$, thus if $\|\rho-\rho'\|=\mathcal{D}(\rho,\rho')$, this map satisfies part (ii) of Theorem 2, i.e., ρ and ρ' can be purified perfectly. Note, that it is also straightforward to prove that the upper bound on δ_{opt} in Eq. (6) vanishes if and only if there is a perfect purifier of ρ and ρ' .

V. CONCLUSIONS

In summary, we have introduced the concept of purification as a physical map, and studied its properties: without any prior knowledge of the input state a perfect purifier cannot exist. Relaxing one of the two characteristic properties of a purifier, purity and faithfulness, does not lead to a nontrivial universal process either. We have investigated the case when the input set contains only two states and found a characterization of the output of any map, which takes both states to a pure state. Using this tool, we derived bounds on the deviation from perfect faithfulness (i.e., the distance of the partial trace of the output state and the original state). We also completely characterized all sets of states that can be purified perfectly. Roughly speaking, any such set can be globally rotated into a set of pure states, tensored with a common mixed contribution. Surprisingly, we found that some sets of noncommuting states can be purified, in contrast to the situation of broadcasting. For the case of sets with only two states, we provided an operational test to check whether perfect purification is possible.

In this paper we have presented some of the basic properties of purifying completely positive maps. Several questions remain open. One direction of future work is to consider the maximal possible purity of a purifier in the case of perfect faithfulness. Furthermore, the analysis of purifiers for sets with more than two states will be the subject of further research.

ACKNOWLEDGMENTS

We acknowledge discussions with Norbert Lütkenhaus, Armin Uhlmann, and Reinhard Werner. This work was partially supported by the EC programmes SECOQC and SCALA.

- L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A 183, 14 (1993).
- [2] A. Bassi and G. Ghirardi, Phys. Lett. A 309, 24 (2003).
- [3] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
- [4] U. Herzog and J. A. Bergou, Phys. Rev. A 70, 022302 (2004).
- [5] W. K. Wootters and W. H. Zurek, Nature (London) 299, 802 (1982).
- [6] D. Dieks, Phys. Lett. 92, 271 (1982).
- [7] H. P. Yuen, Phys. Lett. A 113, 405 (1986).
- [8] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76, 2818 (1996).

- [9] G. W. Stewart and J.-g. Sun, *Matrix Pertubation Theory* (Academic Press, San Diego, 1990).
- [10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [11] A. Uhlmann, Rep. Math. Phys. 9, 273 (1976).
- [12] R. Jozsa, J. Mod. Opt. 41, 2315 (1994).
- [13] A. Uhlmann, Rep. Math. Phys. 46, 319 (2000).
- [14] The output of a probabilistic process Λ_p with success rate $\operatorname{tr} \Lambda_p[\rho]$ is (for our purposes) physically equivalent to a deterministic process $\Lambda_d: \rho \mapsto \Lambda_p[\rho] + (1 \operatorname{tr} \Lambda_p[\rho]) |\varphi\rangle\langle\varphi|$, with $|\varphi\rangle\langle\varphi|$ being orthogonal to all $\Lambda_p[\rho]$.