Minimax discrimination of two Pauli channels

G. Mauro D'Ariano* and Massimiliano F. Sacchi†
QUIT Group of the INFM, Unità di Pavia and Dipartimento di Fisica "A. Volta," Università di Pavia, via Bassi 6, I-27100 Pavia, Italy‡

Jonas Kahn§
Département de Mathématiques, Université Paris-Sud 11, Bâtiment 425 91405 Orsay Cedex, France
(Received 8 July 2005; published 3 November 2005)

We consider the problem of optimally discriminating two Pauli channels in the minimax strategy, maximizing the smallest of the probabilities of correct identification of the channel. We find the optimal input state at the channel and show the conditions under which using entanglement strictly enhances distinguishability. We finally compare the minimax strategy with the Bayesian one.

DOI: 10.1103/PhysRevA.72.052302 PACS number(s): 03.67.−a, 03.65.Ta

I. INTRODUCTION

The concept of distinguishability applies to quantum states [1] and quantum processes [2], and is strictly related to quantum nonorthogonality, a basic feature of quantum mechanics. The problem of discriminating nonorthogonal quantum states has been extensively addressed [3], also with experimental demonstrations [4]. Typically, two discrimination schemes are considered: the minimal-error probability discrimination [5], where each measurement outcome selects one of the possible states and the error probability is minimized, and the optimal unambiguous discrimination [6], where unambiguity is paid by the possibility of getting inconclusive results from the measurement. The problem has been analyzed also in the presence of multiple copies [7], and for bipartite quantum states, and global joint measurements have been compared to LOCC measurements, i.e. local measurements with classical communication [8–10]. More recently, the discrimination of quantum states has been addressed in the minimax approach [11], where there are no *a priori* probabilities, and one maximizes the smallest of the probabilities of correct detection. In such a scheme, interesting results have been obtained, as, for example, optimal solutions that involve unique and nonorthogonal measurements.

The problem of discrimination can be addressed also for quantum operations [12]. This may be of interest in quantum error correction [13], since knowing which error model is the proper one influences the choice of the coding strategy as well as the error estimation employed. Clearly, when a repeated use of the quantum operation is allowed, a full tomography can identify it. On the other hand, a discrimination approach can be useful when a restricted number of uses of the quantum operation is available. Differently from the case of discrimination of unitary transformations [14], for quantum operations there is the possibility of improving the discrimination by means of ancillary-assisted schemes such that quantum entanglement can be exploited [12]. Notably, entanglement can enhance the distinguishability even for entanglement-breaking channels [15]. The use of an arbitrary maximally entangled state turns out to be always an optimal input when we are asked to discriminate two quantum operations that generalize the Pauli channel in any dimension. Moreover, in the case of Pauli channels for qubits, a simple condition reveals if entanglement is needed to achieve the ultimate minimal error probability [12,16]. The above statements about channel discrimination refer to a Bayesian approach.

In this paper we address the problem of optimal discrimination of two Pauli channels in the minimax game-theoretical scenario. Similarly to the case of state discrimination, we will show that the two approaches generally give different results. In Sec. II we briefly review the problem of discrimination of two Pauli channels in the Bayesian framework, where the channels are supposed to be given with assigned *a priori* probabilities. We report the result for the optimal discrimination, along with the condition for which entanglement with an ancillary system at the input of the channel strictly enhances the distinguishability. In Sec. III we review the solution to the problem of state discrimination in the minimax approach, and its relation with the Bayesian problem. In Sec. IV we study the problem of discrimination of two Pauli channels in the minimax approach. We show that when an entangled-input strategy is adopted, the optimal discrimination can always be achieved by sending a maximally entangled state into the channel, as it happens in the Bayesian approach. On the contrary, the optimal input state for a strategy where no ancillary system is used can be different in the minimax approach with respect to the Bayesian one. In the latter the optimal input can always be chosen as an eigenstate of one of the Pauli matrices, whereas in the former this may not be the case. In the concluding section, we summarize the main results of the paper.

II. BAYESIAN DISCRIMINATION OF TWO PAULI CHANNELS

In the problem of optimal Bayesian discrimination of two quantum states ρ_1 and ρ_2, given with *a priori* probability

*Electronic address: dariano@unipv.it
†Electronic address: msacchi@unipv.it
§Electronic address: jokahn@clipper.ens.fr

$p_1=p$ and $p_2=1-p$, respectively, one has to look for the two-values probability operator-valued measure (POVM) $\vec{B}\equiv\{B_1,B_2\}$ with $B_i\geqslant 0$ for $i=1$, 2 and $B_1+B_2=I$ that minimizes the error probability (or "Bayes risk")

$$R_B(p,\vec{B}) = p_1\,\mathrm{Tr}(\rho_1 B_2) + p_2\,\mathrm{Tr}(\rho_2 B_1). \tag{1}$$

We can rewrite

$$\begin{aligned} R_B(p,\vec{B}) &= p_1 - \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)B_1] \\ &= p_2 + \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)B_2] \\ &= \frac{1}{2}\{1 - \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)(B_1 - B_2)]\}, \end{aligned} \tag{2}$$

where the third equality can be obtained by summing and dividing the two previous ones. The minimal-error probability $R_B(p)\equiv\min_{\vec{B}} R_B(p,\vec{B})$ can then be achieved by taking the orthogonal POVM made by the projectors on the support of the positive and negative parts of the Hermitian operator $p_1\rho_1-p_2\rho_2$, and hence one has [5,9]

$$R_B(p) = \frac{1}{2}(1 - \|p_1\rho_1 - p_2\rho_2\|_1), \tag{3}$$

where $\|A\|_1=\mathrm{Tr}\sqrt{A^\dagger A}$ denotes the trace norm of A. Notice that the optimal POVM does not appear in the expression of the minimal-error probability (3), as the trace norm implicitly takes it into account.

The problem of optimally discriminating two quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$ can be reformulated into the problem of finding the state ρ in the input Hilbert space $\mathcal{H}$, such that the error probability in the discrimination of the output states $\mathcal{E}_1(\rho)$ and $\mathcal{E}_2(\rho)$ is minimal. The possibility of exploiting entanglement with an ancillary system can increase the distinguishability of the output states [12]. In this case the output states to be discriminated will be of the form $(\mathcal{E}_1\otimes\mathcal{I}_\mathcal{K})\rho$ and $(\mathcal{E}_2\otimes\mathcal{I}_\mathcal{K})\rho$, where the input ρ is generally a bipartite state of $\mathcal{H}\otimes\mathcal{K}$, and the quantum operations act just on the first party whereas the identity map $\mathcal{I}_\mathcal{K}$ acts on the second.

Upon denoting with $\mathcal{R}'_B(p)$ the minimal-error probability when a strategy without ancilla is adopted, one has

$$\mathcal{R}'_B(p) = \frac{1}{2}\left(1 - \max_{\rho\in\mathcal{H}}\|p_1\mathcal{E}_1(\rho) - p_2\mathcal{E}_2(\rho)\|_1\right). \tag{4}$$

On the other hand, by allowing the use of an ancillary system, we have

$$\mathcal{R}_B(p) = \frac{1}{2}\left(1 - \max_{\xi\in\mathcal{H}\otimes\mathcal{K}}\|p_1(\mathcal{E}_1\otimes\mathcal{I})\xi - p_2(\mathcal{E}_2\otimes\mathcal{I})\xi\|_1\right). \tag{5}$$

The maximum of the trace norm in Eq. (5) with the supremum over the dimension of $\mathcal{K}$ is equivalent to the norm of complete boundedness [17] of the map $p_1\mathcal{E}_1-p_2\mathcal{E}_2$, and in fact for finite-dimensional Hilbert space the supremum is achieved for $\dim(\mathcal{K})=\dim(\mathcal{H})$ [17,18], and in the following we will drop the subindex $\mathcal{K}$ from the identity map. Moreover, due to linearity of quantum operations and convexity of the trace norm, the maximum in both Eqs. (4) and (5) is achieved on pure states.

Clearly, $\mathcal{R}_B(p)\leqslant\mathcal{R}'_B(p)$. In the case of discrimination between two unitary transformations U and V [14], one has $\mathcal{R}_B(p)=\mathcal{R}'_B(p)$, namely, there is no need of entanglement with an ancillary system to achieve the ultimate minimum-error probability, which is given by

$$\begin{aligned} \mathcal{R}_B(p) &= \min_{|\psi\rangle\in\mathcal{H}}\frac{1}{2}(1 - \sqrt{1 - 4p_1p_2|\langle\psi|U^\dagger V|\psi\rangle|^2}) \\ &= \frac{1}{2}(1 - \sqrt{1 - 4p_1p_2D^2}), \end{aligned} \tag{6}$$

where D is the distance between 0 and the polygon in the complex plane whose vertices are the eigenvalues of $U^\dagger V$.

In the case of discrimination of two Pauli channels for qubits, namely,

$$\mathcal{E}_i(\rho) = \sum_{\alpha=0}^{3} q_\alpha^{(i)}\sigma_\alpha\rho\sigma_\alpha, \quad i=1,2, \tag{7}$$

where $\Sigma_{\alpha=0}^3 q_\alpha^{(i)}=1$, $\sigma_0=I$, and $\{\sigma_1,\sigma_2,\sigma_3\}=\{\sigma_x,\sigma_y,\sigma_z\}$ denote the customary spin Pauli matrices, the minimal-error probability can be achieved by using a maximally entangled input state, and one obtains [12]

$$\mathcal{R}_B(p) = \frac{1}{2}\left(1 - \sum_{\alpha=0}^{3}|r_\alpha|\right), \tag{8}$$

with

$$r_\alpha = p_1q_\alpha^{(1)} - p_2q_\alpha^{(2)} = p(q_\alpha^{(1)} + q_\alpha^{(2)}) - q_\alpha^{(2)}, \tag{9}$$

where we fixed the *prior* $p=p_1$ and $p_2=1-p_1$. For a strategy with no ancillary assistance one has [12]

$$\mathcal{R}'_B(p) = \frac{1}{2}(1 - C), \tag{10}$$

where

$$\begin{aligned} C = \max\{&|r_0 + r_3| + |r_1 + r_2|, |r_0 + r_1| + |r_2 + r_3|, |r_0 \\ &+ r_2| + |r_1 + r_3|\}, \end{aligned} \tag{11}$$

and the three cases inside the brackets correspond to using an eigenstate of σ_z, σ_x, and σ_y, respectively, as the input state of the channel. More generally, for a pure input state $\rho=\frac{1}{2}(I+\vec{\sigma}\cdot\vec{n})$, with $\vec{n}=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$, the Bayes risk for discriminating the outputs will be [12,16]

$$\mathcal{R}'_B(p,\vec{\sigma}\cdot\vec{n}) = \frac{1}{2}(1 - \max\{|a+b|, \sqrt{\cos^2\theta(a-b)^2 + \sin^2\theta[c^2+d^2+2cd\cos(2\phi)]}\}), \tag{12}$$

with $a=r_0+r_3$, $b=r_1+r_2$, $c=r_0-r_3$, and $d=r_1-r_2$. Notice that the term $|a+b|=|2p-1|$ corresponds to the trivial guessing $\{\mathcal{E}_1$ if $p_1=p>1/2$, $\mathcal{E}_2$ if $p<1/2\}$.

We can also rewrite Eq. (10) as

$$\mathcal{R}'_B(p)=\min_{i=1,2,3}\mathcal{R}'_B(p,\sigma_i). \tag{13}$$

From Eqs. (8)–(11) one can see that entanglement is not needed to achieve the minimal-error probability as long as $C=\Sigma_{i=0}^{3}|r_i|$, which is equivalent to the condition $\Pi_{i=0}^{3}r_i\geqslant 0$. On the other hand, we can find instances where the channels can be perfectly discriminated only by means of entanglement, for example in the case of two channels of the form

$$\mathcal{E}_1(\rho)=\sum_{\alpha\neq\beta}q_\alpha\sigma_\alpha\rho\sigma_\alpha,\quad \mathcal{E}_2(\rho)=\sigma_\beta\rho\sigma_\beta, \tag{14}$$

with $q_\alpha\neq 0$, and arbitrary *a priori* probability.

III. MINIMAX DISCRIMINATION OF QUANTUM STATES

In the following we briefly review some results of Ref. [11] about minimax discrimination of quantum states that are needed to solve the problem of discrimination of Pauli channels in the next section, namely, we review just the case of two states. We are given two states ρ_1 and ρ_2, and we want to find the optimal measurement to discriminate between them in a minimax approach. In this scenario there are no *a priori* probabilities, and the optimal solution consists in finding the POVM $\{\vec{M}=M_1,M_2\}$ with $M_i\geqslant 0$ for $i=1$, 2 and $M_1+M_2=I$, that achieves the minimax

$$R_M(\rho_1,\rho_2)=\min_{\vec{M}}\max\{\mathrm{Tr}(\rho_1M_2),\mathrm{Tr}(\rho_2M_1)\}, \tag{15}$$

namely, one minimizes the largest of the probabilities of incorrect detection. The minimax and Bayesian schemes of discrimination of two states are connected by the following theorems [11].

Theorem 1. There is a measurement $\vec{B}$ that is optimal in the Bayes scheme for some *a priori* probability $(p_*,1-p_*)$ such that

$$\mathrm{Tr}(\rho_1B_1)=\mathrm{Tr}(\rho_2B_2). \tag{16}$$

This measurement is optimal in the minimax scheme as well, and one has $R_M(\rho_1,\rho_2)=R_B(p_*)=\mathrm{Tr}(\rho_1B_2)$.

Theorem 2. The solution in the minimax problem is equivalent to the solution of the problem

$$R_M(\rho_1,\rho_2)=\max_p R_B(p), \tag{17}$$

and the a priori probability achieving the maximum corresponds to the value $p=p_*$ in Theorem 1.

IV. MINIMAX DISCRIMINATION OF PAULI CHANNELS

As in the Bayesian approach, the minimax discrimination of two channels consists in finding the optimal input state such that the two possible output states are discriminated with minimum risk. Again, we will consider the two cases with and without ancilla, upon defining

$$\mathcal{R}_M=\min_{\xi\in\mathcal{H}\otimes\mathcal{K}}R_M((\mathcal{E}_1\otimes\mathcal{I})(\xi),(\mathcal{E}_2\otimes\mathcal{I})(\xi)),$$

$$\mathcal{R}'_M=\min_{\rho\in\mathcal{H}}R_M(\mathcal{E}_1(\rho),\mathcal{E}_2(\rho)), \tag{18}$$

where $R_M(\rho_1,\rho_2)$ is given in Eq. (15). Since for all $\vec{M}$, ρ, and p, one has

$$\begin{aligned}&\max\{\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2],\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]\}\\&\quad\geqslant p\,\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2]+(1-p)\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1],\end{aligned} \tag{19}$$

then $\mathcal{R}_M\geqslant\mathcal{R}_B(p)$ for all p. Analogously, $\mathcal{R}'_M\geqslant\mathcal{R}'_B(p)$ for all p.

Theorems 1 and 2 can be immediately applied to state that the minimax discrimination of two unitaries is equivalent to the Bayesian one. In fact, the optimal input state in the Bayesian problem which achieves the minimum error probability of Eq. (6) does not depend on the *a priori* probabilities. Therefore it is also optimal for the minimax problem and there is no need of entanglement [and the minimax risk $\mathcal{R}_M$ will be equivalent to the Bayes risk $\mathcal{R}_B(1/2)$].

Let us now consider the problem of discriminating the Pauli channels of Eq. (7) in the minimax framework. In the following theorem, we show that an (arbitrary) maximally entangled state always allows one to achieve the optimal minimax discrimination as in the Bayesian problem.

Theorem 3. The minimax risk $\mathcal{R}_M$ for the discrimination of two Pauli channels can be achieved by using an arbitrary maximally entangled input state. Moreover, the minimax risk is then the Bayes risk for the worst *a priori* probability:

$$\mathcal{R}_M=\max_p\mathcal{R}_B(p). \tag{20}$$

Proof. Let us discriminate between the states $\rho_i=(\mathcal{E}_i\otimes\mathcal{I})(\xi^e)$, where ξ^e is a maximally entangled state. By Theorem 1 there are *a priori* probabilities $(p_*,1-p_*)$ whose optimal Bayes measurement satisfies

$$\mathrm{Tr}(\rho_1B_1)=\mathrm{Tr}(\rho_2B_2). \tag{21}$$

Since the input state ξ^e is always optimal in the Bayes problem we infer $\mathcal{R}_B(p_*)=\mathrm{Tr}(\rho_1B_2)$, and moreover $R_M(\rho_1,\rho_2)=\mathcal{R}_B(p_*)$. Now, one has also $\mathcal{R}_M=R_M(\rho_1,\rho_2)$, since if it were not be true, then there would be an input state ρ and a measurement $\vec{M}$ for which

$$\max\{\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2],\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]\}<R_B(p_*),$$

and hence

$$p_*\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2]+(1-p_*)\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]<R_B(p_*),$$

which is a contradiction. Equation (20) simply comes from the relation $\mathcal{R}_M\geqslant\mathcal{R}_B(p)$ for all p, along with $\mathcal{R}_M=\mathcal{R}_B(p_*)$.

Notice the nice correspondence between Eqs. (17) and (20). Theorem 3 holds true also in the case of generalized Pauli channels in higher dimension, since entangled states

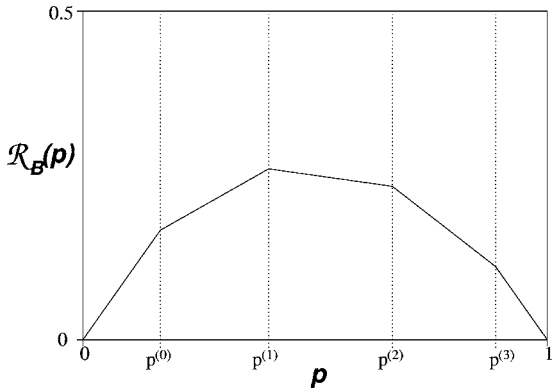

FIG. 1. The optimal Bayes risk $\mathcal{R}_B(p)$ in the discrimination of two Pauli channels versus the *a priori* probability p will usually look like this. Notice that the rightmost and leftmost segments have slope 1 and −1, respectively. The minimal risk for the minimax discrimination corresponds to $\mathcal{R}_M=\max_p \mathcal{R}_B(p)$, and is achieved at one of the break points $p^{(\alpha)}$.

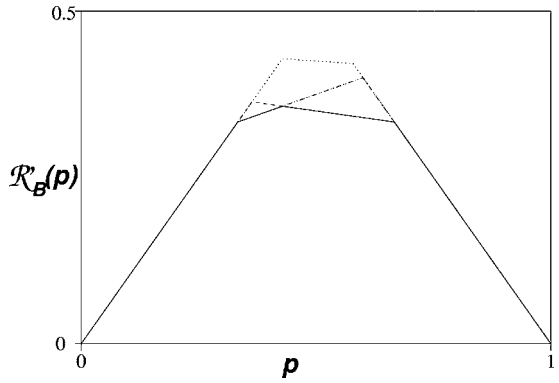

FIG. 2. An example for the Bayes risks $\mathcal{R}'_B(p,\sigma_i)$ with $i=x,y,z$ versus the *a priori* probability p, for discrimination without ancilla. Each of the three different dotted lines corresponds to the Bayes risk $\mathcal{R}'_B(p,\sigma_i)$ when sending an eigenstate of the Pauli matrix σ_i through the channel. The solid line is the optimal Bayes risk $\mathcal{R}'_B(p)$ without ancillary assistance, and corresponds at any p to the minimum of the three $\mathcal{R}'_B(p,\sigma_i)$. The minimal risk for the minimax discrimination with no ancilla corresponds to $\mathcal{R}'_M=\max_p \mathcal{R}'_B(p)$, and is achieved at one of the break points of $\mathcal{R}'_B(p)$.

again achieve the optimal Bayesian discrimination, whatever the *a priori* probability [12]. More generally, Eq. (20) will hold in the discrimination of any couple of quantum operations for which the minimal Bayes risk $\mathcal{R}_B(p)$ can be achieved by the same input state for any p.

Now we establish some visual images on which to read the minimax risks. We must look at the function $\mathcal{R}_B(p)$ given in Eq. (8) drawn on [0, 1]. By Eq. (20), we know that its maximum is $\mathcal{R}_M$. As the r_α defined in Eq. (9) are increasing affine functions of p, their absolute value is a convex piecewise affine function, and hence $\mathcal{R}_B(p)$ is a concave piecewise affine function (see Fig. 1). The four break points correspond to the four values of p for which each r_α vanishes. We define $t_\alpha=q_\alpha^{(1)}+q_\alpha^{(2)}$ as the slopes of the functions r_α and $p^{(\alpha)}=q_\alpha^{(2)}/t_\alpha$ as the value of p for which $r_\alpha=0$. We denote by p_* the point at which $\mathcal{R}_B(p)$ reaches its maximum (the maximum will be attained at one of the break points $p^{(\alpha)}$). We also reorder the index α such that $p^{(0)}\leqslant p^{(1)}\leqslant p^{(2)}\leqslant p^{(3)}$. In this way, $\mathcal{R}_B(p)$ is rewritten

$$\mathcal{R}_B(p)=\frac{1}{2}\left(1-\sum_{\alpha=0}^{3} t_\alpha|p-p^{(\alpha)}|\right). \tag{22}$$

Let us now look at the discrimination strategy without any ancillary system. Another picture, that should be superimposed on Fig. 1, is the Bayes risk $\mathcal{R}'_B(p)$ of Eq. (10) versus p for the strategy with no ancillary system. One can see that $\mathcal{R}'_B(p)$ is the minimum of the three piecewise affine functions $\mathcal{R}'_B(p,\sigma_x),\mathcal{R}'_B(p,\sigma_y),\mathcal{R}'_B(p,\sigma_z)$, corresponding to the Bayes risks when sending an eigenstate of the Pauli matrices. Here again $\mathcal{R}'_B(p)$ is the minimum of concave functions, so it is concave as well, and the maximum will be attained at a break point $p=p'_*$ (see Fig. 2). To "read" more in these pictures, once again we prove that the optimal minimax risk $\mathcal{R}'_M$ for discrimination without ancilla corresponds to the optimal Bayes risk without ancilla for the worst *a priori* probability p'_*.

Theorem 4. The optimal minimax discrimination with no ancilla is equivalent to the solution of the problem

$$\mathcal{R}'_M=\max_p \mathcal{R}'_B(p)\equiv\mathcal{R}'_B(p'_*). \tag{23}$$

Proof. Notice again the similarity between Eqs. (17), (20), and (23). For any ρ one has

$$R_M(\mathcal{E}_1(\rho),\mathcal{E}_2(\rho))\geqslant\mathcal{R}'_M\geqslant\max_p \mathcal{R}'_B(p). \tag{24}$$

If we find an input state $\rho_{\vec{n}}=\frac{1}{2}(I+\vec{\sigma}\cdot\vec{n})$ such that

$$\max_p \mathcal{R}'_B(p)=\max_p \mathcal{R}'_B(p,\vec{\sigma}\cdot\vec{n}) \tag{25}$$

from Eq. (17) of Theorem 2 it follows that

$$R_M(\mathcal{E}_1(\rho_{\vec{n}}),\mathcal{E}_2(\rho_{\vec{n}}))=\max_p \mathcal{R}'_B(p,\vec{\sigma}\cdot\vec{n}), \tag{26}$$

which, along with Eqs. (24) and (25), provides the proof. Moreover, $\rho_{\vec{n}}$ will be the optimal input state for the minimax discrimination without ancilla.

Now we have just to find a state such that condition (25) holds. We already noticed that p'_* is a breaking point of $\mathcal{R}'_B(p)$. Either this break point is also a break point (and the maximum) of $\mathcal{R}'_B(p,\sigma_i)$ for some $i\in x,y,z$, or else at least two of the $\mathcal{R}'_B(p,\sigma_i)$ are crossing in p'_*, one increasing and the other decreasing (Fig. 2). In the first case Eq. (25) is immediately satisfied, and an eigenstate of σ_i will be the optimal input state. In the second case, we show that when two $\mathcal{R}'_B(p,\sigma_i)$ are crossing at p'_* we can find a state $\rho_{\vec{n}}$ such that

$$\mathcal{R}'_B(p'_*,\vec{\sigma}\cdot\vec{n})=\mathcal{R}'_B(p'_*,\sigma_i),$$

$$\partial_p\mathcal{R}'_B(p,\vec{\sigma}\cdot\vec{n})\big|_{p=p'_*}=0, \tag{27}$$

and therefore has the maximum at p'_* by concavity. In fact, the crossing and therefore nonequality of the $\mathcal{R}'_B(p,\sigma_i)$ in a

neighborhood of p'_*, implies that for each of the two $\mathcal{R}'_B(p,\sigma_i)$, the maximum in Eq. (12) for p'_* is attained by the square-root term (since the term $|a+b|$ is just a function of p). Let us assume that the σ_i that give such a crossing are σ_x and σ_y. Then looking at Eq. (12), we have at point p'_*

$$|c+d| = |c-d|,$$

$$\partial_p|c+d|\partial_p|c-d| < 0 \tag{28}$$

(notice that all functions are linear, i.e., differentiable in p'_*). Indeed, the first of Eqs. (28) implies that any linear combination of eigenstate of σ_x and σ_y satisfies the first of Eqs. (27). By taking an input state with $\theta=\pi/2$ and ϕ such that

$$\tan^2\phi = -\left.\frac{\partial_p|c+d|}{\partial_p|c-d|}\right|_{p=p'_*}, \tag{29}$$

the second equation in (27) is satisfied as well. Similarly, if the σ_i are σ_z,σ_x one can take the input state with $\phi=0$ or π and θ such that

$$\tan^2\theta = -\left.\frac{\partial_p|a-b|}{\partial_p|c+d|}\right|_{p=p'_*}. \tag{30}$$

Finally, for σ_z,σ_y one has $\phi=\pm\pi/2$ and

$$\tan^2\theta = -\left.\frac{\partial_p|a-b|}{\partial_p|c-d|}\right|_{p=p'_*}. \tag{31}$$

As a remark, no eigenstate of σ_i for $i=x,y,z$ can be an optimal input in the minimax sense in this situation. This is a typical result of the minimax discrimination. As in the case of discrimination of states [11], when the correspondent Bayes problem presents a kind of degeneracy and has multiple solutions, in the minimax problem the degeneracy is partially or totally removed. In the present situation, if we have the maximum of $\mathcal{R}'_B(p)$ at the crossing point of exactly two $\mathcal{R}'_B(p,\sigma_i)$, one increasing and the other decreasing, we find just four optimal input states: two nonorthogonal states and their respective orthogonal states. We will give an explicit example at the end of the section.

If we want to find in what case entanglement is not necessary for optimal minimax discrimination, then we have just to characterize when $\mathcal{R}'_B(p'_*)=\mathcal{R}_B(p_*)$. We already noticed that we can choose p_* to be one of the $p^{(\alpha)}$. The corresponding r_α is zero, and hence $C=\Sigma_\alpha|r_\alpha|$, namely, $\mathcal{R}'_B(p_*)=\mathcal{R}_B(p_*)$. Since one has

$$\mathcal{R}'_B(p'_*) = \mathcal{R}'_M \geqslant \mathcal{R}_M = \mathcal{R}_B(p_*) = \mathcal{R}'_B(p_*), \tag{32}$$

we only have to check that p_* is a maximum of $\mathcal{R}'_B(p)$, recalling that the function is concave (see Fig. 3).

Ultimately, we will have to list the cases. Reading them might be clearer with the quantities appearing in Eqs. (8)–(11) explicitly written as a function of p. The most useful segmentation of $[0,1]$ is based on the $p^{(\alpha)}$, that is the points where the r_α vanish, and $\mathcal{R}_B(p)$ breaks. Recall that $r_\alpha = t_\alpha(p-p^{(\alpha)})$, and $r_\alpha>0$ for $p>p^{(\alpha)}$. As we have four α, we have five segments (they may become degenerate). Remember that knowing C in Eq. (11) and $\Sigma_\alpha|r_\alpha|$ is tantamount to knowing $\mathcal{R}'_B(p)$ or $\mathcal{R}_B(p)$. Here is a list of the signs of the r_α and the value of C on each open segment (so that all $r_\alpha\neq 0$).

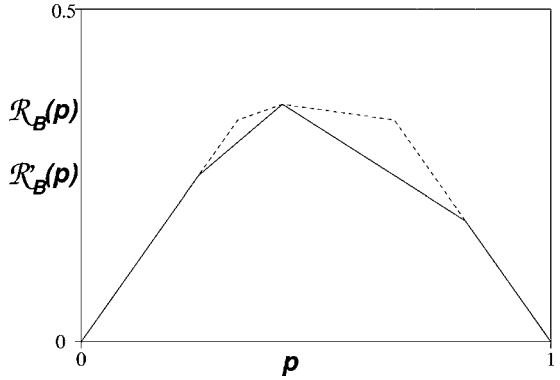

FIG. 3. Optimal Bayes risks versus the *a priori* probability p for the discrimination of the Pauli channels with parameters given in Eq. (39). The solid line gives $\mathcal{R}_B(p)$ for an entanglement-assisted strategy; the dotted line gives $\mathcal{R}'_B(p)$ for a strategy without ancilla. The minimal risk in the optimal minimax discrimination corresponds in both strategies to $\mathcal{R}'_M=\max_p \mathcal{R}'_B(p)=\max_p \mathcal{R}_B(p)=\mathcal{R}_M$, namely, there is no need of an ancillary system.

(1) $(0,p^{(0)}):\Sigma_\alpha|r_\alpha|=-\Sigma_\alpha r_\alpha=C$. Notice that $\mathcal{R}'_B(p)=\mathcal{R}_B(p)$ and that their common slope is 1.

(2) $(p^{(0)},p^{(1)}):\Sigma_\alpha|r_\alpha|=r_0-r_1-r_2-r_3$, so that $C=r_0-r_1-r_2-r_3-2\inf_{\alpha=1,2,3}|r_\alpha|$. On this segment, $\mathcal{R}'_B(p)>\mathcal{R}_B(p)$.

(3) $(p^{(1)},p^{(2)}):\Sigma_\alpha|r_\alpha|=r_0+r_1-r_2-r_3=C$, so that $\mathcal{R}'_B(p)=\mathcal{R}_B(p)$.

(4) $(p^{(2)},p^{(3)}):\Sigma_\alpha|r_\alpha|=r_0+r_1+r_2-r_3$, so that $C=r_0+r_1+r_2-r_3-2\inf_{\alpha=0,1,2}r_\alpha$ and $\mathcal{R}'_B(p)>\mathcal{R}_B(p)$.

(5) $(p^{(3)},1):\Sigma_\alpha|r_\alpha|=\Sigma_\alpha r_\alpha=C$ and $\mathcal{R}'_B(p)=\mathcal{R}_B(p)$. Their common slope is (-1).

A close look at these expressions, as we will show in the following, proves that $\mathcal{R}'_B(p)$ is derivable at $p^{(\alpha)}$ unless there is $\beta\neq\alpha$ such that $p^{(\alpha)}=p^{(\beta)}$. With this in mind, we see that p_* cannot be a maximum of $p^{(\alpha)}$ unless several r_α are null at the same point (with supplementary conditions) or $p_*=p^{(1)}$ and the segment $(p^{(1)},p^{(2)})$ is flat. Here is the full-fledged study, using repeatedly the list above. It is complete as any other case can be handled by symmetry (switching channels, that is mapping p to $1-p$).

(1) $p_*=p^{(0)}<p^{(1)}$: At $p^{(0)}$, we have $r_0=0$ and $r_\alpha<0$ for $\alpha\neq 0$. So that $\inf_\alpha|r_\alpha|=|r_0|$ on a neighborhood of $p^{(0)}$. On that neighborhood, we deduce $C=-\Sigma_\alpha r_\alpha$, and hence $\partial_p\mathcal{R}'_B(p)|_{p=p^{(0)}}=1$, so that $p^{(0)}$ is not a maximum of $\mathcal{R}'_B(p)$. Entanglement is then necessary for optimal discrimination.

(2) $p_*=p^{(0)}=p^{(1)}<p^{(2)}$: On $(0,p^{(0)})\cup(p^{(1)},p^{(2)})$, the equality $\mathcal{R}'_B(p)=\mathcal{R}_B(p)$ holds. Thus, the two functions are equal on a neighborhood of p_*, and since p_* is a (local) maximum of $\mathcal{R}_B(p)$, it is also a local maximum of $\mathcal{R}'_B(p)$. In this case an unentangled strategy is then as efficient as any entangled one.

(3) $p_*=p^{(0)}=p^{(1)}=p^{(2)}<p^{(3)}$: The risk $\mathcal{R}'_B(p)$ is nondecreasing on the left of p_* (slope 1); we then want it to be nonincreasing on a right neighborhood of p_*. Now this is part of the segment $(p^{(2)},p^{(3)})$, where $C=r_0+r_1+r_2-r_3-2\inf_{\alpha=0,1,2}r_\alpha$. Recall that $r_\alpha=t_\alpha(p-p^{(\alpha)})$. Since $r_\alpha=0$ for $\alpha\neq 3$ at p_*, and they are all nondecreasing, $\inf_{\alpha=0,1,2}r_\alpha$ is the

one with the smallest slope t_α. It follows that the slope of $\mathcal{R}'_B(p)$ on the right of p_* is $t_3-t_0-t_1-t_2+2\inf_{\alpha=0,1,2}t_\alpha$, and so entanglement is not needed if and only if

$$t_3+2\inf_{\alpha=0,1,2}t_\alpha \leqslant \sum_{\alpha=0,1,2}t_\alpha. \tag{33}$$

(4) $p_*=p^{(0)}=p^{(1)}=p^{(2)}=p^{(3)}$: This is the trivial case where both channels are the same. Of course, entanglement is useless.

(5) $p^{(0)}<p_*=p^{(1)}<p^{(2)}$: In this case $\mathcal{R}'_B(p)$ is derivable at p_*. Indeed, on $(p^{(1)},p^{(2)})$, we have $C=r_0+r_1-r_2-r_3$ whereas on $(p^{(0)},p^{(1)}), C=r_0-r_1-r_2-r_3-2\inf_{\alpha=1,2,3}|r_\alpha|$. In a neighborhood of p_*, one has $\inf_{\alpha=1,2,3}|r_\alpha|=r_1$, as it is the only one that is 0 at p_*; hence $C=r_0+r_1-r_2-r_3$ also on a left neighborhood of p_* and the slope of $\mathcal{R}'_B(p)$ at p_* is $t_3+t_2-t_1-t_0$. Since p_* is a maximum if and only if this slope is null, we get the condition

$$t_0+t_1=t_2+t_3. \tag{34}$$

(6) $p^{(0)}<p_*=p^{(1)}=p^{(2)}<p^{(3)}$: On the left of p_*, we are on the segment $(p^{(0)},p^{(1)})$, so that $C=r_0-r_1-r_2-r_3-2\inf_{\alpha=1,2,3}|r_\alpha|$. On the right, we are on the segment $(p^{(2)},p^{(3)})$ and $C=r_0+r_1+r_2-r_3-2\inf_{\alpha=0,1,2}r_\alpha$. In a neighborhood of p_*, the r_α with the smallest absolute value will be either r_1 or r_2 (more precisely, the one with the smallest slope t_α), so that we can write in a neighborhood of p_* for both sides $C=r_0-r_3+|r_2-r_1|$. The slope of $\mathcal{R}'_B(p)$ is then $t_3-t_0+|t_2-t_1|$ and $t_3-t_0-|t_2-t_1|$ on the left and on the right of p_*, respectively. Entanglement is not necessary when p_* is a maximum of $\mathcal{R}'_B(p)$, and hence we get the necessary and sufficient condition

$$|t_0-t_3|\leqslant|t_1-t_2|. \tag{35}$$

We can summarize the above discussion as follows.

Theorem 5. The minimax risk without using ancilla is strictly greater than the minimax risk using entanglement, except in the following cases.

(a) The trivial situation where both channels are the same, so that $p_*=p^{(\alpha)}=\frac{1}{2}$ for all α.

(b) If $p_*=p^{(0)}\leqslant p^{(1)}<p^{(2)}$.

(c) If $p_*=p^{(0)}=p^{(1)}=p^{(2)}<p^{(3)}$ and

$$t_3+2\inf_{\alpha=0,1,2}t_\alpha \leqslant \sum_{\alpha=0,1,2}t_\alpha. \tag{36}$$

(d) If $p^{(0)}<p_*=p^{(1)}<p^{(2)}$ and

$$t_0+t_1=t_2+t_3. \tag{37}$$

(e) If $p^{(0)}<p_*=p^{(1)}=p^{(2)}<p^{(3)}$ and

$$|t_0-t_3|\leqslant|t_1-t_2|. \tag{38}$$

(f) The symmetric cases (obtained by exchanging channels 1 and 2, i.e. exchanging indices 0 and 1 with 3 and 2, respectively, in both $p^{(\alpha)}$ and t_α.

Differently from the Bayesian result, we notice that when entanglement is not necessary to achieve the optimal minimax discrimination, the optimal input state may not be an eigenstate of the Pauli matrices. Consider, for example, the two Pauli channels featured in Fig. 3 which correspond to the parameters

$$\begin{aligned} &q_0^{(1)}=0.3,\quad q_1^{(1)}=0.4,\quad q_2^{(1)}=0.2,\quad q_3^{(1)}=0.1,\\ &q_0^{(2)}=0.1,\quad q_1^{(2)}=0.3,\quad q_2^{(2)}=0.15,\quad q_3^{(2)}=0.45. \end{aligned} \tag{39}$$

We can compute $p^{(\alpha)}=q_\alpha^{(2)}/(q_\alpha^{(1)}+q_\alpha^{(2)})$ and get $p^{(\alpha)}=(1/4,3/7,3/7,9/11)$. Here $p_*=3/7$, and we are in the situation of Eq. (38), since $t_\alpha=(q_\alpha^{(1)}+q_\alpha^{(2)})=(0.4,0.7,0.35,0.55)$. Hence, entanglement is not necessary to achieve the optimal minimax risk, but the state to be used is not an eigenstate of the Pauli matrices. In fact, we are in the case of the proof of Theorem 3, where $\mathcal{R}'_B(p,\sigma_x)$ and $\mathcal{R}'_B(p,\sigma_y)$ are crossing in p_*. The optimal input state for the minimax discrimination will be given by $\theta=\pi/2$ and ϕ as in Eq. (29), which gives $\tan^2\phi=2/5$. Then, we have four optimal input states that lie on the equator of the Bloch sphere, with $\vec{n}=(\pm\sqrt{5/7},\pm\sqrt{2/7},0)$.

V. CONCLUSIONS

We addressed the problem of optimally discriminating two Pauli channels in the minimax approach, where no *a priori* probability is assigned. We showed that when an entangled-input strategy is adopted, the optimal discrimination can always be achieved by sending a maximally entangled state into the channel, as happens in the Bayesian approach. On the other hand, the optimal input state for a strategy without ancilla can be different in the minimax approach with respect to the Bayesian one. In the latter the optimal input can always be chosen as an eigenstate of one of the Pauli matrices, whereas in the former this may not be the case. We then characterized the channels where the use of entanglement outperforms the scheme without assistance of ancilla. Notice that even though the Bayesian and the minimax strategies are not comparable, since they address different estimation problems, nevertheless the solution of the general Bayesian problem actually includes also the minimax solution, since the optimal minimax strategy is equivalent to the Bayesian one for the worst risk (Theorems 3 and 4). This is a general feature for the channels analyzed in the present paper. This work extends the study of minimax discrimination of states to the simplest example of quantum operations, and show the relation and the differences with respect to the Bayesian approach.

ACKNOWLEDGMENTS

Support from INFM through Project No. PRA-2002-CLON, and from EC and MIUR through the cosponsored ATESIT Project No. IST-2000-29681 and Cofinanziamento 2003 is acknowledged.

[1] W. K. Wootters, Phys. Rev. D **23**, 357 (1981); S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).
[2] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005); V. P. Belavkin, G. M. D'Ariano, and M. Raginsky, J. Math. Phys. **46**, 062106 (2005).
[3] For a recent review, see J. Bergou, U. Herzog, and M. Hillery, in *Quantum State Estimation*, Lecture Notes in Physics Vol. 649 (Springer, Berlin, 2004), p. 417.
[4] For a recent review, see A. Chefles, in *Quantum State Estimation* (Ref. [3]), p. 467.
[5] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[6] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987); D. Dieks, *ibid.* **126**, 303 (1988); A. Peres, *ibid.* **128**, 19 (1988); G. Jaeger and A. Shimony, *ibid.* **197**, 83 (1995); A. Chefles, *ibid.* **239**, 339 (1998).
[7] A. Acin, E. Bagan, M. Baig, Ll. Masanes, and R. Munoz-Tapia, Phys. Rev. A **71**, 032338 (2005).
[8] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[9] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001).
[10] Y.-X. Chen and D. Yang, Phys. Rev. A **65**, 022320 (2002); Z. Ji, H. Cao and M. Ying, *ibid.* **71**, 032323 (2005).
[11] G. M. D'Ariano, M. F. Sacchi, and J. Kahn, Phys. Rev. A **72**, 032310 (2005).
[12] M. F. Sacchi, Phys. Rev. A **71**, 062340 (2005).
[13] See, for example, D. Gottesman, in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, edited by S. J., Lomonaco, Jr. (American Mathematical Society, Providence, RI, 2002) pp. 221–235; E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W. H. Zurek, Los Alamos Sci. **27**, 188 (2002), and references therein.
[14] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000); A. Acín, Phys. Rev. Lett. **87**, 177901 (2001); G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, *ibid.* **87**, 270404 (2001).
[15] M. F. Sacchi, Phys. Rev. A **72**, 014305 (2005).
[16] M. F. Sacchi, J. Opt. Soc. Am. B **7**, S333 (2005).
[17] V. I. Paulsen, *Completely Bounded Maps and Dilations* (Longman Scientific and Technical, New York, 1986).
[18] D. Aharonov, A. Kitaev, and N. Nisan, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computation* (ACM, New York, 1998), p. 20, also available at quant-ph/9806029.