Optimal partial estimation of multiple phases

Ladislav Mišta, Jr., Jaromír Fiurášek, and Radim Filip
Department of Optics, Palacký University, 17. listopadu 50, 772 07 Olomouc, Czech Republic
(Received 24 March 2005; published 12 July 2005; publisher error corrected 18 August 2005)

We derive the optimal trade-off between the estimation fidelity and the fidelity of the state after the estimation for a single copy of an unknown pure state of a d-level system belonging to a specific subset of the set of all pure states. The set of states to be considered here is formed by all pure states of a d-level system produced by d-independent phase shifts of some reference state. We also propose a measurement scheme realizing such an optimal partial estimation of multiple phases in which the trade-off between the fidelities can be controlled by the state of the ancilla.

DOI: 10.1103/PhysRevA.72.012311 PACS number(s): 03.67.−a

I. INTRODUCTION

A general quantum measurement on an unknown pure quantum state $|\psi\rangle$ provides classical information on the state in the form of the measurement outcome. This information can be converted into an estimate of the state ρ_{est}. Simultaneously, the measurement device produces an output quantum state ρ_{out} that is an approximate replica of the original state. It holds that the better the estimate is, the worse the replica is. To quantify this peculiar property of quantum measurement one can use two mean fidelities [1]: the mean fidelity of the output quantum state with respect to the input state F that characterizes the disturbance introduced by the measurement and the mean fidelity of the state estimation G that describes the information gain. In terms of the fidelities F and G one then can define an optimal *partial* measurement as a measurement that gives for a given output fidelity F the largest possible estimation fidelity G. To seek the optimal trade-off between the fidelities F and G as well as the optimal measurement schemes is an interesting issue as the trade-off varies with the set of input states and it was found to date only in a few cases. To be more specific, recently the optimal fidelity trade-off was found analytically for a single copy of a completely unknown pure state of a d-level particle [1] and numerically for an ensemble of identically prepared 2-level systems [2]. Many quantum information protocols, such as quantum cryptography [3,4] or phase-covariant quantum cloning [4,5], work, however, with pure states of the form

$$|\psi(\phi)\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d} e^{i\phi_j}|j\rangle, \tag{1}$$

where $\phi=(\phi_1,\phi_2,\ldots,\phi_d)$, $\phi_j\in[0,2\pi]$, $j=1,\ldots,d$, and $\{|j\rangle\}_{j=1}^{d}$ is an orthonormal basis of a d-level system. Note that the states (1) can be generated by d independent phase shifts of the reference state $|+\rangle=(1/\sqrt{d})\Sigma_{j=1}^{d}|j\rangle$ [6] and represent a d-dimensional generalization of the well-known equatorial states—i.e., states of qubits ($d=2$) lying on the equator of the Poincaré sphere. The equatorial states also find practical application in quantum cryptography with phase coding [7,8]. In view of the fact that the optimal estimation strategy gives for the set of states (1) a higher estimation fidelity $G_{\max}=(2d-1)/d^2$ [6,9] than the optimal estimation strategy for a completely unknown pure state when $G'_{\max}=2/(d+1)$ [10] we also expect that the optimal trade-off between F and G for a completely unknown pure state derived in [1] will not be optimal for the set of states (1).

In this paper we show that the optimal trade-off between the mean output fidelity F and the mean estimation fidelity G for a generic trace-preserving quantum operation is for the set of states (1) of the form

$$\sqrt{d^2G-d+1}=\sqrt{d(1-F)}+\sqrt{\frac{dF-1}{d-1}} \tag{2}$$

and surpasses the trade-off derived for a completely unknown state [1]. Further, we construct explicitly a scheme performing such an optimal partial estimation of multiple phases. Our scheme is based on the standard quantum nondemolition (QND) coupling programmed by the state of ancilla that allows one to continuously control the flow of information between the output state and the estimated state. Programmable quantum devices implementing unitary operations were considered in [11] and exteded to quantum maps in [12]. Finally, we also show that such an optimal partial estimation can be performed even using a weak QND coupling that encodes the information on the input state into nonorthogonal states of the ancilla.

The paper is organized as follows. In Sec. II we derive the optimal fidelity trade-off. In Sec. III we design a measurement scheme satisfying the trade-off. Finally, Sec. IV contains the conclusions.

II. DERIVATION OF THE OPTIMAL TRADE-OFF

At the outset we establish a general method how to determine the optimal partial measurement on a quantum state which gives for a given mean output fidelity F the largest possible mean estimation fidelity G. We will be concerned with the sets of input states that form an orbit of a group $\mathcal{G}$, $|\psi(g)\rangle=U(g)|\psi(0)\rangle$, where $U(g)$, $g\in\mathcal{G}$, is a unitary representation of the group on the input Hilbert space $\mathcal{H}_{\text{in}}$ and $|\psi(0)\rangle$ is a reference state. We will also assume that the *a priori* distribution of the input states coincides with the invariant measure dg on the group.

With each particular outcome of the considered measurement device labeled by a group element h is associated a trace-decreasing completely positive (CP) map which can be represented by a positive-semidefinite operator $\chi(h)$ on the tensor product of input and output Hilbert spaces [13]. If the measurement outcome h has been detected, then the estimated state is $|\psi(h)\rangle$ whereas the output state reads

$$\rho(h|g) = \mathrm{Tr}_{\mathrm{in}}[\chi(h)\psi(g)^T \otimes \mathbb{1}_{\mathrm{out}}], \tag{3}$$

where we have defined $\psi(g) \equiv |\psi(g)\rangle\langle\psi(g)|$ and $\mathbb{1}_{\mathrm{out}}$ is the identity operator on the output Hilbert space $\mathcal{H}_{\mathrm{out}}$. The output state (3) is normalized such that its trace is equal to the probability density $P(h|g)$ of this outcome, $P(h|g)dh = \mathrm{Tr}_{\mathrm{out}}[\rho(h|g)]dh$. The overall input-output transformation should be a trace-preserving CP map which implies

$$\int_g \mathrm{Tr}_{\mathrm{out}}[\chi(g)]dg = \mathbb{1}_{\mathrm{in}}, \tag{4}$$

where $\int_g$ denotes integration over the whole group $\mathcal{G}$ and $\mathbb{1}_{\mathrm{in}}$ is the identity operator on the input Hilbert space. Performing many times the considered measurement on the input state $|\psi(g)\rangle$ we obtain on average the estimated state $\rho_{\mathrm{est}}(g) = \int_h P(h|g)|\psi(h)\rangle\langle\psi(h)|dh$ and the output state $\rho_{\mathrm{out}}(g) = \int_h \rho(h|g)dh$, where $\int_h dh$ is the averaging over all possible measurement outcomes for a fixed input state. The amount of information acquired on the input state from the considered measurement can be quantified by the mean estimation fidelity defined as

$$G = \int_g \gamma(g)dg, \tag{5}$$

where $\gamma(g) = \langle\psi(g)|\rho_{\mathrm{est}}(g)|\psi(g)\rangle$ is the estimation fidelity. Similarly, the disturbance caused by the measurement can be quantified by the mean output fidelity defined as

$$F = \int_g \varphi(g)dg, \tag{6}$$

where $\varphi(g) = \langle\psi(g)|\rho_{\mathrm{out}}(g)|\psi(g)\rangle$ is the output fidelity. Any device described by the set of CP maps $\chi(g)$ can be converted by twirling operation [14] into a *covariant* machine whose fidelities $\gamma(g)$ and $\varphi(g)$ do not depend on the input state—i.e., $G = \gamma(g)$ and $F = \varphi(g)$. The covariant machine is fully characterized by a single operator χ_0, and all the operators $\chi_{\mathrm{cov}}(g)$ can be obtained as follows:

$$\chi_{\mathrm{cov}}(g) = [U_{\mathrm{in}}^*(g) \otimes U_{\mathrm{out}}(g)]\chi_0[U_{\mathrm{in}}^T(g) \otimes U_{\mathrm{out}}^\dagger(g)]. \tag{7}$$

It can be shown by direct calculation that if the operator χ_0 is chosen to be

$$\chi_0 = \int_g [U_{\mathrm{in}}^T(g) \otimes U_{\mathrm{out}}^\dagger(g)]\chi(g)[U_{\mathrm{in}}^*(g) \otimes U_{\mathrm{out}}(g)]dg, \tag{8}$$

then the mean fidelities F and G for the covariant machine $\chi_{\mathrm{cov}}(g)$ become equal to the mean fidelities for the original machine $\chi(g)$. It follows that without loss of any generality we can restrict our attention to the covariant machines.

For a covariant device, the fidelities can be conveniently expressed as

$$F = \int_g \mathrm{Tr}[\chi_0\psi(g)^T \otimes \psi(g)]dg,$$

$$G = \int_g \mathrm{Tr}[\chi_0\psi(g)^T \otimes \mathbb{1}_{\mathrm{out}}]\mathrm{Tr}[\psi(g)\psi(0)]dg. \tag{9}$$

Next we define positive-semidefinite operators

$$R_F = \int_g \psi(g)^T \otimes \psi(g)dg,$$

$$R_G = \int_g \mathrm{Tr}_{\mathrm{out}}[(\psi(g)^T \otimes \psi(g))(\mathbb{1}_{\mathrm{in}} \otimes \psi(0))] \otimes \mathbb{1}_{\mathrm{out}}dg. \tag{10}$$

Note that $R_G = \mathrm{Tr}_{\mathrm{out}}[R_F \mathbb{1}_{\mathrm{in}} \otimes \psi(0)] \otimes \mathbb{1}_{\mathrm{out}}$. With the use of these operators the mean fidelities can be written as

$$F = \mathrm{Tr}[\chi_0 R_F], \quad G = \mathrm{Tr}[\chi_0 R_G]. \tag{11}$$

We seek the optimal trade-off between the fidelities F and G; i.e., we want to maximize G for a fixed F. This is equivalent to maximizing a convex mixture of these two fidelities, $\mathcal{F} = pF + (1-p)G$, where $p \in [0,1]$ controls the trade-off between the quality of the state estimation and the quality of the output replica of the state. We can write $\mathcal{F} = \mathrm{Tr}[\chi_0 R_p]$, where

$$R_p = pR_F + (1-p)R_G. \tag{12}$$

Taking into account that the trace preservation constraint yields $\mathrm{Tr}[\chi_0] = d$, where $d = \dim \mathcal{H}$ is the dimension of the Hilbert space, we have that $\mathcal{F}$ is upper bounded by the maximum eigenvalue $r_{p,\max}$ of R_p, $\mathcal{F} \leqslant d r_{p,\max}$. If we find an operator χ_0 that saturates this bound and satisfies the trace-preservation constraint (4), then the covariant machine (7) generated from χ_0 is the optimal one that achieves optimal trade-off between F and G.

In what follows we shall use this general method to determine the optimal partial phase-covariant measurement on a single d-level system (qudit). The set of input states has the form (1). The underlying group representation $U(g)$ is a tensor product of representations of d-Abelian groups U(1) and $dg = (2\pi)^{-d} d\phi_1 \cdots d\phi_d$. The state $|\psi(0)\rangle \equiv |+\rangle$, where $|+\rangle = (1/\sqrt{d})\Sigma_{j=1}^d |j\rangle$.

The operators R_F and R_G can be easily evaluated by integration over the d phases ϕ_j, and after some manipulations we arrive at

$$R_F = \frac{1}{d^2}\left[\mathbb{1} + d|\Phi^+\rangle\langle\Phi^+| - \sum_{j=1}^{d} |jj\rangle\langle jj|\right],$$

$$R_G = \frac{1}{d^2}\left[\left(1-\frac{1}{d}\right)\mathbb{1} + |+\rangle\langle+| \otimes \mathbb{1}_{\text{out}}\right]. \tag{13}$$

Here $|\Phi^+\rangle = (1/\sqrt{d})\Sigma_{j=1}^{d}|jj\rangle$ is the maximally entangled state of two qudits and $\mathbb{1}$ is the identity operator on the total Hilbert space $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}}$.

In order to determine the optimal χ_0 we have to investigate the eigenvalues and eigenstates of the operator

$$R_p = \frac{1}{d^2}\left[\left(1-\frac{1-p}{d}\right)\mathbb{1} + Y\right], \tag{14}$$

where

$$Y = pd|\Phi^+\rangle\langle\Phi^+| - p\sum_{j=1}^{d}|jj\rangle\langle jj| + (1-p)|+\rangle\langle+| \otimes \mathbb{1}_{\text{out}}. \tag{15}$$

It is only necessary to determine the eigenvalues μ_j and eigenstates $|\mu_j\rangle$ of the operator Y, and the eigenvalues λ_j of R_p are then given by $\lambda_j = [1-(1-p)/d + \mu_j]/d^2$. It turns out that Y possesses only four different nonzero eigenvalues, and they can be all expressed analytically. The eigenvalues

$$\mu_{1,2} = \frac{1}{2}[1 + p(d-2) \pm \sqrt{(1-pd)^2 + 4p(1-p)(d-1)/d}] \tag{16}$$

are nondegenerate and the corresponding eigenstates are

$$|\mu_{1,2}\rangle = \alpha|\Phi^+\rangle + \beta|+\rangle|+\rangle, \tag{17}$$

with properly chosen α and β. Note that

$$\mu_1 \geqslant \frac{1}{2}[1 + p(d-2) + |1-pd|] \geqslant 1-p. \tag{18}$$

The other two nonzero eigenvalues are $(d-1)$-fold degenerate,

$$\mu_{3,4} = \frac{1}{2}[1 - 2p \pm \sqrt{1-4p(1-p)/d}]. \tag{19}$$

The $(d-1)$-dimensional subspace of the eigenstates with eigenvalue $\mu_3(\mu_4)$ is spanned by the states

$$\alpha'\left[|jj\rangle - \frac{1}{\sqrt{d}}|\Phi^+\rangle\right] + \beta'\left[|+\rangle|j\rangle - \frac{1}{\sqrt{d}}|+\rangle|+\rangle\right]. \tag{20}$$

It follows from Eq. (19) that

$$\mu_3 \leqslant \frac{1-2p+1}{2} = 1-p. \tag{21}$$

Hence, the eigenvalue μ_1 is the largest one and the corresponding eigenstate is given by Eq. (17) with both α and β non-negative. If we choose χ_0 to be proportional to this eigenstate, then the machine will be optimal. The normalization can be determined from the trace-preservation condition, and we find that $\chi_0 = |\chi_0\rangle\langle\chi_0|$, where

$$|\chi_0\rangle = da|+\rangle|+\rangle + \sqrt{d}(b-a)|\Phi^+\rangle, \tag{22}$$

where the coefficients $b \geqslant a \geqslant 0$ satisfy

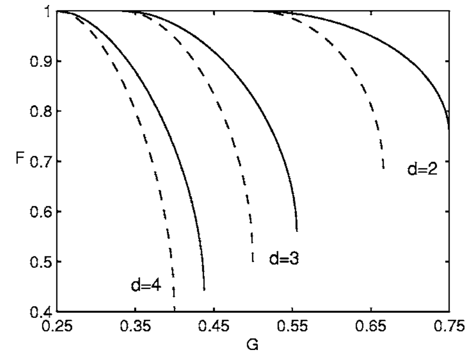

FIG. 1. Optimal trade-off between the fidelities F and G for a partially known state (1) (solid curve) and a completely unknown state (dashed curve).

$$(d-1)a^2 + b^2 = 1, \tag{23}$$

which can be derived from the condition $\text{Tr}[\chi_0] = d$. It can be easily verified that $\chi_{\text{cov}}(\phi)$ satisfies the trace-preservation condition (4), so it represents the optimal phase-covariant partial measuring device. The optimal map (22) is a coherent superposition of two extremal transformations: the term $|\Phi^+\rangle$ represents the identity operation, where the initial state is perfectly preserved and the measurement result is fully random, while the term $|+\rangle|+\rangle$ can be interpreted as the optimal phase-covariant estimation on a single qudit, and the output state coincides with the estimated state.

On inserting the explicit form of χ_0 into Eq. (11) we get the mean fidelities F and G expressed in terms of a and b,

$$F = \frac{1}{d} + b^2\left(1-\frac{1}{d}\right), \quad G = \frac{d-1}{d^2} + \frac{1}{d^2}[a(d-1)+b]^2. \tag{24}$$

If we combine the formula for F with the normalization condition (23), we can express a and b in terms of F. Upon inserting this into the formula for G we finally obtain the sought optimal trade-off (2) between F and G.

Equation (2) describes the optimal trade-off between the mean fidelity G of estimation of an unknown state (1) and the mean fidelity F of the state after the estimation. Squaring this equation two times one finds after some algebra that the bound is a fraction of an ellipse depicted for several values of d in Fig. 1. Figure 1 clearly reveals that the fidelity trade-off (2) indeed surpasses the fidelity trade-off for optimal partial estimation of a completely unknown pure state [1]:

$$\sqrt{F-\frac{1}{d+1}} = \sqrt{G-\frac{1}{d+1}} + \sqrt{(d-1)\left(\frac{2}{d+1}-G\right)}. \tag{25}$$

III. IMPLEMENTATION

The optimal partial estimation of the multiple phases can be easily performed using the QND-type measurement scheme depicted in Fig. 2. Initially, the qudit S is prepared in an unknown state (1) that can be expressed as

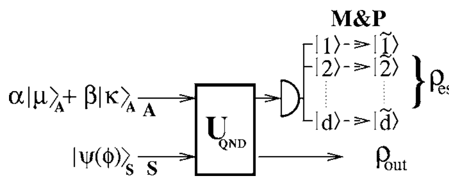

FIG. 2. The scheme of optimal partial estimation of multiple phases: $U_{\rm QND}$: quantum nondemolition coupling. M&P: measurement and preparation. See text for details.

$$|\psi(\phi)\rangle_S = \sum_{j=1}^{d} f_j|\tilde{j}\rangle_S, \tag{26}$$

where $f_j=(1/d)\Sigma_{k=1}^{d}\omega^{*jk}e^{i\phi_k}$ are inverse Fourier images of the original complex amplitudes $e^{i\phi_j}/\sqrt{d}$ and $\{|\tilde{j}\rangle_S \equiv F|j\rangle_S\}_{j=1}^{d}$ is the basis obtained from the original basis $\{|j\rangle_S\}_{j=1}^{d}$ by the finite-dimensional Fourier transform [15]

$$F = \frac{1}{\sqrt{d}}\sum_{j,k=1}^{d}\omega^{jk}|j\rangle\langle k|, \tag{27}$$

where $\omega=\exp(i2\pi/d)$. Then, the optimal partial QND measurement of the basis states $\{|\tilde{j}\rangle_S\}_{j=1}^{d}$ is performed on this qudit. This measurement can be implemented by coupling the qudit S to a single properly prepared ancillary qudit A by the unitary coupling $\mathcal{U}_{\rm QND}$ and performing a suitable measurement on the ancilla [17]. The coupling $\mathcal{U}_{\rm QND}$ has the property that there is a normalized state of the ancilla $|\mu\rangle_A$ such that $\mathcal{U}_{\rm QND}|\tilde{j}\rangle_S|\mu\rangle_A=|\tilde{j}\rangle_S|j\rangle_A$, where $\{|j\rangle_A\}_{j=1}^{d}$ is an orthonormal basis in the state space of the ancilla. Further, we assume that there is another normalized state $|\kappa\rangle_A$ that "switches off" the coupling—i.e., $\mathcal{U}_{\rm QND}|\tilde{j}\rangle_S|\kappa\rangle_A =|\tilde{j}\rangle_S(1/\sqrt{d})\Sigma_{j=1}^{d}|j\rangle_A$. Optimal partial nondemolition measurement of the basis $\{|\tilde{j}\rangle_S\}_{j=1}^{d}$ is achieved if the ancilla is prepared in the coherent superposition $x|\mu\rangle_A+y|\kappa\rangle_A$ of the two states, where the amplitudes x and y are nonnegative real numbers satisfying the normalization condition

$$x^2+y^2+\frac{2xy}{\sqrt{d}}=1 \tag{28}$$

and the qudit A is measured in the basis $\{|j\rangle_A\}_{j=1}^{d}$ after the coupling. If the ancilla is found in the state $|r\rangle_A$, we prepare the state $|\tilde{r}\rangle$ (see Fig. 2). Note that for $y=0$ the proposed measurement scheme satisfies the criteria for ideal QND measurement formulated in [16]. The transformation $\mathcal{U}_{\rm QND}$ can be, for instance, realized by the standard controlled-NOT (CNOT) gate and its d-dimensional generalization [17] $U_{\rm CNOT}|\tilde{i}\rangle_S|\tilde{j}\rangle_A=|\tilde{i}\rangle_S|\tilde{i}\oplus\tilde{j}\rangle_A$, where $\oplus$ denotes addition modulo d [18]. The CNOT gate was already realized experimentally with trapped ions [19] as well as with photons [20].

In order to calculate the fidelities F and G it is convenient to describe the optimal partial QND measurement by the set of operators [1]

$$A_r = x|\tilde{r}\rangle_S\langle\tilde{r}| + \frac{y}{\sqrt{d}}\mathbb{1}_S, \quad r=1,2,\ldots,d. \tag{29}$$

Then, the probability of the measurement of the state $|r\rangle_A$ can be calculated as $p_r={}_S\langle\psi(\phi)|A_r^{\dagger}A_r|\psi(\phi)\rangle_S=(1-y^2)|f_r|^2+y^2/d$. After many runs of the protocol with the same input state we prepare the estimated state $\rho_{\rm est}=\Sigma_{r=1}^{d}p_r|\tilde{r}\rangle\langle\tilde{r}|$ for which we find using Eq. (26) the estimation fidelity

$$\gamma(\phi)=\langle\psi(\phi)|\rho_{\rm est}|\psi(\phi)\rangle=\frac{y^2}{d}+(1-y^2)\sum_{i=1}^{d}|f_i|^4. \tag{30}$$

On the other hand, if the state $|r\rangle_A$ is detected on the ancilla, the state (26) transforms as

$$|\psi(\phi)\rangle_S \to A_r|\psi(\phi)\rangle_S = xf_r|\tilde{r}\rangle_S+\frac{y}{\sqrt{d}}|\psi(\phi)\rangle_S. \tag{31}$$

After repeating our protocol many times with the same input state we obtain at the output the state $\rho_{\rm out} =\Sigma_{r=1}^{d}A_r|\psi(\phi)\rangle_S\langle\psi(\phi)|A_r^{\dagger}$ for which we arrive using Eqs. (26) and (31) at the output fidelity

$$\varphi(\phi)=\langle\psi(\phi)|\rho_{\rm out}|\psi(\phi)\rangle=(1-x^2)+x^2\sum_{i=1}^{d}|f_i|^4. \tag{32}$$

In order to calculate the mean fidelities G and F it remains to integrate the fidelities (30) and (32) over d phases ϕ_j. Expressing the complex amplitudes f_i in Eqs. (30) and (32) in terms of the original complex amplitudes $e^{i\phi_j}/\sqrt{d}$ and performing the integration we finally arrive after some algebra at the following formulas for the mean fidelities F and G:

$$G=\frac{2d-1}{d^2}-\frac{d-1}{d^2}y^2, \quad F=1-\left(\frac{d-1}{d}\right)^2x^2. \tag{33}$$

Substituting these fidelities into Eq. (2) and using the normalization condition (28) we find that the equation is satisfied and therefore the proposed scheme is optimal. In order for the scheme in Fig. 2 to be covariant—i.e., to produce the fidelities $\gamma(\phi)$ and $\varphi(\phi)$ independent of ϕ—one has to implement the twirling operations $U(\phi')$ (ϕ' is chosen randomly with uniform probability distribution) and $U^{-1}(\phi')$ on the qudit S before and after the QND coupling and one has to prepare the state $U^{-1}(\phi')|\tilde{r}\rangle$ if the detected state was $|r\rangle_A$.

The optimal partial estimation can be implemented even with a weak QND coupling $\mathcal{U}$ that encodes the information on the input state into nonorthogonal states of the ancilla—i.e., $\mathcal{U}|\tilde{j}\rangle_S|\mu\rangle_A=|\tilde{j}\rangle_S|\mu_j\rangle_A$, where generally ${}_A\langle\mu_i|\mu_j\rangle_A\neq 0$ for $i\neq j$ and ${}_A\langle\mu_i|\mu_i\rangle_A=1$ for $i=1,\ldots,d$. The coupling transforms the input state $|\psi(\phi)\rangle_S|\mu\rangle_A$ into the state

$$\mathcal{U}|\psi(\phi)\rangle_S|\mu\rangle_A=\sum_{j=1}^{d}f_j|\tilde{j}\rangle_S|\mu_j\rangle_A. \tag{34}$$

After the coupling, we perform the measurement $\{\Pi_i\}_{i=1}^{d}$ on the ancilla which minimizes the error rate of the discrimination among the states $\{|\mu_i\rangle_A\}_{i=1}^{d}$ [21]. As the *a priori* probabilities of these states are not known (the complex amplitudes f_j are unknown) the best strategy is to treat the states as all having equal *a priori* probabilities. If the outcome Π_r is detected, we prepare the state $|\tilde{r}\rangle$. After being repeated many times the described scheme produces the estimated state $\rho_{\text{est}}=\sum_{r=1}^{d} p_r|\tilde{r}\rangle\langle\tilde{r}|$, where $p_r=\sum_{j=1}^{d}|f_j|^2{}_A\langle\mu_j|\Pi_r|\mu_j\rangle_A$ is the probability of detecting the outcome Π_r. Calculating now the fidelity $\gamma(\phi)=\langle\psi(\phi)|\rho_{\text{est}}|\psi(\phi)\rangle$ and integrating it over all d phases ϕ_j we successively arrive at the mean estimation fidelity of the form

$$G=\frac{2d-1}{d^2}-\frac{P_e}{d}, \tag{35}$$

where $P_e=1-(1/d)\sum_{r=1}^{d}{}_A\langle\mu_r|\Pi_r|\mu_r\rangle_A$ is the error rate. At the output of the coupling the qudit S is in the state $\rho_{\text{out}}=\sum_{i,j=1}^{d} f_i^* f_j|\tilde{j}\rangle_S\langle\tilde{i}|_A\langle\mu_i|\mu_j\rangle_A$. Calculating the output fidelity $\varphi(\phi)=\langle\psi(\phi)|\rho_{\text{out}}|\psi(\phi)\rangle$ and integrating it over all d phases ϕ_j one finds that the mean output fidelity is upper bounded as follows:

$$F\leqslant\frac{2d-1}{d^2}+\frac{d-1}{d^3}\sum_{i\neq j=1}^{d}|{}_A\langle\mu_i|\mu_j\rangle_A|. \tag{36}$$

The inequality is saturated if the scalar products $\langle\mu_i|\mu_j\rangle$, $i\neq j$ are non-negative real numbers. In the case of qubits ($d=2$) this condition can be satisfied for any coupling $\mathcal{U}$ by transforming the qubit S after the coupling by phase shift $|\tilde{1}\rangle_S\rightarrow|\tilde{1}\rangle_S$ and $|\tilde{2}\rangle_S\rightarrow\exp(-i\arg\langle\mu_1|\mu_2\rangle)|\tilde{2}\rangle_S$.

Equation (35) reveals that if the coupling $\mathcal{U}$ is such that the states $\{|\mu_i\rangle_A\}_{i=1}^{d}$ of the ancilla are nonorthogonal, the proposed scheme does not allow one to achieve maximum possible estimation fidelity for the state (1) $G_{\max}=(2d-1)/d^2$ [6]. This is because the error rate is always greater than zero in this case—i.e., $P_e>0$—and therefore the estimation fidelity (35) will be always less than $G_{\max}$. Interestingly, however, one can show at least for equatorial qubits ($d=2$) that the considered measurement scheme can be made still optimal in the sense of the trade-off (2). This happens if the discrimination measurement on the ancilla is such that the probability of error P_e is minimum equal to $P_{e,\min}=(1-\sqrt{1-|\langle\mu_1|\mu_2\rangle|^2})/2$ [21]. (In this formula and in what follows we drop the subscript A in states $\{|\mu_i\rangle\}_{i=1}^{d}$.) By using the latter formula and Eqs. (35) and (36) one obtains the output fidelity and the estimation fidelity in the form

$$F_2=\frac{3+|\langle\mu_1|\mu_2\rangle|}{4},\quad G_2=\frac{2+\sqrt{1-|\langle\mu_1|\mu_2\rangle|^2}}{4}. \tag{37}$$

Substituting finally the fidelities back into Eq. (2) for $d=2$ one finds that the equality is satisfied and therefore the considered measurement is indeed optimal. Equation (37) demonstrates that the smaller the overlap $\mathcal{O}=|\langle\mu_1|\mu_2\rangle|^2$ is, the larger the fidelity G_2 is, the optimum $G_{\max,2}=3/4$ being achieved for the case of orthogonal states $\{|\mu_i\rangle\}_{i=1}^{2}$. However, the optimal estimation fidelity $G_{\max,2}=3/4$ can be achieved probabilistically even with the weak coupling $\mathcal{U}$ for which $0<\mathcal{O}<1$. The way to achieve this is via replacing the previous discrimination measurement by the optimal unambiguous discrimination measurement [22] of the states of ancilla $\{|\mu_i\rangle\}_{i=1}^{2}$ similarly as in [17]. The optimal unambiguous discrimination measurement allows one to discriminate these states perfectly as soon as they are linearly independent—i.e., $\mathcal{O}<1$. The price to pay for this is that in the best case these states are discriminated perfectly only with the probability $\mathcal{P}_{\max}=1-|\langle\mu_1|\mu_2\rangle|$. Obviously, on the subensemble corresponding to successful discrimination the estimated state is $\rho_{\text{est,succ}}=\sum_{i=1}^{2}|f_i|^2|\tilde{i}\rangle\langle\tilde{i}|$ for which the mean estimation fidelity achieves the maximum possible value $G_2=G_{\max,2}=3/4$. On the same subensemble, the output state is the same mixed state whence also $F_2=3/4$. The obtained result thus clearly illustrates that it is possible to estimate an equatorial qubit with the highest possible estimation fidelity even using a weak QND interaction $\mathcal{U}$ which encodes the information on the input state into the nonorthogonal states of ancilla.

IV. CONCLUSIONS

In this paper we have derived analytically the optimal trade-off between the mean estimation fidelity and the mean output fidelity for the set of states (1). Further, we have proposed a scheme realizing such optimal partial estimation of these states. The scheme is based on the quantum nondemolition coupling fed by a properly prepared ancilla. For qubits the scheme can be implemented using the controlled-NOT gate recently demonstrated experimentally by several groups [19,20] and for qudits it can be realized using the d-dimensional generalization of this gate. Finally, we have also shown that optimal partial estimation of the considered states can be performed even with weak QND coupling that encodes the information on the input state into the nonorthogonal states of the ancilla.

ACKNOWLEDGMENTS

The research has been supported by the research project "Measurement and Information in Optics," No. MSM 6198959213 and by the EU under project SECOQC (IST-2002-506813). We also acknowledge partial support by the Czech Ministry of Education under Project No. OCP11.003 in the framework of EU Grant No. COST P11. R.F. acknowledges support by Project No. 202/03/D239 of the Grant Agency of the Czech Republic.

[1] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).
[2] K. Banaszek and I. Devetak, Phys. Rev. A **64**, 052307 (2001).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984*, (IEEE, New York, 1984), pp. 175–179.
[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000); D. Bruß and C. Macchiavello, J. Phys. A **34**, 6815 (2001); G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001); H. Fan, K. Matsumoto, X.-B. Wang, and M. Wadati, *ibid.* **65**, 012304 (2001); G. M. D'Ariano and C. Macchiavello, *ibid.* **67**, 042306 (2003); J. Fiurášek, *ibid.* **67**, 052314 (2003); J. Du, T. Durt, P. Zou, H. Li, L. C. Kwek, C. H. Lai, C. H. Oh, and A. Ekert, Phys. Rev. Lett. **94**, 040505 (2005).
[6] C. Macchiavello, Phys. Rev. A **67**, 062302 (2003).
[7] P. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).
[8] H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. **33**, 586 (1997).
[9] G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, Phys. Lett. A **248**, 103 (1998).
[10] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995); D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 149 (1999); A. Acín, J. I. Latorre, and P. Pascual, Phys. Rev. A **61**, 022113 (2000).
[11] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[12] M. Hillery, M. Ziman, and V. Bužek, Phys. Rev. A **66**, 042302 (2002).
[13] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
[14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[15] L. Ip, e-print quant-ph/0205034.
[16] L. Mišta, Jr. and R. Filip, e-print quant-ph/0501031; M. G. Genoni and M. G. A. Paris, Phys. Rev. A **71**, 052307 (2005).
[17] P. Grangier, J. A. Levenson, and J.-P. Poizat, Nature (London) **396**, 537 (1998).
[18] G. Alber, A. Delgado, N. Gisin, and I. Jex, e-print quant-ph/0102035.
[19] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995); F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt, Nature (London) **422**, 408 (2003); D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenković, C. Langer, T. Rosenband, and D. J. Wineland, *ibid.* **422**, 412 (2003).
[20] K. Sanaka, K. Kawahara, and T. Kuga, Phys. Rev. A **66**, 040301(R) (2002); J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature (London) **426**, 264 (2003); T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **68**, 032316 (2003); G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph, Phys. Rev. Lett. **92**, 190402 (2004). S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, *ibid.* **93**, 020504 (2004); Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan, *ibid.* **94**, 030501 (2005).
[21] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[22] I. D. Ivanovich, Phys. Lett. A **123**, 257 (1987); D. Dieks, *ibid.* **126**, 303 (1988); A. Peres, *ibid.* **128**, 19 (1988).