INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF OPTICS B: QUANTUM AND SEMICLASSICAL OPTICS
J. Opt. B: Quantum Semiclass. Opt. **4** (2002) S273–S276 PII: S1464-4266(02)37848-0

Improved discrimination of unitary transformations by entangled probes

G Mauro D'Ariano, Paoloplacido Lo Presti and Matteo G A Paris[1]

Quantum Optics and Information Group, Istituto Nazionale per la Fisica della Materia, Università di Pavia, via Bassi 6, I-27100 Pavia, Italy

E-mail: paris@unipv.it

Received 10 December 2001
Published 29 July 2002
Online at stacks.iop.org/JOptB/4/S273

Abstract
We consider the problem of discriminating among a set of unitary transformations by means of measurements performed on the state undergoing the transformation. We show that the use of entangled probes improves the discrimination in the following two cases: (i) for a set of unitaries that are the unitary irreducible representation of a group; and (ii) for any pair of transformations provided that multiple uses of the channel are allowed.

Keywords: Entanglement, high-precision measurements, quantum hypothesis testing

1. Introduction

Entanglement is perhaps the most distinctive ingredient of quantum mechanics. In recent years it has been recognized that entanglement can be seen as a resource for improving the processing of quantum information and increasing the speed of computation. In this paper, we address the use of entanglement as a resource for improving quantum measurements. In particular, we will deal with measurements that correspond to the estimation of the parameter θ labelling a unitary transformation U_θ which acts on a system described by the Hilbert space $\mathcal{H}$. Usually, the problem is addressed by fixing an input state $|\psi\rangle \in \mathcal{H}$ that undergoes one of the U_θ-transformations (figure 1), and then applying quantum estimation theory [2] to look for the POVM which is able to distinguish the possible output states $U_\theta|\psi\rangle$ with the minimum error probability P_E. In general, this error probability, or any other chosen figure of merit, will be a function of the input state $|\psi\rangle$, and one further optimizes on $|\psi\rangle$.

Here, we will consider the possibilities offered by the use of a bipartite input state $|E\rangle\!\rangle \in \mathcal{H} \otimes \mathcal{H}$ instead of the simpler local state $|\psi\rangle$. The transformation U_θ will act locally on $|E\rangle\!\rangle$, thus giving as output the state $|\Psi_\theta\rangle\!\rangle = U_\theta \otimes I|E\rangle\!\rangle$, as depicted in figure 1. We will show that such a novel configuration can do better than local measurements in discriminating the unitaries.

[1] www.qubit.it

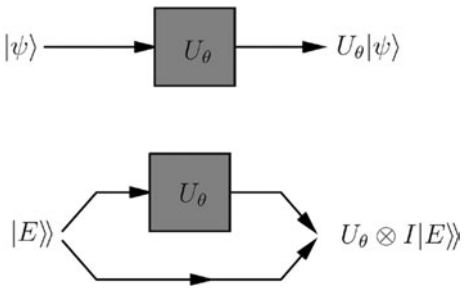

Figure 1. The parameter θ is estimated as the result of a unitary transformation $|\psi\rangle \to U_\theta|\psi\rangle$ (upper figure). In this scenario the use of a possibly entangled input $|E\rangle\!\rangle$ in place of $|\psi\rangle$ is considered, with the unknown transformation U_θ acting locally on one Hilbert space only (lower figure).

In section 2 we focus our attention on the discrimination of unitary transformations drawn from a unitary irreducible representation (UIR) of a group, whereas in section 3 we will treat the problem of distinguishing between two given unitaries. Section 4 closes the paper with some concluding remarks.

2. Discrimination amongst a set of unitary transformations (UIR)

As a first example, consider the problem of discriminating among the four unitary transformations given by the Pauli

matrices $\{\sigma_i\}$ acting on a qubit. By applying these unitaries to any local pure state $|\psi\rangle$, one gets the four non-orthogonal states $\sigma_j|\psi\rangle$, whereas for a maximally entangled input state, one finds four maximally entangled states which are orthogonal, and thus exactly distinguishable, at least in principle. In fact, by adopting the notation $|E\rangle\!\rangle \doteq \sum_{ij} E_{ij}|i\rangle|j\rangle$ that puts vectors $|E\rangle\!\rangle \in \mathcal{H}\otimes\mathcal{H}$ into correspondence with operators E on $\mathcal{H}$, a generic maximally entangled input state can be written as $\frac{1}{\sqrt{d}}|U\rangle\!\rangle$, with U unitary. Thus, in the Pauli example the possible outputs are $\frac{1}{\sqrt{2}}|\sigma_i U\rangle\!\rangle$, and they are orthogonal, since $\langle\!\langle\sigma_i U|\sigma_j U\rangle\!\rangle = \mathrm{Tr}[U^\dagger\sigma_i^\dagger\sigma_j U] = \delta_{ij}$. We notice that, basically, the same kind of configuration has been used for quantum dense coding. The generalization to a d-dimensional system corresponds to the problem of discriminating the d^2 unitary transformations

$$U(m,n) = \sum_{k=0}^{d-1} \mathrm{e}^{2\pi \mathrm{i} km/d}|k\rangle\langle k\oplus n|,$$

with n and m ranging from 0 to $d-1$, and $\oplus$ denoting addition modulo d. Again, if the input is maximally entangled, we have orthogonal output states.

Now, suppose we have a set of unitary transformations $\{U_g\}$, $g\in\boldsymbol{G}$, that form a (projective) representation of the group $\boldsymbol{G}$, i.e. $U_gU_h = \omega(g,h)U_{gh}$, where $\omega(g,h)$ is a phase factor satisfying the Jacobi associativity constraints, namely that $\omega(gh,l)\omega(g,h) = \omega(g,hl)\omega(h,l)$ and $\omega(g,g^{-1}) = \omega(g,e) = 1$, for $g,h,l\in\boldsymbol{G}$, e being the identity element. We will consider the case in which such a representation is irreducible (UIR), i.e. there are no subspaces of $\mathcal{H}$ invariant under the action of all the U_g. This was also the case of the preceding example, with $\{U(m,n)\}$ a UIR of the group $\mathbb{Z}_d\times\mathbb{Z}_d$. Given a UIR, from Schur's lemma it follows that for each operator O on $\mathcal{H}$, one has

$$[U_g O U_g^\dagger]_G = \mathrm{Tr}[O]I, \tag{1}$$

where $[f(g)]_G$ denotes the group averaging $[f(g)]_G \doteq \sum_{g\in G}\mu(g)f(g)$, with $\mu(g) = \frac{d}{|G|}$, $d = \dim(\mathcal{H})$, and $|\boldsymbol{G}|$ the cardinality of $\boldsymbol{G}$. Equation (1) can be generalized to the continuous case by defining group averaging as $[f(g)]_G \doteq \int_G \mu(\mathrm{d}g)\, f(g)$, $\mu(\mathrm{d}g)$ being a properly normalized invariant measure on the group $\boldsymbol{G}$.

In order to show that entanglement is of help in improving the discrimination, and to quantify this improvement, we now consider several state-related parameters. First of all, as in the first two examples, one can see that the dimension of the Hilbert space $\mathcal{H}_{out}$ spanned by the output states is larger for an entangled input than for factorized states. In fact, $\dim(\mathcal{H}_{out})$ can be calculated as the rank of the operator

$$O = [|\Psi_g\rangle\!\rangle\langle\!\langle\Psi_g|]_G = [U_g\otimes I|E\rangle\!\rangle\langle\!\langle E|U_g^\dagger\otimes I]_G, \tag{2}$$

where $\Psi_g = U_gE$. By means of equation (1), one has $O = I\otimes\mathrm{Tr}_1[|E\rangle\!\rangle\langle\!\langle E|] = I\otimes(E^\dagger E)^{\mathrm{T}}$, so

$$\dim(\mathcal{H}_{out}) = d\times\mathrm{rank}(E^\dagger E), \tag{3}$$

i.e. the output space is enlarged by a factor equal to the Schmidt number [1] of the input state. Indeed, since probing the operation with a bipartite entangled system gives access to a larger Hilbert space, we have, literally, more room for improvement. In the following, we refine these concepts, and give conditions under which an entangled scheme is convenient.

The Schmidt number is only a coarse measure of the amount of entanglement stored in $|E\rangle\!\rangle$, and the dimension of the output space is only indirectly connected to the distinguishability of the outputs. A more refined goodness criterion is given by Holevo's information χ for the set of output states, all taken with the same probability $p(g) = 1/|\boldsymbol{G}|$ (or $p(\mathrm{d}g) = \mu(\mathrm{d}g)/\mu(\boldsymbol{G})$ in the continuous case); this quantity is an upper bound for the accessible information [1]. Denoting by $S(\rho) = -\mathrm{Tr}\,\rho\log\rho$ the von Neumann entropy of ρ, Holevo's information χ reads

$$\begin{aligned}\chi &= S\left(\frac{1}{\mu(\boldsymbol{G})}[|\Psi_g\rangle\!\rangle\langle\!\langle\Psi_g|]_G\right) - \frac{1}{\mu(\boldsymbol{G})}[S(|\Psi_g\rangle\!\rangle\langle\!\langle\Psi_g|)]_G\\ &= S\left(\frac{1}{\mu(\boldsymbol{G})}I\otimes E^{\mathrm{T}}E^*\right)\\ &= \frac{d}{\mu(\boldsymbol{G})}\log\mu(\boldsymbol{G}) + \frac{d}{\mu(\boldsymbol{G})}S(E^{\mathrm{T}}E^*),\end{aligned} \tag{4}$$

and thus the bound is increased by an amount proportional to the degree of entanglement[2] $S(E^{\mathrm{T}}E^*)$ of the input state $|E\rangle\!\rangle$ (recall that for discrete groups, $\mu(\boldsymbol{G}) = d$).

Facing the problem with a maximum-likelihood strategy, the optimal covariant POVM that discriminates among the $\{|\Psi_g\rangle\!\rangle\}$ takes the form [4]

$$\Pi_g = \mu(g)(U_g\otimes I)P(U_g^\dagger\otimes I), \tag{5}$$

with $P\geqslant 0$ a positive operator on $\mathcal{H}\otimes\mathcal{H}$ normalized as $\mathrm{Tr}_1[P] = I$. By covariance, the likelihood—i.e. the probability of getting an outcome g when the state is $|\Psi_g\rangle\!\rangle$—is proportional to $\langle\!\langle E|P|E\rangle\!\rangle \leqslant d$, where the bound comes from the normalization condition on P, which limits the largest possible eigenvalue of P to being below d. Again, optimality (saturation of the bound) is reached for a maximally entangled input state, i.e. for $E = d^{-\frac{1}{2}}U$, with U unitary, and $P = |U\rangle\!\rangle\langle\!\langle U|$. The optimality of a maximally entangled input state for the estimation of unitaries in $SU(d)$ has also been noted in [6].

Since the overlap of two states is the only parameter that determines their distinguishability, we will consider the average overlap $\Omega(E)$ of all the couples of states in $\{|\Psi_g\rangle\!\rangle\}$: the lower $\Omega(E)$, the better the overall distinguishability. One has

$$\begin{aligned}\Omega(E) &= \frac{1}{2\mu(\boldsymbol{G})^2}[|\langle\!\langle\Psi_g|\Psi_{g'}\rangle\!\rangle|^2]_{G\times G}\\ &= \frac{1}{2\mu(\boldsymbol{G})}[\langle\!\langle E|\Psi_g\rangle\!\rangle\langle\!\langle\Psi_g|E\rangle\!\rangle]_G\\ &= \frac{1}{2\mu(\boldsymbol{G})}\langle\!\langle E|I\otimes(E^{\mathrm{T}}E^*)|E\rangle\!\rangle\\ &= \frac{1}{2\mu(\boldsymbol{G})}\langle\!\langle E|EE^\dagger E\rangle\!\rangle\\ &= \frac{1}{2\mu(\boldsymbol{G})}\mathrm{Tr}[(E^\dagger E)^2].\end{aligned} \tag{6}$$

In order to analyse the properties of $\Omega(E)$, we have to briefly recall the definition of the 'majorization' relation between

[2] $S(E^{\mathrm{T}}E^*)$ represents the entropy of the partial traces of $|E\rangle\!\rangle$, which is indeed a measure of entanglement for pure states.

entangled pure states and its physical meaning. Given two states $|A\rangle\!\rangle$ and $|B\rangle\!\rangle$ in $\mathcal{H}\otimes\mathcal{H}$, let $\boldsymbol{\lambda}_A^{\downarrow}$ and $\boldsymbol{\lambda}_B^{\downarrow}$ be the vectors of eigenvalues of $A^\dagger A$ and $B^\dagger B$ respectively, sorted in descending order. We say that $|A\rangle\!\rangle \prec |B\rangle\!\rangle$ iff

$$\sum_{j=1}^{k}(\boldsymbol{\lambda}_A^{\downarrow})_j \leqslant \sum_{j=1}^{k}(\boldsymbol{\lambda}_B^{\downarrow})_j \qquad \text{for each } k \leqslant d. \tag{7}$$

The physical meaning of this partial ordering relation has been clarified in [5]: $|A\rangle\!\rangle$ can be transformed into $|B\rangle\!\rangle$ by local operations and classical communication if and only if $|A\rangle\!\rangle \prec |B\rangle\!\rangle$. Our average overlap $\Omega(E)$ is a so-called 'Schur convex function' of the eigenvalues of $E^\dagger E$; that is, if $|A\rangle\!\rangle \prec |B\rangle\!\rangle$, then $\Omega(A) \leqslant \Omega(B)$. Since any maximally entangled state is majorized by any other state, it is clear that the minimum overlap is found in correspondence with $|E\rangle\!\rangle$ maximally entangled, and any manipulation of such a state can only increase $\Omega(E)$, thus reducing the distinguishability, and, as a consequence, the sensitivity of the measurement.

3. Discrimination between two unitary transformations

Let us suppose that we have to distinguish among two unitaries U_1 and U_2. Given an input state $|\psi\rangle$, one optimizes over the possible measurements, and the minimum error probability in discriminating $U_1|\psi\rangle$ and $U_1|\psi\rangle$ [2] is given by

$$P_E = \tfrac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right], \tag{8}$$

so one has to minimize the overlap $|\langle\psi|U_2^\dagger U_1|\psi\rangle|$ with a suitable choice of $|\psi\rangle$. Choosing as a basis the eigenvectors $\{|j\rangle\}$ of $U_2^\dagger U_1$, and writing $|\psi\rangle = \sum_j \psi_j|j\rangle$, we define

$$z_\psi \doteq \langle\psi|U_2^\dagger U_1|\psi\rangle = \sum_j |\psi_j|^2 \mathrm{e}^{\mathrm{i}\gamma_j}, \tag{9}$$

where $\mathrm{e}^{\mathrm{i}\gamma_j}$ are the eigenvalues of $U_2^\dagger U_1$. The normalization condition for $|\psi\rangle$ is $\sum_j |\psi_j|^2 = 1$, so the subset $K(U_2^\dagger U_1) \subset \mathbb{C}$ described by z_ψ for varying $|\psi\rangle$ is the convex polygon having the points $\mathrm{e}^{\mathrm{i}\gamma_j}$ as vertices. The minimum overlap

$$r(U_2^\dagger U_1) \doteq \min_{||\psi||=1} \left|\langle\psi|U_2^\dagger U_1|\psi\rangle\right| \tag{10}$$

is the distance of $K(U_2^\dagger U_1)$ from $z = 0$. This geometrical picture indicates in a simple way what is the best one can do in discriminating U_1 and U_2: if K contains the origin, then the two unitaries can be exactly discriminated; otherwise one has to find the point in K nearest to the origin, and the minimum probability of error is related to its distance from the origin. Once the optimal point in K is found, the optimal states ψ are those corresponding to that point through equation (9).

If $\Delta(U_2^\dagger U_1)$ is the angular spread of the eigenvalues of $U_2^\dagger U_1$ (referring to figure 2, it is $\Delta = \gamma_+ - \gamma_-$), from equation (8) for $\Delta < \pi$ one has

$$P_E = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \cos^4\frac{\Delta}{2}}, \tag{11}$$

whereas for $\Delta \geqslant \pi$ one has $P_E = 0$ and the discrimination is exact.

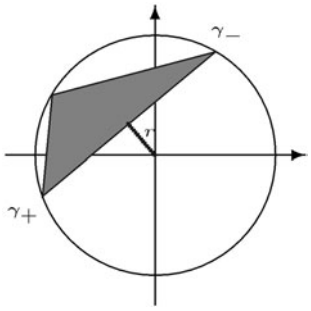

Figure 2. r is the minimum distance between the origin and the polygon K.

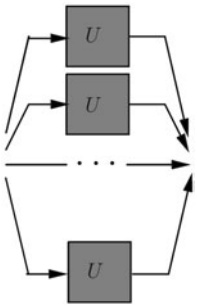

Figure 3. When distinguishing between two unitaries $U = U_{1,2}$, it is possible to achieve perfect discrimination even for non-orthogonal U_1 and U_2 for a sufficiently large number N of copies of the unitary transformation, using an N-part entangled state as in the figure (see the text).

Given U_1 and U_2 not exactly discriminatable, one is interested in understanding whether or not an entangled input state could be of some use. The answer is negative; in fact, using entanglement translates the problem into that of distinguishing between $U_1 \otimes I$ and $U_2 \otimes I$—thus one has to analyse the polygon $K(U_2^\dagger U_1 \otimes I)$. Since $U_2^\dagger U_1 \otimes I$ has the same eigenvalues as $U_2^\dagger U_1$, the polygons $K(U_2^\dagger U_1 \otimes I)$ and $K(U_2^\dagger U_1)$ are exactly the same, so they lead to the same minimum probability of error.

The situation changes dramatically if N copies of the unitary transformation are used, as depicted in figure 3: here one has to compare the 'performance' of $K(U_2^\dagger U_1)$ to that of $K((U_2^\dagger U_1)^{\otimes N})$. Since $\Delta((U_2^\dagger U_1)^{\otimes N}) = \min\{N \times \Delta(U_2^\dagger U_1), 2\pi\}$, it is clear that there will be an $\bar{N}$ such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ will be exactly discriminatable. This same result has been demonstrated in [12] starting from a different approach.

4. Conclusions

We have shown that the use of entangled states as a probe provides an effective scheme for discriminating among a set of unitary transformations. We have analysed the discrimination of a set of unitaries which are the UIR of a group, showing that entanglement is always useful. We have also considered discrimination between two generic transformations, where it is possible to achieve perfect discrimination even for non-orthogonal U_1 and U_2 for a sufficiently large number N of copies of the unitary transformation, if an N-part entangled state is available. The present results for the discrimination of a *discrete* set of unitaries can be generalized to the continuous

case [13], i.e. to the estimation of parameters. In this case, entanglement improves the performance of the measurement scheme also in the presence of losses.

Acknowledgments

This work has been supported by EC through the project ATESIT (contract IST-2000-29681) and by INFM through the project PRA-2002-CLON.

References

[1] Chuang I L and Nielsen M A 2000 *Quantum Information and Quantum Computation* (Cambridge: Cambridge University Press)
[2] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
[3] Shapiro J H and Shepard S R 1991 *Phys. Rev.* A **43** 3795
[4] Holevo A S 1982 *Probabilistic and Statistical Aspects of Quantum Theory* (Amsterdam: North-Holland)
[5] Nielsen M A 1999 *Phys. Rev. Lett.* **83** 436
[6] Acín A, Jané E and Vidal G 2001 *Phys. Rev.* A **64** 050302
[7] Arthurs E and Goodman M S 1988 *Phys. Rev. Lett.* **60** 2447
[8] Yuen H P and Shapiro J H 1980 *IEEE Trans. Inf. Theory* **26** 78
[9] Simon R 2000 *Phys. Rev. Lett.* **84** 2726
[10] Holevo A S and Werner R F 2001 *Phys. Rev* A **63** 032312
[11] Yuen H P, Kennedy R S and Lax M 1975 *IEEE Trans. Inf. Theory* **21** 125
[12] Acín A 2001 *Phys. Rev. Lett.* **87** 177901
[13] D'Ariano G M, Lo Presti P and Paris M G A 2001 *Phys. Rev. Lett.* **87** 270404