Estimation of unitary quantum operations

Manuel A. Ballester*
Department of Mathematics, University of Utrecht, Box 80010, 3508 TA Utrecht, The Netherlands

The problem of optimally estimating an unknown unitary quantum operation with the aid of entanglement is addressed. The idea is to prepare an entangled pair, apply the unknown unitary to one of the two parts, and then measure the joint output state. This measurement could be an entangled one or it could be separable (e.g., measurements which can be implemented with local operations and classical comunication or LOCC). A comparison is made between these possibilities and it is shown that by using nonseparable measurements one can improve the accuracy of the estimation by a factor of $2(d+1)/d$ where d is the dimension of the Hilbert space on which U acts.

PACS numbers: 03.67.-a

I. INTRODUCTION

Consider a one-qubit unitary gate, the following question arises: "how to characterize it?" This question is motivated by recent experiments in quantum optics [1]. A possible approach is to prepare many known states and use them as inputs, and then measure the outputs that they produce; this is known as *quantum process tomography* [2]. It turns out that one needs as inputs a basis of the Hilbert space plus some linear combinations thereof. The disadvantage of this approach is that, in many practical situations, such a set of states is not feasible in the laboratory [1].

Another strategy is described in Refs. [1, 3, 4]. It is enough to use a single bipartite entangled state; one of the states is used as input for the quantum operation and nothing is done to the other one, then the two qubits are measured, as shown in Fig. 1.

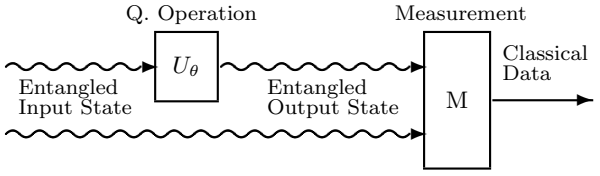

FIG. 1: The use of a single entangled input state suffices.

In Ref.[1] it is pointed out that in this setup there is a one to one correspondence between the quantum operation and the joint output state. A maximally entangled state is used as input and then the three components of the spin in both output particles are measured. One can ask whether it is possible to find a more accurate measurement. Also, is it possible to find a measurement that performs as well as the one in Ref. [1] which has less outcomes? It will turn out that the answer is that one can find a more accurate measurement but this measurement is nonseparable. It is also possible to find a measurement with less outcomes.

In Ref. [3] it is proven that a maximally entangled pure state is a good input state in the sense that if $|\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is maximally entangled, then

$$\forall\ \rho \text{ on } \mathbb{C}^2 \otimes \mathbb{C}^2,\ H_\rho(\theta) \leq H_{|\phi\rangle\langle\phi|}(\theta)$$

where $H_\rho(\theta_0)$ is the quantum Fisher information matrix (QFI) for the joint output state, at $\theta = \theta_0$, if the input state is ρ. This quantity is defined for example in Ref. [5] and explained in more detail in the following section. The inverse of this matrix is a lower bound (quantum Cramér-Rao bound or QCRB) for the mean-square error of estimators based on arbitrary measurements of the output state. A maximally entangled state is a good input also in the sense that the QCRB can be achieved if and only if the input state is maximally entangled. The problem here is that, as will be shown later, the measurement that achieves the bound is actually a basis of projectors onto maximally entangled states. This measurement can be performed using nonlinear optics but is far from being standard.

But perhaps the improvement in the estimation through the use of entangled measurements is not very large. Are entangled measurements worth the trouble? The main aim of this paper is to show that the answer to this question is positive. The value of entangled measurements will be quantified precisely.

Before continuing with this discussion it is necessary to explain what is meant with "better" and "best" and how the quality of different positive operator valued measures or POVMs is actually going to be quantified.

II. QFI, FISHER INFORMATION, AND QCRB

A. Quantum Fisher information

Suppose that the quantum state density matrix σ on $\mathbb{C}^d$ is parametrized by $\theta \in \Theta \subset \mathbb{R}^p$ where p is the number of parameters (less than or equal to d^2-1 for mixed states, $2d-2$ for pure states). In our case σ would be

*Electronic address: ballester@math.uu.nl ; URL: `http://www.math.uu.nl/people/balleste/`

the joint output state. Define the symmetric logarithmic derivatives $\lambda_1, \ldots, \lambda_p$ as the self-adjoint operators that satisfy

$$\sigma_{,i}(\theta) = \partial_{\theta_i}\sigma(\theta) = \tfrac{1}{2}[\sigma(\theta)\lambda_i(\theta) + \lambda_i(\theta)\sigma(\theta)].$$

For pure states, $\sigma = |\psi\rangle\langle\psi|$, they simply are $\lambda_i = 2\sigma_{,i}$. The QFI is defined as the $p \times p$ matrix with elements

$$H_{ij}(\theta) = \mathrm{Re}\ \ \mathrm{tr}\,[\sigma(\theta)\lambda_i(\theta)\lambda_j(\theta)]$$

which for pure states reduces to

$$H_{ij}(\theta) = \mathrm{Re}\langle l_i(\theta)|l_j(\theta)\rangle$$

where $|l_i(\theta)\rangle = \lambda_i(\theta)|\psi(\theta)\rangle$.

B. (Classical) Fisher information

Take a POVM with elements $M_1, \ldots, M_n$. The Fisher information matrix (FI) for this measurement is the $p \times p$ matrix with elements

$$I_{ij}(M,\theta) = \sum_{\xi=1}^{n} \frac{\mathrm{tr}[\sigma_{,i}(\theta)M_\xi]\,\mathrm{tr}[\sigma_{,j}(\theta)M_\xi]}{\mathrm{tr}[\rho(\theta)M_\xi]}.$$

For an estimator $\hat{\theta}$ and a measurement M, locally unbiased at θ_0 [1], the (classical) Cramér-Rao bound is satisfied

$$V(M,\theta_0,\hat{\theta}) \geq I(M,\theta_0)^{-1},$$

i.e., the FI is the smallest variance that a locally unbiased estimator based on this measurement can have. This also means that if one of the eigenvalues of I is zero, then the variance of the function of the parameters corresponding to that eigenvalue is infinity and therefore cannot be estimated.

If one has N copies of the quantum state and performs the same measurement on each of the copies then the FI of the N copies, I^N, satisfies $I^N(M,\theta) = NI(M,\theta)$ where $I(M,\theta)$ is the FI of one system. It follows that

$$V^N(M,\theta_0,\hat{\theta}) \geq I^N(M,\theta_0)^{-1} = I(M,\theta_0)^{-1}/N.$$

It is a well known fact in mathematical statistics that the maximum likelihood estimator (MLE) in the limit of large N is asymptotically unbiased and saturates the classical Cramér-Rao bound. Moreover no other reasonable estimator (unbiased or not) can do better.

[1] This means that the expectation of the estimator satisfies $\mathbb{E}_{M,\theta_0}(\hat{\theta}_i) = \theta_{0i}$ and $\partial_{\theta_j}\,\mathbb{E}_{M,\theta}(\hat{\theta}_i)\Big|_{\theta=\theta_0} = \delta_{ij}$.

C. QCRB

The QCRB states that for any measurement M

$$I(M,\theta) \leq H(\theta). \tag{1}$$

In other words, $H(\theta) - I(M,\theta)$ is a positive semidefinite matrix.

This bound is not achievable in general. A theorem due to Matsumoto [6] states that for pure states, the bound is achievable at $\theta = \theta_0$ if and only if

$$\mathrm{Im}\langle l_i(\theta_0)|l_j(\theta_0)\rangle = 0. \tag{2}$$

Furthermore, if condition (2) holds, there is a measurement with $p+2$ elements that achieves the bound.

In analogy with [7], measurements will be compared using the quantity

$$\mathrm{tr}\,H(\theta)^{-1}I(M,\theta)$$

which is always less than or equal to p, the number of parameters. For example, for the measurement used in [1], $\mathrm{tr}\,H^{-1}I = 1$.

One needs to use a quantity like this because of the extra complexity that quantum theory adds to the problem. Namely, in the most general case there is no POVM that achieves equality in (1). Typically, for any POVM M_1 which cannot be improved, one can find another POVM M_2 such that neither $I(M_1,\theta) \leq I(M_2,\theta)$ nor $I(M_1,\theta) \geq I(M_2,\theta)$ are satisfied. The bound (1) is sharp, i.e., $H(\theta)$ is the smallest matrix larger than $I(M,\theta)$ for every M. The difficulties can be overcome by using a single number (instead of a matrix) to quantify the performance of a POVM. This defines an achievable bound and any two POVMs can be compared according to this quantity. Of course, no single number can be an *absolute* quantification of the performance of a POVM. In applications one must decide what one wants to estimate and accordingly assign weights to the mean square error of the parameters to be estimated. This comes down to using a quantity such as $\mathrm{tr}\,G(\theta)I(M,\theta)$. One needs to maximize this quantity for a general[2] $G(\theta) \geq 0$ tailored to one's specific needs. In this paper the general problem is not solved. Only the case $G(\theta) = H(\theta)^{-1}$ is considered. There are several good reasons for this choice:

1. Since $H(\theta)$ is the smallest upper bound for all the $I(M,\theta)$, it defines a natural scale in which to compare them.

2. $\mathrm{tr}\,H(\theta)^{-1}I(M,\theta)$ is parametrization invariant.

[2] This quantity still has the property that if the inequality $\mathrm{tr}\,G(\theta)I(M_1,\theta) > \mathrm{tr}\,G(\theta)I(M_2,\theta)$ holds, then $I(M_1,\theta) \not< I(M_2,\theta)$.

3. $H(\theta)$ is closely related to the fidelity between true and estimated output states: the metric generated by $H(\theta)$ is locally identical (up to a factor of 4) to the Bures distance, $d_{\rm Bures}(\rho,\sigma)^2 = 2(1-\sqrt{\mathcal{F}(\rho,\sigma)})$, where $\mathcal{F}$ is he fidelity, which for pure states can be defined as $\mathcal{F}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|^2$.

4. Finally, the use of this quantity allows one to obtain simple and striking results.

III. THE CASE $d = 2$

A. Entangled measurements

In [3] it was shown that in this case the best input is any maximally entangled state. Here the singlet state $|\tau\rangle = [|10\rangle - |01\rangle]/\sqrt{2}$ will be used. The output is then $|\psi(\alpha,\theta,\phi)\rangle = [U(\alpha,\theta,\phi]\otimes \mathbb{1})|\tau\rangle$ where $U(\alpha,\theta,\phi) = \cos\alpha\, \mathbb{1} + {\rm i}\sin\alpha\, \vec{n}_{\theta\phi}\cdot\vec{\sigma}$ is a 2×2 unitary matrix, $\vec{n}_{\theta\phi}$ is the unit vector $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ parametrized by its polar coordinates, and $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli matrices.

It is quite straightforward to calculate that the QFI is

$$H(\alpha,\theta,\phi) = 4\begin{pmatrix} 1 & 0 & 0 \\ 0 & (\sin\alpha)^2 & 0 \\ 0 & 0 & (\sin\alpha\sin\theta)^2 \end{pmatrix}$$

and as expected ${\rm Im}\langle l_i(\alpha,\theta,\phi)|l_j(\alpha,\theta,\phi)\rangle = 0$. One can find a simple measurement that achieves the bound; in fact, any measurement of the type

$$\begin{aligned} &M_\alpha = |b_\alpha\rangle\langle b_\alpha| \quad \alpha = 1,\ldots,p+1, \\ &M_{p+2} = \mathbb{1} - \sum_{\alpha=1}^{m+1} M_\alpha, \\ &|b_\alpha\rangle = \sum_{\beta=1}^{p+1} o_{\alpha\beta}|m_\beta\rangle, \\ &|m_k\rangle = \sum_l (H^{-1/2})_{kl}|l_l\rangle, \quad |m_{p+1}\rangle = |\phi\rangle, \end{aligned} \tag{3}$$

with o a $(p+1)\times(p+1)$ real orthogonal matrix satisfying $o_{\alpha,p+1} \neq 0$ achieves the bound. For example measuring the Bell basis

$$\begin{aligned} M_1^{Bell} &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}\frac{\langle 00| - \langle 11|}{\sqrt{2}}, \\ M_2^{Bell} &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}}, \\ M_3^{Bell} &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}\frac{\langle 01| + \langle 10|}{\sqrt{2}}, \\ M_4^{Bell} &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}\frac{\langle 01| - \langle 10|}{\sqrt{2}} \end{aligned} \tag{4}$$

achieves $I(M^{Bell},\theta) = H(\theta)$ for all θ and therefore satisfies

$${\rm tr}\, H^{-1}(\theta) I(M^{Bell},\theta) = 3 \tag{5}$$

everywhere; this is three times the value achieved in [1]. This measurement, which has been implemented using non-linear optics [8], is not widely available in quantum optics labs. On the other hand, a POVM with the two components

$$\begin{aligned} M_1 &= M_k^{Bell}, \\ M_2 &= \mathbb{1} - M_k^{Bell} \end{aligned} \tag{6}$$

for $k = 1, 2, 3$ or 4 has been implemented with linear optics and is much more standard than measuring the whole basis. This is a POVM with only two outcomes (which might be an advantage for its practical implementation) and calculation shows that it satisfies ${\rm tr}\, H^{-1} I = 1$ everywhere, which is as good as the measurement in [1]. It will be shown in the next section that it is actually as good as any separable measurement (in terms of the value of ${\rm tr}\, H^{-1} I$). This measurement does have a serious drawback, namely that one can only identify one function of α, β and ϕ. The drawback can be overcome, for example, by measuring (6) for $k = 1, 2$ and 3 each in one third of the available copies. In this way one is able to identify all three parameters, ${\rm tr}\, H^{-1} I = 1$ is still satisfied, and finally this new POVM should not be harder to implement than the previous one. Again here everything depends on what one wants to estimate.

A measurement with three elements

$$\begin{aligned} M_1 &= M_k^{Bell}, \\ M_2 &= M_l^{Bell}, \\ M_3 &= \mathbb{1} - M_k^{Bell} - M_l^{Bell} \end{aligned} \tag{7}$$

for some $k \neq l$ has also been implemented with linear optics. In fact, it has been shown [9] that, with linear optics, this is the best one can do. This POVM satisfies ${\rm tr}\, H^{-1} I = 2$. This is twice the value that can be achieved with any separable measurement. Note that this measurement has the same weakness as the previous one: it cannot identify all three parameters (it identifies two functions of α, θ and ϕ). It is easily possible to overcome this difficulty in a similar way as before.

B. LOCC measurements

How well can one estimate U using only LOCC measurements: measurements that can be implemented locally and with the aid of classical communication between the two parties. In fact, to begin with, the larger class of *separable* measurements will be studied: measurements whose elements are positive combinations of products of one dimensional projectors. This definition of "separable" is a slight generalization of that of [10], where it was shown that there exist separable measurements which are not LOCC. Nonseparable measurements are called entangled.

Consider a separable POVM with elements $M_\xi = \sum_i c_{\xi i}(|\psi_{\xi i}^A\rangle \otimes |\psi_{\xi i}^B\rangle)(\langle\psi_{\xi i}^A| \otimes \langle\psi_{\xi i}^B|)$. One can *refine* this

POVM to obtain another POVM with elements that are proportional to one-dimensional projectors $M_{\xi i} = c_{\xi i}(|\psi^A_{\xi i}\rangle \otimes |\psi^B_{\xi i}\rangle)(\langle\psi^A_{\xi i}| \otimes \langle\psi^B_{\xi i}|)$. By relabeling $\xi\ i \to \xi$ one obtains

$$M_\xi = c_\xi(|\psi^A_\xi\rangle \otimes |\psi^B_\xi\rangle)(\langle\psi^A_\xi| \otimes \langle\psi^B_\xi|). \tag{8}$$

The Fisher information corresponding to this refined POVM is greater than or equal to the Fisher information of the original POVM. Thus, since one wants to maximize the FI, one may restrict oneself to measurements of the type described in Eq. (8).

For the calculations that follow it is more convenient to express Eq. (8) using the Pauli matrices

$$M_\xi = c_\xi \frac{\mathbb{1} + \vec{a}_\xi \cdot \vec{\sigma}}{2} \otimes \frac{\mathbb{1} + \vec{b}_\xi \cdot \vec{\sigma}}{2}$$

with $|\vec{a}_\xi| = |\vec{b}_\xi| = 1$ and $c_\xi > 0$. The condition $\sum_\xi M_\xi = \mathbb{1}$ can be rewritten as follows:

$$\begin{aligned} &\sum_\xi c_\xi = 4, \sum_\xi c_\xi \vec{a}_\xi = 0, \\ &\sum_\xi c_\xi \vec{b}_\xi = 0, \sum_\xi c_\xi a_{\xi k} b_{\xi l} = 0. \end{aligned} \tag{9}$$

Since

$$\frac{|10\rangle - |01\rangle}{\sqrt{2}} \frac{\langle 10| - \langle 01|}{\sqrt{2}} = \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1} - \sum_{i=1}^3 \sigma_i \otimes \sigma_i\right)$$

the density matrix of the system can be written as

$$\rho(\alpha,\theta,\phi) = \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1} - \sum_{i=1}^3 U(\alpha,\theta,\phi)\sigma_i U^\dagger(\alpha,\theta,\phi) \otimes \sigma_i\right).$$

The probabilities are then

$$p_\xi = \frac{c_\xi}{4}\left(1 - \sum_{i,j=1}^3 b_{\xi i} a_{\xi j} \frac{\operatorname{tr}(U\sigma_i U^\dagger \sigma_j)}{2}\right)$$

and $\frac{1}{2}\operatorname{tr}(U\sigma_i U^\dagger \sigma_j)$ can be calculated to be

$$\cos 2\alpha\ \delta_{ij} - \sin 2\alpha \sum_{k=1}^3 \epsilon_{ijk} n_k + 2\sin^2\alpha\ n_i n_j.$$

Substituting this into the expression for the probabilities one gets

$$\begin{aligned} p_\xi = \frac{c_\xi}{4}\Big(&1 - \cos 2\alpha\ (\vec{a}_\xi \cdot \vec{b}_\xi) + \sin 2\alpha\ (\vec{b}_\xi \times \vec{a}_\xi \cdot \vec{n}) \\ &-2\sin^2\alpha\ (\vec{n}\cdot\vec{a}_\xi)(\vec{n}\cdot\vec{b}_\xi)\Big). \end{aligned} \tag{10}$$

After some not very interesting manipulations one finds

$$\begin{aligned} &\frac{1}{p_\xi}\left(\frac{(p_{\xi,\alpha})^2}{4} + \frac{(p_{\xi,\theta})^2}{4\sin^2\alpha} + \frac{(p_{\xi,\phi})^2}{4\sin^2\alpha\ \sin^2\theta}\right) \\ &= \frac{c_\xi}{4}\Big(1 + \cos 2\alpha\ (\vec{a}_\xi \cdot \vec{b}_\xi) - \sin 2\alpha\ (\vec{b}_\xi \times \vec{a}_\xi \cdot \vec{n}) \\ &+2\sin^2\alpha\ (\vec{n}\cdot\vec{a}_\xi)(\vec{n}\cdot\vec{b}_\xi)\Big). \end{aligned} \tag{11}$$

Finally, using the conditions (9) one obtains that for separable measurements of the type (8)

$$\begin{aligned} &\operatorname{tr}[H^{-1}(\theta) I(M,\theta)] \\ &= \sum_\xi \frac{1}{p_\xi}\left(\frac{(p_{\xi,\alpha})^2}{4} + \frac{(p_{\xi,\theta})^2}{4\sin^2\alpha} + \frac{(p_{\xi,\phi})^2}{4\sin^2\alpha\ \sin^2\theta}\right) \\ &= 1. \end{aligned} \tag{12}$$

Any separable measurement can be refined to a measurement of the type (8). Therefore for all separable measurements M_{sep}

$$\operatorname{tr} H(\theta)^{-1} I(M_{\text{sep}},\theta) \le 1.$$

This bound therefore also holds for LOCC measurements. Since there are LOCC measurements of the type (8), the bound is achievable with LOCC measurements.

IV. THE CASE $d > 2$

A. Entangled Measurements

Before starting with any calculations it will be shown that the quantity that is being analyzed

$$f(\theta) = \sup_M \operatorname{tr} H^{-1}(\theta) I(\theta, M)$$

does not depend on θ.

For any θ_1 and θ_0 there exists a unitary matrix V such that $VU(\theta_0) = U(\theta_1)$. It is easy to see that for such a choice

$$\operatorname{tr} H^{-1}(\theta_1) I(\theta_1, (V\otimes\mathbb{1})M(V\otimes\mathbb{1})^\dagger) = \operatorname{tr} H^{-1}(\theta_0) I(\theta_0, M)$$

This implies that

$$\sup_{M_1} \operatorname{tr} H^{-1}(\theta_1) I(\theta_1, M_1) \ge \sup_{M_0} \operatorname{tr} H^{-1}(\theta_0) I(\theta_0, M_0).$$

Thus $f(\theta_1) \ge f(\theta_0)$, but since θ_0 and θ_1 are arbitrary, the function f must be constant. Therefore one can choose any value of the parameter to perform the calculations. One of the implications this has is that if one proves that the QCRB can (not) be achieved at one value of the parameter, then it can (not) be achieved everywhere (anywhere).

In [3] it is mentioned that in dimension $d > 2$, it is no longer true that a maximally entangled state maximizes the QFI; however it is still true that the QCRB is achieved if and only if the input state is maximally entangled. In order to prove the first statement it is enough to find a counter example. This is not difficult to do for example in $d = 3$. The second statement is also not difficult to prove and because of the last discussion it will be enough to do it for U equal to the identity.

A $SU(d)$ matrix can be written as $\exp\left(\mathrm{i}\sum_{\alpha=1}^{d^2-1}\theta_\alpha T_\alpha\right)$. Here $\theta \in \mathbb{R}^{d^2-1}$ and the T's are in the $su(d)$ Lie Algebra.

They are traceless self-adjoint matrices and are chosen so that they also satisfy:

$$\mathrm{tr}(T_\alpha T_\beta) = \delta_{\alpha\beta}.$$

For U close to the identity (or θ close to zero),

$$U \approx \mathbb{1} + \mathrm{i}\sum_{\alpha=1}^{d^2-1} \theta_\alpha T_\alpha$$

the input state can be written as $\sum_{kl} R_{kl}|kl\rangle$. Normalization implies $\mathrm{tr}\, RR^\dagger = 1$ where R is the $d \times d$ matrix with elements R_{kl}. Since $RR^\dagger$ has trace one and is self-adjoint it can be written $RR^\dagger = \mathbb{1}/d + \sum_\alpha t_\alpha T_\alpha$ where the t's are real numbers. At the identity the output state satisfies

$$\begin{aligned} |\psi\rangle &= \sum_{kl} R_{kl}|kl\rangle, \\ |\psi_{,\alpha}\rangle &= i\sum_{kl} R_{kl} T_\alpha |k\rangle \otimes |l\rangle; \end{aligned} \tag{13}$$

the $|l_\alpha\rangle$ vectors defined in section II can be written as

$$|l_\alpha\rangle = 2(|\psi_{,\alpha}\rangle + \langle\psi_{,\alpha}|\psi\rangle|\psi\rangle)$$

and the condition for achieving the QCRB (2) becomes

$$\mathrm{Im}\langle l_\alpha|l_\beta\rangle = 4\,\mathrm{Im}\langle\psi_{,\alpha}|\psi_{,\beta}\rangle = \frac{2\,\mathrm{tr}(RR^\dagger[T_\alpha, T_\beta])}{\mathrm{i}} = 0 \tag{14}$$

for all α and β. This implies $RR^\dagger = \mathbb{1}/d$ [3]. This means that the input state is maximally entangled [4].

For the calculations the maximally entangled state, $\sum_{k=1}^d |kk\rangle/\sqrt{d}$, is used. H can be very easily calculated to be

$$H_{\alpha\beta} = \frac{4}{d}\delta_{\alpha\beta}. \tag{15}$$

Since the QCRB can be achieved

$$\sup_M \mathrm{tr}\, H^{-1}(\theta) I(M,\theta) = d^2 - 1.$$

B. LOCC measurements

It will be shown here that for all separable measurements M_{sep} the following holds

$$\mathrm{tr}\, H^{-1}(\theta) I(M_{\mathrm{sep}}, \theta) \le \frac{d(d-1)}{2}. \tag{16}$$

This shows that if one allows nonseparable measurements, the estimation can be improved by a factor of $2(d+1)/d$ with respect to separable measurements. This is always more than twice.

In order to prove Eq.(16) a particular representation for the T's will be chosen, namely:

$$\begin{aligned} T_{kls} &= \mathrm{i}^s \frac{|k\rangle\langle l| + (-1)^s |l\rangle\langle k|}{\sqrt{2}} \qquad && k > l,\ s = \{0,1\}, \\ T_m &= \sum_{k=1}^d c_{mk}|k\rangle\langle k| && m = 1,\ldots,d-1, \end{aligned} \tag{17}$$

where the coefficients c_{mk} obey

$$\begin{aligned} \sum_{k=1}^d c_{mk} &= 0, \\ \sum_{k=1}^d c_{mk}c_{nk} &= \delta_{mn}. \end{aligned} \tag{18}$$

From these two one can derive the relation

$$\sum_{m=1}^{d-1} c_{mk}c_{ml} = \delta_{kl} - \frac{1}{d}. \tag{19}$$

Measurements of the form

$$M_\xi = c_\xi |\phi_\xi\rangle\langle\phi_\xi| = c_\xi |a_\xi\rangle\langle a_\xi| \otimes |b_\xi\rangle\langle b_\xi|$$

are considered. The quantity of interest is

$$\begin{aligned} &\mathrm{tr}\, H^{-1} I = \frac{d}{4}\,\mathrm{tr}\, I \\ &= \frac{d}{4}\sum_{\xi\alpha} c_\xi \frac{(\langle\phi_\xi|\psi_{,\alpha}\rangle\langle\psi|\phi_\xi\rangle + \langle\phi_\xi|\psi\rangle\langle\psi_{,\alpha}|\phi_\xi\rangle)^2}{|\langle\phi_\xi|\psi\rangle|^2} \\ &= \frac{d}{2}\sum_\xi c_\xi \left[\mathrm{Re}\left(\frac{\langle\psi|\phi_\xi\rangle}{\langle\phi_\xi|\psi\rangle} \sum_{\alpha=1}^{d^2-1} \langle\phi_\xi|\psi_{,\alpha}\rangle^2 \right) \right. \\ &\left. + \sum_{\alpha=1}^{d^2-1} \langle\phi_\xi|\psi_{,\alpha}\rangle\langle\psi_{,\alpha}|\phi_\xi\rangle \right]. \end{aligned} \tag{20}$$

The second term in the previous equation is easy to calculate,

$$\begin{aligned} &\frac{d}{2}\sum_\xi c_\xi \sum_{\alpha=1}^{d^2-1} \langle\phi_\xi|\psi_{,\alpha}\rangle\langle\psi_{,\alpha}|\phi_\xi\rangle = \frac{d}{2}\sum_{\alpha=1}^{d^2-1}\langle\psi_{,\alpha}|\psi_{,\alpha}\rangle \\ &= \frac{d}{2}\sum_{\alpha=1}^{d^2-1}\frac{\mathrm{tr}\, T_\alpha^2}{d} = \frac{d^2-1}{2}, \end{aligned} \tag{21}$$

but for the first term a little more work will be needed. One needs to calculate

$$\langle\phi_\xi|\psi_{,\alpha}\rangle = \frac{i}{\sqrt{d}}\sum_{k=1}^d \langle a_\xi|T_\alpha|k\rangle\langle b_\xi|k\rangle.$$

---

[3] Since $(RR^\dagger - \mathbb{1}/d) \in su(n)$ and $su(n)$ is a perfect Lie algebra (i.e. can be spanned by commutators), Eq. (14) may be rewritten as $\forall_{Y\in su(n)}\,\mathrm{tr}[(RR^\dagger - \mathbb{1}/d)Y] = 0$, this implies $RR^\dagger - \frac{\mathbb{1}}{d} = 0$ because the trace form is non-degenerate.

[4] The condition for a bipartite state to be maximally entangled is that the partial trace should be proportional to the identity. In our case $\mathrm{tr}_2\,|\psi\rangle\langle\psi| = RR^\dagger$.

For $\alpha = \{kls\}$

$$\begin{aligned}\langle\phi_\xi|\psi_{,kls}\rangle &= \frac{i^{s+1}}{\sqrt{2d}}[\langle a_\xi|k\rangle\langle b_\xi|l\rangle + (-1)^s\langle a_\xi|l\rangle\langle b_\xi|k\rangle],\\ \sum_{s=0}^{1}\langle\phi_\xi|\psi_{,kls}\rangle^2 &= -\frac{2}{d}\langle a_\xi|k\rangle\langle b_\xi|l\rangle\langle a_\xi|l\rangle\langle b_\xi|k\rangle.\end{aligned} \tag{22}$$

Since the last expression is symmetric with respect to exchanging k with l, $\sum_{k>l} = \frac{1}{2}\sum_{k\neq l} = \frac{1}{2}(\sum_{kl} - \sum_{k=l})$ and

$$\sum_{k>l}\sum_{s=0}^{1}\langle\phi_\xi|\psi_{,kls}\rangle^2 = \frac{1}{d}\sum_{k=1}^{d}\langle a_\xi|k\rangle^2\langle b_\xi|k\rangle^2 - \langle\phi_\xi|\psi\rangle^2.$$

In the case $\alpha = m$

$$\begin{aligned}&\sum_{m=1}^{d-1}\langle\phi_\xi|\psi_{,m}\rangle^2\\ &= -\frac{1}{d}\sum_{k,l=1}^{d}\sum_{m=1}^{d-1}c_{mk}c_{ml}\langle a_\xi|k\rangle\langle b_\xi|k\rangle\langle a_\xi|l\rangle\langle b_\xi|l\rangle\\ &= \frac{1}{d}\sum_{kl}(\frac{1}{d} - \delta_{kl})\langle a_\xi|k\rangle\langle b_\xi|k\rangle\langle a_\xi|l\rangle\langle b_\xi|l\rangle\\ &= \frac{1}{d}\langle\phi_\xi|\psi\rangle^2 - \frac{1}{d}\sum_{k=1}^{d}\langle a_\xi|k\rangle^2\langle b_\xi|k\rangle^2\end{aligned}$$

putting things together

$$\sum_{\alpha=1}^{d^2-1}\langle\phi_\xi|\psi_{,\alpha}\rangle^2 = \frac{1-d}{d}\langle\phi_\xi|\psi\rangle^2 \tag{23}$$

and

$$\begin{aligned}&\frac{d}{2}\sum_\xi c_\xi\,\mathrm{Re}\left(\frac{\langle\psi|\phi_\xi\rangle}{\langle\phi_\xi|\psi\rangle}\sum_{\alpha=1}^{d^2-1}\langle\phi_\xi|\psi_{,\alpha}\rangle^2\right)\\ &= \frac{1-d}{2}\sum_\xi c_\xi|\langle\psi|\phi_\xi\rangle|^2 = \frac{1-d}{2}.\end{aligned} \tag{24}$$

Finally, substituting the previous equation and Eq. (21) in (20) one obtains the desired result, namely, for any separable measurement M of the type (8)

$$\mathrm{tr}\,H^{-1}(\theta)I(M,\theta) = \frac{d(d-1)}{2}. \tag{25}$$

Of course this impliesEq. (16). The argument for LOCC measurements is the same as for the two dimensional case and one obtains the same bound for them.

V. CONCLUSIONS AND OPEN PROBLEMS

In this paper it has been shown that by using nonseparable measurements there is a significant improvement in the accuracy of the estimation of unitary operations. It is also proven that in d dimensions the QCRB can be achieved if and only if the input state is maximally entangled. An open problem is the estimation of more general quantum operations, described by the *Kraus decomposition* [2].

Acknowledgments

This research was funded by the Netherlands Organization for Scientific Research (NWO), support from the RESQ (IST-2001-37559) project of the IST-FET programme of the European Union is also acknowledged.

[1] F. de Martini, A. Mazzei, M. Ricci, and G. M. D'Ariano, Phys. Rev. A **67**, 062307 (2003), quant-ph/0210210.
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[3] A. Fujiwara, Phys. Rev. A **65**, 012316 (2001).
[4] A. Acín, E. Jané, and G. Vidal, Phys. Rev. A **64**, 050302 (2001), quant-ph/0012015.
[5] A. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland Publishing, Amsterdam , New York , Oxford, 1982).
[6] K. Matsumoto, J. Phys. A **35**, 3111 (2002), quant-ph/9711008.
[7] R. D. Gill and S. Massar, Phys. Rev. A **61**, 042312 (2000), quant-ph/9902063.
[8] Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001), quant-ph/0010046.
[9] J. Calsamiglia and N. Lutkenhaus, Appl. Phys. B: Lasers Opt. **72**, 67 (2001), quant-ph/0007058.
[10] C. H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999), quant-ph/9804053.