International Journal of Quantum Information
Vol. 3, No. 1 (2005) 57–63

OPTIMAL STATE ESTIMATION AND CLONING FOR EQUATORIAL QUANTUM SYSTEMS WITH ARBITRARY DIMENSION

C. MACCHIAVELLO

INFM & Dipartimento di Fisica 'A. Volta', Università degli Studi di Pavia
via Bassi 6, I-27100 Pavia, Italy

Received 6 July 2004

We review the problem of optimal estimation of multiple phases for systems with arbitrary finite dimension and derive the optimal estimation fidelity for equatorial states. We present optimal phase covariant cloning transformations for d-dimensional systems, relating these results to the optimal estimation procedure.

Keywords: Phase estimation; quantum cloning.

1. Introduction

Much interest has been recently triggered by the possibility of employing quantum systems with (finite) dimensions higher than two in quantum information. In particular, it has been shown that an increase in the dimension leads to a better performance of various quantum information protocols, such as quantum cryptography[1,2] and some problems in distributed quantum computing.[3] Moreover, experimental achievements have been recently reported in the generation, manipulation and detection of quantum systems with higher dimensions.[4]

In this work we review two particular tasks often encountered in quantum information theory, namely phase estimation and quantum cloning, and highlight connections between them. The issue of phase estimation has important applications in quantum computation and quantum information. For example, it was shown that the existing quantum algorithms can be described in a unified way as quantum interference processes among different computational paths where the result of the computation is encoded in a phase shift.[5] The design of optimal phase measurement procedures is also crucial in various tasks of atomic physics, such as, for example, methods for precision spectroscopy,[6] and quantum interferometric experiments in quantum optics.

Moreover, the impossibility of perfectly cloning unknown quantum states selected from a nonorthogonal set is due to the laws of quantum mechanics,[7] and is the basis of the security of quantum cryptography.[8,9] Approximate quantum cloning has been extensively studied in the last few years and has led to relevant results in quantum cryptography. The eavesdropping strategies in quantum key distribution protocols that are known to be optimal so far are actually based on cloning attacks.[2,10] Moreover, quantum cloning allows one to study the sharing of quantum information among several parties and it may also be applied to the study of the security of multi-party cryptographic schemes.[11]

In this work we address the issues of multiple phase estimation and quantum cloning for "equatorial states" of quantum systems with arbitrary finite dimension d, defined as

$$|\psi(\{\phi_j\})\rangle = \frac{1}{\sqrt{d}}\big(|0\rangle + e^{i\phi_1}|1\rangle + e^{i\phi_2}|2\rangle + \cdots + e^{i\phi_{d-1}}|d-1\rangle\big), \tag{1}$$

where $\{|0\rangle, |1\rangle, |2\rangle, \ldots, |d-1\rangle\}$ represents a basis for the system under consideration and $\{\phi_j\}$ denotes a set of $d-1$ independent phase-shifts ($\phi_j \in [0, 2\pi]$).

The paper is organized as follows. In Sec. 2, we review the problem of optimal estimation of multiple phases for finite-dimensional systems and derive the fidelity corresponding to the optimal procedure for equatorial states of the form (1). In Sec. 3, we introduce the problem of optimal phase covariant cloning for equatorial states of finite-dimensional systems and report the optimal cloning transformation for some values of the input and output copies, highlighting the relation with the optimal estimation procedure. In Sec. 4, we summarize the results presented.

2. Optimal Estimation of Multiple Phases

In this section we address the problem of estimating the values of K independent phase-shifts ϕ_j ($j = 1, K$), pertaining to the unitary transformation[13]

$$\rho_{\{\phi_j\}} = e^{-i\sum_{j=1}^{K}\phi_j \hat{H}_j}\rho_0 e^{i\sum_{j=1}^{K}\phi_j \hat{H}_j}, \tag{2}$$

where $\hat{H}_j$ represent K commuting self-adjoint operators, which are in general degenerate on the Hilbert space $\mathcal{H}$ of the considered quantum system and each of them has a discrete spectrum S_j (S_j can be, for example, Z, N, or Z_q, $q > 0$). In Eq. (2), ρ_0 is a generic initial pure state $|\psi_0\rangle\langle\psi_0|$ describing a quantum system with arbitrary dimension.

The estimation problem then consists in minimizing the average cost $\bar{C}$ of the procedure, defined as

$$\begin{aligned}\bar{C} = &\int_0^{2\pi} d\phi_1 \int_0^{2\pi} d\phi_2 \cdots \int_0^{2\pi} d\phi_K \, p_0(\{\phi_j\}) \\ &\times \int_0^{2\pi} d\bar{\phi}_1 \int_0^{2\pi} d\bar{\phi}_2 \cdots \int_0^{2\pi} d\bar{\phi}_K \, C(\{\bar{\phi}_j\}, \{\phi_j\}) p(\{\bar{\phi}_j\}|\{\phi_j\}),\end{aligned} \tag{3}$$

where $C(\{\bar{\phi}_j\}, \{\phi_j\})$ is a cost function which depends on the set of the K estimated values $\{\bar{\phi}_j\}$ that are the results of the estimation procedure, and on the set of the K true values $\{\phi_j\}$. Moreover, $p_0(\{\phi_j\})$ is the *a priori* probability density for the true values $\{\phi_j\}$ and $p(\{\bar{\phi}_j\}|\{\phi_j\})$ is the conditional probability of estimating the set of values $\{\bar{\phi}_j\}$ given the true values $\{\phi_j\}$.

In this work we consider the general scenario where all the values $\{\phi_j\}$ are *a priori* uniformly distributed, i.e. the probability density is simply given by $p_0(\{\phi_j\}) = (1/2\pi)^K$. Moreover, we consider the case where the errors in the estimates are weighted independently of the values ϕ_j of the phases, but they depend only on the values of the differences $\bar{\phi}_j - \phi_j$, so that the cost function becomes an even function of K variables, i.e. $C(\{\bar{\phi}_j\}, \{\phi_j\}) \equiv C(\{\bar{\phi}_j - \phi_j\})$. From these requirements it follows also that the conditional probability corresponding to the optimal estimation procedure will depend only on the variables $\bar{\phi}_j - \phi_j$, and therefore the optimal positive-operator valued measurement (POVM)[12] will be phase-covariant, i.e. of the form

$$d\mu\left(\{\bar{\phi}_j\}\right) = e^{-i\sum_{j=1}^{K}\bar{\phi}_j\hat{H}_j}\chi e^{i\sum_{j=1}^{K}\bar{\phi}_j\hat{H}_j}\frac{d\bar{\phi}_1}{2\pi}\frac{d\bar{\phi}_2}{2\pi}\cdots\frac{d\bar{\phi}_K}{2\pi}. \tag{4}$$

In the above equation χ is a positive operator satisfying the completeness constraints needed for the normalization of the POVM $\int d\mu\left(\{\phi_j\}\right) = \mathbb{1}$, where $\mathbb{1}$ denotes the identity operator.

We will now show explicitly how to derive the optimal POVM for a broad class of cost functions. First of all we will choose the representation where all the operators $\hat{H}_j$ are diagonal. We have assumed that the operators $\hat{H}_j$ commute, so we can identify a common basis of eigenvectors. The operators $\hat{H}_j$ are generally degenerate, and we will denote by $|\{n_j\}\rangle_\nu$ a choice of normalized eigenvectors corresponding to eigenvalue n_j for the operator $\hat{H}_j$, by $\Pi_{\{n_j\}}$ the projector onto the corresponding degenerate eigenspace and by ν a degeneracy index, whose maximum value corresponds to the dimension of the degenerate eigenspace.

We will now generalize the projection method developed in Ref. 14 and define $\mathcal{H}_\parallel$ as the Hilbert space spanned by the vectors $|\{n_j\}\rangle \propto \Pi_{\{n_j\}}|\psi_0\rangle \neq 0$ with the choice of the arbitrary phases such that $\langle\{n_j\}|\psi_0\rangle > 0$. We can then write the Hilbert space of the system as $\mathcal{H} = \mathcal{H}_\parallel \oplus \mathcal{H}_\perp$, where the component $\mathcal{H}_\perp$ is spanned by states that are orthogonal to $|\psi_0\rangle$. Hence the POVM can be chosen of the block diagonal form on $\mathcal{H}_\parallel \oplus \mathcal{H}_\perp$, i.e. $d\mu\left(\{\phi_j\}\right) = d\mu_\parallel\left(\{\phi_j\}\right) \oplus d\mu_\perp\left(\{\phi_j\}\right)$. In this way the component $d\mu_\perp\left(\{\phi_j\}\right)$ of the POVM acting on $\mathcal{H}_\perp$ can be chosen arbitrarily because it does not contribute to the average cost. Therefore, the optimization of the estimation procedure can be performed by optimizing only the component $d\mu_\parallel\left(\{\phi_j\}\right)$ of the POVM.

The cost functions usually considered are 2π-periodic functions in the variables $\{\phi_j\}$, and therefore they can be written as

$$C(\{\phi_j\}) = -\sum_{l_1,l_2,\ldots,l_M=-\infty}^{\infty} c_{\{l_j\}}e^{i\sum_j l_j\phi_j}, \tag{5}$$

with the condition $c_{\{l_j\}} = c_{\{-l_j\}}$ due to the fact that the cost is a real and even function. We will now focus on a general class of cost functions that extends the one considered by Holevo,[15] with

$$c_{\{l_j\}} \geq 0, \quad \forall\{l_j\} \neq 0. \tag{6}$$

For this class the optimal POVM takes the explicit form[13]

$$d\mu_{\|}(\{\phi_j\}) = \frac{d\phi_1}{2\pi}\cdots\frac{d\phi_K}{2\pi}|e(\{\phi_j\})\rangle\langle e(\{\phi_j\})|, \tag{7}$$

where the vectors $|e(\{\phi_j\})\rangle$ are defined as

$$|e(\{\phi_j\})\rangle = \sum_{\{n_j\}} e^{i\sum_j n_j\phi_j}|\{n_j\}\rangle. \tag{8}$$

We will now specify the above results to a system of N equatorial states (1). This case consists of the estimation problem for $d-1$ phase-shifts corresponding to the operators $\hat{H}_j = |j\rangle\langle j|$, $j=1,\ldots,d-1$, and $|\psi_0\rangle = (|0\rangle+|1\rangle+|2\rangle+\cdots+|d-1\rangle)/\sqrt{d}$ for each system (d-dimensional systems will also be called qudits in the following). For the composite system of N qudits we have $\hat{H}_j = \sum_{k=1}^N |j\rangle\langle j|_k$, where $|j\rangle\langle j|_k$ denotes the projection operator onto the state $|j\rangle$ of the kth qudit. Following the projection method specified above, the POVM is optimized by choosing an appropriate basis belonging to the symmetric subspace of the global Hilbert space of the N qudits. We will denote such a basis as $\{|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_s, \sum_{j=0}^{d-1} n_j = N\}$, where $|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_s$ is the symmetric state of N qudits, with n_0 qudits in state $|0\rangle$, n_1 in state $|1\rangle$, and so on.

The optimal POVM for the cost functions of the generalized Holevo form (6) is given by (7), with $K=d-1$ and

$$|e(\{\phi_j\})\rangle = \sum_{\{n_j\}} e^{i\sum_{j=1}^{d-1} n_j\phi_j}|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_s. \tag{9}$$

In the above equation the sum over $\{n_j\}$ means that the variables n_j take all the possible non-negative values compatible with the constraint $\sum_{j=0}^{d-1} n_j = N$.

Let us now compute the fidelity of the optimal multiple phase estimation procedure derived above. We choose a cost function of the form $1-F$, where F is the fidelity of the estimated state $|\psi(\{\bar{\phi}_j\})\rangle$ with respect to the true state $|\psi(\{\phi_j\})\rangle$. This cost belongs to the class (6), and therefore the corresponding optimal POVM is the one mentioned above. By the covariance of the procedure we can write the fidelity as

$$F(\{\phi_j\}) = |\langle\psi_0|\psi(\{\phi_j\})\rangle|^2 = \frac{1}{d^2}\left[d + 2\sum_{j=1}^{d-1}\cos\phi_j + 2\sum_{j>k}\cos(\phi_j-\phi_k)\right]. \tag{10}$$

The average fidelity $\bar{F}$ of the procedure is now given by

$$\bar{F} = \frac{1}{d^2}\int_0^{2\pi}\frac{d\phi_0}{2\pi}\cdots\int_0^{2\pi}\frac{d\phi_{d-1}}{2\pi}F(\{\phi_j\})|\langle\psi_0^{(N)}|e(\{\phi_j\})\rangle|^2, \tag{11}$$

where

$$|\psi_0^{(N)}\rangle \equiv |\psi_0\rangle^{\otimes N} = \frac{1}{\sqrt{d^N}}\sum_{\{n_j\}}\sqrt{\frac{N!}{n_0!n_1!n_2!\cdots n_{d-1}!}}|n_0,n_1,n_2,\ldots,n_{d-1}\rangle_s. \tag{12}$$

By performing the integrations in Eq. (11), we have

$$\bar{F} = \frac{1}{d} + \frac{d-1}{d^{N+1}} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-n_1-1} \cdots \sum_{n_{d-1}=0}^{N-n_1-n_2-\cdots-1} \times \frac{N!}{(N-n_1-n_2-\cdots n_{d-1})!n_1!n_2!\cdots n_{d-1}!} \sqrt{\frac{N-n_1-n_2-\cdots n_{d-1}}{n_1+1}}. \quad (13)$$

3. Optimal Phase Covariant Cloning

In this section we will review the issue of phase covariant cloning for qudits. We will treat a cloning map as a special kind of *quantum channel*, i.e. a trace-preserving completely positive (CP) map. In the general $N \to M$ cloning case, the CP map $\mathcal{C}$ goes from input states in $\mathcal{H}^{\otimes N}$ to output states in $\mathcal{H}^{\otimes M}$, with the output state invariant under the permutations of the M output spaces. More specifically, we consider N identical input copies, and therefore the map goes from an input state $\rho^{\otimes N}$ belonging to the symmetric subspace $(\mathcal{H}^{\otimes N})_+$ of the tensor product $\mathcal{H}^{\otimes N}$ to the output space $\mathcal{H}^{\otimes M}$ with $M > N$. We will consider optimal cloning maps that have the output state restricted to the symmetric subspace $(\mathcal{H}^{\otimes M})_+$, even though permutation invariance of the state does not imply in general that the state has support in the symmetric subspace. In the following we will denote an $N \to M$ cloning map as $\mathcal{C}_{NM}$.

We are interested in phase covariant cloning maps that are optimized for equatorial input states (1), and where all these states are treated in the same way. The phase covariance condition is given by

$$\mathcal{C}_{NM}\left(U_{\{\phi_j\}}^{\otimes N}\,\rho_{\mathcal{N}} U_{\{\phi_j\}}^{\dagger\otimes N}\right) = U_{\{\phi_j\}}^{\otimes M}\mathcal{C}_{NM}(\rho_{\mathcal{N}})U_{\{\phi_j\}}^{\dagger\otimes M}, \quad (14)$$

where $U_{\{\phi_j\}} = \exp\left(i\sum_{j=1}^{d-1}\phi_j|j\rangle\langle j|\right)$ is the unitary phase rotation operator acting on a qudit.

As a figure of merit for the cloning transformation we consider the single particle fidelity, defined as

$$F_{NM} = \mathrm{Tr}\left[\left(|\psi_0\rangle\langle\psi_0|\mathbb{1}^{\otimes M-1}C_{NM}(|\psi_0\rangle\langle\psi_0|^{\otimes N}\right)\right]. \quad (15)$$

Notice that, since the output state of the M copies is supported on the symmetric subspace, the single particle fidelity is the same for any output copy.

The optimal phase covariant cloning maps for the simplest case of $N = 1$ and $M = 2$ were derived in Ref. 16. In this work we address the case of general values for N and M. Following the same approach as in Ref. 17, based on the one-to-one correspondence between invariant positive operators and CP maps,[18] the optimal phase covariant cloning maps can be easily derived for any value of N and for values of M related to N and d as $M = kd + N$,[19] where k can take any positive integer value. We do not report here the details of the derivation but only the main results.[19]

The most interesting aspect in the case $M = kd + N$ is that the optimal phase covariant cloning map can be expressed in the Kraus form[20] simply as

$$\mathcal{C}_{NM}(\rho) = B\rho B^{\dagger}, \tag{16}$$

namely with a single Kraus operator

$$B = \sum_{\{n_j\}} |n_0 + k, n_1 + k, n_2 + k, \ldots, n_{d-1} + k\rangle_s \langle n_0, n_1, n_2, \ldots, n_{d-1}|_s. \tag{17}$$

As in the previous section the sum over $\{n_j\}$ satisfies the constraint $\sum_{j=0}^{d-1} n_j = N$. Notice that the optimal cloning map can be realized in an "economical" way, without the need of auxiliary qudits in addition to the M output copies.[21] This is in contrast to the case of universal cloning[22] and to the case of $1 \to 2$ phase covariant cloning,[16,17] where auxiliary qubits are needed to achieve the optimal transformation.

The optimal fidelity takes the form

$$\begin{aligned} F_{NM} = {} & \frac{1}{d} + \frac{d-1}{d^N M} \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-n_1-1} \cdots \sum_{n_{d-1}=0}^{N-n_1-n_2-\cdots-1} \\ & \times \frac{N!}{(N - n_1 - n_2 - \cdots n_{d-1})! n_1! n_2! \cdots n_{d-1}!} \\ & \times \sqrt{\left(n_0 + \frac{M-N}{d} + 1\right)\left(n_1 + \frac{M-N}{d}\right)} \sqrt{\frac{N - n_1 - n_2 - \cdots n_{d-1}}{n_1 + 1}}. \end{aligned} \tag{18}$$

Notice that in the limit of an infinite number of output copies M, the above fidelity is equal to the fidelity of the optimal multiple phase estimation for N equatorial states (13). This result generalizes to any finite value of the dimension d the analogous connection previously proved for qubits[10] and qutrits.[13]

4. Conclusions

In this work we have addressed two tasks often encountered in quantum information theory, namely phase estimation and quantum cloning, where the information is encoded into finite-dimensional quantum states as phase shifts. We have reported the optimal procedures in the two cases and generalized for any finite dimension the connection between the two tasks.

We want to stress that much interest has been recently triggered by phase covariant cloning and much effort is now devoted to finding efficient experimental implementations of the cloning transformation[23] and new implementation approaches, such as spin networks.[24]

Moreover, we want to point out that the scenario of multiple phases considered in this work may be exploited to design schemes where several variables are encoded into phases in the same quantum states and in this way the efficiency of quantum information processing tasks may be improved.

Acknowledgments

This work was supported in part by the EC programs QUPRODIS (Contract No. IST-2002-38877) and SECOQC (Contract No. IST-2003-506813).

References

1. H. Bechmann-Pasquinucci and A. Peres, *Phys. Rev. Lett.* **85**, 3313 (2000).
2. D. Bruß and C. Macchiavello, *Phys. Rev. Lett.* **88**, 127901 (2002); N. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
3. M. Fitzi, N. Gisin and U. Maurer, *Phys. Rev. Lett.* **87**, 217901 (2002).
4. See, for example, G. Molina-Terriza, A. Vaziri, J. Rehacek, Z. Hradila and A. Zeilinger, *Phys. Rev. Lett.* **92**, 167903 (2004); R. T. Thew, A. Acin, H. Zbinden and N. Gisin, quant-ph/0307122; R. Das, A. Mitra, V. Kumar S. and A. Kumar, quant-ph/0307240.
5. R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, in *Proc. Roy. Soc. London* **A454**, 339 (1998).
6. See, for example, J. J. Bollinger, W. M. Itano, D. J. Wineland and D. J. Heinzen, *Phys. Rev.* **A54**, R4649 (1996).
7. W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).
8. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
9. A. Ekert, *Phys. Rev. Lett.* **68**, 661 (1991).
10. D. Bruß, M. Cinchetti, G. M. D'Ariano and C. Macchiavello, *Phys. Rev.* **A62**, 012302 (2000).
11. V. Scarani and N. Gisin, *J. Phys.* **A34**, 6043 (2001).
12. C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
13. C. Macchiavello, *Phys. Rev.* **A67**, 062302 (2003).
14. G. M. D'Ariano, C. Macchiavello and M. F. Sacchi, *Phys. Lett.* **A248**, 103 (1998).
15. A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
16. H. Fan, H. Imai, K. Matsumoto and X.-B. Wang, *Phys. Rev.* **A67**, 022317 (2003).
17. G. M. D'Ariano and C. Macchiavello, *Phys. Rev.* **A67**, 042306 (2003).
18. G. M. D'Ariano and P. Lo Presti, *Phys. Rev.* **A64**, 042308 (2001).
19. F. Buscemi, G. M. D'Ariano and C. Macchiavello, quant-ph/0407103.
20. K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
21. The first "economical" map was found for qubits in C.-S. Niu and R. B. Griffiths, *Phys. Rev.* **A60**, 2764 (1999).
22. R. F. Werner, *Phys. Rev.* **A58**, 1827 (1998).
23. See, for example, J. Du *et al.*, quant-ph/0311010.
24. G. De Chiara, R. Fazio, C. Macchiavello, S. Montangero and G. M. Palma, quant-ph/0402071.