19 June 2000

PHYSICS LETTERS A

ELSEVIER

Physics Letters A 271 (2000) 31–34

www.elsevier.nl/locate/pla

Quantum clone and states estimation for *n*-state system

Chuan-Wei Zhang, Chuan-Feng Li *, Guang-Can Guo

Laboratory of Quantum Communication and Quantum, Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, PR China

Received 1 February 2000; received in revised form 3 May 2000; accepted 5 May 2000
Communicated by V.M. Agranovich

Abstract

We derive a lower bound for the optimal fidelity for deterministic cloning a set of n pure states. In connection with states estimation, we obtain a lower bound about average maximum correct states estimation probability. © 2000 Published by Elsevier Science B.V.

PACS: 03.67.-a; 03.65.Bz; 89.70.+c

Quantum no-cloning theorem [1,2] has prohibited cloning and estimating an arbitrary quantum state exactly by any physical means in a consequence of linearity of quantum theory. The unitarity of quantum theory does not allow to clone (identify) no-orthogonal states though orthogonal states can be cloned (identified) perfectly [3,4]. However, clone and estimation of quantum states with a limited degree of success are always possible. Universal quantum cloning machine (UQCM) [5–13] acts on any unknown quantum state and produce optimal approximate copies. This machine is called universal because it produces copies that are state-independent. State-dependent quantum cloning machines is designed to clone states belonging to a finite set and may be divided into two main categories: deterministic [14,15], probabilistic [16–19] and hybrid [20]. Deterministic state-dependent cloning machine generates approximate clones with probability 1. Deterministic exact clone violates the no-cloning theorem, thus perfectly clone must be probabilistic. Probabilistic quantum cloning machines can clone states perfectly, though the success probability cannot be unit all the time. It is shown that a set of non-orthogonal states can be probabilistically cloned if and only if the states are linearly independent. Hybrid clone interpolates between deterministic and probabilistic ones, that is, the copies (not exact) are better than those in deterministic clone, but the success probability (less than 1) is greater than probabilistic exact clone. Universal quantum states estimation were considered in Ref. [21,22], given M independent realizations. What's more, we [23] have discussed general states discrimination strategies for state-dependent system.

* Corresponding author.
E-mail addresses: cfli@ustc.edu.cn (C.-F. Li), gcguo@ustc.edu.cn (G.-C. Guo).

PII: S0375-9601(00)00352-2

Optimal results for two-state deterministic clone have been obtained in Refs. [14,15,20]. In this Letter we consider deterministic clone for a set of n pure states $\{|\psi_i\rangle, i=1,2,\dots,n\}$. When $|\psi_i\rangle$ are non-orthogonal, they cannot be cloned perfectly. What we require is that the final states should be most similar as the target states, that is, the fidelity between the final and target states should be optimal. We derive a lower bound for the optimal fidelity of the cloning machine. Applying it to states estimation, we obtain the lower bound about average maximum correct identification probability in deterministic states estimation.

A quantum state-dependent cloning device is a quantum machine which performs a prescribed unitary transformation on an extended input which contains M original states in system A and $N-M$ blank states in system B with N output copies. The unitary evolution transfers states as follows

$$U|\psi_i^M\rangle_A|\Sigma^{N-M}\rangle_B = |\alpha_i\rangle, \tag{1}$$

where $|\psi_i^M\rangle_A = |\psi_i\rangle_1 \otimes \dots \otimes |\psi_i\rangle_M$ are the M original states, $|\Sigma^{N-M}\rangle_B$ are the blank states and $|\alpha_i\rangle$ are the output cloned states. The $n \times n$ inter-inner-products of Eq. (1) yield the matrix equation[1]

$$X^{(M)} = \tilde{X}, \tag{2}$$

where $n \times n$ matrices $\tilde{X} = [\langle\alpha_i|\alpha_j\rangle]$, $X^{(M)} = [\langle\psi_i|\psi_j\rangle^M]$.

We require a figure of merit to characterize how closely our copies $|\alpha_i\rangle$ resemble exact copies $|\psi_i^N\rangle$. Denoting the priori probability of the state $|\psi_i^M\rangle$ by η_i, one interesting measure of the final states is the global fidelity introduced by Bruß et al. [14,15], which is defined formally as

$$F = \sum_{i=1}^{n} \eta_i |\langle\alpha_i|\psi_i^N\rangle|^2. \tag{3}$$

As a criterion for optimality of the state-dependent cloner, the unitary evolution U should maximize the global fidelity F of n final states $|\alpha_i\rangle$ with respect to the perfect cloned states $|\psi_i^N\rangle$. We focus here on the global fidelity since it has an important interpretation in connection with states estimation [20].

Now the remained problem is to find the maximum value of the fidelity F, which means optimal clone. It is equivalent to the problem of maximizing F under the condition of Eq. (2). This problem is a nonlinear programming and fairly difficult to solve. Nevertheless a lower bound of the optimal fidelity could still be derived by adopting an auxiliary function F', which is defined as

$$F' = \sum_{i=1}^{n} \eta_i |\langle\psi_i^N|\alpha_i\rangle|. \tag{4}$$

Such function also describes how closely our output copies resemble exact copies. There exists a bound between F and F' (see below, inequality (9)), therefore a bound for F may be obtained by optimizing F'.

We find that the optimal output states $|\alpha_i\rangle$ must lie in the subspace spanned by the exact clones $|\psi_i^N\rangle$. This conclusion may be easily come to with the method of Lagrange Multipliers (please refer to [14,15], where $n=2$) and here we omit the proof.

If a set of states $|\tilde{\alpha}_i\rangle$ fulfil Eq. (2), that is, $X^{(M)} = \tilde{X} = [\langle\tilde{\alpha}_i|\tilde{\alpha}_j\rangle]$, there must exist a unitary transformation V satisfies $V|\tilde{\alpha}_i\rangle = |\alpha_i\rangle$, thus we can vary V to optimize F' with chosen states $|\tilde{\alpha}_i\rangle$. Suppose $|\langle\psi_i^N|\alpha_i\rangle| = \lambda_i\langle\psi_i^N|\alpha_i\rangle$ with $\lambda_i \in \{\pm 1\}$ in the optimal situation (the determination of λ_i will be shown in later part), the optimal F' is

$$F'_{\text{opt}} = \max_V F' = \max_V \left|\sum_{i=1}^{n} \eta_i \lambda_i \langle\psi_i^N|V|\tilde{\alpha}_i\rangle\right|. \tag{5}$$

Choose n orthogonal states $|\chi_i\rangle$ which span a space $\mathscr{H}$ and the space spanned by $|\psi_i^N\rangle$ is a subspace of $\mathscr{H}$[2]. Set $|\tilde{\alpha}_i\rangle = \sum_{j=1}^{n} a_{ij}|\chi_j\rangle$, $|\psi_i^N\rangle =$

[1] We notice the preserving inner-product property of unitary transformation, that is, if two sets of states $\{|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle\}$ and $\{|\tilde{\phi}_1\rangle, |\tilde{\phi}_2\rangle, \dots, |\tilde{\phi}_n\rangle\}$ satisfy the condition $\langle\phi_i|\phi_j\rangle = \langle\tilde{\phi}_i|\tilde{\phi}_j\rangle$, there exists a unitary operate U to make $U|\phi_i\rangle = |\tilde{\phi}_i\rangle$ $(i=1,2,\dots,n)$.

[2] We consider space $\{|\psi_i^N\rangle, i=1,2,\dots,n\}$ may be a subspace of $\mathscr{H}$ since $|\psi_i\rangle$ may be linear-dependent and cannot span a n-dimensional Hilbert space.

$\sum_{j=1}^{n} b_{ij} | \chi_j \rangle$ on the orthogonal bases $|\chi_i\rangle$, $i = 1,2,\ldots,n$, we get

$$F'_{\mathrm{opt}} = \max_V |\mathrm{tr}(\eta\lambda BVA^+)| = \max_V |\mathrm{tr}(VO)|$$
$$= \mathrm{tr}\sqrt{O^+O}\,, \tag{6}$$

where $A = [a_{ij}]$, $B = [b_{ij}]$, $\eta = \mathrm{diag}(\eta_1,\eta_2,\ldots,\eta_n)$, $\lambda = \mathrm{diag}(\lambda_1,\lambda_2,\ldots,\lambda_n)$, $O = A^+\eta\lambda B$. We have used the freedom in V to make the inequality as tight as possible. To do this we have recalled [24,25] that $\max_V |\mathrm{tr}(VO)| = \mathrm{tr}\sqrt{O^+O}$, where O is any operator and the maximum is achieved only by those V such that

$$VO = \mathrm{e}^{i\nu}\sqrt{O^+O}\,, \tag{7}$$

where ν is arbitrary. Generally, we choose $\nu = 0$.

As we require above, λ_i should satisfy $\lambda_i \langle \psi_i^N | V | \tilde{\alpha}_i \rangle \geq 0$. This condition can be represented as $\langle \chi_i | \lambda BVA^+ | \chi_i \rangle \geq 0$, which means the diagonal elements of matrix λBVA^+ should be positive. Since $\lambda_i \in \{\pm 1\}$, a simple method to determine λ_i is to enumerate the 2^n possible results of $\lambda = \mathrm{diag}(\lambda_1,\lambda_2,\ldots,\lambda_n)$ and verify which one fulfils above inequality. With a chosen basis $|\chi_i\rangle$, matrix A, B can be given by equations $A^+A = X^{(M)}$ and $B^+B = X^{(N)}$ respectively, V can be represented with parameters λ_i, thus above postcalculation method can determine matrix λ and then give the maximum F'_{opt}. According to Eq. (6), we obtain a tight upper bound for the function F',

$$F' \leq \mathrm{tr}\sqrt{B^+\lambda\eta X^{(M)}\eta\lambda B}\,. \tag{8}$$

The fidelity F of the cloning machine is constrained by the following inequality

$$F = \left(\sum_{i=1}^{n} \eta_i |\langle \alpha_i | \psi_i^N \rangle|^2 \right) \left(\sum_{i=1}^{n} \eta_i \right)$$
$$\geq \left(\sum_{i=1}^{n} \eta_i |\langle \alpha_i | \psi_i^N \rangle| \right)^2 = (F')^2, \tag{9}$$

where the equation is met if and only if $|\langle \alpha_i | \psi_i^N \rangle|$ are constant. Obviously F is not always optimal even if F' is optimal. However optimal F should be greater than or equal to $(F'_{\mathrm{opt}})^2$. When $n = 2$ and $\eta_1 = \eta_2$, equation in Ineq. (9) is satisfied and gives the optimal results, which has been provided in Refs. [14,15,20].

State-dependent clone has a close connection with states estimation in the limit as $N \to \infty$. Given infinite copies of n non-orthogonal states, we can discriminate them exactly with probability 1. On the other hand, if we can discriminate n states, we can obtain infinite copies. There are two ways in which an attempt to discriminate between non-orthogonal states; it can give either an erroneous or an inconclusive result [23]. In the following we will consider a strategy without inconclusive results using above results in the limit as $N \to \infty$. In fact, since the optimal output states $|\alpha_i\rangle$ lie in the subspace spanned by the exact clones $|\psi_i^N\rangle$, Eq. (1) may be rewritten as

$$U|\psi_i^M\rangle|\Sigma^{N-M}\rangle = \sum_{j=1}^{n} c_{ij} |\psi_j^N\rangle, \tag{10}$$

where $c_{ij} = \langle \psi_j^N | \alpha_i \rangle$. If $N \to \infty$, $\{|\psi_j^N\rangle$, $j = 1,2,\ldots,n\}$ are orthogonal. After the evolution, the cloning system is measured and if $|\psi_j^\infty\rangle$ is obtained, the original state is estimated as $|\psi_j^M\rangle$. The states estimation is correct with probability $|c_{ii}|^2$ when $j = i$. If $j \neq i$, errors occur with probability $\sum_{j\neq i} |c_{ij}|^2$. The inter-inner products of Eq. (10) give the matrix equation in the limit $N \to \infty$,

$$X^{(M)} - EE^+ = 0, \tag{11}$$

where $E = [c_{ij}]$. The diagonal elements is corresponding to the probabilities of correct states estimation while non-diagonal elements to those of error. This equation describes the bound between the maximum probabilities of correct discrimination and those of incorrect one. In fact, this result is a special case of that we have derived in [23]. In Ref. [23], we have consider two possible ways in which an attempt to discriminate between non-orthogonal states can fail, by giving either an erroneous or an inconclusive result. Above strategy just gives an erroneous result with some probability. Our principal result in Ref. [23] is the matrix inequality which prescribes the bound among the probabilities of correct, error and inconclusive discrimination results. Such bound may have intriguing implications for quantum communication theory and cryptography [26] since it offers a potential eavesdropper increased flexibility by a compromise between inconclusive and erroneous results.

An important optimality criterion of the states estimation is the average maximum correct probability, that is, $P=\sum_i \eta_i |c_{ii}|^2 = F$ in the limit $N \to \infty$[3]. In this situation $|\psi_j^N\rangle$ are orthogonal, thus matrix $B = I_n$. Applying Eqs. (8) and (9), we obtain

$$P = \sum_i \eta_i |c_{ii}|^2 \geq \left(\mathrm{tr}\sqrt{\lambda\eta X^{(M)}\eta\lambda}\right)^2. \tag{12}$$

Such F is not always optimal bound of the average maximum probability of correct states estimation, however, the optimal one is always greater than $\left(\mathrm{tr}\sqrt{\lambda\eta X^{(M)}\eta\lambda}\right)^2$.

We note that above bound about F and P have the meaning in average. They describe the optimality approach to the final states we can reach in average of the n initial states and does not mean the best for each initial state. However, since we do not know which one the initial state is in the clone or estimation process, such average may be the most important value to describe the efficiencies of cloning (estimating) machines.

In summary, we have derived a lower bound for the optimal fidelity for the state-dependent quantum clone. In connection with states estimation, we obtained the matrix inequality which describes the bound between the maximum probabilities of correct discrimination and those of incorrect one. A lower bound about average maximum probability of correct identification has also been presented. Our results give some bounds which the optimal cloner and states estimation can be better than in average, however, we have not found a limit which optimal cloner can reach at most. It is still an open question needed to be explored.

[3] It is the reason why we choose the definition of F as that in Eq. (3).

Acknowledgements

This work was supported by the National Natural Science Foundation of China.

References

[1] W.K. Wootters, W.H. Zurek, Nature 299 (1982) 802.
[2] D. Dieks, Phys. Lett. A 92 (1982) 271.
[3] H.P. Yuen, Phys. Lett. A 113 (1986) 405.
[4] G.M. D'Ariano, H.P. Yuen, Phys. Rev. Lett. 76 (1996) 2832.
[5] V. Bužek, M. Hillery, Phys. Rev. A 54 (1996) 1844.
[6] V. Bužek, S.L. Braunstein, M. Hillery, D. Bruß, Phys. Rev. A 56 (1997) 3446.
[7] N. Gisin, S. Massar, Phys. Rev. Lett. 79 (1997) 2153.
[8] D. Bruß, A. Ekert, C. Macchiavello, Phys. Rev. Lett. 81 (1998) 2598.
[9] R.F. Werner, Phys. Rev. A 58 (1998) 1827.
[10] M. Keyl, R.F. Werner, J. Math. Phys. 40 (1999) 3283.
[11] V. Bužek, M. Hillery, Phys. Rev. Lett. 81 (1998) 5003.
[12] C.-S. Niu, R.B. Griffiths, Phys. Rev. A 60 (1999) 2764.
[13] N.J. Cerf, J. Mod. Opt. 47 (2000) 187.
[14] M. Hillery, V. Bužek, Phys. Rev. A 56 (1997) 1212.
[15] D. Bruß, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello, J.A. Smolin, Phys. Rev. A 57 (1998) 2368.
[16] L.-M. Duan, G.-C. Guo, Phys. Rev. Lett. 80 (1998) 4999.
[17] L.-M. Duan, G.-C. Guo, Phys. Lett. A 243 (1998) 261.
[18] C.-W. Zhang, Z.-Y. Wang, C.-F. Li, G.-C. Guo, Phys. Rev. A 61 (2000) 062310.
[19] A.K. Pati, Phys. Rev. Lett. 83 (1999) 2849.
[20] A. Chefles, S.M. Barnett, Phys. Rev. A 60 (1999) 136.
[21] S. Massar, S. Popescu, Phys. Rev. Lett. 74 (1995) 1259.
[22] R. Derka, V. Bužek, A. Ekert, Phys. Rev. Lett. 80 (1998) 1571.
[23] C.-W. Zhang, C.-F. Li, G.-C. Guo, Phys. Lett. A 261 (1999) 25.
[24] R. Jozsa, J. Mod. Opt. 41 (1994) 2315.
[25] R. Schatten, Norm Ideals of Completely Continuous Operators, Springer, Berlin, 1960.
[26] C.H. Bennett, Phys. Rev. Lett. 68 (1997) 3121.