

Asymptotic Quantum Cloning Is State Estimation

Joonwoo Bae and Antonio Acín

ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
(Received 15 March 2006; published 19 July 2006)

The impossibility of perfect cloning and state estimation are two fundamental results in quantum mechanics. It has been conjectured that quantum cloning becomes equivalent to state estimation in the asymptotic regime where the number of clones tends to infinity. We prove this conjecture using two known results of quantum information theory: the monogamy of quantum correlations and the properties of entanglement breaking channels.

DOI: 10.1103/PhysRevLett.97.030402

PACS numbers: 03.65.-w, 03.67.-a

The impossibility of perfect state estimation is a major consequence of the nonorthogonality of quantum states: The state of a single quantum system cannot be perfectly measured. In other words, a measurement on a system in order to acquire information on its quantum state perturbs the system itself. The full reconstruction of the state is possible only by computing statistical averages of different observables on a large number of identically prepared systems. Thus, any measurement at the single-copy level provides only partial information.

The fact that state estimation is, in general, imperfect leads in a natural way to the problem of building *optimal measurements*. A perfect reconstruction being impossible, it is relevant to find the measurement strategy that maximizes the gain of information about the unknown state. A standard approach to this problem in quantum information theory (QIT) is to quantify the quality of a measurement by means of the so-called *fidelity* [1]. This quantity is defined as follows. Consider the situation in which a quantum state $|\psi\rangle$ is chosen from the ensemble $\{p_i, |\psi_i\rangle\}$; i.e., $|\psi\rangle$ can be equal to $|\psi_i\rangle$ with probability p_i . A measurement, defined by N_M positive operators $M_j \geq 0$, summing up to the identity $\sum_j M_j = 1$, is applied on this unknown state. For each obtained outcome j , a guess $|\phi_j\rangle$ for the input state is made. The overlap between the guessed state and the input state $|\langle\psi_i|\phi_j\rangle|^2$ quantifies the quality of the estimation process. The averaged fidelity of the measurement then reads

$$\bar{F}_M = \sum_{i,j} p_i \text{tr}(M_j |\psi_i\rangle\langle\psi_i|) |\langle\psi_i|\phi_j\rangle|^2. \quad (1)$$

A measurement is optimal according to the fidelity criterion when it provides the largest possible value of \bar{F}_M , denoted in what follows by F_M .

The no-cloning theorem [2], one of the cornerstones of QIT [3], represents another known consequence of the nonorthogonality of quantum states. It proves that, given a quantum system in an unknown state $|\psi\rangle$, it is impossible to design a device producing two identical copies $|\psi\rangle|\psi\rangle$. Indeed, two nonorthogonal quantum states suffice to prove the no-cloning theorem.

As happens for state estimation, the impossibility of perfect cloning leads to the characterization of *optimal cloning machines* [4]. In this case, one looks for the quantum map \mathcal{L} that, given a state $|\psi\rangle$ chosen from an ensemble $\{p_i, |\psi_i\rangle\}$ in \mathbb{C}^d , produces a state $\mathcal{L}(\psi) = \rho_{C_1 \dots C_N}$ in $(\mathbb{C}^d)^{\otimes N}$, such that each individual clone $\rho_{C_k} = \text{tr}_{\bar{k}}(\rho_{C_1 \dots C_N})$ resembles as much as possible the input state. Here \bar{k} denotes the complement of k , so $\text{tr}_{\bar{k}}$ is the trace with respect to all the systems C_i but C_k . The average fidelity of the cloning process is then

$$\bar{F}_C(N) = \sum_{i,k} p_i \frac{1}{N} \langle\psi_i|\text{tr}_{\bar{k}} \mathcal{L}(\psi_i)|\psi_i\rangle. \quad (2)$$

The goal of the optimal machine is to maximize this quantity, this optimal value being denoted by $F_C(N)$.

One can easily realize that the no-cloning theorem and the impossibility of perfect state estimation are closely related. On the one hand, if perfect state estimation were possible, one could use it to prepare any number of clones of a given state, just by measurement and preparation. On the other hand, if perfect cloning were possible, one could perfectly estimate the unknown state of a quantum system by preparing infinite clones of it and then measuring them. Beyond these qualitative arguments, the connection between state estimation and cloning was strengthened in Refs. [5,6]. The results of these works suggested that asymptotic cloning, i.e., the optimal cloning process when $N \rightarrow \infty$, is equivalent to state estimation, in the sense that, for any ensemble of states,

$$F_C = F_C(N \rightarrow \infty) = F_M. \quad (3)$$

Actually, this equality was proven in Ref. [6] for the case of universal cloning, that is, when the initial ensemble consists of a randomly chosen pure state in \mathbb{C}^d , under the assumption that the output of the cloning machine is supported on the symmetric subspace. Later, it was shown in Ref. [7] that this assumption does not imply any loss of optimality, so the equality of the two fidelities for universal cloning and state estimation followed. This equivalence has also been proven for phase covariant qubit cloning [8], where the initial ensemble corresponds to a state in \mathbb{C}^2

lying on one of the equators of the Bloch sphere. Since then, the validity of this equality for any ensemble has been conjectured and, indeed, has been identified as one of the open problems in QIT [9].

In this work, we show that the fidelities of optimal asymptotic cloning and of state estimation are indeed equal for any initial ensemble of pure states. Actually, we prove that asymptotic cloning does effectively correspond to state estimation, from which the equality of the two fidelities automatically follows. The proof of this equivalence is based on two known results of QIT: the monogamy of quantum correlations and the properties of the so-called entanglement breaking channels (EBC).

It is easy to prove that $F_M \leq F_C$. Indeed, given the initial state $|\psi\rangle$, a possible asymptotic cloning map, not necessarily optimal, consists of first applying state estimation and then preparing infinite copies of the guessed state. It is sometimes said that the opposite has to be true since “asymptotic cloning cannot represent a way of circumventing optimal state estimation.” As already mentioned in Ref. [9], this reasoning is too naive, since it neglects the role correlations play in state estimation. For instance, take the simplest case of universal cloning of a qubit, i.e., a state in \mathbb{C}^2 isotropically distributed over the Bloch sphere. The optimal cloning machine produces N approximate clones pointing in the same direction in the Bloch sphere as the input state, but with a shrunk Bloch vector [7]. If the output of the asymptotic cloning machine were in a product form, it would be possible to perfectly estimate the direction of the local Bloch vector, whatever the shrinking was. Then a perfect estimation of the initial state would be possible. And, of course, after the perfect estimation, one could prepare an infinite number of perfect clones. This simple reasoning shows that the correlations between the clones play an important role in the discussion. Actually, it has recently been shown that the correlations present in the output of the universal cloning machine are the worst for the estimation of the reduced density matrix [10].

As announced, the proof of the conjecture is based on two known results of QIT: the monogamy of entanglement and the properties of EBC. For the sake of completeness, we state here these results, without proof.

Quantum correlations, or entanglement, represent a monogamous resource, in the sense that they cannot be arbitrarily shared. One of the strongest results in this direction was obtained by Werner in 1989 [11]. There, it was shown that the only states that can be arbitrarily shared are the separable ones. Recall that a bipartite quantum state ρ_{AC} in $\mathbb{C}^d \otimes \mathbb{C}^d$ is said to be N -shareable when it is possible to find a quantum state $\rho_{AC_1 \dots C_N}$ in $\mathbb{C}^d \otimes (\mathbb{C}^d)^{\otimes N}$ such that $\rho_{AC_k} = \text{tr}_{\bar{k}} \rho_{AC_1 \dots C_N} = \rho_{AC}$, $\forall k$. The state $\rho_{AC_1 \dots C_N}$ is then said to be an N extension of ρ_{AC} . The initial correlations between subsystems A and C are now shared between A and each of the N subsystems C_i ; see Fig. 1. It is straightforward to see that

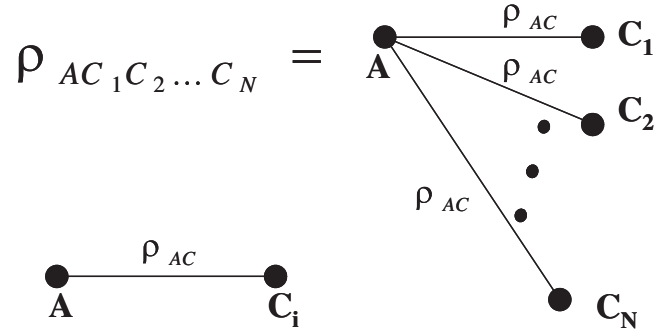


FIG. 1. The state ρ_{AC} is said to be N -shareable when there exists a global state $\rho_{AC_1 \dots C_N}$ such that the local state shared between A and C_i is equal to ρ_{AC} , for all i .

$$\rho_{AC_1 \dots C_N} = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|^{\otimes N} \quad (4)$$

gives a valid N extension of a separable state $\rho_{AC}^s = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|$ for all N . As proven by Werner, if a state ρ_{AC} is entangled, there exists a finite number $N(\rho_{AC})$ such that no valid extension can be found.

The second ingredient needed in what follows are the properties of EBC. A channel \mathcal{Y} is said to be entanglement breaking when it cannot be used to distribute entanglement. In Ref. [12], it was proven that the following three statements are equivalent: (i) \mathcal{Y} is entanglement breaking, (ii) \mathcal{Y} can be written in the form

$$\mathcal{Y}(\rho) = \sum_j \text{tr}(M_j \rho) \rho_j, \quad (5)$$

where ρ_j are quantum states and $\{M_j\}$ defines a measurement, and (iii) $(1 \otimes \mathcal{Y})|\Phi^+\rangle$ is a separable state, where $|\Phi^+\rangle = \sum_i |ii\rangle/\sqrt{d}$ is a maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$. The equivalence of (i) and (ii) simply means that any EBC can be understood as the measurement of the input state ρ , followed by the preparation of a new state ρ_j depending on the obtained outcome. The equivalence of (i) and (iii) reflects that the intuitive strategy for entanglement distribution where half of a maximally entangled state is sent through the channel is enough to detect if \mathcal{Y} is entanglement breaking.

After collecting all these results, we are now ready to prove the following.

Theorem.—Asymptotic cloning corresponds to state estimation. Thus, $F_M = F_C$ for any ensemble of states.

Proof.—First of all, note that, for any number of clones, we can restrict our considerations to symmetric cloning machines \mathcal{L}_N^s , where the N clones are all in the same state. Indeed, given a machine where this is not the case, one can construct a symmetric machine achieving the same fidelity $F_C(N)$, just by making a convex combination of all the permutations of the N clones [13]. Now denote by \mathcal{L}_N^c the effective cloning map consisting of, first, the application of a symmetric machine \mathcal{L}_N^s and then tracing all but one of the

clones, say the first one. The N -cloning problem can be rephrased as [see Eq. (2)]

$$\max_{\mathcal{L}_N^c} \sum_i p_i \langle \psi_i | \mathcal{L}_N^c(\psi_i) | \psi_i \rangle. \quad (6)$$

Note that this maximization runs over all channels that can be written as $\mathcal{L}_N^c = \text{tr}_1 \mathcal{L}_N^s$. For instance, the identity map, where $\psi \rightarrow \psi$, $\forall \psi$, does not satisfy this constraint. Denote by L_N the set of these channels. These are convex sets such that $L_N \supseteq L_{N+1} \supseteq \dots \supseteq L_\infty$. The key point of the proof is to show that all the channels in L_∞ , and therefore all the channels associated to asymptotic cloning machines, are EBC. To prove this result, we proceed by contradiction.

First, note that any EBC belongs to L_∞ . Assume now there is a channel $\mathcal{L}_\infty^c \in L_\infty$ which is not EBC, i.e., such that the state

$$\rho_{AC} = (1 \otimes \mathcal{L}_\infty^c) |\Phi^+\rangle \quad (7)$$

is entangled. Since $L_N \supseteq L_\infty$ for all N , \mathcal{L}_∞^c is an element of all these sets. Thus, for any finite N , there exists a symmetric channel \mathcal{L}_N^s such that

$$\rho_{AC_{1\dots C_N}} = (1 \otimes \mathcal{L}_N^s) |\Phi^+\rangle \quad (8)$$

is a valid N extension of the entangled state ρ_{AC} of Eq. (7). But this is in contradiction with the nonshareability of entangled states. Thus, all the channels in L_∞ have to be EBC. Since any EBC can be seen as measurement followed by state preparation, asymptotic quantum cloning, i.e., Eq. (6) in the limit $N \rightarrow \infty$, can be written as [14]

$$\max_{\{M_j, \phi_j\}} \sum_{i,j} p_i \text{tr}(M_j |\psi_i\rangle \langle \psi_i|) |\langle \psi_i | \phi_j \rangle|^2, \quad (9)$$

which defines the optimal state estimation problem. Therefore, $F_M = F_C$ for any ensemble of states. \square

The same argument applies to the case in which K copies of the initial state $|\psi\rangle$ are given. The measurement and cloning fidelities now read [see Eqs. (1) and (2)]

$$\begin{aligned} \bar{F}_M(L) &= \sum_{i,j} p_i \text{tr}(M_j |\psi_i\rangle \langle \psi_i|^{\otimes K}) |\langle \psi_i | \phi_j \rangle|^2 \bar{F}_C(N, K) \\ &= \sum_{i,k} p_i \frac{1}{N} \langle \psi_i | \text{tr}_k \mathcal{L}(\psi_i^{\otimes K}) | \psi_i \rangle. \end{aligned} \quad (10)$$

Using the same ideas as in the previous theorem, it is straightforward to prove that

$$F_M(K) = F_C(N \rightarrow \infty, K), \quad (11)$$

where $F_M(K)$ and $F_C(N, K)$ denote the optimal values of $\bar{F}_M(K)$ and $\bar{F}_C(N, K)$, as above.

One can also extend this result to asymmetric scenarios. An asymmetric cloning machine [15] produces N_A clones of fidelity $F_C(N_A)$ and N_B clones of fidelity $F_C(N_B)$ of a state chosen from an ensemble $\{p_i, |\psi_i\rangle\}$, the total number of clones being $N = N_A + N_B$. The machine is optimal when it gives the largest $F_C(N_A)$ for fixed $F_C(N_B)$. Extending the previous formalism, this optimal fidelity is

then

$$F_C(N_A) = \max_{\mathcal{L}_{N_A, N_B}} \sum_i p_i \langle \psi_i | \text{tr}_1 \mathcal{L}_{N_A, N_B}(\psi_i) | \psi_i \rangle, \quad (12)$$

where the maximization now runs over all maps $\mathbb{C}^d \rightarrow (\mathbb{C}^d)^{\otimes N}$, symmetric under permutation among the first N_A clones or among the N_B clones, and such that

$$\sum_i p_i \langle \psi_i | \text{tr}_N \mathcal{L}_{N_A, N_B}(\psi_i) | \psi_i \rangle = F_C(N_B). \quad (13)$$

In the case of measurement, we are thinking of measurement strategies where the goal is to obtain information on an unknown state introducing the minimal disturbance. As above, we consider that a guess $|\phi_j\rangle$ for the input state is done depending on the measurement outcome j . The information vs disturbance trade-off can be expressed in terms of fidelities [16]: The information gain is given by the overlap G between the initial and the guessed state, while the disturbance is quantified by the overlap F between the state after the measurement and the initial state. The whole process can be seen as a global map \mathcal{M} transforming the initial state into two approximate copies of it: the state left after the measurement and the guessed state. A measurement is optimal when for fixed gain G it provides the minimal disturbance, i.e., the largest overlap F . So, the goal is to solve

$$\max_{\mathcal{M}} \sum_i p_i \langle \psi_i | \text{tr}_2 \mathcal{M}(\psi_i) | \psi_i \rangle, \quad (14)$$

where the maximization is over all channels \mathcal{M} such that $\text{tr}_1 \mathcal{M}$ defines an EBC (5) with $\rho_j = |\phi_j\rangle \langle \phi_j|$ [14] and $\sum_i p_i \langle \psi_i | \text{tr}_1 \mathcal{M}(\psi_i) | \psi_i \rangle = G$. The optimal trade-off between F and G is known only for the case in which the input ensemble consists of any pure state in \mathbb{C}^d with uniform probability [16].

As happens for the symmetric case, a connection between this state estimation problem and asymmetric cloning machines can be expected when $N_A = 1$ and $N_B \rightarrow \infty$. Note that the previous measurement strategy gives a possible realization of an asymmetric cloning machine, not necessarily optimal, when N_B identical copies of the guessed state are prepared. In other words, if $G = F_C(N_B)$, then $F \leq F_C(N_A)$. Actually, this connection is indeed true for the particular case in which the input state is any pure state in \mathbb{C}^2 , isotropically distributed on the Bloch sphere: The optimal measurement strategy of Ref. [16] turns out to saturate the optimal cloning $1 \rightarrow N_A + N_B$ fidelities of Ref. [17], when $N_A = 1$ and $N_B \rightarrow \infty$. Now the equality between the measurement and asymptotic cloning fidelities in the asymmetric scenario can be proven in full generality exploiting the same arguments as above. Using the monogamy of entangled states, one can see that the channels (13), defining the $N_B \rightarrow \infty$ clones, must be EBC. This means that the set of maps \mathcal{L}_{1, N_B} and \mathcal{M} corresponding to asymmetric $1 \rightarrow 1 + N_B$ cloning ma-

chines and asymmetric measurement strategies [see Eqs. (12) and (14)] coincide when $N_B \rightarrow \infty$. Therefore, the two corresponding fidelities have to be equal.

From a more speculative point of view, there exist several works relating the impossibility of perfect cloning to the no-signaling principle, e.g. Ref. [18]. Most of these works, however, study the relation between these two principles inside the quantum formalism. Recently, a form of no-cloning theorem has been derived just from the no-signaling principle, without invoking any additional quantum feature [19]. In view of the strong connection between cloning and state estimation, it would be interesting to study whether a similar link could also be established between the no-signaling principle and the impossibility of perfect state estimation, without exploiting any intrinsically quantum property such as nonorthogonality.

To conclude, this work proves the long-standing conjecture on the equivalence between asymptotic cloning and state estimation. It represents the strongest link between two fundamental no-go theorems of quantum mechanics, namely, the impossibilities of perfect cloning and state estimation.

We thank Emili Bagan, John Calsamiglia, Sofyan Iblisdir, and Ramon Muñoz-Tapia for discussion. This work is supported by the Spanish MCyT, under a ‘‘Ramón y Cajal’’ grant, and the Generalitat de Catalunya, Grant No. 2006FIR-000082.

-
- [1] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
- [2] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982).
- [3] Two independent reviews on the no-cloning theorem have recently appeared: V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005); N.J. Cerf and J. Fiurášek, quant-ph/0512172.
- [4] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
- [5] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
- [6] D. Bruß, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
- [7] M. Keyl and R.F. Werner, J. Math. Phys. (N.Y.) **40**, 3283 (1999).
- [8] D. Bruß, M. Cinchetti, G.M. D’Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
- [9] See problem 22 in <http://www.imaph.tu-bs.de/qi/problems/>.
- [10] R. Demkowicz-Dobrzanski, Phys. Rev. A **71**, 062321 (2005).
- [11] R.F. Werner, Lett. Math. Phys. **17**, 359 (1989); another, and somehow extended, proof of this result can also be found in A.C. Doherty, P.A. Parrilo, and F.M. Spedalieri, Phys. Rev. A **69**, 022308 (2004); recently, a beautifully simple proof of the same result has been given in D. Yang, quant-ph/0604168.
- [12] M. Horodecki, P.W. Shor, and M.B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).
- [13] Notice that this does not mean that the output of the cloning machine lives in the symmetric subspace.
- [14] We can already restrict the guessed states to be pure, without any loss of optimality.
- [15] C.-S. Niu and R.B. Griffiths, Phys. Rev. A **58**, 4377 (1998); N.J. Cerf, Acta Phys. Slovaca **48**, 115 (1998); V. Bužek, M. Hillery, and M. Bendik, *ibid.* **48**, 177 (1998); N.J. Cerf, J. Mod. Opt. **47**, 187 (2000).
- [16] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).
- [17] S. Iblisdir, A. Acín, N.J. Cerf, J. Fiurášek, R. Filip, and N. Gisin, Phys. Rev. A **72**, 042328 (2005).
- [18] N. Gisin, Phys. Lett. A **242**, 1 (1998).
- [19] Ll. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006); J. Barrett, quant-ph/0508211.