Optimal universal quantum cloning and state estimation

Dagmar Bruß[1], Artur Ekert[2], Chiara Macchiavello[3,1]
[1] *ISI, Villa Gualino, Viale Settimio Severo 65, 10133 Torino, Italy*
[2] *Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, UK*
[3] *Dipartimento di Fisica "A. Volta" and I.N.F.M., Via Bassi 6, 27100 Pavia, Italy*
(Received February 1, 2008)

We derive a tight upper bound for the fidelity of a universal $N \to M$ qubit cloner, valid for any $M \geq N$, where the output of the cloner is required to be supported on the symmetric subspace. Our proof is based on the concatenation of two cloners and the connection between quantum cloning and quantum state estimation. We generalise the operation of a quantum cloner to mixed and/or entangled input qubits described by a density matrix supported on the symmetric subspace of the constituent qubits. We also extend the validity of optimal state estimation methods to inputs of this kind.

03.65.Bz, 03.67.-a

Perfect quantum cloning is impossible [1]. This notwithstanding, we may ask how well we can clone quantum states. Bužek and Hillery, who were the first to address this problem, provided an example of a quantum device which can clone an unknown pure state of a single input qubit (a two-state system) into two output qubits, albeit with a certain fidelity smaller than one [2]. Their construction was subsequently shown to be optimal by Bruß *et al.* [3]. In this letter we derive the optimal fidelity of a universal and symmetric quantum cloning machine (QCM) which acts on N original qubits and generates M clones.

A universal $N \to M$ quantum cloner is a quantum machine which performs a prescribed unitary transformation on an extended input which contains N original qubits, $M-N$ "blank" qubits and K auxiliary qubits, and which outputs M clones together with the K auxiliary qubits. The original qubits are all in the same (unknown and pure) quantum state described by the density operator $\varrho^{in} = \frac{1}{2}(\mathbb{1} + \vec{s}^{\,in} \cdot \vec{\sigma})$, where $\vec{s}^{\,in}$ is the original Bloch vector. Both "blanks" and the auxiliary qubits are initially in some prescribed quantum state. The output qubits are in an entangled state and in the present work we require that the density operator describing the state of the M clones is supported on the symmetric subspace. This guarantees that all the output qubits are indistinguishable and in the same state described by the reduced density operator ϱ^{out}. We comment on relaxing this assumption at the end of the paper.

It has been shown that *universal* $1 \to 2$ cloners can only shrink the original Bloch vector, without changing its orientation in the Bloch sphere [3]. The same argument as given in [3] (namely the impossibility to find a transformation that rotates *any* Bloch vector of the 1-particle reduced density matrix by the same angle) applies also generally for an $N \to M$ qubit cloner. Therefore, the operation of a universal QCM can be characterised by the shrinking factor $\eta(N,M)$, which is also known in the literature as the Black Cow factor [4], and the reduced output density operator is of the form $\varrho^{out} = \frac{1}{2}(\mathbb{1} + \eta(N,M)\vec{s}^{\,in} \cdot \vec{\sigma})$. Universal $N \to M$ quantum cloning machines may be constructed in many different ways, the best constructions are those which maximize $\eta(N,M)$ (i.e. which maximize the fidelity of the cloning machine) and we refer to them as the optimal cloners.

Gisin and Massar have constructed a class of universal $N \to M$ QCMs and showed, using numerical methods, that for $N \leq 7$ their cloners are optimal [5]. Our derivation of the upper bound for $\eta(N,M)$ is quite general and does not refer to any specific realisation of the universal cloning machines. In particular it shows that the Gisin-Massar cloners saturate this bound for any N and $M \geq N$. Our approach avoids an elaborate optimisation procedure, extends the class of allowed inputs to mixed and/or entangled states of the original qubits which belong to the symmetric subspace and sheds some light on the connection between optimal quantum cloning and optimal quantum state estimation. The proof is based on the concatenation of two quantum cloners and on associating the upper bound on the fidelity of an $M \to \infty$ cloner with the fidelity of the optimal state estimation of M qubits, given in [6].

We concatenate two cloning machines in the following way. The first cloner is an $N \to M$ universal machine characterised by the shrinking factor $\eta(N,M)$. The M clones from the output of the first cloner are then taken as originals for the input into the second cloning machine which creates infinitely many clones with the shrinking factor $\eta(M,\infty)$. We now write down two statements which will be proved after unfolding the main result:

a) The shrinking factors for concatenated cloners multiply.

b) The equality

$$\eta^{opt}_{QCM}(M,\infty) = \bar{\eta}^{opt}_{meas}(M) \tag{1}$$

holds. Here $\bar{\eta}^{opt}_{meas}(M)$ corresponds to the optimal state estimation derived in [6], and its meaning will be explained below.

Due to statement a), the shrinking factors of universal cloning machines in sequence multiply. Moreover, the sequence of the two machines cannot perform better than the optimal $N \to \infty$ universal cloner, otherwise the $N \to \infty$ universal cloner would not be optimal. Thus we arrive at the following inequality:

$$\eta_{QCM}(N,M) \cdot \eta_{QCM}(M,\infty) \leq \eta^{opt}_{QCM}(N,\infty) \quad . \tag{2}$$

This means that the lowest upper bound for the general $N \to M$ cloner is given by

$$\eta_{QCM}(N,M) \leq \frac{\eta^{opt}_{QCM}(N,\infty)}{\eta^{opt}_{QCM}(M,\infty)} \quad . \tag{3}$$

We have thus reduced the optimality problem of the $N \to M$ cloner to the task of finding the optimal $N \to \infty$ cloner.

Now we can use statement b) and the explicit form of $\bar{\eta}^{opt}_{meas}(M)$ (see [6]), namely

$$\bar{\eta}^{opt}_{meas}(M) = \frac{M}{M+2} \tag{4}$$

to conclude the central result that for any $M \geq N$

$$\eta^{opt}_{QCM}(N,M) = \frac{N}{M}\frac{M+2}{N+2} \ . \tag{5}$$

For pure input states this corresponds to the optimal fidelity

$$F^{opt}_{QCM}(N,M) = \frac{NM+N+M}{M(N+2)} \quad , \tag{6}$$

which is achieved by the cloning transformations proposed in [5]. (For $\varrho^{in} = |\psi\rangle\langle\psi|$ the fidelity is defined as $F = \langle\psi|\varrho^{out}|\psi\rangle$.)

Let us note in passing that as the consequence of the factorisation property (3) we can produce M clones from N originals either by applying directly the optimal $N \to M$ cloner or by taking any number of intermediate steps in order to realise the cloning process, using the optimal transformation at each step; both ways lead to the same overall shrinking factor.

Let us now justify statements a) and b).

In order to prove a) we describe an $N \to M$ cloner in terms of a completely positive map C_{NM} which maps input density operators of N identical pure originals into output density operators of M clones, such that for any state $|\psi\rangle\langle\psi|$ of a single input qubit (original) we have

$$\mathrm{Tr}_{M-1}[C_{NM}(|\psi\rangle\langle\psi|^{\otimes N})] = \eta(N,M)|\psi\rangle\langle\psi| + (1-\eta(N,M))\frac{1}{2}\mathbb{1} \ , \tag{7}$$

where the trace is performed on any $M-1$ qubits (for an overview of completely positive operators see [7]).

Let ϱ_N be a density operator of N qubits which is supported on the symmetric subspace of the 2^N dimensional Hilbert space. We can always write ϱ_N as a linear combination of direct products of identical pure states, $\varrho_N = \sum_i \alpha_i |\psi_i\rangle\langle\psi_i|^{\otimes N}$, where $\sum_i \alpha_i = 1$; N.B. we do not require that all values α_i are positive [4,8]. The linearity of the completely positive map and its universality, i.e. the fact that $\eta(N,M)$ does not depend on $|\psi\rangle$, allow us to extend Eq.(7) to the more general form

$$\mathrm{Tr}_{M-1}[C_{NM}(\varrho_N)] = \eta(N,M)\varrho + (1-\eta(N,M))\frac{1}{2}\mathbb{1} \tag{8}$$

where $\varrho = \mathrm{Tr}_{N-1}[\varrho_N]$. Now, suppose we concatenate an $N \to M$ and an $M \to L$ cloner and view it as an $N \to L$ cloner. It evolves the initial N qubit state ϱ_N first into the M qubit state $\varrho^{'}_M$ and then into the L qubit state $\varrho^{''}_L$. The corresponding single qubit reduced density operators are ϱ, $\varrho^{'} = \mathrm{Tr}_{M-1}[\varrho^{'}_M]$ and $\varrho^{''} = \mathrm{Tr}_{L-1}[\varrho^{''}_L]$. Following Eq.(8) we can write

$$\varrho^{''} = \eta(M,L)\varrho^{'} + (1-\eta(M,L))\frac{1}{2}\mathbb{1} = \eta(N,M)\cdot\eta(M,L)\varrho + (1-\eta(N,M)\cdot\eta(M,L))\frac{1}{2}\mathbb{1} \tag{9}$$

i.e. indeed $\eta(N,L)=\eta(N,M)\cdot\eta(M,L)$.

We will now prove statement b). Equation (5) was obtained assuming the following result (due to [6]): given M qubits all in an unknown quantum state $|\,\psi\rangle$ there exists a universal POVM measurement $\{P_\mu\}$ [9] which leads to the best possible estimation of $|\,\psi\rangle$ with fidelity $\bar{F}(M)=\frac{M+1}{M+2}$, or, equivalently, with $\bar{\eta}(M)=\frac{M}{M+2}$. The outcome of each instance of the measurement provides, with probability $p_\mu(\psi)=\mathrm{Tr}(P_\mu|\psi\rangle\langle\psi|^{\otimes M})$, the "candidate" $|\,\psi_\mu\rangle$ for $|\,\psi\rangle$. The fidelity $\bar{F}_{meas}(M)$ is then calculated from the outcomes of the measurement as

$$\bar{F}_{meas}(M)=\sum_\mu p_\mu(\psi)|\langle\psi|\psi_\mu\rangle|^2=\langle\psi|\bar{\varrho}|\,\psi\rangle, \tag{10}$$

where $\bar{\varrho}=\sum_\mu p_\mu(\psi)|\psi_\mu\rangle\langle\psi_\mu|$. In the optimal, universal state estimating procedure the fidelity must not depend on ψ, thus $\bar{\varrho}$ can also be written as

$$\bar{\varrho}=\bar{\eta}^{opt}_{meas}(M)|\psi\rangle\langle\psi|+(1-\bar{\eta}^{opt}_{meas}(M))\frac{1}{2}\mathbb{1}. \tag{11}$$

The optimal measurement of this type can be viewed as an $M\to\infty$ cloner because after reading each outcome we can prepare any number of "candidates", in particular infinitely many of them, with the average reconstruction fidelity $\bar{F}^{opt}_{meas}(M)$ with respect to the originals. Clearly this procedure cannot provide a larger shrinking factor than the optimal $M\to L$ cloner and we find

$$\bar{\eta}^{opt}_{meas}(M)\le\eta^{opt}_{QCM}(M,L) \tag{12}$$

for any $L\ge M$, in particular for $L\to\infty$.

Let us now show that for $L\to\infty$ the formula (12) becomes the equality. To see this let us concatenate an $M\to L$ cloner with a subsequent optimal state estimating measurement. The input to the cloner is of the form $|\psi\rangle\langle\psi|^{\otimes M}$ and the output is described by the density operator ϱ_L which is of the form $\sum_i\alpha_i|\psi_i\rangle\langle\psi_i|^{\otimes L}$, where $\sum_i\alpha_i=1$. The reduced density operator of each output qubit is $\varrho=\mathrm{Tr}_{L-1}\varrho_L=\sum_i\alpha_i|\psi_i\rangle\langle\psi_i|=\eta(M,L)|\psi\rangle\langle\psi|+(1-\eta(M,L))\frac{1}{2}\mathbb{1}$. The cloner $M\to L$ concatenated with the state estimation on L qubits can be viewed as the state estimation performed on M qubits. The total procedure gives the fidelity of estimating $|\psi\rangle$ which can be written as

$$\bar{F}_{meas}(M)=\langle\psi|\sum_\mu\mathrm{Tr}(P_\mu\varrho_L)|\psi_\mu\rangle\langle\psi_\mu|\,\psi\rangle=\sum_{\mu,i}\langle\psi|\alpha_i\mathrm{Tr}(P_\mu|\psi_i\rangle\langle\psi_i|^{\otimes L})|\psi_\mu\rangle\langle\psi_\mu|\psi\rangle \tag{13}$$

$$=\sum_i\langle\psi|\alpha_i[\bar{\eta}^{opt}_{meas}(L)|\psi_i\rangle\langle\psi_i|+(1-\bar{\eta}^{opt}_{meas}(L))\frac{1}{2}\mathbb{1}]|\psi\rangle \tag{14}$$

which for $L\to\infty$ becomes (due to $\bar{\eta}^{opt}_{meas}(L)\to 1$)

$$\bar{F}_{meas}(M)\to\sum_i\langle\psi|\alpha_i|\psi_i\rangle\langle\psi_i|\psi\rangle=\langle\psi|\varrho|\psi\rangle=\frac{1}{2}(1+\eta_{QCM}(M,\infty)). \tag{15}$$

The concatenation of a cloner with a measurement cannot perform better than the optimal measurement, thus we can write

$$\eta^{opt}_{QCM}(M,\infty)\le\bar{\eta}^{opt}_{meas}(M)\quad . \tag{16}$$

Combining equations (12) and (16) finally leads to

$$\eta^{opt}_{QCM}(M,\infty)=\bar{\eta}^{opt}_{meas}(M)\quad , \tag{17}$$

thus proving statement b).

Before concluding, we want to stress that, as a consequence of what was shown above, we can extend the operation of a cloning machine and the application of an optimal measurement to any input density operator of N qubits which has support on the symmetric subspace. The properties of the universal cloning machine as defined at the beginning of this paper allow us to conclude that the same machine can operate on *any* such symmetric density operator and shrinks the Bloch vector of the reduced input density matrix by a fixed amount, independent of the initial length. Notice also that the optimal machine, for products of pure inputs specified by the shrinking factor (5), is still optimal for this extended class of inputs. Actually, if a better cloning machine existed for mixed input states, we would use it as the second cloner $M \to \infty$ in Eq. (2), giving a smaller lower bound in Eq. (3). This would lead to a contradiction because we already know that universal cloners for pure states saturating the bound (5) exist [5].

One may want to relax our restriction and consider quantum cloners which produce identical clones (i.e. with the same single-qubit density operator ϱ^{out}), but for which the state of all outputs does not belong to the symmetric subspace. This case, in principle, may provide a higher shrinking factor, however, we could neither prove nor disprove this with our approach. We leave this problem as a challenge to other colleagues.

In a similar way as for the cloner we can extend the validity of an optimal universal measurement procedure to inputs from the symmetric subspace. In this case the goal is to find the optimal measurement for the reduced density operator for each input copy. Since we require the process to be universal, we know that the reduced density operator reconstructed as the result of the measurement given in Eq. (11) is just the shrunk version of the initial one. We can then describe the quality of the procedure in terms of the shrinking factor. We conclude that the optimal measurement derived in Ref. [6] is also optimal for any input symmetric state. Actually, if this were not the case, we could devise a measurement procedure on N initial pure qubits by first applying an $N \to M$ cloner and then an optimal measurement on the mixed state of the output M clones. If this global measurement were better than the optimal one of Ref. [6] we would then obtain with the above procedure a universal measurement for pure states which performs better than the one in Ref. [6], thus finding a contradiction.

Let us mention in passing that in our discussion we found it convenient to use the shrinking factor, because it has an intuitive geometrical meaning both for pure and mixed states, however, one can rephrase the optimality argument for universal operations using, for example, the Uhlmann fidelity [10] for the reduced density operators.

In conclusion, we have derived the optimal shrinking factor/fidelity for a universal $N \to M$ cloner and generalised its operation to a more general case of mixed and/or entangled input states which belong to the symmetric subspace. Furthermore we have established the connection between optimal quantum state estimation and optimal quantum cloning which allowed us to extend the validity of the optimal state estimation methods [6] to inputs of the above form.

We would like to express our special thanks to J. I. Cirac, who helped us to clarify the ideas presented in the paper.

It is a pleasure to thank C.H. Bennett, V. Bužek, D. DiVincenzo, N. Gisin, M. Palma, S. Popescu and R. Werner for helpful discussions. We acknowledge support from the Black Cow Café, which provided an excellent working environment for numerous discussions on quantum cloning.

This work was supported in part by the European TMR Research Network ERP-4061PL95-1412, Hewlett-Packard, The Royal Society of London and Elsag-Bailey, a Finmeccanica Company.

---

[1] W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).
[2] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[3] D. Bruß, D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello and J. Smolin, Phys. Rev. A **57**, 2368 (1998).
[4] R.Werner, quant-ph/9804001.
[5] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[6] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[7] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).
[8] A. Sanpera, R. Tarrach and G. Vidal, quant-ph/9801024.
[9] It was shown that the optimal measurements of Ref. [6] can be realised by a finite set of operators P_μ by R. Derka, V. Buzek, A. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).
[10] The Uhlmann fidelity is a good definition of fidelity for mixed states. See A. Uhlmann, Rep. Math. Phys.. **9**, 273 (1976)