

Optimal universal quantum cloning and state estimation

Dagmar Bruß¹, Artur Ekert², Chiara Macchiavello^{3,1}

¹ISI, Villa Gualino, Viale Settimio Severo 65, 10133 Torino, Italy

²Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, UK

³Dipartimento di Fisica “A. Volta”, INFN, Via Bassi 6, 27100 Pavia, Italy

(Received December 9, 1997)

We derive an upper bound for the fidelity of a universal $N \rightarrow M$ qubit cloner, valid for any $M \geq N$. 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 which is invariant under any permutation 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

Ideal quantum cloning does not exist [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, with a certain fidelity smaller than one, an unknown pure state of a single input qubit (a two-state system) into two output qubits [2]. Their construction was subsequently shown to be optimal [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 $N \rightarrow M$ 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 $\rho^{in} = \frac{1}{2}(\mathbf{1} + \vec{s}^{in} \cdot \vec{\sigma})$, 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, however, we require that each out of the M clones is in the same quantum state described by the reduced density operator ρ^{out} . It has been shown that all *universal* cloners can only shrink the original Bloch vector, without changing its orientation in the Bloch sphere [3]. Therefore, the operation of a universal QCM can be characterised by the shrinking factor $\eta(N, M)$, and the reduced output density operator is of the form $\rho^{out} = \frac{1}{2}(\mathbf{1} + \eta(N, M)\vec{s}^{in} \cdot \vec{\sigma})$. Universal $N \rightarrow M$ 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 $N \rightarrow M$ QCMs and showed that for $N \leq 7$ their cloners are optimal [4]. Our derivation of the upper bound for $\eta(N, M)$ is quite general and does not refer to any particular 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 are invariant under any permutation and sheds some light on the connection between optimal quantum cloning and optimal quantum measurement. The proof is based on the concatenation of two quantum cloners and on associating the upper bound on the fidelity of an $M \rightarrow \infty$ cloner with the fidelity of the optimal state estimation of M qubits, given in [5].

We concatenate two cloning machines in the following way. The first cloner is an $N \rightarrow M$ 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 will now write down four statements which will be proved after unfolding the main result:

- a) The output of an optimal cloning machine can always be chosen to be invariant under any permutation of the states, or, in other words: symmetrisation of the output does not change the shrinking factor.
- b) The optimal shrinking factor is the same for the class of inputs that have the same one particle reduced density operators and are invariant under all possible permutations of the qubits. This statement holds for any universal operation on the input density matrix, i.e. also for a measurement process.
- c) The shrinking factors for concatenated symmetrised cloners multiply.
- d) The equality

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

holds. Here $\bar{\eta}_{meas}^{opt}(M)$ corresponds to the optimal state estimation derived in [5], and its meaning will be explained below.

According to statement a) we can focus our attention on an optimal machine which produces a symmetric output in the first step. Such machine is characterised by the optimal shrinking factor $\eta(N, M)$ which is the same as for an optimal machine which is not symmetrised. We can then use statement b), i.e. the fact that any symmetrised input for the second cloner leads to the same shrinking factor $\eta(M, \infty)$. Due to statement c), the shrinking factors of universal cloning machines in sequence multiply. Moreover, the sequence of the two machines can not perform better than the optimal $N \rightarrow \infty$ universal cloner, otherwise the $N \rightarrow \infty$ universal cloner would not be optimal. Thus we arrive at the following inequality:

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

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

$$\eta_{QCM}^{opt}(N, M) = \frac{\eta_{QCM}^{opt}(N, \infty)}{\eta_{QCM}^{opt}(M, \infty)} \quad . \quad (3)$$

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

Now we can use statement d) and the explicit form of $\bar{\eta}_{meas}^{opt}(M)$ (see [5]), namely

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

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

$$\eta_{QCM}^{opt}(N, M) = \frac{N}{M} \frac{M+2}{N+2} \quad . \quad (5)$$

For pure input states this corresponds to the optimal fidelity

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

which is achieved by the cloning transformations proposed in [4]. (For $\rho^{in} = |\psi\rangle\langle\psi|$ the fidelity is defined as $F = \langle\psi|\rho^{out}|\psi\rangle$.)

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 $N \rightarrow M$ 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.

In the following we will justify statements a) to d).

In order to prove statement a) we need to show that we can always restrict our attention to a universal cloning machine which generates symmetrised states. Following the symmetrisation argument proposed by Cirac and Gisin [6], we notice that the total density matrix of the outputs of a cloning machine can always be symmetrised in the following way: let us assume that there exist qubits i and j for which $\rho_{i\dots j\dots}^{out} \neq \rho_{\dots j\dots i\dots}^{out}$, namely the output density operator is not invariant under the exchange of the two qubits. By definition of the cloner, the one particle reduced density operators still have to be identical. We can then make use of an additional ancilla bit in state $|\psi_a\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ such that for the ancilla being $|0\rangle$ the output will be $\varrho_{\dots i\dots j\dots}^{out}$ and for the ancilla being $|1\rangle$ the output will be $\varrho_{\dots j\dots i\dots}^{out}$. Thus after tracing over this ancilla the output is symmetric under exchange of i and j . The shrinking factor η is not affected by this procedure. Therefore an optimal $N \rightarrow M$ cloning machine can always be constructed such that the output density matrix of the M qubits is invariant under any permutation of qubits.

To justify statements b) and c) we need to show that *any* input state of the original qubits described by a density matrix which remains invariant under any permutation of the qubits will be transformed according to the *same* optimal shrinking factor. This basically follows from the universality and linearity of the cloning transformation, however, the direct calculations, as presented below, bring some additional insights.

Let us consider the evolution of the original and blank qubits (without auxiliary qubits) described by a completely positive map [7]. In this description the output state of the M qubits is given by

$$\varrho^{out} = \sum_k A_k \varrho^{in} A_k^\dagger \quad , \quad (7)$$

where the operators A_k satisfy

$$\sum_k A_k^\dagger A_k = \mathbf{1} . \quad (8)$$

In the following the density matrix of the N original qubits is denoted as $\varrho^{N,in}$ and the one for the $M - N$ blank qubits as $\varrho^{(M-N),in}$, so that the input state is

$$\varrho^{in} = \varrho^{N,in} \otimes \varrho^{(M-N),in} . \quad (9)$$

The initial state of the $M - N$ blank qubits $\varrho^{(M-N),in}$ can be chosen arbitrarily. We can assume for simplicity that all such qubits are in a pure state and their Bloch vectors point in the z direction, namely

$$\varrho^{(M-N),in} = \frac{1}{2^{(M-N)}} \sum_{i=0}^{M-N} \mathcal{P}[i \cdot \sigma_z, (M - N - i) \cdot \mathbf{1}] , \quad (10)$$

where $\mathcal{P}[i \cdot \sigma_z, (n - i) \cdot \mathbf{1}]$ represents a sum of all terms which contain a direct product of σ_z in i locations and $\mathbf{1}$ in $n - i$ locations.

Let us now consider different directions of the Bloch vector of the original N qubits and then impose the universality requirement. First, we take as the input a product of N pure states with

$$\vec{s}^{in} = (0, 0, 1) , \quad (11)$$

i.e. an initial density operator is of the form

$$\varrho^{N,in} = \frac{1}{2^N} \sum_{i=0}^N \mathcal{P}[i \cdot \sigma_z, (N - i) \cdot \mathbf{1}] . \quad (12)$$

We can then conveniently (for our purposes) write the input density operator of the M qubits as

$$\varrho^{in} = \frac{1}{2^M} \{ \mathcal{P}[0 \cdot \sigma_z, M \cdot \mathbf{1}] + \sum_{i=0}^N \sum_{j=0}^{M-N} (1 - \delta_{i0} \delta_{j0}) \mathcal{P}[i \cdot \sigma_z, (N - i) \cdot \mathbf{1}] \otimes \mathcal{P}[j \cdot \sigma_z, (M - N - j) \cdot \mathbf{1}] \} . \quad (13)$$

The cloning machine then performs the following transformation

$$\sum_k A_k \varrho^{in} A_k^\dagger = \frac{1}{2^M} \{ \mathcal{P}[0 \cdot \sigma_z, M \cdot \mathbf{1}] + \eta(N, M) \mathcal{P}[\sigma_z, (M - 1) \cdot \mathbf{1}] + R_z(\sigma^2) \} . \quad (14)$$

Here $R_z(\sigma^2)$ is a short-hand notation for terms which have $\sigma_x, \sigma_y, \sigma_z$ in at least two locations. Since $\text{Tr}[\sigma_i] = 0$, these terms do not contribute to the density operator of a single qubit.

Analogously, by taking the Bloch vectors of the N original qubits to be unit vectors along the x -direction and $M - N$ blank qubits in state (10), due to the universality condition, we obtain the right hand side of equation (14) with z replaced by x . The same also holds for the y -direction.

Let us now consider as input a direct product of N states with

$$\vec{s}^{in} = (\cos \alpha, 0, \sin \alpha) . \quad (15)$$

The initial product state can then be written in the compact form:

$$\varrho^{N,in} = \frac{1}{2^N} \sum_{i=0}^N \sum_{j=0}^i (\cos \alpha)^{i-j} (\sin \alpha)^j \mathcal{P}[(i - j) \cdot \sigma_x, j \cdot \sigma_z, (N - i) \cdot \mathbf{1}] . \quad (16)$$

For our purposes we rewrite this in a more convenient way by collecting the terms corresponding only to the x and the z component of the Bloch vector:

$$\begin{aligned}
\rho^{N,in} &= \frac{1}{2^N} \{ \mathcal{P}[0 \cdot \sigma_x, 0 \cdot \sigma_z, N \cdot \mathbf{1}] + \cos \alpha \sum_{i=1}^N \mathcal{P}[i \cdot \sigma_x, 0 \cdot \sigma_z, (N-i) \cdot \mathbf{1}] \\
&\quad + \sin \alpha \sum_{i=1}^N \mathcal{P}[0 \cdot \sigma_x, i \cdot \sigma_z, (N-i) \cdot \mathbf{1}] \\
&\quad + \sum_{i=2}^N \sum_{j=0}^i ((\cos \alpha)^{i-j} (\sin \alpha)^j - \delta_{j,0} \cos \alpha - \delta_{i-j,0} \sin \alpha) \mathcal{P}[(i-j) \cdot \sigma_x, j \cdot \sigma_z, (N-i) \cdot \mathbf{1}] \} .
\end{aligned} \tag{17}$$

The cloning transformation is linear, thus taking into account Eq. (14) we obtain

$$\begin{aligned}
\sum_k A_k \rho^{in} A_k^\dagger &= \frac{1}{2^M} \{ \mathcal{P}[0 \cdot \sigma_x, 0 \cdot \sigma_z, M \cdot \mathbf{1}] \\
&\quad + \eta(N, M) \cos \alpha \mathcal{P}[\sigma_x, 0 \cdot \sigma_z, (M-1) \cdot \mathbf{1}] + \cos \alpha R_x(\sigma^2) \\
&\quad + \eta(N, M) \sin \alpha \mathcal{P}[0 \cdot \sigma_x, \sigma_z, (M-1) \cdot \mathbf{1}] + \sin \alpha R_z(\sigma^2) \\
&\quad + \sum_k A_k \sum_{i=2}^N \sum_{j=0}^i ((\cos \alpha)^{i-j} (\sin \alpha)^j - \delta_{j,0} \cos \alpha - \delta_{i-j,0} \sin \alpha) \mathcal{P}[(i-j) \cdot \sigma_x, j \cdot \sigma_z, (N-i) \cdot \mathbf{1}] A_k^\dagger \} \tag{18}
\end{aligned}$$

The universality condition requires that the last row in the equation above does not contribute to the terms linear in σ for all values of α . This implies that terms $\sum_k A_k \mathcal{P}[(i-j) \cdot \sigma_x, j \cdot \sigma_z, (N-i) \cdot \mathbf{1}] A_k^\dagger$ (for $i = 2, \dots, N; j = 0, \dots, i$) do not contribute to the terms linear in σ . It turns out that only the linear input terms $\mathcal{P}[0 \cdot \sigma_x, \sigma_z, (N-1) \cdot \mathbf{1}]$ and $\mathcal{P}[\sigma_x, 0 \cdot \sigma_z, (N-1) \cdot \mathbf{1}]$ contribute to the linear output terms. This argument can be easily extended to the most general case of a direct product of pure states with the Bloch vector in an arbitrary direction.

Let us now consider the case of an input density matrix which is not a direct product of N original qubits but is still invariant under any possible permutation of the N bits. This can be written as

$$\rho_{inv} = \sum_{i=0}^N \sum_{j=0}^i \sum_{l=0}^j T_{N-i, i-j, j-l, l} \mathcal{P}[(i-j) \cdot \sigma_x, (j-l) \cdot \sigma_y, l \cdot \sigma_z, (N-i) \cdot \mathbf{1}] , \tag{19}$$

and can describe entangled and/or mixed states. In this case, as we can see from Eq. (18), the components of the Bloch vector of each particle are also reduced by the shrinking factor η . Thus a universal cloning machine which clones pure product states also acts as a cloner for states described by Eq.(19). Therefore, a universal cloning machine which is optimal for pure product states is also optimal for any state invariant under all possible permutations of the original qubits. A particular case is the one where the input state is of the form $\rho \otimes \rho \cdots \otimes \rho$, a product of mixed states. We have thus extended the definition and the operation of a universal cloning machine to a more general class of states of the form (19). 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 our calculations using, for example, the Uhlmann fidelity [8]: optimising the shrinking factor is equivalent to optimising the Uhlmann fidelity.

Note that the argument above covers also the optimal state estimation via any POVM measurement specified by (7) and (8). In this case ρ^{in} describes the N qubits whose state we want to estimate, and ρ^{out} is the density matrix which we can reconstruct after learning the result of the measurement (see also justification of statement d)). We can thus generalise the results on the optimal estimation of quantum states presented in Ref. [5] to any initial state of the form (19), and in particular to an arbitrary number of independent copies of a mixed state.

Equation (18) shows that if we concatenate two universal cloning machines in sequence, provided that the output of the first machine is of the form (19), the corresponding shrinking factors just multiply.

It finally only remains to prove statement d). Equation (5) was obtained assuming the following result (due to [5]): given M qubits all in an unknown quantum state $|\Psi\rangle$ there exists a POVM measurement which leads to the best possible estimation of $|\Psi\rangle$ with fidelity $\bar{F}(M) = \frac{M+1}{M+2}$, or, equivalently, with

$$\bar{\eta}_{meas}^{opt}(M) = \frac{M}{M+2} . \tag{20}$$

Information about the state $|\Psi\rangle$, gained in the POVM measurement, can be represented as a probability distribution $P(\theta, \phi)$, where θ and ϕ specify the direction of the qubit Bloch vector. When we generate an ensemble of states with

the Bloch vectors distributed according to $P(\theta, \phi)$ we effectively reconstruct the state $\bar{\rho} = \bar{\eta}(M)|\Psi\rangle\langle\Psi| + (1 - \bar{\eta}(M))\frac{1}{2}\mathbb{1}$ (or equivalently $\bar{\rho} = \bar{F}(M)|\Psi\rangle\langle\Psi| + (1 - \bar{F}(M))|\Psi_{\perp}\rangle\langle\Psi_{\perp}|$, where $\langle\Psi|\Psi_{\perp}\rangle = 0$). We notice that this procedure is universal, namely its efficiency does not depend on the explicit form of the initial state $|\Psi\rangle$. This is the reason why the state we can reconstruct after the POVM measurement can be simply viewed as the shrunk version of the initial one.

The optimal measurement of this type can be viewed as an $M \rightarrow \infty$ cloner because from the *a posteriori* probability distribution $P(\theta, \phi)$ we can generate any number of copies, in particular infinitely many, with the reconstruction fidelity $\bar{F}(M)$ with respect to the original qubits. Clearly this procedure cannot provide a greater shrinking factor than the optimal $M \rightarrow L$ cloner and we find

$$\bar{\eta}_{meas}^{opt}(M) \leq \eta_{QCM}^{opt}(M, L) \quad (21)$$

for any $L \geq M$, in particular for $L \rightarrow \infty$.

In order to show that for $L \rightarrow \infty$ the equal sign holds in eq. (21), we establish an inequality resulting from concatenating a symmetrised $M \rightarrow L$ cloner with a subsequent quantum measurement. Note that the output of the cloner is entangled, but due to statement b) we know that $\bar{\eta}_{meas}^{opt}(L)$ is the same as for pure states, namely Eq. (20). This global procedure cannot be better than the optimal measurement performed directly on the M inputs. Thus we find:

$$\eta_{QCM}(M, L) \cdot \bar{\eta}_{meas}(L) \leq \bar{\eta}_{meas}^{opt}(M) \quad (22)$$

In the limit $L \rightarrow \infty$ we have $\bar{\eta}_{meas}(\infty) = 1$ and equation (22) reads

$$\eta_{QCM}(M, \infty) \leq \bar{\eta}_{meas}^{opt}(M) \quad (23)$$

Combining equations (21) and (23) finally leads to

$$\eta_{QCM}^{opt}(M, \infty) = \bar{\eta}_{meas}^{opt}(M) \quad (24)$$

We have thus derived the optimal shrinking factor/fidelity for a universal $N \rightarrow M$ cloner and generalised its operation to a more general case of mixed and/or entangled input states which are invariant under all possible permutations of the N qubits. 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 [5] to the case of mixed states.

It is a pleasure to thank C.H. Bennett, V. Bužek, J.I. Cirac, D. DiVincenzo, N. Gisin, M. Palma, S. Popescu and R. Werner for helpful discussions and the Black Cow Café for a stimulating working environment.

After finishing this paper we learned that a different derivation of the best cloning fidelity was also obtained by R. Werner [9].

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, quant-ph/9705038.
- [4] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
- [5] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
- [6] J.I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
- [7] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).
- [8] The Uhlmann fidelity is a good definition of fidelity for mixed states. See A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976)
- [9] R. Werner, private communication.