Optimal Quantum Cloning Machines

N. Gisin[1] and S. Massar[2]
[1]*Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[2]*Raymond and Beverly Sackler Faculty of Exact Sciences, School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 69978, Israel*
(Received 27 May 1997)

We present quantum cloning machines that transform N identical qubits into $M > N$ identical copies and we prove that the fidelity (quality) of these copies is optimal. The connection between cloning and measurement is discussed in detail. When the number of clones M tends towards infinity, the fidelity of each clone tends towards the optimal fidelity that can be obtained by a measurement on the input qubits. More generally, quantum cloning machines are universal devices to translate quantum information into classical information. [S0031-9007(97)03916-1]

PACS numbers: 89.70.+c, 03.65.–w

Quantum cloning machines (QCM) act on an unknown quantum state and make one, or more, copies of it. The superposition principle of quantum mechanics prohibits the copies from being perfect [1,2]. This basic result is maybe the most fundamental difference between classical and quantum information theory, and QCM therefore probe in a detailed way the structure of quantum information. For example, the $U_{1,2,}$ QCM makes two copies of one qubit (i.e., of a spin $\frac{1}{2}$ state) with a fidelity independent of the state of the input qubit [3]. Other recent related work has been concerned with deriving inequalities governing the quality of QCM [4], and in applying QCM to concrete problems such as eavesdropping in quantum cryptography [5], quantum entanglement [5–7], and building quantum computer networks to realize QCM [8].

A conceptually simple cloning machine, which we shall call the classical copying machine (CCM), is obtained by making a measurement on the input state. The (classical) result of the measurement is then used to make an arbitrary number M of identical copies. Such a copying machine only makes use of the information about the input state that is available through measurement. It is therefore less efficient than the QCM's proper. Indeed the most general QCM consists of the N input qubits all in the same state, the $M - N$ blank copies all in the same neutral state, and an eventual ancilla, which evolve unitarily into an (entangled) state of the M clones and the ancilla. For any finite number M of copies, these QCM make better copies than the CCM. But in the limit $M \to \infty$, the quality of the two copying machines are equal. This shows that not only do QCM necessarily make imperfect copies, but that information is necessarily diluted during the copying process, since when M is large the copies contain no more information than that which is available classically. Note that the quantum information has not disappeared, but is hidden in the correlations between the copies and the ancilla.

In this article, for simplicity, we concentrate on QCM that transform one qubit into M identical copies, though many results are also stated for an arbitrary number N of input qubits. When $N = 1$ and $M = 2$ our QCM reduces to the QCM of Bužek and Hillery [3]. Furthermore we prove that these QCM are optimal, i.e., that no other QCM can make better copies. We use this result to make precise the above discussion relating cloning and measurement.

The input state of our QCM is a qubit $|\psi\rangle = \cos\theta/2|\uparrow\rangle + e^{i\phi}\sin\theta/2|\downarrow\rangle$. The *a priori* probability distribution of the polarization direction ψ is uniform over the Poincaré sphere. We measure the quality of the copies by their fidelity $\mathcal{F}$, i.e., the mean overlap between any of the copies (they are all identical) and the input state,

$$\mathcal{F} = \int d\Omega \, \langle\psi|\rho_{\text{out}}|\psi\rangle , \tag{1}$$

where $\int d\Omega = \int_0^{2\pi} d\phi \int_0^{\pi} d\theta \sin\theta/4\pi$, and ρ_{out} is the reduced density matrix of one of the copies.

The $U_{1,M}$ QCM is described by the following unitary operator:

$$\begin{aligned} U_{1,M}|\uparrow\rangle \otimes R &= \sum_{j=0}^{M-1} \alpha_j |(M-j)\uparrow, j\downarrow\rangle \otimes R_j , \\ U_{1,M}|\downarrow\rangle \otimes R &= \sum_{j=0}^{M-1} \alpha_{M-1-j} \\ &\quad \times |(M-1-j)\uparrow, (j+1)\downarrow\rangle \otimes R_j , \\ \alpha_j &= \sqrt{\frac{2(M-j)}{M(M+1)}} , \end{aligned} \tag{2}$$

where R denotes the initial state of the copy machine and the $M - 1$ blank copies, R_j are orthogonal normalized internal states of the QCM, and we have denoted $|M - j\psi, j\psi^{\perp}\rangle$ the symmetric and normalized state with $M - j$ qubits in the state ψ and j qubits in the orthogonal state $\psi^{\perp}$.

A somewhat lengthy computation involving combinatorial series shows that this unitary operator acts on an arbitrary input state ψ as follows:

$$U_{1,M}|\psi\rangle \otimes R = \sum_{j=0}^{M-1} \alpha_j |(M-j)\psi, j\psi^{\perp}\rangle \otimes R_j(\psi) , \tag{3}$$

where $R_j(\psi)$ represents the internal state of our QCM with $R_j(\psi) \perp R_k(\psi)$ for all $j \neq k$. In order to give a synthetic expression for $R_j(\psi)$, let us introduce the qubits $\psi^* = \cos\theta/2|\uparrow^*\rangle + e^{-i\phi}\sin\theta/2|\downarrow^*\rangle$ which transforms under rotations as the complex conjugate representation. If we formally identify the internal states of the QCM R_j with the states $R_j = |(M-1-j)\uparrow^*, j\downarrow^*\rangle$, then the states $R_j(\psi)$ are succinctly expressed as $R_j(\psi) = |(M-1-j)\psi^*, j(\psi^*)^\perp\rangle$.

The density matrix describing the output qubits is the same for all copies, and has the form $\rho_{\text{out}} = \mathcal{F}|\psi\rangle\langle\psi| + (1-\mathcal{F})|\psi^\perp\rangle\langle\psi^\perp|$. To calculate the fidelity $\mathcal{F}$ we first note that α_j^2 is the probability that there are j errors among the M output copies. Then, concentrating on the first output qubit, we have

$$\begin{aligned}\mathcal{F}_{1,M} &= \sum_{j=0}^{M-1} \text{Prob}(\, j \text{ errors in the } M-1 \text{ last qubits}) \\ &= \sum_{j=0}^{M-1} \frac{M-j}{M}\,\alpha_j^2 = \frac{2M+1}{3M}\,,\end{aligned} \tag{4}$$

where $\frac{M-j}{M}$ is the ratio of the number of ways to choose j errors among $M-1$ qubits over the number of ways to choose j errors among M qubits. Note that since the possible final states of the QCM are orthogonal, one can know whether the copy process went through without error or not. However, this requires *a priori* knowledge of the initial state, since the two possible final states of the QCM depend on it. If one does not have any *a priori* knowledge about the initial state (and this is what we assume), then it is impossible to learn by making a measurement on the QCM whether or not the cloning has succeeded.

We have also constructed a more general QCM that takes N identical input qubit into M identical copies. It is described by

$$\begin{aligned}U_{N,M}|N\psi\rangle &= \sum_{j=0}^{M-N} \alpha_j |(M-j)\psi, j\psi^\perp\rangle \otimes R_j(\psi), \\ \alpha_j &= \sqrt{\frac{N+1}{M+1}}\sqrt{\frac{(M-N)!\,(M-j)!}{(M-N-j)!\,M!}}\,,\end{aligned} \tag{5}$$

where $|N\psi\rangle$ is the input state consisting of N spins all in the state ψ, and the other notations are as above. Note that the number j of errors in the copies is smaller or equal to the number $M-N$ of additional qubits. The fidelity of each output qubit is

$$\mathcal{F}_{N,M} = \sum_{j=0}^{M-1} \frac{M-j}{M}\,\alpha_j^2 = \frac{M(N+1)+N}{M(N+2)}\,. \tag{6}$$

The N to $N+1$ cloning machine is particularly simple since the right-hand side in Eq. (5) contains only two terms. In this case the fidelity $\mathcal{F}_{N,N+1} = \frac{N^2+3N+1}{N^2+3N+2}$ tends rapidly towards 1 as N grows, corresponding to the fact that the input state is quasiclassical.

The fidelity $\mathcal{F}_{N,M}$ of these QCM (5) tends to $N + 1/N + 2$ for large M which is the optimal fidelity achievable by carrying out a measurement on N identical qubits [9,10]. This suggests that the QCM tends towards the CCM as M increases. We now prove that this is indeed the case. Let us first consider the case $N = 1$. In [10] it was shown that an optimal measurement on a single qubit is simply a Stern Gerlach measurement that is a projection onto two (randomly chosen) orthogonal states $|\phi\rangle$ and $|\phi^\perp\rangle$. The corresponding CCM consists of making M copies of the ϕ state ($|M\phi\rangle$) if the outcome of the measurement is ϕ, and M copies of the $\phi^\perp$ state ($|M\phi^\perp\rangle$) if the outcome of the measurement is $\phi^\perp$. The density matrix describing the M copies, averaged over the orientations of the measuring basis $|\phi\rangle$, is

$$\begin{aligned}\rho_{\text{CCM}} = \int d\Omega_\phi\, &|\langle\psi|\phi\rangle|^2 P_{|M\psi\rangle} \\ &+ |\langle\psi|\phi^\perp\rangle|^2 P_{|M\phi^\perp\rangle}\,,\end{aligned} \tag{7}$$

where the first factor is the probability to have outcome ϕ ($\phi^\perp$), and $P_{|M\phi\rangle}$ ($P_{|M\phi^\perp\rangle}$) is the projector onto the state $|M\phi\rangle$ ($|M\phi^\perp\rangle$). In order to compare the CCM to the QCM, we express ρ_{CCM} in the basis ψ, $\psi^\perp$ to obtain

$$\rho_{\text{CCM}} = \sum_{s=0}^{M} \frac{2(M+1-s)}{(M+1)(M+2)}\, P_{|(M-s)\psi, s\psi^\perp\rangle}\,. \tag{8}$$

It is then easy to show that the QCM tends towards the CCM as M increases. For instance, one has $\text{Tr}[\rho_{\text{QCM}} - \rho_{\text{CCM}}]^2 \simeq M^{-3}$. Other measures of the "distance" between ρ_{CCM} and ρ_{QCM} similarly decrease as M increases. A more complicated procedure, based on the coveriant measurements of [9], see also [10], show that for an arbitrary number N of input qubits

$$\begin{aligned}\rho_{\text{CCM}} = (N+1)\sum_{s=0}^{M} &\frac{M!\,(M+N-s)!}{(M+N-s)!\,(M-s)!} \\ &\times P_{|(M-s)\psi, s\psi^\perp\rangle}\end{aligned}$$

and $\text{Tr}[\rho_{\text{QCM}} - \rho_{\text{CCM}}]^2 \simeq N^4 M^{-3}$. Thus when the number of copies M increases, the QCM tends towards the CCM. Conversely one can consider QCM as measuring devices. Indeed, given N qubits all in the same unknown state ψ, one can either make a coherent measurement of all N qubits, or equivalently use the QCM to produce a very large number M of clones and then do separable measurements on the clones. Indeed, since for large M, ρ_{QCM} is a mixture of product states of the form $|M \times \phi\rangle$ it suffices to measure them with a classical polarimeter. The fidelity of these two ways of gaining information about ψ are equal. Hence the QCM can be considered as a universal device transforming quantum information into classical information. This is illustrated in Fig. 1. Note that in the first case all the difficulty for experiments lies in the coherent measurement, whereas in the second case all the difficulty is in the QCM.

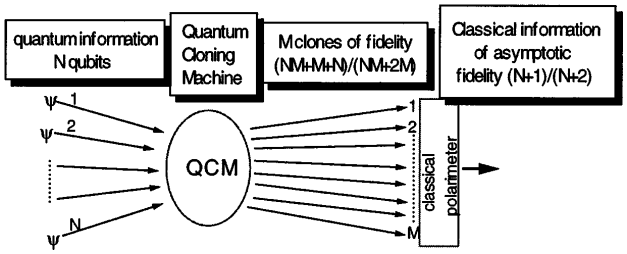

FIG. 1. Diagram of the flow of quantum information to classical information.

We now prove that the QCM we have described are optimal. For simplicity we consider the case where there is only one input qubit, but an arbitrary number M of output qubits. The idea of the calculation follows closely the analysis of optimal measurements of [10]. We first express in full generality the average fidelity $\mathcal{F}$ of a quantum cloning machine in terms of the final state $|R_{jk}\rangle$ (see below) of the machine. These final states are subject to the condition that the evolution is unitary. One must then maximize $\mathcal{F}$ subject to the unitarity conditions which are introduced by using Lagrange multipliers. The problem then reduces to an eigenvalue equation for a matrix A, and the extremal value of $\mathcal{F}$ is expressed in terms of the largest eigenvalue of this matrix.

The most general QCM acts on the input qubits $\uparrow, \downarrow$ in the following way:

$$|j\rangle|R\rangle \rightarrow |M - k\uparrow, k\downarrow\rangle|R_{jk}\rangle, \qquad j = \uparrow, \downarrow, \tag{9}$$

where $|R\rangle$ is the initial state of the QCM and the blank copies, $|R_{jk}\rangle$ are unnormalized final states of the ancilla, and we use a summation convention: repeated indices are summed over. Unitarity of the evolution imposes that

$$\langle R_{j'k}|R_{jk}\rangle = \delta_{j',j}\,. \tag{10}$$

Note that because $|M - k\uparrow, k\downarrow\rangle$ is completely symmetric, we have made the hypothesis that the output of the QCM is completely symmetric. As discussed below, this hypothesis can be dropped without affecting our conclusions. Our task is to maximize the fidelity of this QCM subject to the unitary constraints (10). The rotational symmetry of the input qubits is exploited by expressing an arbitrary input qubit as a SU(2) rotation $O_{j'j}(\Omega)$ acting on the $\uparrow$ state, $|\psi\rangle = \cos\theta/2\uparrow + e^{i\phi}\sin\theta/2\downarrow = O_{\uparrow j}|j\rangle$. The evolution of an arbitrary input qubit is then

$$\begin{aligned} |\psi\rangle|R\rangle &= O_{\uparrow j}|j\rangle|R\rangle \rightarrow |\psi_{\text{out}}\rangle \\ &= O_{\uparrow j}|M - k\uparrow, k\downarrow\rangle|R_{jk}\rangle\,. \end{aligned} \tag{11}$$

Because the output state is symmetric under permutations, the fidelity of the copies is obtained by calculating the overlap of the reduced density matrix of one copy, say the first, with the input state $|\psi\rangle$ and averaging over the input states. One finds

$$\begin{aligned} \mathcal{F} &= \text{Tr}[\langle\psi_{\text{out}}|O_{\uparrow i'}|i'\rangle\langle i|O^*_{\uparrow i}|\psi_{\text{out}}\rangle] \quad i, i' = \uparrow, \downarrow \\ &= \langle R_{j'k'}|R_{jk}\rangle\left(\int d\Omega\; O^*_{\uparrow j'}O_{\uparrow i'}O^*_{\uparrow i}O_{\uparrow j}\right) \\ &\quad \times \text{Tr}[\langle M - k'\uparrow, k'\downarrow||i'\rangle\langle i||M - k\uparrow, k\downarrow\rangle] \\ &= \langle R_{j'k'}|R_{jk}\rangle A_{j',k',j,k}\,, \end{aligned} \tag{12}$$

where we have expressed everything in terms of the SU(2) rotation matrices and introduced the matrix $A_{j',k',j,k}$ which plays an essential role in this calculation. Our problem is to maximize $\mathcal{F}$ subject to the unitary constraints Eq. (10). We impose the unitary constraints by adding them via Lagrange multipliers $\lambda_{j'j}$. Thus we must extremize

$$\begin{aligned} \mathcal{F} &= \langle R_{j'k'}|R_{jk}\rangle A_{j',k',j,k} \\ &\quad - \lambda_{j'j}(\langle R_{j'k'}|R_{jk}\rangle\delta_{k',k} - \delta_{j',j})\,, \end{aligned} \tag{13}$$

with respect to the final states of the QCM $|R_{jk}\rangle$ and the multipliers $\lambda_{j'j}$. It is, however, useful to consider a simpler problem in which we impose only one constraint, namely, the trace of Eq. (10). Obviously the extrema of this reduced problem are greater or equal to the extrema of the full problem Eq. (13), and we will thus obtain an upper bound on the fidelity of QCM. We shall show below that rotational symmetry implies that this upper bound is attained by optimal QCM. Thus we have to extremize

$$\begin{aligned} \mathcal{F} &= \langle R_{j'k'}|R_{jk}\rangle A_{j',k',j,k} \\ &\quad - \lambda(\langle R_{j'k'}|R_{jk}\rangle\delta_{k',k}\delta_{j',j} - 2)\,. \end{aligned} \tag{14}$$

Varying with respect to $\langle R_{j'k'}|$ (more properly one should vary with respect to the components of $\langle R_{j'k'}|$ in a basis), we obtain the equations

$$(A_{j',k',j,k} - \lambda\delta_{k',k}\delta_{j',j})|R_{jk}\rangle = 0\,. \tag{15}$$

Thus λ are the eigenvalues of $A_{j',k',j,k}$ and $|R_{jk}\rangle$ its eigenvectors. Suppose we have found a solution $\lambda, |R_{jk}\rangle$ of Eq. (15) and of the unitary constraints Eq. (10). Then multiplying Eq. (15) on the left by $\langle R_{j'k'}|$ and summing over j', k' yields

$$\langle R_{j'k'}|R_{jk}\rangle A_{j',k',j,k} = \langle R_{j'k'}|R_{jk}\rangle\lambda\delta_{k',k}\delta_{j',j} = 2\lambda\,, \tag{16}$$

where the last equality follows from the constraint Eq. (10). But the left-hand side is equal to the fidelity $\mathcal{F}$ Eq. (12). So the maximal eigenvalue of A is related to the optimal fidelity of the QCM by $\mathcal{F} = 2\lambda_{\max}$. It remains to calculate the matrix A. After some algebra one finds that it is block diagonal $A_{j',k',j,k} = \delta_{k-j,k'-j'}B_{k+j,k'+j'}$ with

$$B = \frac{1}{6M}\begin{pmatrix} 2M - K & \sqrt{(M-K)(K+1)} \\ \sqrt{(M-K)(K+1)} & M + K + 1 \end{pmatrix}, \tag{17}$$

where $K = k - j$. The largest eigenvalue of A is $(2M + 1)/6M$ corresponding to an upper bound on the optimal fidelity $\mathcal{F} \leq (2M + 1)/3M$. This bound is saturated by the QCM Eq. (2) thereby proving that it is optimal. We have generalized this proof to show that the QCM Eq. (5) that transform N identical qubits into an arbitrary number M of copies are optimal. Our proof is at present only valid for $N = 1, 2, \ldots, 7$, although we expect it to generalize to arbitrary N. The difficulty when N is large is that the matrix B is $N + 1 \times N + 1$ and its eigenvalues are correspondingly difficult to calculate.

Throughout this Letter we have considered QCM that are symmetric in their output qubits. If we want to generalize our results to QCM that are not symmetric, we must adopt a more general definition of the fidelity of the copies which we take to be the average fidelity of each copy. We will now show that there necessarily exist QCM that are optimal in this more general sense and symmetric. Indeed, suppose one has constructed a (not necessarily symmetric) optimal QCM. One can then build another QCM which is identical to the proceeding one, except that some of the output states have been permuted. This QCM is obviously also optimal because of the symmetry of the definition of fidelity. If one takes a coherent superposition of these QCM, averaged over all possible permutations of the output qubits, one obtains still another optimal QCM, but which is symmetric in its output qubits.

One can similarly show that there necessarily exist optimal QCM that are rotation invariant. Indeed suppose that one has built a (not necessarily rotationally invariant) optimal QCM. By rotating the whole apparatus one obtains another optimal QCM. [This follows from the rotation invariance of the definition of fidelity Eq. (1), which is averaged over all possible orientations of the input qubits.] If one takes a coherent superposition of these QCM, averaged over the orientations of the apparatus, one obtains an optimal and rotationally invariant QCM [11]. We further note that the Lagrange multipliers $\lambda_{jj'}$ associated with such an optimal rotationally invariant QCM must also be invariant under rotation, which can only be the case if $\lambda_{jj'} = \lambda\delta_{jj'}$ (Shur's Lemma). This explains why the extrema of the reduced problem Eq. (13) are also extrema of the full problem Eq. (14).

In summary, the QCM that have been presented are optimal as well for copying quantum information as for translating quantum information to classical information, thus establishing the connection between cloning quantum information and gaining classical information. For example, the $1 \rightarrow 2$ QCM provides the optimal eavesdropping strategy for a quantum cryptography protocol based on 3 nonorthogonal bases X, Y, and Z on the Poincaré sphere, as conjectured by Ch. Fuchs (private communication). The experimental realization of such optimal QCM is a worthwhile challenge. Indeed, it would provide a universal device for copying and reading quantum information.

We would like to thank V. Buzek, A. Ekert, L. Goldenberg, B. Huttner, Ch. Macchiavello, S. Popescu, and D. Rohrlich for helpful discussions. N. G. acknowledges financial support by the Swiss National Science Foundation and by the European TMR network ERB-FMRX-CT96-0087, and S. M. acknowledges support from Grant No. 614/95 of the Israel Science Foundation.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[3] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] M. Hillery and V. Bužek, Report No. quant-ph/9701034.
[5] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[6] V. Bužek, V. Vedral, M. B. Plenio, P. L. Knight, and M. Hillery, Phys. Rev. A **55**, 3327 (1997).
[7] M. Horodecki and R. Horodecki, Report No. quant-ph/9705003.
[8] V. Bužek, S. L. Braunstein, M. Hillery, and D. BruB, Report No. quant-ph/9703046.
[9] A. S. Helovo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[10] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[11] A similar argument has been used to discuss the symmetry of optimal measurements: A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973); and the symmetry of eavesdropping strategies in quantum cryptography: I. Cirac and N. Gisin, Report No. quant-ph 9702002 [Phys. Lett. A (to be published)]; Ch. Fuchs *et al.*, Report No. quant-ph 9701039 [Phys. Rev. A (to be published)].