Fortschr. Phys. **46** (1998) 4–5, 521–533

Flocks of Quantum Clones: Multiple Copying of Qubits

V. Bužek[1,2], M. Hillery[3] and P. L. Knight[4]

1 Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratislava, Slovakia
2 Department of Mathematics and Physics, Comenius University, Mlynská dolina F2, 842 15 Bratislava, Slovakia
3 Department of Physics and Astronomy, Hunter College, CUNY, 695 Park Avenue, New York, U.S.A.
4 Optics Section, The Blackett Laboratory, Imperial College, London SW7 2BZ, U.K.

Abstract

We present a quantum netwoprk for an optimal quantum copying "machine" (transformation) which poduces $N+1$ identical copies from the original qubit. The quality (fidelity) of the copies does not depend on the state of the original and is only a function of the number of copies, N.

I. Introduction

The most fundamental difference between classical and quantum information is that while classical information can be copied perfectly, quantum information cannot. In particular, it follows from the *no-cloning theorem* [1] (see also [2, 3]) that one cannot create a perfect duplicate of an *arbitrary* qubit. For example, using the well-known *teleportation protocol* [4], one can create a perfect copy of the original qubit but this will be at the expense of the *complete* destruction of information encoded in the original qubit. In contrast, the main goal of quantum copying is to produce a copy of the original qubit which is as close as possible to the original state while the output state of the original qubit is minimally disturbed.

If one is only interested in producing imperfect copies, then it is possible to design machines (actually, to find unitary transformations) which copy quantum states. A number of these were analyzed in a recent paper by two of us [5] (see also [6–8]). The copy machine considered by Wootters and Zurek [1] in their proof of the no-cloning theorem, for example, produces two identical copies at its output, but the quality of these copies depends upon the input state. They are perfect for the basis vectors which we denote as $|0\rangle$ and $|1\rangle$, but, because the copying process destroys the off-diagonal information of the input density matrix, they are poor for input states of the form $(|1\rangle + e^{i\varphi}\,|0\rangle)/\sqrt{2}$, where φ is arbitrary. A different copy machine, the Universal Quantum Copy Machine (UQCM), produces two identical copies whose quality is independent of the input state. In addition, its performance is, on average, better than that of the Wootters-Zurek machine, and the action of the machine simply scales the expectations values of certain operators. In particular the expectation value in one of the copies of any operator which is a linear combination of the Pauli matrices is equal to $2/3$ of its expectation value in the input state.

In this paper we introduce the copying machine which produces $N+1$ identical copies (i.e. "flocks" of quantum clones) from the original qubit. The quality (fidelity) of copies does not depend on the state of the original and is only a function of a number N of produced copies. We present a quantum network for the quantum copying machine. We show that this machine is formally described by the same unitary transformation as recently discussed by GISIN and MASSAR [9].

The paper is organized as follows: In Section II we briefly review the basic properties of the UQCM and in Section III we describe a quantum network which realizes this copy machine. In Section IV we introduce copying machine which produces multiple copies out of a single qubit and describe a corresponding quantum network. In the final section we discuss properties of copied qubits.

II. Universal Quantum Copying Machine

Let us assume we want to copy an arbitrary pure state $|\Psi\rangle_{a_0}$ which in particular basis $\{|0\rangle_{a_0}, |1\rangle_{a_0}\}$ is described by the state vector $|\Psi\rangle_{a_0}$

$$|\Psi\rangle_{a_0} = \alpha\,|0\rangle_{a_0} + \beta\,|1\rangle_{a_0}\,; \qquad \alpha = \sin\vartheta\, e^{i\varphi}\,; \quad \beta = \cos\vartheta\,. \tag{2.1}$$

The two numbers which characterize that state (2.1) can be associated with the "amplitude" $|\alpha|$ and the "phase" φ of the qubit. Even though ideal copying, i.e., the transformation

$$|\Psi\rangle_{a_0} \to |\Psi\rangle_{a_0}\,|\Psi\rangle_{a_1} \tag{2.2}$$

is prohibited by the laws of quantum mechanics for an *arbitrary* state (2.1), it is still possible to design quantum copiers which operate reasonably well. In particular, the UQCM [5] is specified by the following conditions.

(i) The state of the original system and its quantum copy at the output of the quantum copier, described by density operators $\hat{\varrho}_{a_0}^{(\mathrm{out})}$ and $\hat{\varrho}_{a_1}^{(\mathrm{out})}$, respectively, are identical, i.e.,

$$\hat{\varrho}_{a_0}^{(\mathrm{out})} = \hat{\varrho}_{a_1}^{(\mathrm{out})} \tag{2.3}$$

(ii) If no *a priori* information about the *in*-state of the original system is available, then it is reasonable to require that *all* pure states should be copied equally well. One way to implement this assumption is to design a quantum copier such that the distance between density operators of each system at the output ($\hat{\varrho}_{a_j}^{(\mathrm{out})}$ where $j = 0,\,1$) and the ideal density operator $\hat{\varrho}^{(\mathrm{id})}$ which describes the *in*-state of the original mode are input state independent. Quantitatively this means that if we employ the square of the Hilbert-Schmidt norm

$$d(\hat{\varrho}_1;\,\hat{\varrho}_2) := \mathrm{Tr}\,[(\hat{\varrho}_1 - \hat{\varrho}_2)^2]\,, \tag{2.4}$$

as a measure of distance between two operators, then the quantum copier should be such that

$$d_1(\hat{\varrho}_{a_j}^{(\mathrm{out})};\,\hat{\varrho}_{a_j}^{(\mathrm{id})}) = \mathrm{const.}; \qquad j = 0,\,1\,. \tag{2.5}$$

Here we use the subscript 1 in the definition of the distance d_1 to denote the distance between single-qubit states.

(iii) Finally, we would also like to require that the copies are as close as possible to the ideal output state, which is, of course, just the input state. This means that we want our quantum copying transformation to minimize the distance between the output state $\hat{\varrho}_{a_j}^{(\mathrm{out})}$ of the copied qubit and the ideal state $\hat{\varrho}_{a_j}^{(\mathrm{id})}$. The distance is minimized with respect to all possible unitary transformations U acting on the Hilbert space $\mathcal{H}$ of two qubits and the quantum copying machine (i.e., $\mathcal{H} = \mathcal{H}_{a_0} \otimes \mathcal{H}_{a_1} \otimes \mathcal{H}_x$)

$$d_1(\hat{\varrho}_{a_j}^{(\mathrm{out})};\,\hat{\varrho}_{a_j}^{(\mathrm{id})}) = \min\,\{d_1^{(U)}(\hat{\varrho}_{a_j}^{(\mathrm{out})};\,\hat{\varrho}_{a_j}^{(\mathrm{id})});\ \forall U\}; \qquad (j = 0,\,1)\,. \tag{2.6}$$

Originally, the UQCM was found by analyzing a transformation which contained two free parameters, and then determining them by demanding that condition (ii) be satisfied, and that the distance between the two-qubit output density matrix and the ideal two-qubit output be input state independent. That the UQCM machine obeys the condition (2.6) has only been shown recently [9, 10].

The unitary transformation which implements the UQCM [5] is given by

$$|0\rangle_{a_0}|Q\rangle_x \to \sqrt{\frac{2}{3}}\,|00\rangle_{a_0a_1}|\uparrow\rangle_x + \sqrt{\frac{1}{3}}\,|+\rangle_{a_0a_1}|\downarrow\rangle_x$$

$$|1\rangle_{a_0}|Q\rangle_x \to \sqrt{\frac{2}{3}}\,|11\rangle_{a_0a_1}|\downarrow\rangle_x + \sqrt{\frac{1}{3}}\,|+\rangle_{a_0a_1}|\uparrow\rangle_x \tag{2.7}$$

where

$$|+\rangle_{a_0a_1} = \frac{1}{\sqrt{2}}\,(|10\rangle_{a_0a_1} + |01\rangle_{a_0a_1})\,, \tag{2.8}$$

and satisfies the conditions (2.3–2.6). The system labelled by a_0 is the original (input) qubit, while the other system a_1 represents the qubit onto which the information is copied. This qubit is supposed to be prepared initially in a state $|0\rangle_{a_1}$ (the "blank paper" in a copier). The sates of the copy machine are labelled by x. The state space of the copy machine is two dimensional, and we assume that it is always in the same state $|Q\rangle_x$ initially. If the original qubit is in the superposition state (2.1) then the reduced density operator of both copies at the output are equal [see condition (2.3)] and they can be expressed as

$$\hat{\varrho}^{(\text{out})}_{a_j} = \frac{5}{6}\,|\Psi\rangle_{a_j}\langle\Psi| + \frac{1}{6}\,|\Psi_\perp\rangle_{a_j}\langle\Psi_\perp|\,, \qquad j = 0,\,1 \tag{2.9}$$

where

$$|\Psi_\perp\rangle_{a_j} = \beta^*\,|0\rangle_{a_j} - \alpha^*\,|1\rangle_{a_j}\,, \tag{2.10}$$

is the state orthogonal to $|\Psi\rangle_{a_j}$. This implies that the copy contains 5/6 of the state we want and 1/6 of the one we do not.

The density operator $\varrho^{(\text{out})}_{a_j}$ given by Eq. (2.9) can be rewritten in a "scaled" form:

$$\hat{\varrho}^{(\text{out})}_{a_j} = s_j\hat{\varrho}^{(\text{id})}_{a_j} + \frac{1-s_j}{2}\,\hat{1}; \qquad j = 0,\,1\,, \tag{2.11}$$

which guarantees that the distance (2.4) is input-state independent, i.e. the condition (2.5) is automatically fulfilled. The scaling factor in Eq. (2.11) is $s_j = 2/3$ $(j = 0,\,1)$.

We note once again that the UQCM copies all input states with the same quality and therefore is suitable for copying when no *a priori* information about the state of the original qubit is available. This corresponds to a uniform prior probability distribution on the state space of a qubit (Poincare sphere). Correspondingly, one can measure the quality of copies by the fidelity $\mathcal{F}$, which is equal to the mean overlap between a copy and the input state [9]

$$\mathcal{F} = \int d\Omega_{a_j}\langle\Psi|\,\hat{\varrho}^{\text{out})}_{a_j}\,|\Psi\rangle_{a_j}\,, \tag{2.12}$$

where $\int d\Omega = \int_0^{2\pi} d\varphi \int_0^{\pi} d\vartheta \sin\vartheta/4\pi$. It is easy to show that the relation between the fidelity $\mathcal{F}$ and the scaling factor s is

$$s = 2\mathcal{F} - 1 . \tag{2.13}$$

III. Copying Network

In what follows we show how, with simple quantum logic gates, we can copy quantum information encoded in the original qubit onto other qubits. The copying procedure can be understood as a "spread" of information via a "controlled" entanglement between the original qubit and the copy qubits. This controlled entanglement is implemented by a sequence of controlled-NOT operations operating on the original qubit and the copy qubits which are initially prepared in a specific state.

In designing a network for the UQCM we first note that since the state space of the copy machine itself is two dimensional, we can consider it to be an additional qubit. Our network, then, will take 3 input qubits (one for the input, one which becomes the copy, and one for the machine) and transform them into 3 output qubits. In what follows we will denote the quantum copier qubit as b_1 rather than x. The operation of this network is such, that in order to transfer information from the original a_0 qubit to the target qubit a_1 we will need one *idle* qubit b_1 which plays the role of quantum copier.

Before proceeding with the network itself let us specify the one and two-qubit gates from which it will be constructed. Firstly we define a single-qubit rotation $\hat{R}_j(\theta)$ which acts on the basis vectors of qubits as

$$\begin{aligned} \hat{R}_j(\theta)\,|0\rangle_j &= \quad \cos\theta\,|0\rangle_j + \sin\theta\,|1\rangle_j ; \\ \hat{R}_j(\theta)\,|1\rangle_j &= -\sin\theta\,|0\rangle_j + \cos\theta\,|1\rangle_j ; \end{aligned} \tag{3.1}$$

We also will utilize a two-qubit operator (a two-bit quantum gate), the so-called controlled-NOT gate, which has as its inputs a control qubit (denoted as • in Fig. 1) and a

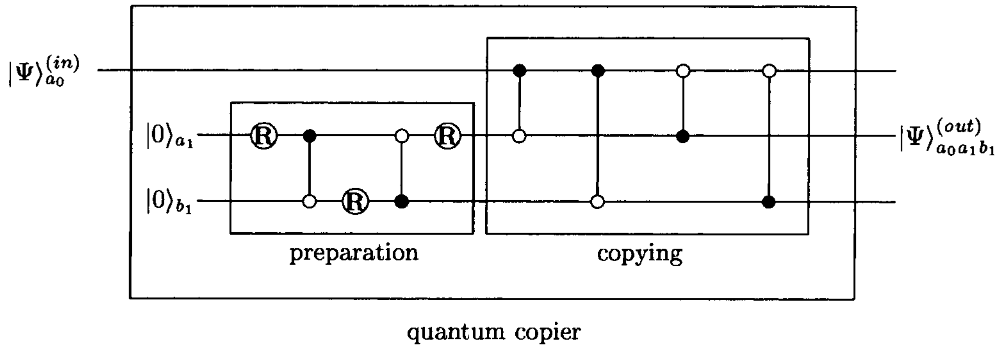

Figure 1: Graphical representation of the UQCM network. The logical controlled-NOT $\hat{P}_{kl}$ given by Eq. (3.2) has as its input a control qubit (denoted as •) and a target qubit (denoted as ∘). The action of the single-qubit operator $\boldsymbol{R}$ is specified by the transformation (3.1). We separate the preparation of the quantum copier from the copying process itself. The copying, i.e. the transfer of quantum information from the original qubit, is performed by a sequence of four controlled-NOTs. We note that the amplitude information from the original qubit is copied in the obvious direction in a XOR or the controlled-NOT operation. Simultaneously, the phase information is copied in the opposite direction making the XOR a simple model of quantum non-demolition measurement and its back-action.

target qubit (denoted as $\circ$ in Fig. 1). The control qubit is unaffected by the action of the gate, and if the control qubit is $|0\rangle$, the target qubit is unaffected as well. However, if the control qubit is in the $|1\rangle$ state, then a NOT operation is performed on the target qubit. The operator which implements this gate, $\hat{P}_{kl}$, acts on the basis vectors of the two qubits as follows (k denotes the control qubit and l the target):

$$\begin{aligned}
\hat{P}_{kl}\,|0\rangle_k\,|0\rangle_l &= |0\rangle_k\,|0\rangle_l\,;\\
\hat{P}_{kl}\,|0\rangle_k\,|1\rangle_l &= |0\rangle_k\,|1\rangle_l\,;\\
\hat{P}_{kl}\,|1\rangle_k\,|0\rangle_l &= |1\rangle_k\,|1\rangle_l\,;\\
\hat{P}_{kl}\,|1\rangle_k\,|1\rangle_l &= |1\rangle_k\,|0\rangle_l\,.
\end{aligned} \tag{3.2}$$

We can decompose the quantum copier network into two parts. In the first part the copy (a_1) and the idle (b_1) qubits are prepared in a specific state $|\Psi\rangle^{(\text{prep})}_{a_1b_1}$. Then in the second part of the copying network the original information from the original qubit a_0 is *redistributed* among the three qubits. That is, the action of the quantum copier can be described as a sequence of two unitary transformations

$$|\Psi\rangle^{(\text{in})}_{a_0}\,|0\rangle_{a_1}\,|0\rangle_{b_1} \to |\Psi\rangle^{(\text{in})}_{a_0}\,|\Psi\rangle^{(\text{prep})}_{a_1b_1} \to |\Psi\rangle^{(\text{out})}_{a_0a_1b_1}\,. \tag{3.3}$$

The network for the quantum copying machine is displayed in Fig. 1.

A. Preparation of quantum copier

Let us first look at the preparation stage. Prior to any interaction with the input qubit we have to prepare the two quantum copier qubits (a_1 and b_1) in a very specific state $|\Psi\rangle^{(\text{prep})}_{a_1b_1}$. If we assume that initially these two qubits are in the state

$$|\Psi\rangle^{(\text{in})}_{a_1b_1} = |0\rangle_{a_1}\,|0\rangle_{b_1}\,, \tag{3.4}$$

then the arbitrary state $|\Psi\rangle^{(\text{prep})}_{a_1b_1}$

$$|\Psi\rangle^{(\text{prep})}_{a_1b_1} = C_1\,|00\rangle_{a_1b_1} + C_2\,|01\rangle_{a_1b_1} + C_3\,|10\rangle_{a_1b_1} + C_4\,|11\rangle_{a_1b_1}\,, \tag{3.5}$$

with real amplitudes C_i (such that $\sum_{i=1}^4 C_i^2 = 1$) can be prepared by a simple quantum network (see the "preparation" box in Fig. 1) with two controlled-NOTs $\hat{P}_{kl}$ and three rotations $\hat{R}(\theta_j)$, i.e.

$$|\Psi\rangle^{(\text{prep})}_{a_1b_1} = \hat{R}_{a_1}(\theta_3)\,\hat{P}_{b_1a_1}\hat{R}_{b_1}(\theta_2)\,\hat{P}_{a_1b_1}\hat{R}_{a_1}(\theta_1)\,|0\rangle_{a_1}\,|0\rangle_{b_1}\,. \tag{3.6}$$

Comparing Eqs. (3.5) and (3.6) we find a set of equations

$$\begin{aligned}
\cos\theta_1\cos\theta_2\cos\theta_3 + \sin\theta_1\sin\theta_2\sin\theta_3 &= C_1\,;\\
-\cos\theta_1\sin\theta_2\sin\theta_3 + \sin\theta_1\cos\theta_2\cos\theta_3 &= C_2\,;\\
\cos\theta_1\cos\theta_2\sin\theta_3 - \sin\theta_1\sin\theta_2\cos\theta_3 &= C_3\,;\\
\cos\theta_1\sin\theta_2\cos\theta_3 + \sin\theta_1\cos\theta_2\sin\theta_3 &= C_4\,,
\end{aligned} \tag{3.7}$$

from which the angles θ_j ($j = 1, 2, 3$) of rotations can be specified as functions of parameters C_i. In particular, for the purpose of the UQCM we need that

$$|\Psi\rangle^{(\mathrm{prep})}_{a_1 b_1} = \frac{1}{\sqrt{6}} \left(2\,|00\rangle_{a_1 b_1} + |01\rangle_{a_1 b_1} + |11\rangle_{a_1 b_1}\right). \tag{3.8}$$

With the help of Eq. (3.7) we find that the rotation angles necessary for the preparation of the state given in Eq. (3.8) are

$$\cos 2\theta_1 = \frac{1}{\sqrt{5}}\,; \qquad \cos 2\theta_2 = \frac{\sqrt{5}}{3}\,; \qquad \cos 2\theta_3 = \frac{2}{\sqrt{5}}\,. \tag{3.9}$$

B. Quantum copying

Once the qubits of the quantum copier are properly prepared then the copying of the initial state $|\Psi\rangle^{(\mathrm{in})}_{a_0}$ of the original qubit can be performed by a sequence of four controlled-NOT operations (see Fig. 1)

$$|\Psi\rangle^{(\mathrm{out})}_{a_0 a_1 b_1} = \hat{P}_{b_1 a_0} \hat{P}_{a_1 a_0} \hat{P}_{a_0 b_1} \hat{P}_{a_0 a_1}\, |\Psi\rangle^{(\mathrm{in})}_{a_0}\, |\Psi\rangle^{(\mathrm{prep})}_{a_1 b_1}\,. \tag{3.10}$$

When this operation is combined with the preparation stage, we find that the basis states of the original qubit (a_0) are copied as described by Eq. (2.7) with $|\!\uparrow\rangle_x \equiv |0\rangle_{b_1}$ and $|\!\downarrow\rangle_x \equiv |0\rangle_{b_1}$. When the original qubit is in the superposition state (2.1) then the state vector of the three qubits after the copying has been performed reads

$$|\Psi\rangle^{(\mathrm{out})}_{a_0 a_1 b_1} = |\Phi_0\rangle_{a_0 a_1}\, |0\rangle_{b_1} + |\Phi_1\rangle_{a_0 a_1}\, |1\rangle_{b_1}\,, \tag{3.11}$$

with

$$\begin{aligned} |\Phi_0\rangle_{a_0 a_1} &= \alpha \sqrt{\frac{2}{3}}\, |00\rangle_{a_0 a_1} + \beta\, \frac{1}{\sqrt{3}}\, |+\rangle_{a_0 a_1}\,; \\ |\Phi_1\rangle_{a_0 a_1} &= \beta \sqrt{\frac{2}{3}}\, |11\rangle_{a_0 a_1} + \alpha\, \frac{1}{\sqrt{3}}\, |+\rangle_{a_0 a_1}\,. \end{aligned} \tag{3.12}$$

From this it follows that at the output of the quantum copier we find a pair of entangled qubits in a state described by the density operator

$$\hat{\varrho}^{(\mathrm{out})}_{a_0 a_1} = |\Phi_0\rangle_{a_0 a_1} \langle \Phi_0| + |\Phi_1\rangle_{a_0 a_1} \langle \Phi_1|\,. \tag{3.13}$$

Each of the copy qubits at the output of the quantum copier has a reduced density operator $\hat{\varrho}^{(\mathrm{out})}_{a_j}$ ($j = 0, 1$) given by Eq. (2.11). The distance $d_1(\hat{\varrho}^{(\mathrm{out})}_{a_j}\,;\, \hat{\varrho}^{(\mathrm{id})}_{a_j})$ ($j = 0, 1$) between the output qubit and the ideal qubit is constant and can be expressed as a function of the scaling prameter s in Eq. (2.11):

$$d_1(\hat{\varrho}^{(\mathrm{out})}_{a_j}\,;\, \hat{\varrho}^{(\mathrm{id})}_{a_j}) = \frac{(1-s)^2}{2} = \frac{1}{18}\,. \tag{3.14}$$

Analogously we find the distance $d_1(\hat{\varrho}^{(\text{out})}_{a_0 a_1}; \hat{\varrho}^{(\text{id})}_{a_0 a_1})$ between the two-qubit output of the quantum copying and the ideal output to be constant, i.e.

$$d_2(\hat{\varrho}^{(\text{out})}_{a_0 a_1}; \hat{\varrho}^{(\text{id})}_{a_0 a_1}) = \frac{s^2}{2} = \frac{2}{9} . \tag{3.15}$$

The idle qubit after the copying is performed is in a state

$$\hat{\varrho}^{(\text{out})}_{b_1} = \frac{1}{3} \, (\hat{\varrho}^{(\text{id})}_{b_1})^T + \frac{1}{3} \, \hat{1} , \tag{3.16}$$

where the superscript T denotes the transpose. We note that in spite of the fact that the distance between this density operator and the ideal qubit depends on the initial state of the original qubit, i.e.

$$d_1(\hat{\varrho}^{(\text{out})}_{b_1}; \hat{\varrho}^{(\text{id})}_{b_1}) = \frac{2}{9} \, (1 + 12 \, |\alpha|^2 \, |\beta|^2 \sin^2 \varphi) , \tag{3.17}$$

the output state of the original qubit still contains information about the input state, though less than either of the copies a_0 and a_1. In order to extract this information we note that for an Hermitian operator $\hat{A}$

$$\text{Tr} \, (\hat{\varrho}^{(\text{in})}_{b_1} \hat{A}) = \text{Tr} \, ((\hat{\varrho}^{(\text{in})}_{b_1})^T \, \hat{A}^T) . \tag{3.18}$$

This means that to obtain information about $\hat{A}$ at the input, we must measure $\hat{A}^T$ for the original qubit at the output.

IV. Multiple Copying

Here we propose a generalization of the transformation (2.7) to the case when a "flock" of N copy qubits a_j $(j = 1, \ldots, N)$ are produced out of the original qubit a_0. We also propose a simple quantum network which realizes this multiple quantum copying $1 \to 1 + N$.

We already know that ideal multiple copying of the form

$$|\Psi\rangle_{a_0} \to |\Psi\rangle_{a_0} \, |\Psi\rangle_{a_1} \ldots |\Psi\rangle_{a_N} \tag{4.1}$$

does not exist. But, as we shall show, one can generalize the copying procedure described in Section 3, and find a transformation such that

$$\hat{\varrho}^{(\text{out})}_{a_0} = \hat{\varrho}^{(\text{out})}_{a_j} , \qquad j = 1, \ldots, N , \tag{4.2}$$

with the distances d_1 [see Eq. (2.4)] which do not depend on the initial state (2.1) of the original qubit.

To find the $1 \to 1 + N$ network we assume the following:

(1) We assume that the information from the original qubit is copied to N copy qubits a_j which are initially prepared in the state $|N; 0\rangle_{\vec{a}} \equiv |0\rangle_{a_1} \ldots |0\rangle_{a_N}$ (here the subscript $\vec{a}$ is a shorthand notation indicating that $|N; 0\rangle_{\vec{a}}$ is a vector in the Hilbert space of N qubits a_j).

(2) To implement multiple quantum copying we need to associate an *idle* qubit b_j with each copy qubit, a_j. These N idle qubits, which play the role of the copying machine itself, are initially prepared in the state $|N; 0\rangle_{\vec{b}} \equiv |0\rangle_{b_1} \ldots |0\rangle_{b_N}$.

(3) Prior to the transfer of information from the original qubit, the copy and the idle qubits have been prepared in a specific state $|\Psi\rangle^{(\mathrm{prep})}_{\vec{a}\vec{b}}$. Once this is done the copying is performed by a simple sequence of controlled-NOT operations.

A. Preparation of the quantum copier

In order to find the explicit form for the quantum network for $1 \to 1+N$ copying we introduce normalized state vectors $|N;\, k\rangle_{\vec{a}}$ describing a *symmetric* N-qubic state with k qubits in the state $|1\rangle$ and $(N-k)$ qubits in the state $|0\rangle$. For example, the state $|3;\, 2\rangle_{a_1a_2a_3}$ can be expressed as

$$|3;\, 2\rangle_{a_1a_2a_3} = \binom{3}{2}^{-1/2} [|110\rangle_{a_1a_2a_3} + |101\rangle_{a_1a_2a_3} + |011\rangle_{a_1a_2a_3}]\,. \tag{4.3}$$

These states are orthonormalized, i.e.

$${}_{\vec{a}}\langle N;\, l\,|\,N;\, k\rangle_{\vec{a}} = \delta_{k,l} \tag{4.4}$$

and have the property

$$|N;\, l\rangle_{\vec{a}} = \sqrt{\frac{N-l}{N}}\,|0\rangle_{a_m}\,|N-1;\, l\rangle_{a_1\,\ldots\,a_{m-1}a_{m+1}\,\ldots\,a_N} \tag{4.5}$$

$$+\sqrt{\frac{l}{N}}\,|0\rangle_{a_m}\,|N-1;\, l-1\rangle_{a_1\,\ldots\,a_{m-1}a_{m+1}\,\ldots\,a_N}\,. \tag{4.6}$$

As we have already said, we assume that the copy + idle qubits are initially prepared in the state

$$|\Psi\rangle^{(\mathrm{in})}_{\vec{a}\vec{b}} = |N;\, 0\rangle_{\vec{a}}\,|N;\, 0\rangle_{\vec{b}}\,. \tag{4.7}$$

By performing a sequence[1]) of local rotations $\boldsymbol{R}$ and controlled-NOT operations analogous to Eq. (3.6) we can obtain the state $|\Psi\rangle^{(\mathrm{prep})}_{\vec{a}\vec{b}}$

$$|\Psi\rangle^{(\mathrm{prep})}_{\vec{a}\vec{b}} = \sum_{k=0}^{N} [e_k\,|N;\, k\rangle_{\vec{a}} + f_k\,|N;\, k-1\rangle_{\vec{a}}]\,|N;\, k\rangle_{\vec{b}}\,, \tag{4.8}$$

where

$$e_k = \sqrt{\frac{2}{N+2}}\,\frac{\binom{N}{k}}{\binom{N+1}{k}}\,; \qquad f_k = \sqrt{\frac{k}{N-k+1}}\,e_k\,. \tag{4.9}$$

Once the copying machine is prepared in the state $|\Psi\rangle^{(\mathrm{prep})}_{\vec{a}\vec{b}}$ we can start to copy information from the original qubit a_0.

[1]) We do not specify here this sequence of operations explicitly. From the universality of one and two-qubit gates [11] it follows that this sequence does exist. As an example, we present the preparation of the state $|\Psi\rangle^{(\mathrm{prep})}_{a_1b_1}$ given by Eq. (3.8), see also Fig. 1.

B. Copying of information

To describe the copying network we firstly introduce an operator $\hat{Q}_{a_0\vec{a}}$ which is a product of the controlled-NOTs defined by Eq. (3.2) with a_0 being a control qubit and a_j $(j = 1, \ldots, N)$ being targets:

$$\hat{Q}_{a_0\vec{a}} = \hat{P}_{a_0a_N}\hat{P}_{a_0a_{N-1}} \ldots \hat{P}_{a_0a_1} . \tag{4.10}$$

We also introduce the operator $\hat{Q}_{\vec{a}a_0}$ describing the controlled-NOT process with a_0 playing the role of the target qubit, i.e.

$$\hat{Q}_{\vec{a}a_0} = \hat{P}_{a_Na_0}\hat{P}_{a_{N-1}a_0} \ldots \hat{P}_{a_1a_0} . \tag{4.11}$$

Now we find the $1 \to 1 + N$ copying network to be

$$|\Psi\rangle_{a_0}^{(\mathrm{in})} |N;\, 0\rangle_{\vec{a}} |N;\, 0\rangle_{\vec{b}} \to |\Psi\rangle_{a_0}^{(\mathrm{in})} |\Psi\rangle_{\vec{a}\vec{b}}^{(\mathrm{prep})} \to |\Psi\rangle_{a_0\vec{a}\vec{b}}^{(\mathrm{out})} , \tag{4.12}$$

where the $(2N + 1)$ qubit output of the copying process is described by the state vector $|\Psi\rangle_{a_0\vec{a}\vec{b}}^{(\mathrm{out})}$ which is defined as

$$|\Psi\rangle_{a_0\vec{a}\vec{b}}^{(\mathrm{out})} = \hat{Q}_{\vec{b}a_0}\hat{Q}_{\vec{a}a_0}\hat{Q}_{a_0\vec{b}}\hat{Q}_{a_0\vec{a}} |\Psi\rangle_{a_0}^{(\mathrm{in})} |\Psi\rangle_{\vec{a}\vec{b}}^{(\mathrm{prep})} . \tag{4.13}$$

This last equation describes a simple quantum network when firstly the original qubit controls the target qubits of the quantum copier. Then the qubits $\vec{a}$ and $\vec{b}$ "control" the state of the original qubit via another sequence of controlled-NOTs (see Fig. 2). In this way one can produce out of a single original qubit a "flock" of quantum clones.

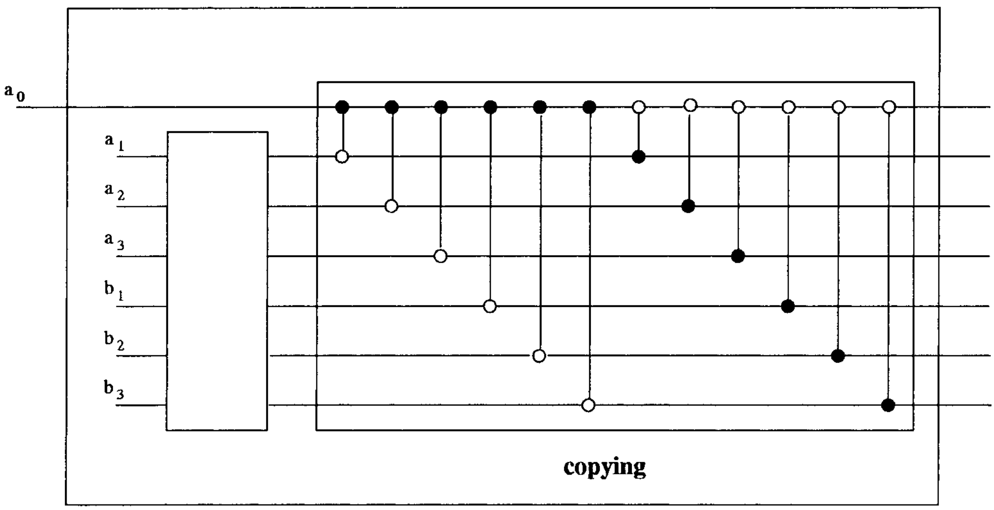

Figure 2: Graphical representation of the network for the $1 \to 1 + N$ copying. The logical controlled-NOT $\hat{P}_{kl}$ given by Eq. (3.2) has as its input a control qubit (denoted as •) and a target qubit (denoted as ○). We separate the preparation of the quantum copier from the copying process itself. The copying, i.e. the transfer of quantum information from the original qubit, is performed by a sequence of controlled-NOTs as described by Eq. (4.13).

V. Properties of Copied Qubits

Using the explicit expression for the output state $|\Psi\rangle^{(\text{out})}_{a_0\vec{a}\vec{b}}$ we find that the original and the copy qubits at the output of the quantum copier are in the same state described by the density operator

$$\hat{\varrho}^{(\text{out})}_{a_j} = s^{(N)}\hat{\varrho}^{(\text{id})}_{a_j} + \frac{1-s^{(N)}}{2}\,\hat{1}\,; \qquad j = 0,\,1,\ldots,\,N\,, \tag{5.1}$$

where the scaling factor $s^{(N)}$ depends on the number N of copies, i.e.

$$s^{(N)} = \frac{1}{3} + \frac{2}{3(N+1)}\,, \tag{5.2}$$

which corresponds to the fidelity $\mathcal{F} = 2/3 + 1/3(N+1)$. We see that this result for $N = 1$ reduces to the case of the UQCM discussed in Section 3. We also note that in the limit $N \to \infty$, i.e. when an infinite number of copies is *simultaneously* produced via the generalization of the UQCM, the copy qubits still carry information about the original qubit, because their density operators are given by the relation

$$\hat{\varrho}^{(\text{out})}_{a_j} = \frac{1}{3}\,\hat{\varrho}^{(\text{id})}_{a_j} + \frac{1}{3}\,\hat{1}\,; \qquad j = 0,\,1,\ldots,\infty\,, \tag{5.3}$$

which corresponds to the fidelity $\mathcal{F} = 2/3$. This is the optimal fidelity achievable when an *optimal* measurement is performed on a single qubit [12, 13]. From this point of view one can consider quantum copying as a transformation of quantum information into classical information [9]. This also suggests that quantum copying can be utilized to obtain novel insight into the quantum theory of measurement [e.g., a simultaneous measurement of conjugated observables on two copies of the original qubit; or a specific realization of the generalized (POVM) measurement perform on the original qubit (see [9])].

Comment 1

We note that if the original qubit is copied sequentially by a system of N copying machines of the type $1 \to 1+1$ (each machine copies two outcomes of the previous copier) then 2^N copies of the original qubit in the limit $N \to \infty$ are in the state $\hat{\varrho}^{(\text{out})}_{a_j} = \hat{1}/2$. In this case the copied qubits do not carry information about the original qubit, while all idle qubits are in the state (3.16).

Comment 2

The two-qubit density operator $\hat{\varrho}^{(\text{out})}_{a_m a_n}$ (here $m,\, n = 0,\, 1\ldots,\, N$ and $m \neq n$) associated with the output state $|\Psi\rangle^{(\text{out})}_{a_0\vec{a}\vec{b}}$ [see Eq. (4.13)] in the basis $|11\rangle_{a_m a_n}$, $|10\rangle_{a_m a_n}$, $|01\rangle_{a_m a_n}$, $|00\rangle_{a_m a_n}$ is described by the matrix

$$\hat{\varrho}^{(\text{out})}_{a_m a_n} = \frac{1}{6}\begin{pmatrix} \dfrac{(3N+5)\,|\beta|^2 + (N-1)\,|\alpha|^2}{N+1} & \dfrac{\alpha^*\beta(N+3)}{N+1} & \dfrac{\alpha^*\beta(N+3)}{N+1} & 0 \\ \dfrac{\alpha\beta^*(N+3)}{N+1} & 1 & 1 & \dfrac{\alpha^*\beta(N+3)}{N+1} \\ \dfrac{\alpha\beta^*(N+3)}{N+1} & 1 & 1 & \dfrac{\alpha^*\beta(N+3)}{N+1} \\ 0 & \dfrac{\alpha\beta^*(N+3)}{N+1} & \dfrac{\alpha\beta^*(N+3)}{N+1} & \dfrac{(3N+5)\,|\alpha|^2 + (N-1)\,|\beta|^2}{N+1} \end{pmatrix}. \tag{5.4}$$

From Eq. (5.4) we find that the eigenvalues $\vec{E} = \{E_1, E_2, E_3, E_4\}$ of the partially transposed matrix $(\hat{\varrho}^{(\text{out})}_{a_m a_n})^{T_2}$ are input-state independent

$$\vec{E} = \left\{ \frac{1}{6}, \frac{1}{6}, \frac{1}{3} + \frac{\sqrt{2(5+4N+N^2)}}{6(N+1)}, \frac{1}{3} - \frac{\sqrt{2(5+4N+N^2)}}{6(N+1)} \right\}. \tag{5.5}$$

Using the Peres-Horodecki theorem [14, 15] we can conclude that the two copied qubits at the output of the copier are iseparable only in the case $N = 1$. In this case one of the eigenvalues (5.5) is negative, which is the necessary and sufficient condition for the inseparability of the matrix (5.4). For $N > 1$ all pairs of copied qubits at the output of the quantum copier are separable (i.e. the eigenvalues given by Eq. (5.5) are positive).

Comment 3

Using the copying transformation (4.13) we find that the basis vectors $|0\rangle_{a_0}$ and $|1\rangle_{a_0}$ of the original qubit are transformed as [compare with Eq. (2.7)]

$$\begin{aligned} |0\rangle_{a_0} |\Psi\rangle^{(\text{in})}_{\vec{a}\vec{b}} &\to \sum_{k=0}^{N} \lambda_k^{(N+1)} |N+1;\, k\rangle_{a_0\vec{a}} |N;\, k\rangle_{\vec{b}}\,; \\ |1\rangle_{a_0} |\Psi\rangle^{(\text{in})}_{\vec{a}\vec{b}} &\to \sum_{k=0}^{N} \lambda_{N-k}^{(N+1)} |N+1;\, k+1\rangle_{a_0\vec{a}} |N;\, k\rangle_{\vec{b}}\,, \end{aligned} \tag{5.6}$$

where

$$\lambda_k^{(N+1)} = \sqrt{\frac{2(N+1-k)}{(N+1)\,(N+2)}}\,. \tag{5.7}$$

We clearly see that the set of $N+1$ completely symmetric orthonormal states $|N;\, k\rangle_{\vec{b}}$ (with $k = 0, 1, \ldots, N$) of the idle qubits b_j plays the role of a set of basis vectors of the abstract quantum copier and in this form the transformation (5.6) describes the action of the quantum copier as discussed by Gisin and Massar [9]. These authors have also shown that transformation (5.6) describes the *optimal* input-state independent $1 \to 1+N$ quantum copier.

Comment 4

We note that idle qubits b_j after the copying is performed are always in the state

$$\hat{\varrho}^{(\text{out})}_{b_j} = \frac{1}{3}\, (\hat{\varrho}^{(\text{id})}_{b_j})^T + \frac{1}{3}\, \hat{1}\,, \qquad j = 1, \ldots, N\,, \tag{5.8}$$

irrespective of the number of copies created from the original qubit. The density operator $\hat{\varrho}^{(\text{out})}_{b_m b_n}$ (here $m, n = 1, \ldots, N$ and $m \neq n$) describing an arbitrary two-idle qubit state at the output is described by the matrix

$$\hat{\varrho}^{(\text{out})}_{b_m b_n} = \frac{1}{6} \begin{pmatrix} 3\,|\beta|^2 + |\alpha|^2 & \alpha\beta^* & \alpha\beta^* & 0 \\ \alpha^*\beta & 1 & 1 & \alpha\beta^* \\ \alpha^*\beta & 1 & 1 & \alpha\beta^* \\ 0 & \alpha^*\beta & \alpha^*\beta & 3\,|\alpha|^2 + |\beta|^2 \end{pmatrix}. \tag{5.9}$$

Firstly, from Eq. (5.9) we see that this density operator does not depend on the number N of copied qubits a_j. Secondly, from Eq. (5.9) we find that eigenvalues $\vec{E} = \{E_1, E_2, E_3, E_4\}$ of the partially transposed matrix $(\hat{\varrho}^{(\mathrm{out})}_{b_m b_n})^{T_2}$ are input-state independent

$$\vec{E} = \left\{ \frac{1}{6}, \frac{1}{6}, \frac{1}{3} + \frac{\sqrt{2}}{6}, \frac{1}{3} - \frac{\sqrt{2}}{6} \right\}. \tag{5.10}$$

and they do not depend on the number of copies a_j. Moreover, these eigenvalues are positive, from which it follows that pairs of the idle qubits at the output of the copier are *not* quantum-mechanically entangled.

Comment 5

To quantify how the "quantum copier" (i.e., the idle qubits) is entangled with the original and the copy qubits at the output, we evaluat the parameter $\xi^{(N)} = \mathrm{Tr}\,[\hat{\varrho}^{(\mathrm{out})}_{\vec{b}}]^2$, which quantifies the purity of the quantum copier. If $\xi = 1$, then the copier (i.e., the subsystem of the whole system $a_0\vec{a}\vec{b}$) is in a pure state. Otherwise (i.e., when $\xi < 1$) it is in an impure state. If the whole system is in a pure state, i.e. $\mathrm{Tr}\,[\hat{\varrho}^{(\mathrm{out})}_{a_0\vec{a}\vec{b}}]^2 = 1$, then ξ quantifies the degree of entanglement between the two subsystem. From Eq. (4.13) we find

$$\xi^{(N)} = \frac{1}{N+1}\,\frac{2(2N^2 + 7N + 6)}{3(N+2)^2}, \tag{5.11}$$

from which it follows that in the limit of large N

$$\xi^{(N)} \simeq \frac{4}{3(N+1)}. \tag{5.12}$$

The lower bound $\xi_{\min}$ of the purity parameter ξ of an arbitrary quantum system in the $N+1$ dimensional Hilbert space (i.e., this is the size of the Hilbert space of the quantum copier) is

$$\xi_{\min} = \frac{1}{N+1}. \tag{5.13}$$

We see that for all values of N the parameter $\xi^{(N)}$ is very close to its lower bound, i.e. the quantum copier and the copies are highly entangled. To understand the nature of this entanglement, we briefly consider the $1 \to 1+1$ quantum copying. In this case, we can evaluate the density operator $\hat{\varrho}^{(\mathrm{out})}_{a_1 b_1}$ which in matrix form can be written as:

$$\hat{\varrho}^{(\mathrm{out})}_{a_1 b_1} = \frac{1}{6}\begin{pmatrix} 4\,|\beta|^2 + |\alpha|^2 & \alpha\beta^* & 2\alpha^*\beta & 2 \\ \alpha^*\beta & |\beta|^2 & 0 & 2\alpha^*\beta \\ 2\alpha\beta^* & 0 & |\alpha|^2 & \alpha\beta^* \\ 2 & 2\alpha\beta^* & \alpha^*\beta & 4\,|\alpha|^2 + |\beta|^2 \end{pmatrix}. \tag{5.14}$$

For α and β real, the eigenvalues of the corresponding partially transposed matrix do not depend on these parameters and they read:

$$\vec{E} = \left\{ \frac{1}{3}, \frac{2}{3}, \frac{1-\sqrt{17}}{12}, \frac{1+\sqrt{17}}{12} \right\}. \tag{5.15}$$

We see that one of the eigenvalues is negative which means that each copy qubit (i.e., either a_0 or a_1) and the idle qubit are *quantum-mechanically* entangled. In the case when α and β are complex, the eigenvalues of the partially transposed matrix associated with the matrix Eq. (5.14) do depend on α and β and one of the eigenvalues is *always* negative. So these qubits are quantum-mechanically entangled.

VI. Conclusions

We have presented a generalization of the universal quantum copying machine which optimally redistributes information from a single original qubit to $N+1$ qubits. We have found a simple quantum network which realizes this quantum copier. Quantum copiers can be effectively utilized in various processes designed for manipulation with quantum information. In particular, quantum copiers can be used for an optimal eavesdropping [16]; they can be applied for realization of the optimal generalized (POVM) measurements [13], or they can be utilized for storage and retrieval of information in quantum computers [17].

Acknowledgements

We would like to that N. Gisin, T. Beth, S. Massar, N. Cerf, D. Bruß, S. Braunstein, and A. Ekert for helpful discussions and correspondence. This work was supported by the United Kingdom Engineering and Physical Sciences Research Council, the Royal Society, and by the National Science Foundation under the grant INT 9221716.

References

[1] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).
[2] D. Diekes, *Phys. Lett. A* **92**, 271 (1982).
[3] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, *Phys. Rev. Lett.* **76**, 2818 (1996).
[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
[5] V. Bužek and M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).
[6] M. Hillery and V. Bužek, *Phys. Rev. A* **56**, 1212 (1997).
[7] V. Bužek, V. Vedral, M. Plenio, P. L. Knight, and M. Hillery, *Phys. Rev. A* **55**, 3327 (1997).
[8] V. Bužek, S. Braunstein, M. Hillery, and D. Bruss, *Phys. Rev. A* **56**, 3446 (1997).
[9] N. Gisin and S. Massar, *Phys. Rev. Lett.* **97**, 2153 (1997).
[10] D. Bruss, D. P. DiVicenzo, A. K. Ekert, C. Machiavello, and J. Smolin: *"Optimal universal and state-dependent quantum cloning"*, [*Los Alamos e-print archive* quant-ph/9703046 (1997)].
[11] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Phys. Rev. A* **52**, 3457.
[12] S. Massar and S. Popescu, *Phys., Rev. Lett.* **74**, 1259 (1995).
[13] R. Derka, V. Bužek, and A. K. Ekert, *Phys. Rev. Lett.* **80**, 1571 (1998).
[14] A. Peres, *Phys. Rev. Lett.* **77**, 1423 (1996).
[15] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1997).
[16] N. Gisin and B. Huttner, *Phys. Lett. A* **228**, 13 (1997).
[17] D. P. DiVincenzo, *Science* **279**, 255 (1995).

(Manuscript received: August 31, 1997)