acta physica slovaca vol. 47 No. 3/4, 193 – 200 June 1997

QUANTUM COPYING[1]

V. Bužek[2]
Optics Section, Blackett Laboratory, Imperial College, London SW7 2BZ, England

M. Hillery[3]
Department of Physics and Astronomy, Hunter College, CUNY,
695 Park Avenue, New York, NY 10021, USA

Received 25 April 1997, accepted 12 May 1997

How well can one copy an arbitrary quantum state? It has been known since the results of Wooters and Zurek that perfect copies cannot be made. This then leads one to ask how well one can do. We analyze the copy machine discussed by Wooters and Zurek in their proof of the "No Cloning" theorem, and a second one in which the quality of the copies is independent of the input state. Problems arising from the entanglement of the copies are discussed and measurement schemes to overcome them are presented. We also find fundamental limits on the quality of the copies which are produced, both in the case of a machine which makes 2 copies and one which makes n copies. Quantum logic circuits which realize the action of a quantum copier are presented.

1. Introduction

One of the most fundamental differences between classical and quantum information is that while classical information can be copied perfectly, quantum cannot. In particular, we cannot create a duplicate of an *arbitrary* quantum bit (*qubit*) [1] without destroying the original. This follows from the *no-cloning theorem* of Wootters and Zurek [2] (see also [3,4]). There are many consequences of this theorem. For example, if one has a string of qubits which one would like to process in more than one way, it represents a serious limitation. With a string of classical bits, one could simply copy the string and process the original one way and the copy another. Quantum mechanically this is impossible. On the other hand, the fact that information cannot be copied is sometimes an advantage. One can view the impossibility of quantum copying as one

[1] Presented at the **Fifth Central-European Workshop on Quantum Optics**, Prague, Czech Republic, April 25 - 28, 1997

[2] E-mail address: v.buzek@ic.ac.uk

[3] E-mail address: mhillery@shiva.hunter.cuny.edu

0323-0465/97 © Institute of Physics, SAS, Bratislava, Slovakia

of the main reasons why quantum cryptography works. In a quantum cryptographic system [5,6] qubits are exchanged between a sender (Alice) and a receiver (Bob) in such a way that the presence of an eavesdropper (Eve) can be detected. If quantum copying were possible the eavesdropper could simply copy the qubits which Alice is sending to Bob, and they would not be able to detect this procedure. This would leave the eavesdropper with a perfect record of their communication. The fact that quantum information cannot be copied rules out this possibility.

Even though one cannot copy quantum information perfectly, it is useful to know how well one can do. One would like to know to what extent it is possible to split the information in a given qubit among several others. In addition, if it is possible to make close to perfect copies quantum cryptographic schemes could still be at risk [7]. Finally, quantum copying can become essential in storage and retrieval of information in quantum computers [8].

If one is only interested in producing imperfect copies, however, then it is possible to design machines (actually, find unitary transformations) which copy quantum states. A number of these were analyzed in a recent paper by two of us [9] (see also [10–12]). The copy machine considered by Wootters and Zurek [2], 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 expectation 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 2/3 that of its expectation value in the input state. Gisin has recently generalized the UQCM for the cases in which there are N identical inputs and $N+1$ outputs, that is one copy is produced, and also in which there are N inputs and $N+2$ outputs, i. e. there are two copies produced [13]. In both cases all of the output copies are identical and their fidelity, that is their overlap with the input state, goes to 1 as N goes to infinity.

2. Universal quantum copying machine

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

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

The two numbers which characterize the state (1) can be associated with the "amplitude" $|\alpha|$ and the "phase" φ of the qubit. Even though ideal copying, i.e., the transformation

$$|\Psi\rangle_{a_0}\longrightarrow|\Psi\rangle_{a_0}|\Psi\rangle_{a_1} \tag{2}$$

is prohibited by the laws of quantum mechanics for an *arbitrary* state (1), it is still possible to design quantum copiers which operate reasonably well. In particular, the UQCM [9] 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 $\hat{\rho}_{a_0}^{(out)}$ and $\hat{\rho}_{a_1}^{(out)}$, respectively, are identical, i.e.,

$$\hat{\rho}_{a_0}^{(out)}=\hat{\rho}_{a_1}^{(out)} \tag{3}$$

(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 distances between density operators of each system at the output ($\hat{\rho}_{a_j}^{(out)}$ where $j=0,1$) and the ideal density operator $\hat{\rho}^{(id)}$ 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

$$d(\hat{\rho}_1;\hat{\rho}_2):=\mathrm{Tr}\left[(\hat{\rho}_1-\hat{\rho}_2)^2\right], \tag{4}$$

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

$$d_1(\hat{\rho}_{a_j}^{(out)};\hat{\rho}_{a_j}^{(id)})=\text{const.};\qquad j=0,1. \tag{5}$$

Here we use the subscript 1 in the definition of the distance d_1, to signify that this is 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 satisfy

$$d_1(\hat{\rho}_{a_j}^{(out)};\hat{\rho}_{a_j}^{(id)})=\min\left\{d_1(\hat{\rho}_{a_j}^{(out)};\hat{\rho}_{a_j}^{(id)})\right\};\qquad (j=0,1). \tag{6}$$

Originally, the UQCM was found by guessing 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 (6) has only been shown recently [13,14].

The unitary transformation which implements the UQCM [9] is given by

$$\begin{aligned}|0\rangle_{a_0}|Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}}|00\rangle_{a_0a_1}|\uparrow\rangle_x+\sqrt{\frac{1}{3}}|+\rangle_{a_0a_1}|\downarrow\rangle_x\\ |1\rangle_{a_0}|Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}}|11\rangle_{a_0a_1}|\downarrow\rangle_x+\sqrt{\frac{1}{3}}|+\rangle_{a_0a_1}|\uparrow\rangle_x,\end{aligned} \tag{7}$$

where

$$|+\rangle_{a_0a_1}=\frac{1}{\sqrt{2}}(|10\rangle_{a_0a_1}+|01\rangle_{a_0a_1}), \tag{8}$$

and satisfies the conditions (3-6). 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 initially in a state $|0\rangle_{a_1}$ ("blank paper" in a copier). The states 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 (1) then the reduced density operators of both copies at the output are equal [see condition (3)] and they can be expressed as

$$\hat{\rho}_{a_j}^{(out)} = \frac{5}{6}|\Psi\rangle_{a_j}\langle\Psi| + \frac{1}{6}|\Psi_\perp\rangle_{a_j}\langle\Psi_\perp|, \qquad j = 0,1 \tag{9}$$

where

$$|\Psi_\perp\rangle_{a_j} = \beta^\star|0\rangle_{a_j} - \alpha^\star|1\rangle_{a_j}, \tag{10}$$

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 that one we did not.

We note that the density operator $\rho_{a_j}^{(out)}$ given by Eq. (9) can be rewritten in a "scaled" form:

$$\hat{\rho}_{a_j}^{(out)} = s_j\hat{\rho}_{a_j}^{(id)} + \frac{1-s_j}{2}\hat{1}; \qquad j = 0,1, \tag{11}$$

which guarantees that the distance (4) is input-state independent, i.e. the condition (5) is automatically fulfilled. The scaling factor in Eq. (11) is $s_j = 2/3$ $(j = 0,1)$.

3. 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 one 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

$$\begin{aligned} \hat{R}_j(\theta)|0\rangle_j &= \cos\theta|0\rangle_j + \sin\theta|1\rangle_j; \\ \hat{R}_j(\theta)|1\rangle_j &= -\sin\theta|0\rangle_j + \cos\theta|1\rangle_j. \end{aligned} \tag{12}$$

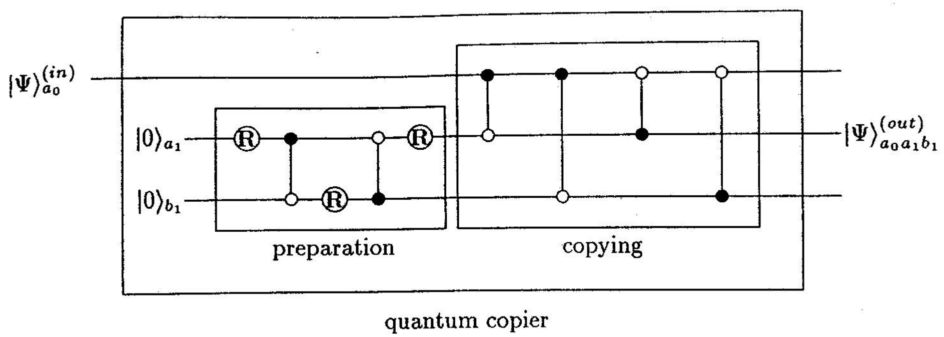

Fig. 1. Graphical representation of the UQCM network. The logical controlled-NOT $\hat{P}_{kl}$ given by Eq. (13) has as its input a control qubit (denoted as •) and a target qubit (denoted as o). The action of the single-qubit operator **R** is specified by the transformation (12). We separate the preparation 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 an 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.

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

$$\begin{aligned} \hat{P}_{kl}|0\rangle_k|0\rangle_l &= |0\rangle_k|0\rangle_l; \\ \hat{P}_{kl}|0\rangle_k|1\rangle_l &= |0\rangle_k|1\rangle_l; \\ \hat{P}_{kl}|1\rangle_k|0\rangle_l &= |1\rangle_k|1\rangle_l; \\ \hat{P}_{kl}|1\rangle_k|1\rangle_l &= |1\rangle_k|0\rangle_l. \end{aligned} \tag{13}$$

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 $|\Psi\rangle_{a_1b_1}^{(prep)}$. 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

$$|\Psi\rangle_{a_0}^{(in)}|0\rangle_{a_1}|0\rangle_{b_1} \longrightarrow |\Psi\rangle_{a_0}^{(in)}|\Psi\rangle_{a_1b_1}^{(prep)} \longrightarrow |\Psi\rangle_{a_0a_1b_1}^{(out)}. \tag{14}$$

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

3.1 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 $|\Psi\rangle^{(prep)}_{a_1b_1}$. If we assume that initially these two qubits are in the state

$$|\Psi\rangle^{(in)}_{a_1b_1} = |0\rangle_{a_1}|0\rangle_{b_1}, \tag{15}$$

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

$$|\Psi\rangle^{(prep)}_{a_1b_1} = C_1|00\rangle_{a_1b_1} + C_2|01\rangle_{a_1b_1} + C_3|10\rangle_{a_1b_1} + C_4|11\rangle_{a_1b_1}, \tag{16}$$

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.

$$|\Psi\rangle^{(prep)}_{a_1b_1} = \hat{R}_{a_1}(\theta_3)\hat{P}_{b_1a_1}\hat{R}_{b_1}(\theta_2)\hat{P}_{a_1b_1}\hat{R}_{a_1}(\theta_1)|0\rangle_{a_1}|0\rangle_{b_1}. \tag{17}$$

Comparing Eqs. (16) and (17) we find a set of equations

$$\begin{array}{rcl} \cos\theta_1\cos\theta_2\cos\theta_3 + \sin\theta_1\sin\theta_2\sin\theta_3 & = & C_1; \\ -\cos\theta_1\sin\theta_2\sin\theta_3 + \sin\theta_1\cos\theta_2\cos\theta_3 & = & C_2; \\ \cos\theta_1\cos\theta_2\sin\theta_3 - \sin\theta_1\sin\theta_2\cos\theta_3 & = & C_3; \\ \cos\theta_1\sin\theta_2\cos\theta_3 + \sin\theta_1\cos\theta_2\sin\theta_3 & = & C_{4,}. \end{array} \tag{18}$$

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

$$|\Psi\rangle^{(prep)}_{a_1b_1} = \frac{1}{\sqrt{6}}\left(2|00\rangle_{a_1b_1} + |01\rangle_{a_1b_1} + |11\rangle_{a_1b_1}\right). \tag{19}$$

With the help of Eq. (18) we find that the rotation angles necessary for the preparation of the state given in Eq. (19) are such that

$$\cos 2\theta_1 = \frac{1}{\sqrt{5}}; \qquad \cos 2\theta_2 = \frac{\sqrt{5}}{3}; \qquad \cos 2\theta_3 = \frac{2}{\sqrt{5}}. \tag{20}$$

3.2 Quantum copying

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

$$|\Psi\rangle^{(out)}_{a_0a_1b_1} = \hat{P}_{b_1a_0}\hat{P}_{a_1a_0}\hat{P}_{a_0b_1}\hat{P}_{a_0a_1}|\Psi\rangle^{(in)}_{a_0}|\Psi\rangle^{(prep)}_{a_1b_1}. \tag{21}$$

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. (7) with $|\uparrow\rangle_x \equiv |0\rangle_{b_1}$ and $|\downarrow\rangle_x \equiv |1\rangle_{b_1}$. When the original qubit is in the superposition state (1) then the state vector of the three qubits after the copying has been performed reads

$$|\Psi\rangle^{(out)}_{a_0a_1b_1} = |\Phi_0\rangle_{a_0a_1}|0\rangle_{b_1} + |\Phi_1\rangle_{a_0a_1}|1\rangle_{b_1}, \tag{22}$$

with

$$|\Phi_0\rangle_{a_0a_1} = \alpha\sqrt{\frac{2}{3}}|00\rangle_{a_0a_1} + \beta\frac{1}{\sqrt{3}}|+\rangle_{a_0a_1}; \quad |\Phi_1\rangle_{a_0a_1} = \beta\sqrt{\frac{2}{3}}|11\rangle_{a_0a_1} + \alpha\frac{1}{\sqrt{3}}|+\rangle_{a_0a_1}. \tag{23}$$

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

$$\hat{\rho}^{(out)}_{a_0a_1} = |\Phi_0\rangle_{a_0a_1}\langle\Phi_0| + |\Phi_1\rangle_{a_0a_1}\langle\Phi_1|. \tag{24}$$

Each of the copy qubits at the output of the quantum copier has a reduced density operator $\hat{\rho}^{(out)}_{a_j}$ ($j = 0,1$) given by Eq. (11). The distance $d_1(\hat{\rho}^{(out)}_{a_j};\hat{\rho}^{(id)}_{a_j})$ ($j = 0,1$) between the output qubit and the ideal qubit is constant and can expressed as a function of the scaling parameter s in Eq. (11):

$$d_1(\hat{\rho}^{(out)}_{a_j};\hat{\rho}^{(id)}_{a_j}) = \frac{(1-s)^2}{2} = \frac{1}{18}. \tag{25}$$

Analogously we find the distance $d_2(\hat{\rho}^{(out)}_{a_0a_1};\hat{\rho}^{(id)}_{a_0a_1})$ between the two-qubit output of the quantum copying and the ideal output to be constant, i.e.

$$d_2(\hat{\rho}^{(out)}_{a_0a_1};\hat{\rho}^{(id)}_{a_0a_1}) = \frac{s^2}{2} = \frac{2}{9}. \tag{26}$$

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

$$\hat{\rho}^{(out)}_{b_1} = \frac{1}{3}\left(\hat{\rho}^{(id)}_{b_1}\right)^{\mathrm{T}} + \frac{1}{3}\hat{1}, \tag{27}$$

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 output qubit depends on the initial state of the original qubit, i.e.

$$d_1(\hat{\rho}^{(out)}_{b_1};\hat{\rho}^{(id)}_{b_1}) = \frac{2}{9}\left(1 + 12|\alpha|^2|\beta|^2\sin^2\varphi\right), \tag{28}$$

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 $\hat{A}$

$$\mathrm{Tr}(\hat{\rho}^{(in)}_{b_1}\hat{A}) = \mathrm{Tr}\left((\hat{\rho}^{(in)}_{b_1})^{\mathrm{T}}\hat{A}^{\mathrm{T}}\right). \tag{29}$$

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

4. Conclusion

Here we have discussed the UQCM and its realization as a quantum logic network. We would now like to mention two other issues in the theory of quantum copying. One involves how good quantum copies can be while the other concerns the production of multiple copies.

Suppose we want to build a copy machine which will copy only two input states. If the states are orthogonal they can be copied without error, while if they are not, the copies will be imperfect. It is possible to use the fact that a copying transformation must be unitary to find lower bounds on the copying error in terms of the overlap of the vectors [10]. These bounds can in turn be used to find a weak lower bound for the copying error produced by a copier which copies all, and not just two, input states. The same methods are also able to provide lower bounds for the copying error introduced by copy machines which produce N, instead of just two, copies. One finds that as N increases so must the error in each copy.

A 1 → N quantum copier which copies all input states equally well was recently found by Gisin [13]. The single-copy density matrixes are of the form given in Eq. (11) and the scaling factor s decreases as N increases. A quantum logic network which realizes this copier has also been found [15].

The study of quantum information, its manipulation and transmission, is a relatively new subject. Quantum copying should be a useful tool in its exploration.

Acknowledgements We thank N. Gisin for communication of his resent results to us. We also thank P.L. Knight, S. Braunstein, D. Bruß, J. Smolin, D.P. DiVincenzo, and A.K. Ekert for useful discussions. This work was supported by the United Kingdom Engineering and Physical Sciences Research Council, by the grant agency VEGA of the Slovak Academy of Sciences (under the project 2/1152/96), and by the National Science Foundation under the grant INT 9221716.

References

[1] A. Barenco, A.K. Ekert: *Acta Physica Slovaca* **45** (1995) 205

[2] W.K. Wootters, W.H. Zurek: *Nature* **299** (1982) 802

[3] D. Diekes: *Phys. Lett. A* **92** (1982) 271

[4] H. Barnum et al.: *Phys. Rev. Lett.* **76** (1996) 2818

[5] A.K. Ekert: *Phys. Rev. Lett.* **67** (1991) 661

[6] C.H. Bennett: *Phys. Rev. Lett.* **68** (1992) 3121

[7] N. Gisin, B. Huttner: *Phys. Lett. A* **228** (1997) 13

[8] D.P. DiVincenzo: *Science* **279** (1995) 255

[9] V. Bužek, M. Hillery: *Phys. Rev. A* **54** (1996) 1844

[10] M. Hillery, V. Bužek: *"Quantum copying: Fundamental inequalities"*, *Phys. Rev. A*, to appear

[11] V. Bužek, V. Vedral, M. Plenio, P.L. Knight, M. Hillery: *Phys. Rev. A* **55** (1997) 3327

[12] V. Bužek, S. Braunstein, M. Hillery, D. Bruß: *http://xxx.lanl.gov/abs/quant-ph/9703046*

[13] N. Gisin: *"Quantum cloning machines"*, unpublished

[14] D. Bruß: private communication

[15] V. Bužek, M. Hillery: unpublished