

# Universal Optimal Cloning of Qubits and Quantum Registers

V. Bužek<sup>1</sup> and M. Hillery<sup>2</sup>

<sup>1</sup> Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28  
Bratislava, Slovakia

<sup>2</sup> Department of Physics and Astronomy, Hunter College, CUNY, 695 Park Avenue,  
New York, NY 10021, USA

**Abstract.** We review our recent work on the universal (i.e. input state independent) optimal quantum copying (cloning) of qubits. We present unitary transformations which describe the optimal cloning of a qubit, and we present the corresponding quantum logic network. We also present a network for an optimal quantum copying “machine” (transformation) which produces  $N + 1$  identical copies from the original qubit. Here again 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,  $N$ . In addition, we present the machine which universally clones states of quantum objects in arbitrary-dimensional Hilbert spaces. In particular, we discuss universal cloning of quantum registers.

**Keywords:** quantum cloning, quantum logic networks, inseparability

## 1 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 while preserving the state of the original qubit. In the quantum *teleportation* (see [4] and references therein), 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.

We have shown recently [5,6] that if one is only interested in producing *imperfect* copies, then it is possible to make quantum clones of the original qubit. For example, the copy machine considered by Wootters and Zurek [1] in their proof of the no-cloning theorem 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  $\varphi$  is arbitrary. We have introduced [5,6,7] a different copying machine, the Universal Quantum

Copying Machine (UQCM), which 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 relevant observables. This UQCM was shown to be optimal, in the sense that it maximizes the average fidelity between the input and output qubits, by Gisin and Massar [8] and by Bruß et al. [9]. Gisin and Massar have also been able to find copying transformations which produce  $N$  copies from  $M$  originals (where  $N > M$ ) [8]. In addition, we have proposed quantum logic networks for quantum copying (cloning) machines [7,10], and bounds have been placed on how good copies can be [11,12].

In this paper we will firstly review our original ideas on the universal quantum copying of a single qubit (Section II). In Section III we will present a quantum network describing the UQCM. Secondly, in Section IV we will introduce the copying machine which produces  $N + 1$  identical copies from the original qubit and present a quantum network which implements it. The quality (fidelity) of the copies does not depend on the state of the original and is only a function of a number  $N$  of copies produced. This machine is formally described by the same unitary transformation recently introduced by Gisin and Massar [8]. In Section V we will analyze the properties of multiply cloned qubits. Thirdly, in Section VI we show how quantum registers (i.e. systems composed of many entangled qubits) can be universally cloned. One approach is to use single-qubit copiers to individually (locally) copy each qubit. We have shown earlier [13] that in the case of two qubits this local copying will preserve some of the quantum correlations between qubits, but as we will show, it does not make a particularly good copy of the two-qubit state. As an alternative we propose a copy machine which universally clones quantum states in arbitrary-dimensional Hilbert spaces. This allow us to discuss the cloning of quantum registers.

## 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  $|\Psi\rangle_{a_0}$

$$|\Psi\rangle_{a_0} = \alpha|0\rangle_{a_0} + \beta|1\rangle_{a_0}; \quad \alpha = \sin \vartheta/2e^{i\varphi}; \quad \beta = \cos \vartheta/2. \quad (1)$$

The two numbers which characterize the state (1) can be associated with the “amplitude”  $|\alpha|$  and the “phase”  $\varphi$  of the qubit. Even though ideal copying, i.e., the transformation  $|\Psi\rangle_{a_0} \longrightarrow |\Psi\rangle_{a_0}|\Psi\rangle_{a_1}$  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 [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  $\hat{\rho}_{a_0}^{(out)}$  and  $\hat{\rho}_{a_1}^{(out)}$ , respectively, are identical, i.e.,

$$\hat{\rho}_{a_0}^{(out)} = \hat{\rho}_{a_1}^{(out)} \quad (2)$$

(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 Bures distance [14]

$$d_B(\hat{\rho}_1, \hat{\rho}_2) = \sqrt{2} \left( 1 - \text{Tr} \sqrt{\hat{\rho}_1^{1/2} \hat{\rho}_2 \hat{\rho}_1^{1/2}} \right)^{1/2}, \quad (3)$$

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

$$d_B(\hat{\rho}_{a_j}^{(out)}; \hat{\rho}_{a_j}^{(id)}) = \text{const.}; \quad j = 0, 1. \quad (4)$$

(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  $\hat{\rho}_{a_j}^{(out)}$  of the copied qubit and the ideal state  $\hat{\rho}_{a_j}^{(id)}$ . 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.,  $\mathcal{H} = \mathcal{H}_{a_0} \otimes \mathcal{H}_{a_1} \otimes \mathcal{H}_x$ )

$$d_B(\hat{\rho}_{a_j}^{(out)}; \hat{\rho}_{a_j}^{(id)}) = \min \left\{ d_B^{(U)}(\hat{\rho}_{a_j}^{(out)}; \hat{\rho}_{a_j}^{(id)}); \forall U \right\}; \quad (j = 0, 1). \quad (5)$$

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 (5) has only been shown recently [8,9].

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

$$\begin{aligned} |0\rangle_{a_0} |Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}} |00\rangle_{a_0 a_1} |\uparrow\rangle_x + \sqrt{\frac{1}{3}} |+\rangle_{a_0 a_1} |\downarrow\rangle_x \\ |1\rangle_{a_0} |Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}} |11\rangle_{a_0 a_1} |\downarrow\rangle_x + \sqrt{\frac{1}{3}} |+\rangle_{a_0 a_1} |\uparrow\rangle_x, \end{aligned} \quad (6)$$

where  $|+\rangle_{a_0 a_1} = (|10\rangle_{a_0 a_1} + |01\rangle_{a_0 a_1})/\sqrt{2}$ . This transformation satisfies the conditions (2-5). 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 prepared initially in the state  $|0\rangle_{a_1}$  (it plays the role that a blank piece of paper plays in a copier). 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 (2)] and they can be expressed as

$$\hat{\rho}_{a_j}^{(out)} = \frac{5}{6} |\Psi\rangle_{a_j} \langle \Psi| + \frac{1}{6} |\Psi_{\perp}\rangle_{a_j} \langle \Psi_{\perp}|, \quad j = 0, 1 \tag{7}$$

where  $|\Psi_{\perp}\rangle_{a_j} = \beta^* |0\rangle_{a_j} - \alpha^* |1\rangle_{a_j}$ , 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  $\hat{\rho}_{a_j}^{(out)}$  given by Eq.(7) can be rewritten in a “scaled” form:

$$\hat{\rho}_{a_j}^{(out)} = s_j \hat{\rho}_{a_j}^{(id)} + \frac{1 - s_j}{2} \hat{1}; \quad j = 0, 1, \tag{8}$$

which guarantees that the distance (3) is input-state independent, i.e. the condition (4) is automatically fulfilled. The scaling factor in Eq.(8) is  $s_j = 2/3$  ( $j = 0, 1$ ).

The Bures distance  $d_B(\hat{\rho}_{a_j}^{(out)}; \hat{\rho}_{a_j}^{(id)})$  ( $j = 0, 1$ ) between the output qubit and the ideal qubit is constant and it reads

$$d_B(\hat{\rho}_{a_j}^{(out)}; \hat{\rho}_{a_j}^{(id)}) = \sqrt{2} \left( 1 - \sqrt{\frac{5}{6}} \right). \tag{9}$$

We note, that the idle qubit after the copying is performed is in a state

$$\hat{\rho}_{b_1}^{(out)} = \frac{1}{3} \left( \hat{\rho}_{b_1}^{(id)} \right)^T + \frac{1}{3} \hat{1}, \tag{10}$$

where the superscript T denotes the transpose.

We stress 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 [8]

$$\mathcal{F} = \int d\Omega_{a_j} \langle \Psi | \hat{\rho}_{a_j}^{(out)} | \Psi \rangle_{a_j}, \tag{11}$$

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

### 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 a 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

$$\hat{R}_j(\theta)|0\rangle_j = \cos\theta|0\rangle_j + \sin\theta|1\rangle_j; \quad \hat{R}_j(\theta)|1\rangle_j = -\sin\theta|0\rangle_j + \cos\theta|1\rangle_j. \quad (12)$$

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 and a 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):

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

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  $|\Psi\rangle_{a_1 b_1}^{(prep)}$ . Then in the second part, the 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

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

### 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 specific state  $|\Psi\rangle_{a_1 b_1}^{(prep)}$

$$|\Psi\rangle_{a_1 b_1}^{(prep)} = \frac{1}{\sqrt{6}}(2|00\rangle_{a_1 b_1} + |01\rangle_{a_1 b_1} + |11\rangle_{a_1 b_1}), \quad (15)$$

which can be prepared by a simple quantum network with two controlled-NOTs  $\hat{P}_{kl}$  and three rotations  $\hat{R}(\theta_j)$ , i.e.

$$|\Psi\rangle_{a_1 b_1}^{(prep)} = \hat{R}_{a_1}(\theta_3)\hat{P}_{b_1 a_1}\hat{R}_{b_1}(\theta_2)\hat{P}_{a_1 b_1}\hat{R}_{a_1}(\theta_1)|0\rangle_{a_1}|0\rangle_{b_1}, \quad (16)$$

with the rotation angles defined as [7]

$$\cos 2\theta_1 = \frac{1}{\sqrt{5}}; \quad \cos 2\theta_2 = \frac{\sqrt{5}}{3}; \quad \cos 2\theta_3 = \frac{2}{\sqrt{5}}. \quad (17)$$

### 3.2 Quantum Copying

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

$$|\Psi\rangle_{a_0 a_1 b_1}^{(out)} = \hat{P}_{b_1 a_0} \hat{P}_{a_1 a_0} \hat{P}_{a_0 b_1} \hat{P}_{a_0 a_1} |\Psi\rangle_{a_0}^{(in)} |\Psi\rangle_{a_1 b_1}^{(prep)}. \quad (18)$$

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.(6) with  $|\uparrow\rangle_x \equiv |0\rangle_{b_1}$  and  $|\downarrow\rangle_x \equiv |1\rangle_{b_1}$ .

## 4 Multiple Copying

Here we present a generalization of the quantum network (18) to the case when a set of  $N$  copy qubits  $a_j$  ( $j = 1, \dots, N$ ) are produced out of the original qubit  $a_0$  [10].

To find the  $1 \rightarrow 1 + N$  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  $|N; 0\rangle_{\mathbf{a}} \equiv |0\rangle_{a_1} \dots |0\rangle_{a_N}$  (here the subscript  $\mathbf{a}$  is a shorthand notation indicating that  $|N; 0\rangle_{\mathbf{a}}$  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  $|N; 0\rangle_{\mathbf{b}} \equiv |0\rangle_{b_1} \dots |0\rangle_{b_N}$ .

(3) Prior to the transfer of information from the original qubit, the copy and the idle qubits have to be prepared in a specific state  $|\Psi\rangle_{\mathbf{ab}}^{(prep)}$

$$|\Psi\rangle_{\mathbf{ab}}^{(prep)} = \sum_{k=0}^N [e_k |N; k\rangle_{\mathbf{a}} + f_k |N; k-1\rangle_{\mathbf{a}}] |N; k\rangle_{\mathbf{b}}, \quad (19)$$

where

$$e_k = \sqrt{\frac{2}{N+2}} \frac{\binom{N}{k}}{\binom{N+1}{k}}; \quad f_k = \sqrt{\frac{k}{N-k+1}} e_k, \quad (20)$$

and  $|N; k\rangle_{\mathbf{a}}$  are normalized *symmetric*  $N$ -qubit state vectors with  $k$  qubits in the state  $|1\rangle$  and  $(N - k)$  qubits in the state  $|0\rangle$ . The states (19) can be obtained by performing a sequence of local rotations  $\mathbf{R}$  and controlled-NOT operations analogous to Eq.(16) [15]. Once the copying machine is prepared in the state  $|\Psi\rangle_{\mathbf{ab}}^{(prep)}$  we can start to copy information from the original qubit  $a_0$ .

To describe the copying network we firstly introduce an operator  $\hat{Q}_{a_0 \mathbf{a}}$  which is a product of the controlled-NOTs defined by Eq.(13) with  $a_0$  being a control qubit and  $a_j$  ( $j = 1, \dots, N$ ) being targets:

$$\hat{Q}_{a_0 \mathbf{a}} \equiv \hat{P}_{a_0 a_N} \hat{P}_{a_0 a_{N-1}} \dots \hat{P}_{a_0 a_1}. \quad (21)$$

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

$$\hat{Q}_{\mathbf{a}a_0} \equiv \hat{P}_{a_N a_0} \hat{P}_{a_{N-1} a_0} \dots \hat{P}_{a_1 a_0}. \quad (22)$$

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

$$|\Psi\rangle_{a_0}^{(in)} |N; 0\rangle_{\mathbf{a}} |N; 0\rangle_{\mathbf{b}} \longrightarrow |\Psi\rangle_{a_0}^{(in)} |\Psi\rangle_{\mathbf{ab}}^{(prep)} \longrightarrow |\Psi\rangle_{a_0 \mathbf{ab}}^{(out)}, \quad (23)$$

where the  $(2N + 1)$  qubit output of the copying process is described by the state vector  $|\Psi\rangle_{a_0 \mathbf{ab}}^{(out)}$  which is obtained after the following sequence of operations

$$|\Psi\rangle_{a_0 \mathbf{ab}}^{(out)} = \hat{Q}_{\mathbf{b}a_0} \hat{Q}_{\mathbf{a}a_0} \hat{Q}_{a_0 \mathbf{b}} \hat{Q}_{a_0 \mathbf{a}} |\Psi\rangle_{a_0}^{(in)} \cdot |\Psi\rangle_{\mathbf{ab}}^{(prep)}. \quad (24)$$

This last equation describes a simple quantum network when firstly the original qubit controls the target qubits of the quantum copier. Then the qubits  $\mathbf{a}$  and  $\mathbf{b}$  “control” the state of the original qubit via another sequence of controlled-NOTs. In this way one can produce out of a single original qubit a set of quantum clones. This quantum network realizes the unitary transformation for  $1 \rightarrow 1 + N$  cloning as introduced by Gisin and Massar [8].

## 5 Properties of Copied Qubits

Using the explicit expression for the output state  $|\Psi\rangle_{a_0 \mathbf{ab}}^{(out)}$  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

$$\hat{\rho}_{a_j}^{(out)} = s^{(N)} \hat{\rho}_{a_j}^{(id)} + \frac{1 - s^{(N)}}{2} \hat{1}; \quad j = 0, 1, \dots, N, \quad (25)$$

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

$$s^{(N)} = \frac{1}{3} + \frac{2}{3(N + 1)}, \quad (26)$$

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 III. We also note that in the limit  $N \rightarrow \infty$ , 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

$$\hat{\rho}_{a_j}^{(out)} = \frac{1}{3} \hat{\rho}_{a_j}^{(id)} + \frac{1}{3} \hat{1}; \quad j = 0, 1, \dots, \infty, \quad (27)$$

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 [16,17]. From this

point of view one can consider quantum copying as a transformation of quantum information into classical information [8]. This also suggests that quantum copying can be utilized to obtain novel insights 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 performed on the original qubit].

**Comment 1**

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

$$\hat{\rho}_{b_j}^{(out)} = \frac{1}{3} \left( \hat{\rho}_{b_j}^{(id)} \right)^T + \frac{1}{3} \hat{1}, \quad j = 1, \dots, N, \tag{28}$$

*irrespective* of the number of copies created from the original qubit.

**Comment 2**

Using the Peres-Horodecki theorem [18,19] we can conclude that an arbitrary pair  $\hat{\rho}_{a_m a_n}^{(out)}$  out of  $N + 1$  of copied qubits at the output of the copier is inseparable *only* in the case  $N = 1$ . In this case one of the eigenvalues of the partially transposed operator  $[\hat{\rho}_{a_0 a_1}^{(out)}]^{T_2}$  is negative, which is the necessary and sufficient condition for the inseparability of the matrix  $\hat{\rho}_{a_0 a_1}^{(out)}$ . For  $N > 1$  all pairs of copied qubits at the output of the quantum copier are separable.

## 6 Cloning of Quantum Registers

In what follows we will propose a copy machine which universally copies higher dimensional systems. We shall be particularly interested in how the quality of the copies scales with the dimensionality,  $M$ , of the system being copied. What we find is that the fidelity of the copies decreases with  $M$ , as expected, but, somewhat surprisingly, does not go to zero as  $M$  goes to infinity.

Let us consider a quantum system prepared in a pure state which is described by the vector

$$|\Phi\rangle_{a_0} = \sum_{i=1}^M \alpha_i |\Psi_i\rangle_{a_0} \tag{29}$$

in an  $M$ -dimensional Hilbert space spanned by  $M$  orthonormal basis vectors  $|\Psi_i\rangle_{a_0}$  ( $i = 1, \dots, M$ ). The complex amplitudes  $\alpha_i$  are normalized to unity, i.e.  $\sum |\alpha_i|^2 = 1$ . In particular, one can consider  $M = 2^m$  where  $m$  is the number of qubits in a given quantum register. One can generalize the no-cloning theorem which has been proven for spin-1/2 particles (qubits) by Wootters and Zurek [1] for arbitrary quantum systems. That is, there does not exist a unitary transformation such that the state given in Eq. (29) can be ideally cloned (copied), i.e. it is impossible to find a unitary transformation such that  $|\Phi\rangle_{a_0} \longrightarrow |\Phi\rangle_{a_0} |\Phi\rangle_{a_1}$  for an arbitrary input states.

Following our previous discussion we can ask whether a universal cloning transformation exists which will generate two imperfect copies from the original

state,  $|\Phi\rangle_{a_0}$ . The quality of the cloning should not depend on the particular state (in the given Hilbert space) which is going to be copied. This input-state independence (invariance) of the cloning can be formally expressed as

$$\hat{\rho}_{a_j}^{(out)} = s\hat{\rho}_{a_j}^{(id)} + \frac{1-s}{M}\hat{1}, \quad (30)$$

where  $\hat{\rho}_{a_j}^{(id)} = |\Phi\rangle_{a_0 a_0} \langle\Phi|$  is the density operator describing the original state which is going to be copied. This scaling form of Eq.(30) guarantees that the Bures distance (3) between the input and the output density operators is input-state independent.

The quantum copying machine we shall use is itself an  $M$  dimensional quantum system, and we shall let  $|X_i\rangle_x$  ( $i = 1, \dots, M$ ) be an orthonormal basis of the copying machine Hilbert space. This copier is initially prepared in a particular state  $|X\rangle_x$ . The action of the cloning transformation can be specified by a unitary transformation acting on basis vectors of the tensor product space of the original quantum system  $|\Psi_i\rangle_{a_0}$ , the copier, and an additional  $M$ -dimensional system which is to become the copy (which is initially prepared in a state  $|0\rangle_{a_1}$ ). We have found the transformation of the basis vectors  $|\Psi_i\rangle_{a_0}$

$$\begin{aligned} |\Psi_i\rangle_{a_0} |0\rangle_{a_1} |X\rangle_x \longrightarrow & c|\Psi_i\rangle_{a_0} |\Psi_i\rangle_{a_1} |X_i\rangle_x \\ & + d \sum_{j \neq i}^M (|\Psi_i\rangle_{a_0} |\Psi_j\rangle_{a_1} + |\Psi_j\rangle_{a_0} |\Psi_i\rangle_{a_1}) |X_j\rangle_x; \end{aligned} \quad (31)$$

(where  $i = 1, \dots, M$ ) with the coefficients

$$c = \frac{2}{\sqrt{2(M+1)}}; \quad d = \frac{1}{\sqrt{2(M+1)}}, \quad (32)$$

such that the input-state independence of cloning is satisfied. That is, the clones have density operators given by Eq.(30) with the scaling factor

$$s = c^2 + (M-2)d^2 = \frac{(M+2)}{2(M+1)}. \quad (33)$$

If  $M = 2$ , then the transformation (31) reduces to the copying transformation for qubits given by Eq.(6). From earlier results of Gisin and Massar [8] the optimality of the transformation (31) for  $M = 2$  directly follows. At the moment we are not able to prove rigorously that the cloning transformation (31) is *optimal* for arbitrary  $M > 2$ . Nevertheless, we have performed numerical tests which suggest that the cloning transformation (31) is optimal.

We note that the scaling factor (33), which describes the quality of the copy, is a decreasing function of  $M$ . This is not surprising, because a quantum state in a large dimensional space contains more quantum information than one in a small dimensional one (e. g. a state in a 4 dimensional space contains information about 2 qubits while a state in a 2 dimensional one describes only a single qubit), so that as  $M$  increases one is trying to copy more and more quantum information.

On the other hand, it is interesting to note that in the limit  $M \rightarrow \infty$ , i.e. in the case when the Hilbert space of the given quantum system is infinite dimensional (e.g. quantum-mechanical harmonic oscillator), the cloning can still be performed efficiently with the scaling factor equal to  $1/2$ .

In order to confirm that the quality of the copies which the copying transformation (31) produces is input-state independent (i.e., all states are cloned equally well) we evaluate the Bures distance (3). In our particular case we find, that the distance between  $\hat{\rho}_{a_k}^{(out)}$  and  $\hat{\rho}_{a_k}^{(id)}$  depends only on the dimension of the Hilbert space  $M$ , but not on the state which is cloned, i.e.

$$d_B(\hat{\rho}_{a_k}^{(out)}, \hat{\rho}_{a_k}^{(id)}) = \sqrt{2} \left( 1 - \sqrt{\frac{M+3}{2(M+1)}} \right)^{1/2}. \tag{34}$$

The Bures distance given by Eq. (34) is maximal when states in the infinite-dimensional Hilbert space are cloned, and in that case we find

$$\lim_{M \rightarrow \infty} d_B(\hat{\rho}_{a_k}^{(out)}, \hat{\rho}_{a_k}^{(id)}) = \sqrt{2 - \sqrt{2}}. \tag{35}$$

This means that even for an infinite-dimensional system, reasonable cloning can be performed, which is reflected in the fact that the corresponding scaling factor  $s$  is equal to  $1/2$ .

### 6.1 Local vs. Nonlocal Cloning

Finally, we compare two methods of copying quantum registers. In particular, we shall consider cloning an entangled state of two qubits. We assume that the two qubits are prepared in the state

$$|\Phi\rangle_{a_0 b_0} = \alpha|00\rangle_{a_0 b_0} + \beta|11\rangle_{a_0 b_0}, \tag{36}$$

where, for simplicity, we have taken  $\alpha$  and  $\beta$  to be real, and  $\alpha^2 + \beta^2 = 1$ . First, we shall consider the case in which each of the two qubits  $a_0$  and  $b_0$  is copied *locally* by two independent quantum copiers [13]. Each of these two copiers is described by the transformation (31) with  $M = 2$ . Next, we shall consider a *nonlocal* cloning of the two-qubit state (36) when this system is cloned via the unitary transformation (31) with  $M = 4$ , i.e. the cloner in this case acts non-locally on the two qubits. Our chief task will be to analyze how inseparability is cloned in these two scenarios, but we shall also examine the quality of the copies which are produced. From the Peres-Horodecki theorem it follows that the state (36) is inseparable for all values of  $\alpha^2$  such that  $0 < \alpha^2 < 1$ .

Firstly, let us suppose that the two original qubits  $a_0$  and  $b_0$  are cloned independently (locally) by two independent local cloners  $X_I$  and  $X_{II}$ , each described by the transformation (31) with  $M = 2$ . The cloner  $X_I$  ( $X_{II}$ ) generates out of qubit  $a_0$  ( $b_0$ ) two qubits  $a_0$  and  $a_1$  ( $b_0$  and  $b_1$ ). After we perform trace over the two cloners we obtain a four-qubit density operator  $\hat{\rho}_{a_0 a_1 b_0 b_1}^{(out)}$  which also describes two nonlocal two-qubit systems, i.e.  $\hat{\rho}_{a_0 b_1}$  and  $\hat{\rho}_{a_1 b_0}$ . These two two-qubit

systems are the clones of the original two-qubit register (36). We note that these density matrices cannot be expressed in the scaled form (30), and that the quality of the copies depends on the input state. From the Peres-Horodecki theorem we immediately find that the density operators  $\hat{\rho}_{a_0 b_1}$  and  $\hat{\rho}_{a_1 b_0}$  are inseparable if

$$\frac{1}{2} - \frac{\sqrt{39}}{16} \leq \alpha^2 \leq \frac{1}{2} + \frac{\sqrt{39}}{16}. \quad (37)$$

This proves that for a restricted set of pure two-qubit states (36) satisfying the condition (37), it is possible to perform a *local* cloning such that the original inseparability of entangled pair of qubits is (partially) preserved.

Secondly, let us see what happens when we copy the entire two-qubit register at once. We would like to determine whether the set of original two-qubit states (36), which after the cloning exhibit inseparability, is larger (i.e., the restriction of the form given in Eq. (37) is weaker) than when a local cloning is performed. To do so, we introduce four basis vectors  $|\Psi_1\rangle = |00\rangle$ ;  $|\Psi_2\rangle = |01\rangle$ ;  $|\Psi_3\rangle = |10\rangle$ ; and  $|\Psi_4\rangle = |11\rangle$ , so that the original two-qubit state in Eq. (36) is expressed as  $|\Phi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_4\rangle$ . The copying is now performed according to the transformation (31) with  $M = 4$ . We find that each of the two pairs of two-qubit copies at the output of the copier is described by the same density operator, i.e.  $\hat{\rho}_{a_0 b_1} = \hat{\rho}_{a_1 b_0}$ . Moreover, the fidelity of copying is input-state independent, and the quality of cloned registers is higher than that in the case of local cloning. Again, using the Peres-Horodecki theorem we find that the density operators  $\hat{\rho}_{a_0 b_1}$  and  $\hat{\rho}_{a_1 b_0}$  are inseparable if

$$\frac{1}{2} - \frac{\sqrt{2}}{3} \leq \alpha^2 \leq \frac{1}{2} + \frac{\sqrt{2}}{3}. \quad (38)$$

We conclude that quantum inseparability can be copied better (i.e. for much larger range of the parameter  $\alpha$ ) by using a nonlocal copier than when two local copiers are used.

## 7 Conclusions

We have presented the universal optimal quantum copying (cloning) machine which optimally clones a single original qubit to  $N + 1$  qubits. We have found a simple quantum network which realizes this quantum copier. In addition we have presented a universal cloner for quantum registers. We have numerically tested the optimality of this cloner, but a rigorous proof has yet to be found.

Quantum copiers can be effectively utilized in various processes designed for the manipulation of quantum information. In particular, quantum copiers can be used for eavesdropping [20], they can be applied for realization of generalized (POVM) measurements [21], or they can be utilized for storage and retrieval of information in quantum computers [22].

## Acknowledgments

We thank Sam Braunstein, Dagmar Bruß, Peter Knight, Martin Plenio, and Vlatko Vedral for collaboration and helpful discussions. This work was supported by the Royal Society.

## 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. V. Bužek and M. Hillery, *Acta Physica Slovaca* **47**, 193 (1997).
7. V. Bužek, S. Braunstein, M. Hillery, and D. Bruß, *Phys. Rev. A* **56**, 3446 (1997).
8. N. Gisin and S. Massar, *Phys. Rev. Lett.* **79**, 2153 (1997).
9. D. Bruß, D.P. DiVincenzo, A.K. Ekert, C. Machiavello, and J. Smolin: “Optimal universal and state-dependent quantum cloning,” [Los Alamos e-print archive quant-ph/9703046 (1997)].
10. V. Bužek, M. Hillery, and P.L. Knight, “Flocks of quantum clones: Multiple copying of qubits”, to appear in the special issue of *Fort. der Physik* edited by S. Braunstein.
11. M. Hillery and V. Bužek, *Phys. Rev. A* **56**, 1212 (1997).
12. D. Bruß, A.K. Ekert, and C. Machiavello, “Optimal universal quantum cloning and state estimation,” [Los Alamos e-print archive quant-ph/9712019(1997)].
13. V. Bužek, V. Vedral, M. Plenio, P.L. Knight and M. Hillery, *Phys. Rev. A* **55**, 3327 (1997).
14. D. Bures, *Trans. Am. Math. Soc.* **135**, 199 (1969); see also A. Uhlmann, *Rep. Math. Phys.* **9**, 273 (1976); **24** 229 (1986); W.K. Wootters, *Phys. Rev. D* **23**, 357 (1981).
15. 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.
16. S. Massar and S. Popescu, *Phys. Rev. Lett.* **74**, 1259 (1995).
17. R. Derka, V. Bužek, and A.K. Ekert, *Phys. Rev. Lett.* **80**, 1571 (1998), and references therein.
18. A. Peres, *Phys. Rev. Lett.* **77**, 1423 (1996).
19. M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1997).
20. N. Gisin and B. Huttner, *Phys. Lett. A* **228**, 13 (1997).
21. R. Derka and V. Bužek: “Optimal estimation of quantum states from finite ensembles: From pure theory to hypothetic experiments” (unpublished).
22. D.P. DiVincenzo, *Science* **279**, 255 (1995).