acta physica slovaca vol. 48 No. 3, 177 – 184 June 1998

CONTROLLING THE FLOW OF INFORMATION IN QUANTUM CLONERS: ASYMMETRIC CLONING [1]

V. Bužek[ac2], **M. Hillery**[b], **R. Bednik**[c]
(*a*) *Institute of Physics, SLovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratislava, Slovakia*
(*b*) *Department of Physics and Astronomy, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10021, U.S.A.*
(*c*) *Faculty of Mathematics and Physics, Comenius University, Mlynská dolina F-1, 842 15 Bratislava, Slovakia*

Received 15 May 1998, accepted 29 May 1998

We show that the distribution of information at the output of the quantum cloner can be efficiently controlled via preparation of the quantum cloner. We present a universal cloning network with the help of which asymmetric cloning can be performed.

1. Introduction

An *unknown* pure state of a qubit can be "swapped" between two parties (Alice and Bob) by a unitary transformation. To be specific, let us assume that Alice has a qubit initially prepared in a pure quantum state $|\Psi\rangle_{a_0}$

$$|\Psi\rangle_{a_0} = \alpha_0|0\rangle_{a_0} + \alpha_1|1\rangle_{a_0} \tag{1}$$

described as a vector in an 2-dimensional Hilbert space $\mathcal{H}_{a_0}$ spanned by two orthonormal basis vectors $|0\rangle_{a_0}$ and $|1\rangle_{a_0}$. The complex amplitudes α_i are normalized to unity, i.e. $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Simultaneously Bob has a qubit initially prepared in a specific (i.e., known) state $|0\rangle_{a_1}$ which is a vector in the Hilbert space $\mathcal{H}_{a_1}$. From the general rules of quantum mechanics it follows that there always exists a *unitary* transformation $\hat{U}$ acting on $\mathcal{H}_{a_0} \otimes \mathcal{H}_{a_1}$ which swaps Alice's and Bob's states, i.e.

$$|\Psi\rangle_{a_0}|0\rangle_{a_1} \stackrel{\hat{U}}{\longrightarrow} |0\rangle_{a_0}|\Psi\rangle_{a_1}. \tag{2}$$

[1]Special Issue on Quantum Optics and Quantum Information
[2]E-mail address: buzek@savba.sk

Operational meaning of this state swapping is as follows:
(1) Prior the swapping Alice does not know what is the state of her qubit. But, in principle she can perform an optimal measurement on her system (see [1, 2]) which would allow her to estimate the state. The quality of this estimation is characterized by the mean fidelity $\mathcal{F}$ [3, 4]. Taking into account that Alice has only a single qubit, then the maximal value of the mean fidelity of the estimation is $\mathcal{F} = 2/3$. After the measurement is performed Alice can communicate classically her result to Bob (and, in fact, to an arbitrary number of recipients) who can recreate the estimated state. If this type of classical communication is not allowed by the rules of the game, then Bob can only guess what is the state (this estimation via "wild guessing" corresponds to the minimal value of the mean fidelity, which in the case of a single qubit is $\mathcal{F} = 1/2$) [3, 4]. Obviously, as soon as Alice performs the measurement the state $|\Psi\rangle_{a_0}$ is "lost", so there is nothing relevant to swap.
(2) If Alice does not perform a measurement on her quantum system she can quantum-mechanically swap the state $|\Psi\rangle$ to Bob. After the swapping she cannot gain information about $|\Psi\rangle$ (except, if Bob classically communicates any results of his measurements to her).

In this swapping scenario, when no classical communication is allowed, *either* Alice *or* Bob has the state $|\Psi\rangle$ and it has to be decided *a priori* (i.e., before the measurement) who is going to have the qubit (Alice or Bob). At this point one can ask a question whether it would be possible to find a unitary transformation such that both Alice and Bob would have the state $|\Psi\rangle$ *simultaneously*. That is, the question is whether a unitary transformation $\hat{U}$ such that

$$|\Psi\rangle_{a_0}|0\rangle_{a_1} \xrightarrow{\hat{U}} |\Psi\rangle_{a_0}|\Psi\rangle_{a_1}, \tag{3}$$

does exist for an arbitrary (unknown) input state $|\Psi\rangle$.

Generalizing the proof of the Wootters-Zurek no-cloning theorem [5] it is easy to show that the linearity of quantum mechanics prohibits the existence of the perfect cloning expressed by Eq.(3). This is a major difference between quantum and classical information: it is possible to make perfect copies of classical information, but quantum information cannot be copied perfectly, i.e., quantum states cannot be cloned perfectly. Nevertheless, if the requirement that the copies are perfect is dropped, then it is possible to make quantum copies. This was first shown in Ref. [6], where a transformation which produces two mutually identical copies of an arbitrary input qubit state was given. This transformation was shown to be optimal, in the sense that it maximizes the average fidelity between the input and output qubits, by Gisin and Massar [7] and by Bruss, et. al. [8]. Gisin and Huttner [9] have shown that the quantum cloning can be efficiently used for eavesdropping. Gisin and Massar have also been able to find copying transformations which produce k copies from l originals (where $k > l$) [7]. In addition, quantum logic networks for quantum copying machines of qubits have been developed [10, 11, 12], and bounds have been placed on how good copies can be [13, 14]. It has been shown recently [15] that the inseparability of quantum states can be partially cloned (broadcasted) with the help of local quantum cloning machines, i.e. distant parties sharing an entangled pair of qubits can generate two pairs of partially *nonlocally* entangled states using only *local* operations. Gisin has presented an interesting proof [16] of the optimality of the quantum cloner showing that the bound on the fidelity of the universal quantum cloner [6] is compatible with the no-signaling constraint. Cerf [17, 18] has introduced a family of quantum cloning machines that produce two approximate copies from a single qubit, while the overall input-to-output operation for each copy is a Pauli channel. Cerf has also introduced a concept of asymmetric quantum cloning when at the output of the cloner the two clones are not identical, but simultaneously they are specifically related to the original qubit (see below). It has been shown in Ref. [19] that states of quantum systems in arbitrary-dimensional Hilbert spaces can be universally cloned (i.e., the fidelity of cloning does not depend on the input). The cloning transformation presented in [19] allows one to study how quantum registers can be cloned. It has been shown later by Werner [20] that this cloning transformation is optimal. Moreover, Werner in his elegant paper have constructed a universal transformation for an optimal cloning which produces k copies from l originals (where $k > l$) of an M dimensional system. Zanardi [21] has presented a group-theoretical analysis of the universal quantum cloning.

1.1 The problem

Let us assume the initial qubit to be in an *unknown* state $\hat{\rho}_{a_0}$. Our task is to clone this qubit universally, i.e. input-state independently, in such a way, that we can control the scaling of the original and the clone at the output. That is, we are looking for a cloner (the asymmetric cloner [17, 18]) in which we can control a flow of quantum information in such a way that the two clones at the output can be represented as

$$\hat{\rho}_{a_j}^{(out)} = s_j \hat{\rho}_{a_j}^{(id)} + \frac{1-s_j}{2}\hat{1}, \tag{4}$$

where $j = 0, 1$. Here we assume that the original qubit after the cloning is "scaled" by the factor s_0, while the copy is scaled by the factor s_1. These two scaling parameters are not independent and they are related by a specific inequality (see below). We note the two extreme cases, when **(a)** $s_0 = 1$ and $s_1 = 0$ and, vice versa, when **(b)** $s_0 = 0$ and $s_1 = 1$. These correspond to the following situations: **(a)** the information is completely preserved in the original qubit, and **(b)** the information is totally transfered (swapped) to the copy. Symmetric cloning corresponds to the situation when $s_0 = s_1$.

Our main task in this paper is to find a cloning network in which the control over the flow of information (i.e. the control over the values of the scaling parameters s_0 and s_1) can be performed via preparation of the initial state of the cloner.

2. Network for asymmetric cloner

For simplicity, let us assume that the original qubit is initially in a pure state (1), i.e. $|\Psi\rangle_{a_0}^{(in)} = \alpha_0|0\rangle + \alpha_1|1\rangle$. To perform asymmetric cloning we have to unitarily couple to the original qubit with two additional qubits denoted as a_1 and b_1 which are initially in a pure state $|0\rangle_{a_0} \otimes |0\rangle_{b_1} \equiv |00\rangle$.

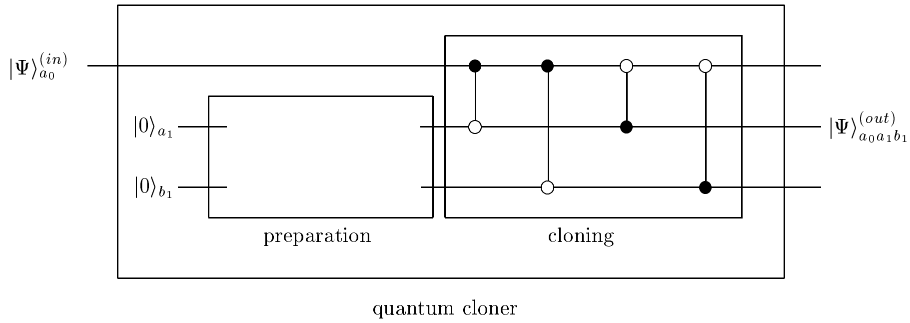

Fig. 1. Graphical representation of the network for the asymmetric cloner. The logical controlled-NOT $\hat{P}_{kl}$ given by Eq.(6) has as its input a control qubit (denoted as $\bullet$) and a target qubit (denoted as $\circ$). We separate the preparation of the quantum copier from the cloning process itself. The cloning, i.e. the transfer of quantum information from the original qubit, is performed by a sequence of four controlled-NOTs. We do not specify the details of the preparation part of the network which generates the state $|\Psi\rangle_{a_1b_1}^{(prep)}$ out of the input $|00\rangle_{a_1b_1}$. This is a well known network for generation of an arbitrary two-qubit state.

At the first stage of the cloning these two qubits are transformed from the state $|00\rangle$ into the state

$$|\Psi\rangle_{a_1b_1}^{(prep)} = C_1|00\rangle + C_2|01\rangle + C_3|10\rangle + C_4|11\rangle, \tag{5}$$

where the complex amplitudes C_i will be specified so that the conditions given by Eq.(4) are fulfilled[3]. At this stage the original qubit is still not involved in the process of cloning, but the choice of C_i's later affects the flow of information in the cloner.

After the preparation stage we assume that the interaction between the original qubit and two additional qubits a_1 and b_1 is performed via a simple sequence of four C-NOT gates (see Fig. 1). The operator which implements the C-NOT gate, $\hat{P}_{kl}$, acts on the basis vectors of the two qubits as follows (k denotes the control qubit and l the target):

$$\begin{array}{rcl} \hat{P}_{kl}|0\rangle_k|0\rangle_l &=& |0\rangle_k|0\rangle_l; \\ \hat{P}_{kl}|0\rangle_k|1\rangle_l &=& |0\rangle_k|1\rangle_l; \\ \hat{P}_{kl}|1\rangle_k|0\rangle_l &=& |1\rangle_k|1\rangle_l; \\ \hat{P}_{kl}|1\rangle_k|1\rangle_l &=& |1\rangle_k|0\rangle_l. \end{array} \tag{6}$$

We assume the specific action of four controlled-NOT operations

$$|\Psi\rangle_{a_0a_1b_1}^{(out)} = \hat{P}_{b_1a_0}\hat{P}_{a_1a_0}\hat{P}_{a_0b_1}\hat{P}_{a_0a_1}|\Psi\rangle_{a_0}^{(in)}|\Psi\rangle_{a_1b_1}^{(prep)}, \tag{7}$$

[3]We do not specify this preparation part of the cloning network (see Fig. 1) because it is well know that the state (5) can be prepared from $|00\rangle$ via a simple sequence of local operations and C-NOT gates [22].

(see Fig. 1) during which the information is transfered from a_0 qubit to other two qubits. From the state vector $|\Psi\rangle^{(out)}_{a_0a_1b_1}$ given by Eq.(7) we obtain single-qubit density operators

$$\begin{aligned}\hat{\rho}^{(out)}_{a_0} &= \mathrm{Tr}_{a_1b_1}\left[|\Psi\rangle^{(out)}_{a_0a_1b_1}\langle\Psi|\right];\\ \hat{\rho}^{(out)}_{a_1} &= \mathrm{Tr}_{a_0b_1}\left[|\Psi\rangle^{(out)}_{a_0a_1b_1}\langle\Psi|\right],\end{aligned} \tag{8}$$

which explicitly depend on the complex amplitudes $C_j = c_j e^{i\theta_j}$ (here $c_j = |C_j|$). These amplitudes come into play via the preparation of the state $|\Psi\rangle^{(prep)}_{a_1b_1}$ (5). Our task now is to specify these four amplitudes so that the density operators (8) fulfill the scaling condition (4). Comparing Eqs.(4) and (8) we find that the density operators (8) can be written in the scaled form (4) if the complex amplitudes C_j and the two scaling factors s_0 and s_1 are related as

$$c_1 = \sqrt{\frac{s_0+s_1}{2}}; \qquad c_2 = \sqrt{\frac{1-s_0}{2}}; \qquad c_4 = \sqrt{\frac{1-s_1}{2}}, \tag{9}$$

and

$$\begin{aligned}\cos(\theta_1-\theta_2) &= \frac{s_1}{\sqrt{(s_0+s_1)(1-s_0)}};\\ \cos(\theta_1-\theta_4) &= \frac{s_0}{\sqrt{(s_0+s_1)(1-s_1)}};\end{aligned} \tag{10}$$

while $C_3 = 0$. With these complex amplitudes C_j the quantum network as described by Eq.(7) realizes the asymmetric cloner. From Eqs.(9) and (10) we find that the scaling factors s_0 and s_1 have to be related as (see Fig. 2)

$$s_0^2 + s_1^2 + s_0s_1 - s_0 - s_1 \le 0. \tag{11}$$

To understand more clearly how the asymmetric cloner works we assume three specific preparation states (5) of the cloner:
(i) Let us assume that the cloner is initially prepared in the maximally entangled two-qubit (Bell) state

$$|\Psi\rangle^{(prep)}_{a_1b_1} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{12}$$

which can be prepared from $|00\rangle$ via a simple sequence of the Hadamard transformation on the qubit a_1 followed by the C-NOT operation with a_1 being the control. It easy to see that the cloner which is prepared in the state (12) does not affect the original qubit which at the output is in the same state as in the input, i.e. we find that $s_0 = 1$ and $s_1 = 0$.
(ii) The cloner, which is initially in the completely disentangled state

$$|\Psi\rangle^{(prep)}_{a_1b_1} = |0\rangle_{a_1} \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{b_1}, \tag{13}$$

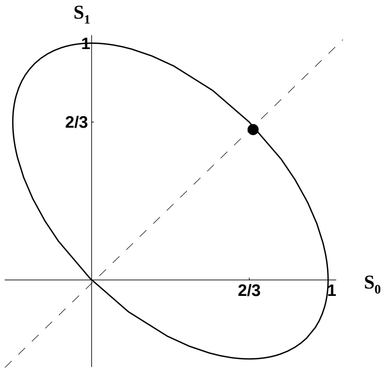

Fig. 2. The ellipse delimiting the range of possible value of the scaling parameters s_0 and s_1 of the two clones that simultaneously emerge as outputs of the asymmetric cloner. We see that the symmetric universal cloner corresponds to $s_0 = s_1 = 2/3$.

acts as the state swapper, i.e. in this case $s_0 = 0$ and $s_1 = 1$, which means that the initial state of the original qubit a_0 is "unitarily teleported" to the qubit a_1. The state (13) can be obtained from $|00\rangle$ by the action of the Hadamard transformation on the qubit b_1.

(iii) The optimal universal quantum cloning [6] of the original qubit (i.e. $s_0 = s_1 = 2/3$) can be realized when the cloner is initially prepared in the state

$$|\Psi\rangle_{a_1 b_1}^{(prep)} = \sqrt{\frac{2}{3}}|00\rangle + \frac{1}{\sqrt{6}}(|01\rangle + |11\rangle). \tag{14}$$

This state can be prepared with the help of a simple network presented in Ref.[11].

3. Instead of conclusions: Pauli cloners

We have presented a simple logical network with the help of which asymmetric cloning of qubits can be performed. This network is suitable for cloning of pure as well as impure input states. In fact, an impure state of a qubit can be represented as a state of a subsystem of a composite system of two qubits. This composite two-qubit system itself is assumed to be in a pure state. Let us therefore consider cloning of the initial qubit a_0 which is initially entangled with a reference qubit r. To be specific, let us assume that the two qubits are prepared initially in the maximally entangled Bell state $|\Phi^+\rangle_{ra_0}$. Here the four maximally entangled states of two qubits are defined as usually

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle);$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{15}$$

Let us assume that the cloner is initially prepared in the state

$$|\Psi\rangle_{a_1 b_1}^{(prep)} = X_1|\Phi^+\rangle + X_2|\Phi^-\rangle + X_3|\Psi^+\rangle + X_4|\Psi^-\rangle, \tag{16}$$

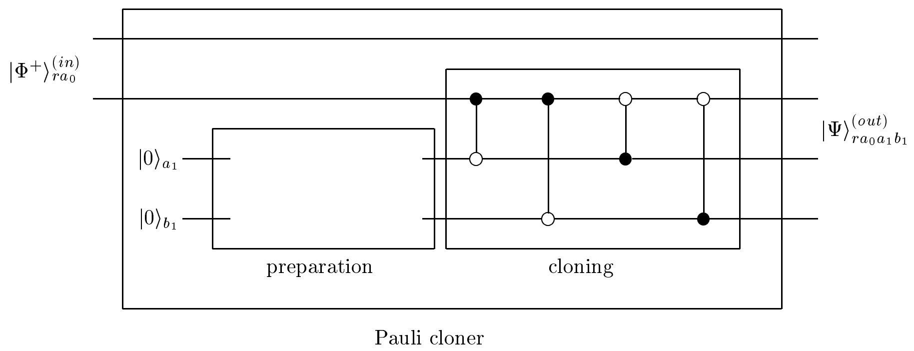

Fig. 3. Graphical representation of the network for the Pauli cloner. The logical controlled-NOT $\hat{P}_{kl}$ are specified as in Fig. 1. Here again, the cloning, i.e. the transfer of quantum information from the original qubit, is performed by a sequence of four controlled-NOTs.

and we apply the sequence

$$|\Psi\rangle^{(out)}_{ra_0a_1b_1} = \hat{P}_{b_1a_0}\hat{P}_{a_1a_0}\hat{P}_{a_0b_1}\hat{P}_{a_0a_1}|\Phi^+\rangle^{(in)}_{ra_0}|\Psi\rangle^{(prep)}_{a_1b_1}, \tag{17}$$

of four C-NOT's on the qubits a_0 and a_1b_1 (see Fig. 3). The 4-qubit state $|\Psi\rangle^{(out)}_{ra_0a_1b_1}$ at the output reads

$$|\Psi\rangle^{(out)}_{ra_0a_1b_1} = \left\{X_1|\Phi^+\rangle|\Phi^+\rangle + X_2|\Phi^-\rangle|\Phi^-\rangle + X_3|\Psi^+\rangle|\Psi^+\rangle + X_4|\Psi^-\rangle|\Psi^-\rangle\right\}_{ra_0;a_1b_1}, \tag{18}$$

which means that the network (17) realizes the Pauli cloner introduced recently by Cerf [18].

Acknowledgements One of us (V.B.) thanks Nicolas Cerf for helpful discussions and correspondence. This research was supported by a grant from the Royal Society.

Note added After this paper was completed a paper by Niu and Griffiths [24] appeared in the Los Alamos e-print archive in which asymmetric cloning is studied from a different perspective and alternative cloning networks are presented.

References

[1] C.W. Helstrom: *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976)

[2] A.S. Holevo: *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982)

[3] S. Massar, S. Popescu: *Phys. Rev. Lett.* **74** (1995) 1259

[4] R. Derka, V. Bužek, A.K. Ekert: *Phys. Rev. Lett.* **80** (1998) 1571

[5] W.K. Wootters, W.H. Zurek: *Nature* **299** (1982) 802; see also D. Diekes: *Phys. Lett. A* **92** (1982) 271; H. Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa, B. Schumacher: *Phys. Rev. Lett.* **76** (1996) 2818

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

[7] N. Gisin, S. Massar: *Phys. Rev. Lett.* **79** (1997) 2153

[8] D. Bruß, D.P. DiVincenzo, A. Ekert, A. Fuchs, C. Macchiavello, J. Smolin: *Phys. Rev. A* **57** (1998) 2368

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

[10] V. Bužek, S. Braunstein, M. Hillery, D. Bruß: *Phys. Rev. A* **56** (1997) 3446

[11] V. Bužek, M. Hillery: *acta physica slovaca* **47** (1997) 193

[12] V. Bužek, M. Hillery, P.L. Knight: "*Flocks of quantum clones: Multiple cloning of qubits*", to appear in *Fort. der Physik* (1998) (special issue on Quantum Computing, ed. S. Braunstein)

[13] M. Hillery, V. Bužek: *Phys. Rev. A* **56** (1997) 1244

[14] D. Bruß, A. Ekert, C. Macchiavello: "*Optimal universal cloning and state estimation*", *Los Alamos e-print quant-ph/9712019*

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

[16] N. Gisin: "*Quantum cloning without signaling*", *Los Alamos e-print quant-ph/9801005*

[17] N.J. Cerf: "*Quantum cloning and the capacity of the Pauli channel*", *Los Alamos e-print quant-ph/9803058 v.2*

[18] N.J. Cerf: in this issue of *acta physica slovaca* **48** (1998) 115

[19] V. Bužek, M. Hillery: "*Universal optimal cloning of qubits and quantum registers* ", *Los Alamos e-print quant-ph9801/009*

[20] R.F. Werner: "*Optimal cloning of pure states*", *Los Alamos e-print quant-ph/9804001*

[21] P. Zanardi: "*A note on quantum cloning in d dimensions*", *Los Alamos e-print quant-ph/9804011*

[22] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter: *Phys. Rev. A* **52** (1995) 3457

[23] V. Bužek, M. Hillery: "*Quantum information tapping* ", unpublished.

[24] C.-S. Niu, R.B. Griffiths: "*Optimal copying of one quantum bit*", *Los Alamos e-print quant-ph/9805073*