Mathematical Physics and Quantum Field Theory,
Electron. J. Diff. Eqns., Conf. 04, 2000, pp. 113–120
http://ejde.math.swt.edu or http://ejde.math.unt.edu
ftp ejde.math.swt.edu or ejde.math.unt.edu (login: ftp)

Quantum copying: A review *

Mark Hillery

Abstract

Quantum information is stored in two-level quantum systems known as qubits. The no-cloning theorem states that the state of an unknown qubit cannot be copied. This is in contrast to classical information which can be copied. If one drops the requirement that the copies be perfect it is possible to design quantum copiers. This paper presents a short review of the theory of quantum copying.

1 Introduction

The relatively recent confluence of quantum mechanics and computer science has led to rapid and unexpected progress in both fields. In computer science it was shown that by increasing the class of allowable algorithms to include ones which operate according to quantum principles, it is possible to perform certain tasks, such as factorization and data base searching, much faster than had been previously believed possible [1, 2]. In quantum mechanics, it has led to the study of entirely new questions, as well as some extremely interesting new applications. For example, quantum error correcting codes provide novel ways of protecting quantum systems from the effects of decoherence [3].

This work grew out of the consideration of the limits which physics places on computers. Early work by Landauer and Bennett focused on the limits due to thermodynamics, and had the rather surprising outcome that thermodynamics places no restrictions on what a computer can do [4]. The next task was to see if quantum mechanics might place any restrictions on what could be done, but Benioff and Feynman independently showed that it did not [5, 6]. Deutsch, considering the matter further, showed that not only does quantum mechanics not hurt, it can, in fact, help [7]. This conclusion was dramatically confirmed by Shor, when he constructed a quantum algorithm which can find the prime factors of an N-digit number in a time which is polynomial in N [1].

In addition to the work directly on quantum computation, a second, but related, line of work emerged, that of quantum information. Classical information is carried by bits which can have one of two values, 0 or 1. The kind of information on which a quantum computer relies, quantum information, is carried by

* *Mathematics Subject Classifications:* 81P68.

Key words: Quantum computing, qubits, no-cloning theorem, quantum copying.

Published July 12, 2000.

two-level quantum systems, known as qubits, where one level corresponds to 0 and the other to 1. Qubits, unlike bits, can exist in a superposition of 0 and 1, and it is this fact that leads to their unusual properties. For example, a register consisting of qubits can be put into a superposition of all possible input values, e.g. $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ for a two-qubit register, and any operation which acts on the register acts on all of these values simultaneously. This means that using quantum information instead of classical leads automatically to a kind of parallel processing. The study of the properties of the information carried by qubits comprises the field of quantum information.

Here we shall consider one of the more unusual properties of quantum information - it cannot be copied, or, to be more precise, it cannot be copied perfectly. This is not true of classical information, which can, in principle, be copied without any difficulty (though, as anyone who has struggled with a recalcitrant copy machine can attest, the phrase “in principle” here covers up a lot). The inability to copy quantum information makes it useful in cryptography, and prototype quantum cryptographic system have been constructed in several laboratories. If one considers approximate copies, however, or perfect copies which can be produced with a probability less than one, of only a limited set of quantum states, then quantum copying becomes possible. Here we shall review both kinds of copiers (more frequently known as quantum cloners).

This paper is dedicated to Professor Eyvind Wichmann on his 70th birthday. While I had taken previous courses in quantum mechanics, I really learned the subject from a one-year graduate course which Eyvind taught, and this knowledge was deepened during my Ph.D. studies with him. It was one of the most challenging and one of the best courses which I have ever taken (the only other candidate was the quantum field theory course I took from him the following year), and I still refer rather often to the set of notes which he distributed during this course. I hope what is in this paper will demonstrate that what he taught has been put to good use.

2 No-cloning theorem

The original realization that quantum information cannot be cloned is due to Wooters and Zurek [8]. The argument is very short and depends only on the linearity of quantum mechanics. We assume that the cloner has degrees of freedom of its own and operates by means of a unitary transformation acting on a Hilbert space which is a tensor product of the space of the cloner itself, $\mathcal{H}_x$, that of the input qubit, $\mathcal{H}_a$, and the space of a “blank” qubit, $\mathcal{H}_b$ which is to become the copy. The input qubit is in an arbitrary input state, $|\psi\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$, while we assume that the “blank” qubit is always initially in the state $|0\rangle_b$. The cloner is assumed to be initially in the state $|Q\rangle_x$, no matter what the state of the input qubit. An ideal cloner would have the following action:

$$|\psi\rangle_a|0\rangle_b|Q\rangle_x \rightarrow |\psi\rangle_a|\psi\rangle_b|Q'\rangle_x. \tag{1}$$

If the cloner is to duplicate any initial state, then clearly it must duplicate the basis states properly. This means that

$$\begin{aligned} |0\rangle_a|0\rangle_b|Q\rangle_x &\rightarrow |0\rangle_a|0\rangle_b|Q_0\rangle_x \\ |1\rangle_a|0\rangle_b|Q\rangle_x &\rightarrow |1\rangle_a|1\rangle_b|Q_1\rangle_x . \end{aligned} \tag{2}$$

These equations, however, determine the transformation on any input state, because it is realized by a linear transformation. In particular

$$|\psi\rangle_a|0\rangle_b|Q\rangle_x \rightarrow \alpha|0\rangle_a|0\rangle_b|Q_0\rangle_x + \beta|1\rangle_a|1\rangle_b|Q_1\rangle_x . \tag{3}$$

A comparison of Eqs. (1) and (3) shows that the right-hand sides cannot be equal for all values of α and β; the dependence of one is quadratic while that of the other is linear. Therefore, a perfect cloner cannot exist.

3 Universal quantum copiers

Now let us assume we want to copy the state $|\psi\rangle$ given above, but we shall drop the requirement that the copies be perfect. It will be useful in what follows to parameterize α and β as

$$\alpha = \sin\vartheta e^{i\varphi}, \qquad \beta = \cos\vartheta . \tag{4}$$

We now need to ask ourselves what requirement we would like our imperfect copy machine to satisfy. One possibility is the Universal Quantum Copy Machine (UQCM) [9], which 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 the reduced density operators $\hat{\rho}_a^{(out)}$ and $\hat{\rho}_b^{(out)}$, respectively, are identical, i.e.,

$$\hat{\rho}_a^{(out)} = \hat{\rho}_b^{(out)} \tag{5}$$

(ii) If no *a priori* information about the input 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 condition is to design a quantum copier so that the distances between density operators of each system at the output ($\hat{\rho}_a^{(out)}$ and $\hat{\rho}_b^{(out)}$) and the ideal density operator $\hat{\rho}^{(id)}$ which describes the input state of the original qubit, are input state independent. Quantitatively this means that if we employ the Hilbert-Schmidt norm to define our distance between two density matrices,

$$d(\hat{\rho}_1;\hat{\rho}_2) := \left(\mathrm{Tr}\left[(\hat{\rho}_1-\hat{\rho}_2)^2\right]\right)^{1/2} , \tag{6}$$

then the quantum copier should be such that

$$d(\hat{\rho}_a^{(out)};\hat{\rho}^{(id)}) = \mathrm{const.} \tag{7}$$

(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 the constant in Eq. (7) to be as small as possible.

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 satisfies condition (iii) has been shown by Gisin and Massar, and by Bruss, et. al. [10, 11].

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

$$\begin{aligned} |0\rangle_a|0\rangle_b|Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}}|00\rangle_{ab}|\uparrow\rangle_x + \sqrt{\frac{1}{3}}|+\rangle_{ab}|\downarrow\rangle_x \\ |1\rangle_a|0\rangle_b|Q\rangle_x &\rightarrow \sqrt{\frac{2}{3}}|11\rangle_{ab}|\downarrow\rangle_x + \sqrt{\frac{1}{3}}|+\rangle_{ab}|\uparrow\rangle_x, \end{aligned} \tag{8}$$

where

$$|+\rangle_{ab} = \frac{1}{\sqrt{2}}(|10\rangle_{ab} + |01\rangle_{ab}), \tag{9}$$

and satisfies conditions (i), (ii), and (iii). The system labeled by a is the original (input) qubit, while the other system b represents the qubit onto which the information is copied, and is analogous to “blank paper” in a copier. The states of the copy machine are labeled by x. The state space of the copy machine is two dimensional, and it is spanned by the vectors $|\uparrow\rangle_x$ and $|\downarrow\rangle_x$. We assume that copy machine is always in the same state, $|Q\rangle_x$, initially. The reduced density operators of both copies at the output are equal and they can be expressed as (we give the expressions for qubit a, the ones for qubit b are similar)

$$\hat{\rho}_a^{(out)} = \frac{5}{6}|\psi\rangle_a\langle\psi| + \frac{1}{6}|\psi_\perp\rangle_a\langle\psi_\perp|, \tag{10}$$

where

$$|\psi_\perp\rangle_a = \beta^*|0\rangle_a - \alpha^*|1\rangle_a, \tag{11}$$

is the state orthogonal to $|\psi\rangle_a$. 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 $\rho_a^{(out)}$ given by Eq.(10) can be rewritten in a “scaled” form:

$$\hat{\rho}_a^{(out)} = s\hat{\rho}_a^{(id)} + \frac{1-s}{2}\hat{1}, \tag{12}$$

which guarantees that the distance (6) is input-state independent, i.e. the condition specified by Eq. (7) is automatically fulfilled. The scaling factor in Eq.(12) is $s = 2/3$.

We note once again that the UQCM copies all input states equally well, and, therefore, it 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). This suggests that another measure of the quality of the copies is the average fidelity $\mathcal{F}$ which is equal to the mean overlap between a copy and the input state [10]

$$\mathcal{F} = \int d\Omega_a \langle\psi|\hat{\rho}_a^{(out)}|\psi\rangle_a, \tag{13}$$

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

$$s = 2\mathcal{F} - 1. \tag{14}$$

The UQCM transformation is the one which minimizes $\mathcal{F}$ [10].

It is possible to generalize universal, that is, input-state-independent, quantum copiers in several ways. One is to suppose that you wish to produce more than two copies (by the number of copies we mean the number of output qubits which are similar to the input qubit). One would expect that the more copies one produces, the lower the quality of each copy. It is also possible to imagine that instead of feeding in just one original qubit into the copier, if one had several identical qubits one could feed all of them into the copier to produce better copies. For example, starting with two identical originals, one could produce 3 copies. The quality of these copies would presumably be better than that of 3 copies produced from only one original. Specific transformations have been found for a copier which starts with N originals and produces $M \geq N$ copies [10], and these have been shown to be optimal [10]-[13]. The reduced density matrixes of the output qubits are in the scaled form (see Eq. (12)) with a scaling factor

$$s = \frac{N(M+2)}{M(N+2)}. \tag{15}$$

Note that the scaling factor is an increasing function of the number of originals and a decreasing function of the number of copies, as expected.

Another possible generalization is to consider copying systems of dimension higher than two. In this case, because a system with $d > 2$ dimensions contains more quantum information than a two-dimensional one, we would expect that the quality of the copies will be an decreasing function of d. An explicit copying transformation is known for general d in the case in which we have one original and produce two copies [14]. In the case in which we have N identical originals and produce $M \geq N$ copies, it is known that the optimal transformation again leads to reduced density matrixes for the individual copies of scaled form with the scaling factor [12, 13]

$$s = \frac{N(M+d)}{M(N+d)}. \tag{16}$$

As expected, it is a decreasing function of d.

4 Probabilistic copiers

Instead of trying to construct a device which will copy all possible input states, one could design one which will copy only states from a particular set of allowed input states. Presumably a copier of this type can achieve higher fidelities for its copies than one which is required to accept all possible states as inputs. In fact, it might even be possible for the copier to be perfect for certain input sets. This suspicion is correct, but the size of the input sets for which it is true is small. If the input set contains any two states which are not orthogonal, a perfect copier is impossible [15], and if we are copying qubits, then this means that it is not possible to build a perfect copier for input sets of more than two states.

There is a way around this problem, however. What we have been discussing in the previous paragraph is a copier which produces perfect copies and works every time. What happens if we relax this latter requirement? We still demand that the copies for our allowed input set be perfect, and we permit the copier to have a certain probability of failure, but impose the requirement that the copier lets us know when it has failed and when it has succeeded. One can think of the copier as having a red light on top. We put in one of our allowed input states, and the copier produces an output. If the red light stays off, the copying process has succeeded, and our output consists of perfect copies. If it goes on, which it does with a certain nonzero probability if the input set contains nonorthogonal states, then the copying process has failed, and we discard the output.

This type of copier was proposed and the transformation for it constructed by Duan and Guo [16, 17]. Let us suppose that we want to copy one of two states, $|\psi_1\rangle$ and $|\psi_2\rangle$, where, for simplicity, we shall assume that their inner product is real and nonnegative, $\langle\psi_1|\psi_2\rangle = r \geq 0$. The copying transformation is given by

$$|\psi_j\rangle_a|0\rangle_b|Q\rangle_x \rightarrow \frac{1}{\sqrt{1+r}}(|\psi_j\rangle_a|\psi_j\rangle_b|X_0\rangle_x + \sqrt{r}|\Phi\rangle_{ab}|X_1\rangle_x), \tag{17}$$

for $j = 1, 2$. Here we have that ${}_x\langle X_j|X_k\rangle_x = \delta_{jk}$ and $|\Phi\rangle_{ab}$ is an arbitrary state of the $a - b$ system with norm one. This transformation is consistent with unitarity, has the same failure probability for each input state, and gives the lowest possible failure probability. The way it works is that we take a qubit, which is either in the state $|\psi_1\rangle_a$ or $|\psi_2\rangle_a$, but we do not know which, and send it through a device which implements the above transformation. We then measure the device itself in order to determine whether it is in the state $|X_0\rangle_x$ or $|X_1\rangle_x$. If it is in the former, the transformation has succeeded, and we have two copies of the input state as our output. The probability of this happening is $1/(1 + r)$. If it is the latter the transformation has failed, and we discard the output.

A number of generalizations of this type of copier are possible. Larger sets of allowed states can be considered [17] or one might have multiple copies of the input state and wish to produce more than two copies at the output [18]. It is also possible to design copiers which lie between the universal and probabilistic ones. In particular, they are designed to copy a finite set of allowed states, the copies they produce are not perfect, and these are produced with only a certain probability [19]. In these one finds that there is a trade-off between the quality of the copies and the probability of successfully producing them. The success probability for producing perfect copies is the smallest, and this probability increases as the quality of the copies decreases.

5 Conclusion

The study of quantum copying has increased our understanding of the properties of quantum information. What its role in devices which process quantum will be is not yet clear. It can perhaps best be used to split the quantum information in a qubit, allowing some of that information to be processed in one way and some in another. The development of quantum algorithms is a very active field of research, and quantum copying should prove to be a useful part of the quantum programmer's tool kit.

A final question is how can one actually build a quantum copier. Designs in terms of quantum logic networks exist [19]-[21], and the gates from which these are constructed have actually been realized in several laboratories. However, putting together enough of them to build a quantum copier is still a major problem. Nevertheless, it may soon be possible to actually construct a quantum copier due to a clever proposal by Simon, Weihs, and Zeilinger [22]. They showed how two-photon down conversion can be utilized to realize the UQCM on a single qubit . This proposal can be realized with present technology, and the hope is that a working quantum copier will be a reality in a few years.

Acknowledgments

I would like to thank Vladimir Bužek for what has been, and continues to be, a very fruitful collaboration. In addition, I would like to thank the National Science Foundation for their support of this effort, most recently under grant PHY-9970507.

References

[1] P. Shor, SIAM J. on Comp. **26**, 1484 (1997).

[2] L. Grover, Phys. Rev. Lett. **78**, 325 (1997).

[3] For an introduction see *Quantum Computing* by J. Gruska (McGraw-Hill, London, 1999), section 7.4.

[4] For reprints of some of the earlier papers on the physics of information and computing see *Maxwell's Demon Entropy, Information, Computing* edited by H. Leff and A. Rex (Princeton University Press, Princeton, 1990).

[5] P. Benioff, J. Stat. Phys. **22**, 563 (1980).

[6] R. Feynman, Found. of Physics, **16** 507 (1986).

[7] D. Deutsch, Proc. Royal Soc London A **400**, 97 (1985).

[8] W. Wooters and W. Zurek, Nature **299**, 802 (1982).

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

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

[11] D. Bruss, D. DiVincenzo, A. Ekert, C. Fuchs, C, Macchiavello, and J. Smolin, Phys. Rev. A **57**, 2368 (1998).

[12] R. Werner, Phys. Rev. A **58**, 1287 (1998).

[13] M. Keyl and R. Werner, quant-ph/9807010.

[14] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).

[15] M. Hillery and V. Bužek, Phys. Rev. A **56** 1212 (1997).

[16] L-M. Duan and G-C. Guo, quant-ph/9704020.

[17] L-M. Duan and G-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).

[18] A. Chefles and S. Barnett, quant-ph/9808018.

[19] A. Chefles and S. Barnett, quant-ph/9812035.

[20] V. Bužek, S. Braunstein, M. Hillery, and D. Bruss, Phys. Rev. A **56**, 3446 (1997).

[21] V. Bužek, M. Hillery, and P. Knight, Fort. der Physik **46**, 521 (1998).

[22] C. Simon, G. Weihs, and A. Zeilinger, Acta Physica Slovaka **49**, 755 (1999).

Mark Hillery
Department of Physics and Astronomy
Hunter College of the City University of New York
695 Park Avenue
New York, NY 10021, USA
e-mail: mhillery@shiva.hunter.cuny.edu