Quantum copying: Fundamental inequalities

M. Hillery [1] and V. Bužek [2]
[1]*Department of Physics and Astronomy, Hunter College, CUNY, 695 Park Avenue, New York, New York 10021*
[2]*Optics Section, The Blackett Laboratory, Imperial College, London SW7 2BZ, England*
(Received 23 October 1996; revised manuscript received 22 April 1997)

How well can one copy an arbitrary qubit? To answer this question we consider two arbitrary vectors in a two-dimensional state space and an abstract copying transformation which will copy these two vectors. If the vectors are orthogonal, then perfect copies can be made. If they are not, then errors will be introduced. The size of the error depends on the inner product of the two original vectors. We derive a lower bound for the amount of noise induced by quantum copying. We examine both copying transformations which produce one copy and transformations which produce many, and show that the quality of each copy decreases as the number of copies increases. [S1050-2947(97)05908-8]

PACS number(s): 03.65.Bz

I. INTRODUCTION

One of the greatest 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 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].

In our previous paper we examined several possible quantum-copying machines[1] and studied how they would perform copying a single *arbitrary* qubit [9]. The copier proposed in Wootters and Zurek's paper [2] on quantum cloning copies two orthogonal states perfectly but introduces errors when superpositions of these states are copied. A second copying machine, which we called the universal quantum-copying machine, copies all input states to the same accuracy, and, on average, its performance is much better than that of the Wootters-Zurek machine. Here we would like to establish some fundamental limits on how well quantum states can be copied by considering the following problem. Suppose we have two arbitrary vectors in a Hilbert space and we want to build a machine which will copy these two vectors. How well can we do? If the vectors are orthogonal, then perfect copies can be made. If they are not, then, as we shall show, errors will be introduced. The amount of error depends on the inner product of the two original vectors. This problem is relevant to the global problem of copying an arbitrary qubit. If one has a lower bound for the amount of noise which must be introduced for the two-state problem, then the best one can do in the general case is the maximum of this lower bound over all pairs of states. Thus we can get a lower bound for the amount of noise induced by a quantum-copying machine.

The approach which we use here has the advantage that it allows us to consider more general problems than simply producing a single copy of an arbitrary qubit. We are able to find a lower bound for the noise which is introduced when n copies of a qubit are produced simultaneously, and determine how the noise depends on n. In addition, even though our discussion is phrased in terms of qubits, which are two-level systems, our results are more general; the limitations we find on quantum copying apply to systems of arbitrary dimension, because our arguments are completely independent of the dimension of the Hilbert space in which the vectors to be copied lie. Therefore, if one is trying to copy an n-level system, for example, several qubits in an entangled state, then the amount of noise introduced by the copying process must be greater than the lower bounds which are given here.

II. TWO-STATE PROBLEM

Suppose we have two states $|s_1\rangle_a$ and $|s_2\rangle_a$, in a two-dimensional state space which we would like to copy. If the

[1]In what follows we will use a ''copying machine'' for a particular unitary transformation applied to the original particle. We do this keeping in mind that the copying unitary transformations under consideration can be realized in terms of a sequence of logical gates.

initial state of the copying machine is $|Q\rangle_x$, then the action of the copying machine on our two vectors can be expressed as

$$|s_j\rangle_a|Q\rangle_x \rightarrow |\Psi_j\rangle_{abx} = |s_j\rangle_a|s_j\rangle_b|Q_j\rangle_x + |\Phi_j\rangle_{abx}, \quad (2.1)$$

where $j=1,2$. In our analysis we do not specify the *in-state* of the copy mode (this possible eavesdropper's mode we denote as the b mode). We only require that it is the same for all inputs into the a mode, and that it is normalized to unity. In Eq. (2.1) we have expressed the full output state of the copying machine as the sum of two parts, the first representing the ideal output state and the second what is left over. The two parts can be expressed in terms of the projection onto the two mode state $|s_j\rangle_a|s_j\rangle_b$ as

$$|\Gamma_j\rangle_{abx} \equiv |s_j\rangle_a|s_j\rangle_b|Q_j\rangle_x = P_j|\Psi_j\rangle_{abx}; \quad (2.2)$$

$$|\Phi\rangle_{abx} \equiv (I-P_j)|\Psi\rangle_{abx}, \quad (2.3)$$

where the projectors P_j are defined as

$$P_j = (|s_j\rangle\langle s_j|)_a \otimes (|s_j\rangle\langle s_j|)_b. \quad (2.4)$$

This definition implies that

$${}_{abx}\langle\Gamma_j|\Phi_j\rangle_{abx} = 0; \quad j=1,2. \quad (2.5)$$

In addition we also assume that the initial quantum-copying machine state is normalized to unity, i.e., ${}_x\langle Q|Q\rangle_x = 1$. In order to produce good copies we want to make the norms $\|Q_1\|$ and $\|Q_2\|$ as large as possible and $\|\Phi_1\|$ and $\|\Phi_2\|$, which represent the size of the errors, as small as possible. The norm of the state vector $|A\rangle$ is defined as $\|A\| = (\langle A|A\rangle)^{1/2}$.

The copying machine can be represented as a unitary operator and this unitarity imposes constraints on the transformations shown in Eq. (2.1). In particular, we have that

$$1 = \|Q_j\|^2 + \|\Phi_j\|^2, \quad j=1,2 \quad (2.6)$$

and

$$z = z_x^2\langle Q_1|Q_2\rangle_x + {}_{abx}\langle\Gamma_1|\Phi_2\rangle_{abx} + {}_{abx}\langle\Phi_1|\Gamma_2\rangle_{abx} + {}_{abx}\langle\Phi_1|\Phi_2\rangle_{abx}, \quad (2.7)$$

where $z = {}_a\langle s_1|s_2\rangle_a$. We note that in derivation of Eq. (2.7) we have utilized the fact that the *in-state* of the copy mode is normalized to unity. From these equations it is possible to derive a number of inequalities which restrict the behavior of the copying machine. We shall begin with the strongest restriction, which is relatively difficult to work with, and then we proceed to weaker ones which are more transparent.

Let us first find an upper bound on $|{}_{abx}\langle\Gamma_1|\Phi_2\rangle_{abx}|$ and $|{}_{abx}\langle\Phi_1|\Gamma_2\rangle_{abx}|$. We begin by expressing $|\Gamma_1\rangle_{abx}$ as

$$|\Gamma_1\rangle_{abx} = P_2|\Gamma_1\rangle_{abx} + |\Gamma_1'\rangle_{abx}, \quad (2.8)$$

where $|\Gamma_1'\rangle_{abx} = (I-P_2)|\Gamma_1\rangle_{abx}$. The two states on the right-hand side of Eq. (2.8) are orthogonal which implies that

$$\eta_{11} = \eta_{11}|z|^4 + \|\Gamma_1'\|^2, \quad (2.9)$$

where $\eta_{ij} = {}_x\langle Q_i|Q_j\rangle_x$, so that

$$\|\Gamma_1'\| = [\eta_{11}(1-|z|^4)]^{1/2}. \quad (2.10)$$

Similarly, if we express $|\Gamma_2\rangle_{abx}$ as

$$|\Gamma_2\rangle_{abx} = P_1|\Gamma_2\rangle_{abx} + |\Gamma_2'\rangle_{abx}, \quad (2.11)$$

where $|\Gamma_2'\rangle_{abx} = (I-P_1)|\Gamma_2\rangle_{abx}$, we find

$$\|\Gamma_2'\| = [\eta_{22}(1-|z|^4)]^{1/2}. \quad (2.12)$$

Because $P_2|\Phi_2\rangle_{abx} = 0$ we have that

$$|{}_{abx}\langle\Phi_2|\Gamma_1\rangle_{abx}| = |{}_{abx}\langle\Phi_2|\Gamma_1'\rangle_{abx}| \leq \|\Gamma_1'\| \cdot \|\Phi_2\| = (1-\eta_{22})^{1/2}[\eta_{11}(1-|z|^4)]^{1/2}, \quad (2.13)$$

and similarly

$$|{}_{abx}\langle\Phi_1|\Gamma_2\rangle_{abx}| \leq (1-\eta_{11})^{1/2}[\eta_{22}(1-|z|^4)]^{1/2}. \quad (2.14)$$

We can now take these results and insert them into Eq. (2.7). This gives us

$$|z| \leq |z|^2|\eta_{12}| + (1-\eta_{11})^{1/2}(1-\eta_{22})^{1/2} + (1-|z|^4)^{1/2} \times [\eta_{11}^{1/2}(1-\eta_{22})^{1/2} + \eta_{22}^{1/2}(1-\eta_{11})^{1/2}]. \quad (2.15)$$

For a given value of $|z|$ this inequality restricts the values of $\|Q_1\|$, $\|Q_2\|$, and $|\eta_{12}| = |\langle Q_2|Q_1\rangle|$. It defines a region in a three-dimensional parametric space in which the values of the parameters can lie. For $|z| \neq 0$ this region does not include the line $\|Q_1\| = \|Q_2\| = 1$ which implies that perfect copying is impossible. It is only for $|z| = 0$, i.e., $|s_1\rangle$ and $|s_2\rangle$ are mutually orthogonal, that we can have $\|Q_1\| = \|Q_2\| = 1$ which implies error-free copying.

In order to simplify these results we use the Schwarz inequality from which it follows that:

$$|\eta_{12}| \leq \|Q_1\|\|Q_2\| = (\eta_{11}\eta_{22})^{1/2}. \quad (2.16)$$

This last inequality allows us to rewrite the right-hand side of the relation (2.15) in terms of only two parameters, η_{11} and η_{22}. It is useful to express the resulting inequality in terms of the size of the errors. We introduce the quantities $X_j = (1-\eta_{jj})^{1/2} = \|\Phi_j\|$ (for $j=1,2$) which are associated with the amount of noise induced by copying the vectors $|s_j\rangle_a$. In particular, the smaller X_1 and X_2 are the better is the copying procedure, and in the limit $X_j \rightarrow 0$ two perfect copies $|s_j\rangle_a$ and $|s_j\rangle_b$ of the initial state $|s_j\rangle_a$ are obtained at the output of the copying machine. If we now express the inequality which follows from Eqs. (2.15) and (2.16) in terms of X_1 and X_2, we have

$$|z| \leq |z|^2(1-X_1^2)^{1/2}(1-X_2^2)^{1/2} + X_1X_2 + (1-|z|^4)^{1/2} \times [(1-X_1^2)^{1/2}X_2 + (1-X_2^2)^{1/2}X_1]. \quad (2.17)$$

It is easier to understand the implications of Eq. (2.17) if we look at particular cases.

(A) Let us first suppose that $X_1 = \|\Phi_1\| = 0$, i.e., $|s_1\rangle$ is copied perfectly, which implies that $\|Q_1\| = 1$. From Eq. (2.17) we find

$$|z| \leq |z|^2(1-X_2^2)^{1/2} + (1-|z|^4)^{1/2}X_2, \quad (2.18)$$

which in turn implies that

$$X_2 \geq |z|(1-|z|^2)^{1/2}[(1+|z|^2)^{1/2}-|z|]. \tag{2.19}$$

Therefore, if $|s_1\rangle$ is copied perfectly, then $\|\Phi_2\|$, which represents the size of the error made in copying $|s_2\rangle$, must be *at least* as large as the right-hand side of Eq. (2.19). For small $|z|$ the right-hand side of this inequality is approximately $|z|$. We note that the maximum value of the lower bound on the error X_2 given by the right-hand side of Eq. (2.19) is equal to $(2/27)^{1/2} \simeq 0.272$ and is obtained for $|z| = 1/\sqrt{3} \simeq 0.577$.

(B) Let us now consider the case $X_1 = X_2 = X$, i.e., equal errors in both copies. Making use of Eq. (2.17) we then have that

$$|z| \leq |z|^2(1-X^2)+X^2+2X[(1-|z|^4)(1-X^2)]^{1/2}, \tag{2.20}$$

which implies that

$$X \geq \left[\frac{r_1-2r_2^{1/2}}{r_3}\right]^{1/2}, \tag{2.21}$$

where

$$\begin{aligned} r_1 &= 2+3|z|+2|z|^2+|z|^3; \\ r_2 &= 1+3|z|+3|z|^2+4|z|^3+3|z|^4+|z|^5+|z|^6; \\ r_3 &= 5+5|z|+3|z|^2+3|z|^3. \end{aligned} \tag{2.22}$$

For $|z|$ small the right-hand side is approximately $|z|/2$. If both vectors are copied equally well, then there is a minimum value to the copying error. The right-hand side of Eq. (2.21) takes its maximum value approximately equal to 0.125 when $z \simeq 0.553$.

III. GENERAL BOUND

Taking into account, that

$$0 \leq X_i^2 \leq 1; \quad \text{and} \quad 0 \leq |z|^2 \leq 1 \tag{3.1}$$

we can simplify the inequality in Eq. (2.17), i.e.,

$$|z| \leq |z|^2 + X_1 + X_2 + X_1X_2. \tag{3.2}$$

This allows us to go beyond specific cases and to derive a general result.

We shall adopt the quantity X_1+X_2 as a measure of the total error made in copying the two states $|s_1\rangle$ and $|s_2\rangle$. The copies are perfect if $X_1+X_2=0$ and become progressively worse as its value increase. Solving Eq. (3.2) for X_2 we find

$$X_2 \geq \frac{|z|(1-|z|)-X_1}{1+X_1}, \tag{3.3}$$

which implies that

$$X_1+X_2 \geq \frac{|z|(1-|z|)+X_1^2}{1+X_1}. \tag{3.4}$$

Minimizing the right-hand side with respect to X_1 we find that

$$X_1+X_2 \geq 2\{[1+|z|(1-|z|)]^{1/2}-1\}. \tag{3.5}$$

A general quantum-copying machine will have to copy pairs of vectors with all values of $|z|$. In particular, it will have to copy two vectors for which $|z|=1/2$, a value which maximizes the right-hand side of Eq. (3.5). For such a pair of vectors we have

$$X_1+X_2 \geq \sqrt{5}-2. \tag{3.6}$$

For this to be true, it must be the case that either $X_1 \geq (\sqrt{5}-2)/2$ or $X_2 \geq (\sqrt{5}-2)/2$. This means, that for a general quantum-copying machine one has to expect that for at least one vector the size of the copying error is $(\sqrt{5}-2)/2 \simeq 0.118$.

These considerations are closely related to recent work by Fuchs and Peres [10]. They considered the tradeoff between disturbance and information acquisition in quantum cryptography. Alice sends a qubit to Bob, but in between, it is intercepted by Eve. She allows it to interact with another qubit and sends the original on to Bob. Eve wants to disturb the qubit she sends to Bob as little as possible, yet have the qubit she keeps contain as much information about the qubit Alice sent as possible. Fuchs and Peres found a relation between the discrepancy rate for Bob (disturbance) and the mutual information (Eve's information gain). In our case we consider an interaction which produces copies. That is Eve puts into the copying machine her qubit and Alice's qubit and what emerges are, she hopes, two reasonably good copies of Alice's original qubit. The assumption is then that if the copies are good the disturbance will be small and the information gain large.

IV. MULTIPLE COPIES

Suppose that instead of making only two copies of $|s_1\rangle$ and $|s_2\rangle$ we want to construct a device which will produce $(n+1)$ copies (n actual copies plus the original). We would like to find out what the limitations on the quality of the copies are. Let us assume the copying transformation to be

$$|s_j\rangle_a|Q\rangle_x \rightarrow |s_j\rangle_a|s_j\rangle_{b_1}\cdots|s_j\rangle_{b_n}|Q_j\rangle_x + |\Phi_j\rangle_{ab_1\cdots b_nx}; \quad j=1,2. \tag{4.1}$$

As before we let

$$|\Gamma_j\rangle_{ab_1\cdots b_nx} = |s_j\rangle_a|s_j\rangle_{b_1}|s_j\rangle_{b_n}|Q_j\rangle_x, \tag{4.2}$$

and assume that $\langle\Gamma_j|\Phi_j\rangle=0$ $(j=1,2)$ [in what follows we will omit state vector subscripts indicating the modes under consideration, instead of $|\Gamma_j\rangle_{ab_1\cdots b_nx}$ we will write $|\Gamma_j\rangle$]. What we might expect is that the more copies we make, the poorer the quality of each copy will be. This is indeed the case.

The derivations of the inequalities are similar to those in the previous two sections so we shall only give the results. The inequality analogous to that in Eq. (2.17) is

$$|z| \leq |z|^{n+1}(1-X_1^2)^{1/2}(1-X_2^2)^{1/2}+X_1X_2+(1-|z|^{2(n+1)})^{1/2} \times [X_1(1-X_2^2)^{1/2}+X_2(1-X_1^2)^{1/2}]. \tag{4.3}$$

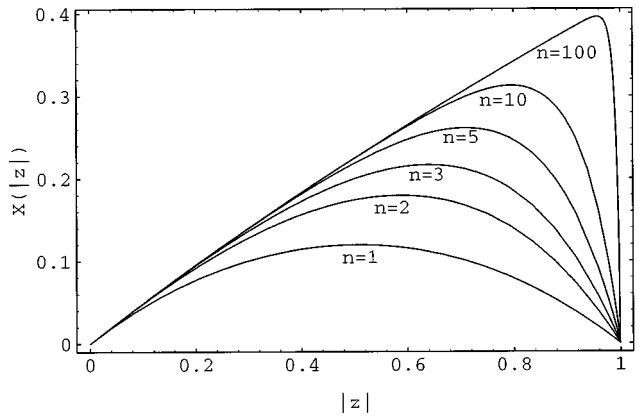

FIG. 1. We plot the right-hand side of Eq. (4.5) as a function of $|z|$ for various values of n ($n=1,2,3,5,10$, and 100).

To analyze the multiple-copy inequalities in a transparent way, we take into account Eq. (3.1) and we simplify Eq. (4.3) to obtain

$$|z|\leqslant|z|^{n+1}(1-X_1^2)^{1/2}(1-X_2^2)^{1/2}+X_1+X_2+X_1X_2. \tag{4.4}$$

It is useful to look at this last result in the case $X_1=X_2=X$. Then one finds that

$$X\geqslant\frac{[1+(1-|z|^{n+1})(|z|-|z|^{n+1})]^{1/2}-1}{1-|z|^{n+1}}\equiv X_{\min}. \tag{4.5}$$

The right-hand side is plotted as a function of $|z|$ for several different values of n in Fig. 1. One sees that $X_{\min}$ is equal to zero for $|z|=0$ and $|z|=1$ for arbitrary $n\geqslant1$. This is not surprising because we know that two mutually orthogonal states ($|z|=0$) can be copied perfectly as many times as we wish. The case $|z|=1$ is essentially trivial, because here the two states $|s_1\rangle$ and $|s_2\rangle$ are equal up to a phase factor, so we are dealing with only one state. What we also see from the figure is that for a given value of $|z|$ the bound $X_{\min}$ increases as a function of n, that is

$$\left.\frac{\partial X_{\min}}{\partial n}\right|_{|z|=\text{const}}\geqslant0. \tag{4.6}$$

This relation represents the tradeoff between the number of copies and the noise induced by the copying procedure, i.e., the larger the number of copies the larger the noise. Figure 1 also reveals a striking asymmetry with respect to the point $|z|=1/2$ of $X_{\min}$ as a function of $|z|$. We see that the maximum value of the function $X(|z|)$ shifts towards $|z|=1$ as n increases. Simultaneously the maximum value increases as well and in the limit of large n is approximately equal to 0.41. It is also interesting to note, that for $|z|$ small (when the states $|s_1\rangle$ and $|s_2\rangle$ are almost orthogonal), then

$$X_{\min}(|z|)\simeq\epsilon/2, \tag{4.7}$$

where we put $|z|=\epsilon$ ($\epsilon\ll1$). The relation (4.7) represents the fact that the noise induced by copying of states which are almost orthogonal does not depend on the number of copies produced. On the contrary, if we assume that $|z|=1-\epsilon$ (i.e., copying of states which are almost equal), then

$$X_{\min}(|z|)\simeq n\epsilon/2, \tag{4.8}$$

which means that in the multiple-copy production of *almost* identical states the error increases linearly as a function of the number of copies.

Let us briefly see what happens when $X_1=0$, i.e., $|s_1\rangle$ is duplicated perfectly. In the limit $n\to\infty$ with $|z|<1$ we find that $X_2\geqslant|z|$, but if $|z|=1$, then the lower bound for X_2 is zero for all n. For n large but finite, the lower bound is approximately equal to $|z|$ except for a region near $|z|=1$ where it drops sharply to zero.

Finally, let us examine the $(n+1)$-copy version of Eq. (3.2). We find

$$|z|\leqslant|z|^{n+1}+X_1+X_2+X_1X_2, \tag{4.9}$$

which implies that

$$X_1+X_2\geqslant2\{[1+|z|-|z|^{n+1}]^{1/2}-1\}. \tag{4.10}$$

The right-hand side achieves it maximum value, which is

$$2\left\{\left[1+\left(\frac{1}{n+1}\right)^{1/n}\left(\frac{n}{n+1}\right)\right]^{1/2}-1\right\}, \tag{4.11}$$

when $|z|=(n+1)^{-1/n}$. This is an increasing function of n and for large n goes to the value $2(\sqrt{2}-1)\simeq0.83$. This implies that for a general quantum-copying machine which produces simultaneously a large number of copies of an arbitrary input state, there must be at least one input state for which $X_1\geqslant(\sqrt{2}-1)\simeq0.41$.

Thus we see that for a quantum-copying machine which only copies two vectors or for one which copies arbitrary input states, the lower bound for the error in the copies increases with the number of copies made. There is clearly a tradeoff in the number of copies made versus the quality of each copy.

V. COMPARISON TO COPYING MACHINES

We would now like to compare our bounds to the performance of two different copying machines which copy quantum qubits. The first is the Wootters-Zurek copying machine [2,9] which copies two basis vectors $|0\rangle$ and $|1\rangle$ perfectly, but copies superpositions of them poorly. The second is the universal quantum-copying machine (UQCM) which copies all input states of quantum qubits equally well [9]. The Wootters-Zurek copying machine is specified by the transformation:

$$|0\rangle_a|Q\rangle_x\to|0\rangle_a|0\rangle_b|Q_0\rangle_x;$$

$$|1\rangle_a|Q\rangle_x\to|1\rangle_a|1\rangle_b|Q_1\rangle_x, \tag{5.1}$$

where $|Q\rangle_x$, $|Q_0\rangle_x$, and $Q_1\rangle_x$ are the internal states of the copying machine. The superposition $\cos\theta|0\rangle_a+\sin\theta|1\rangle_a$ is copied as

$$(\cos\theta|0\rangle_a+\cos\theta|1\rangle_a)|Q\rangle_x$$

$$\to\cos\theta|0\rangle_a|0\rangle_b|Q_0\rangle_x+\sin\theta|1\rangle_a|1\rangle_b|Q_1\rangle_x, \tag{5.2}$$

and the application of Eq. (2.3) gives us that the size of the error is

$$X=[1-\cos^6\theta-\sin^6\theta-({}_x\langle Q_0|Q_1\rangle_x + {}_x\langle Q_1|Q_0\rangle_x)\sin^3\theta\cos^3\theta]^{1/2}. \quad (5.3)$$

This will be the smallest if we choose the machine vectors $|Q_0\rangle_x$ and $|Q_1\rangle_x$ to be the same, giving

$$X=[1-(\cos^3\theta+\sin^3\theta)^2]^{1/2}. \quad (5.4)$$

Let us now compare this result to the bound given by Eq. (2.19). We consider the case when we want to copy the vectors $|0\rangle_a$, which is copied perfectly, and $\cos\theta|0\rangle_a+\sin\theta|1\rangle_a$, which is copied with an error X. The inequality in Eq. (2.19) gives us the condition ($|z|=\cos\theta$)

$$X\geq|\cos\theta\sin\theta|[(1+\cos^2\theta)^{1/2}-|\cos\theta|]. \quad (5.5)$$

This bound lies below the actual error given by Eq. (5.4). They coincide only when $\theta=0$ or $\theta=\pi/2$. On the other hand, if $\theta=\pi/4$ we find that $X=1/\sqrt{2}\simeq 0.707$, while the bound in Eq. (5.5) is 0.259.

The UQCM is specified by the unitary transformation

$$|0\rangle_a|Q\rangle_x\rightarrow\sqrt{2/3}|0\rangle_a|0\rangle_b|\uparrow\rangle_x+\sqrt{1/6}(|0\rangle_a|1\rangle_b+|1\rangle_a|0\rangle_b)|\downarrow\rangle_x;$$

$$|1\rangle_a|Q\rangle_x\rightarrow\sqrt{2/3}|1\rangle_a|1\rangle_b|\downarrow\rangle_x+\sqrt{1/6}(|0\rangle_a|1\rangle_b+|1\rangle_a|0\rangle_b)|\uparrow\rangle_x, \quad (5.6)$$

where the state space of the copying machine is two dimensional and is spanned by the orthonormal basis $|\uparrow\rangle_x$ and $|\downarrow\rangle_x$. For this copying machine the error is independent of the initial state and is given by

$$X=\frac{1}{\sqrt{3}}\simeq 0.577. \quad (5.7)$$

We can compare this error to the bound in Eq. (2.21) which applies when the error in both copied vectors is the same. If we consider the case $|z|=1/2$ we find that Eq. (2.21) gives us the condition

$$X\geq 0.124. \quad (5.8)$$

For both copying machines we note that the lower bounds are considerably smaller than the actual errors. What this strongly suggests is that one can design *one-purpose* copying machines which copy only two *a priori* known (nonorthogonal) states much better than the universal copying machine which is designed to copy all vectors equally well.

VI. CONCLUSION

The unitarity of quantum-mechanical transformations has allowed us to place limits on how well quantum states can be copied. Recent work has shown that these limits cannot be achieved by the UQCM, which copies all vectors equally well [11,12], but we believe that they can be achieved by copying machines which are designed to copy two *a priori* known state vectors.

Our results can also be used to find noise limits in more general kinds of quantum-copying problems. When assessing the performance of a quantum-copying machine one needs to know not only which states are to be copied, but how often it will be necessary to copy each one. For example, in the case where the states $|s_1\rangle$ and $|s_2\rangle$ are to be copied, if we need to copy $|s_1\rangle$ more often than $|s_2\rangle$, it would be better to use a copying machine which is less noisy for $|s_1\rangle$ than for $|s_2\rangle$. This would result in less noise in the output, on average, than if one were to use a copying machine which copies both states equally well. The bounds presented in the previous sections can be used to place lower limits on the average amount of noise in the output for this kind of situation.

Finally, the analysis here reveals that the feature of qubits which makes it impossible to copy them, in general, is the fact that different qubits need not be orthogonal. Classical information consists of bits, each of which is in one of two completely distinguishable, and therefore orthogonal, states. Classical information can be copied. Quantum information consists of qubits each of which can be in any superposition of the two basis states. This implies that two different qubits can have a nonzero inner product and are, consequently, not completely distinguishable. It is this basic difference between quantum and classical information which is responsible for their different copying properties.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation under Grant No. INT 9221716, by the grant agency VEGA of the Slovak Academy of Sciences (Grant No. 2/1152/96), and by the United Kingdom Engineering and Physical Sciences Research Council.

[1] A. Barenco and A.K. Ekert, Acta Phys. Slov. **45**, 205 (1995).
[2] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982).
[3] D. Diekes, Phys. Lett. **92A**, 271 (1982).
[4] H. Barnum, C.M. Caves, C.A. Fuchs, R. Josza, and B. Schumaker, Phys. Rev. Lett. **76**, 2818 (1996).
[5] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[7] N. Gisin and B. Huttner, quant-ph/9611041 (1996).
[8] D.P. DiVincenzo, Science **279**, 255 (1995).
[9] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996); see also V. Bužek, V. Vedral, M. Plenio, P.L. Knight, and M. Hillery, *ibid.* **55**, 3323 (1997); and V. Bužek, S. Braunstein, M. Hillery, and D. Bruß, quant-ph/9703046 (1997).
[10] C.A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996); see also C.A. Fuchs, quant-ph/9611010 (1996); and C.A. Fuchs, Ph.D. thesis, University of New Mexico, 1995, quant-ph/9601020 (1996).
[11] N. Gisin (unpublished).
[12] D. Bruß (private communication).