JOURNAL OF MATHEMATICAL PHYSICS **46**, 082102 (2005)

No-cloning of nonorthogonal states does not require inner product preserving

Dafa Li[a]
Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

Xiangrong Li
Department of Mathematics, University of California, Irvine, California 92697-3875

Hongtao Huang
Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, Michigan 48109

Xinxin Li
Department of Computer Science, Wayne State University, Detroit, Michigan 48202

(Received 20 February 2005; accepted 31 May 2005; published online 29 July 2005)

The no-cloning theorem says there is no quantum copy machine which can copy any one-qubit state. Inner product preserving was always used to prove the no-cloning of nonorthogonal states. In this paper we show that the no-cloning of nonorthogonal states does not require inner product preserving and discuss the minimal properties which a linear operator possesses to copy two different states at the same device. In this paper, we obtain the following necessary and sufficient condition. For any two different states $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\varphi\rangle = c|0\rangle + d|1\rangle$, assume that a linear operator L can copy them, that is, $L(|\psi,0\rangle) = |\psi,\psi\rangle$ and $L(|\varphi,0\rangle) = |\varphi,\varphi\rangle$. Then the two states are orthogonal if and only if $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states. Thus we only need linearity and that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states to prove the no-cloning of nonorthogonal states. It implies that inner product preserving is not necessary for the no-cloning of nonorthogonal states. © *2005 American Institute of Physics.* [DOI: 10.1063/1.1996327]

I. INTRODUCTION

The no-cloning theorem from the work of Wootters and Zurek said there is no quantum copy machine which can copy any quantum state.[1–3] The authors in Refs. 1 and 4 demonstrated if a quantum copy machine can copy two basis states, then it cannot copy their suppositions. Another version of the no-cloning theorem was stated in Ref. 5. The authors in Refs. 6–8 used inner product preserving to show that nonorthogonal states cannot be cloned by a unitary operator. The no-cloning theorem was extended to mixed states by Barnum *et al.*[3] Some authors presented approximate copies of qubits.[4,8] Mor suggested a type of the no-cloning principle and discussed various cases in which orthogonal states cannot be cloned in principle.[9]

Let $|0\rangle$ and $|1\rangle$ be the basis states of a one-qubit system and $|0,0\rangle$, $|0,1\rangle$, $|1,0\rangle$ and $|1,1\rangle$ be the basis states of a two-qubit system.

Let $|\psi\rangle = a|0\rangle + b|1\rangle$, where a and b are complex and

$$\|a\|^2 + \|b\|^2 = 1. \tag{1}$$

Let $|\varphi\rangle = c|0\rangle + d|1\rangle$, where c and d are complex and

[a] Electronic mail: dli@math.tsinghua.edu.cn

$$\|c\|^2 + \|d\|^2 = 1. \tag{2}$$

Assume that a linear operator L can copy states $|\psi\rangle$ and $|\varphi\rangle$, that is, $L(|\psi,0\rangle)=|\psi,\psi\rangle$ and $L(|\varphi,0\rangle)=|\varphi,\varphi\rangle$. By tensor product $|\psi,\psi\rangle=(a|0\rangle+b|1\rangle)\otimes(a|0\rangle+b|1\rangle)=a^2|0,0\rangle+ab|0,1\rangle+ab|1,0\rangle+b^2|1,1\rangle$. By the linearity of L, $L(|\psi,0\rangle)=aL(|0,0\rangle)+bL(|1,0\rangle)$. So we get

$$aL(|0,0\rangle) + bL(|1,0\rangle) = a^2|0,0\rangle + ab|0,1\rangle + ab|1,0\rangle + b^2|1,1\rangle. \tag{3}$$

From that $L(|\varphi,0\rangle)=|\varphi,\varphi\rangle$, similarly we get

$$cL(|0,0\rangle) + dL(|1,0\rangle) = c^2|0,0\rangle + cd|0,1\rangle + cd|1,0\rangle + d^2|1,1\rangle. \tag{4}$$

Since $|\psi\rangle$ and $|\varphi\rangle$ are different, the determinant of the coefficient matrix

$$ad - bc \neq 0. \tag{5}$$

Thus from Eqs. (3) and (4) we get by Gramer's rule the following $L(|0,0\rangle)$ and $L(|1,0\rangle)$: $L(|0,0\rangle)=(1/(ad-bc))((a^2d-bc^2)|0,0\rangle+bd(a-c)|0,1\rangle+bd(a-c)|1,0\rangle+bd(b-d)|1,1\rangle)$, $L(|1,0\rangle)=(1/(ad-bc))(ac(c-a)|0,0\rangle+ac(d-b)|0,1\rangle+ac(d-b)|1,0\rangle+(ad^2-b^2c)|1,1\rangle)$.

In this paper $\|x\|$ denotes the norm of $|x\rangle$ or a complex number x. Let $|\alpha\rangle=L(|0,0\rangle)$ and $|\beta\rangle=L(|1,0\rangle)$, $P=\|a^2d-bc^2\|^2+2\|bd(a-c)\|^2+\|bd(b-d)\|^2$ and $Q=\|ac(c-a))\|^2+2\|ac(d-b)\|^2+\|ad^2-b^2c\|^2$. Then

$$\|\alpha\|^2 = P/\|(ad-bc)\|^2 \tag{6}$$

and

$$\|\beta\|^2 = Q/\|(ad-bc)\|^2. \tag{7}$$

II. LEMMA 1

Assume that a linear operator L can copy different states $|\psi\rangle$ and $|\varphi\rangle$. If $|\psi\rangle$ and $|\varphi\rangle$ are orthonormal, then $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are orthonormal.

Proof: First let us prove that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states. Since $|\psi\rangle$ and $|\varphi\rangle$ are orthonormal, $\langle\psi|\varphi\rangle=0$, i.e.,

$$a\bar{c} + b\bar{d} = 0 \tag{8}$$

where $\bar{c}$ and $\bar{d}$ are complex conjugates of c and d, respectively. From Eq. (8) we obtain that $\|a\|^2\|c\|^2=\|b\|^2\|d\|^2$. By using Eqs. (1) and (2) $\|a\|^2\|c\|^2=(1-\|a\|^2)(1-\|c\|^2)$. It follows that $\|a\|^2+\|c\|^2=1$. We can as well get $\|b\|^2+\|d\|^2=1$.

We assume that a, b, c, and d are all real. It is not hard to extend the results in this paper to complex a, b, c, and d. Thus we obtain that

$$a^2 + c^2 = 1, \tag{9}$$

$P=(a^2d-bc^2)^2+2(bd(a-c))^2+(bd(b-d))^2$ and $Q=(ac(c-a))^2+2(ac(d-b))^2+(ad^2-b^2c)^2$. In P and Q, simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)] and d^2 by $(1-c^2)$ [see Eq. (2)], respectively, P and Q are reduced into the following forms:

$$P = 2 + 2bda^2 + 2bdc^2 - a^2 - c^2 - 4a^2c^2db + 4ac^3 + 4a^3c - 4a^3c^3 - 4ac - 2bd, \tag{10}$$

$$Q = -4a^3c^3 - 4a^2c^2db + a^2 - 2ac + 2ac^3 + 2a^3c + c^2. \tag{11}$$

Let us compute P and Q when $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Replacing bd by $-ac$ [see Eq. (8)] and using Eq. (9) in Eqs. (10) and (11), respectively, we obtain that $P=(a^2+c^2)^2=1$ and $Q=(1+2ac)(a^2+c^2)-2ac=1$.

Next let us compute the determinant of the coefficient matrix in Eq. (5) when $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)] and d^2 by $(1-c^2)$ [see Eq. (2)] and bd by $-ac$ [see Eq. (8)] and using Eq. (9), we derive that $\|ad-bc\|^2=(a^2+c^2)=1$.

From Eqs. (6) and (7) and the above it is easy to get $\|\alpha\|=1$ and $\|\beta\|=1$. That is, $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states.

Second, we show that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are orthogonal. After omitting the factor the inner product of $L(|0,0\rangle)$ and $L(|1,0\rangle)$ is $(a^2d-bc^2)ac(c-a)+2bd(a-c)ac(d-b)+bd(b-d)(ad^2-b^2c)$ (replacing b^2 by $(1-a^2)$ [see Eq. (1)] and d^2 by $(1-c^2)$ [see Eq. (2)])

$$=-(a-c)(a^3cd-bd^2ac+b^2dac-ac^3b-b^2d+bd^2)$$

(using $a^2+b^2=1$ and $c^2+d^2=1$)

$$=-(a-c)(d-b)(ac+bd).$$

Equation (8) implies that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are orthogonal.

Examples: The following combinations of a, b, c, and d satisfy $ac+bd=0$, that is, $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. It is easy to verify that $\|\alpha\|^2=1=\|\beta\|^2$.

1. $a=\sqrt{2}/2$, $b=\sqrt{2}/2$, $c=\sqrt{2}/2$, $d=-\sqrt{2}/2$.
2. $a=\sqrt{3}/2$, $b=1/2$, $c=1/2$, $d=-\sqrt{3}/2$.
3. $a=3/5$, $b=4/5$, $c=4/5$, $d=-3/5$.

Remark: However, that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are orthogonal cannot guarantee that $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. For example, $|\psi\rangle=a|0\rangle+b|1\rangle$ and $|\varphi\rangle=a|0\rangle-b|1\rangle$, where $a^2+b^2=1$ and $a\neq\pm b$. Though $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are orthogonal, $\langle\psi|\varphi\rangle\neq 0$, namely, $|\psi\rangle$ and $|\varphi\rangle$ are not orthogonal.

Corollary: For any two orthogonal states, there is a unitary operator which can copy them.

Proof: Let $|\psi\rangle=a|0\rangle+b|1\rangle$ and $|\varphi\rangle=c|0\rangle+d|1\rangle$ be orthogonal states. Let the truth table be the following matrix L.

	$\|0,0\rangle$	$\|0,1\rangle$	$\|1,0\rangle$	$\|1,1\rangle$
$\|0,0\rangle$	$\dfrac{a^2d-bc^2}{ad-bc}$	$\dfrac{bd(a-c)}{ad-bc}$	$\dfrac{bd(a-c)}{ad-bc}$	$\dfrac{bd(b-d)}{ad-bc}$
$\|0,1\rangle$	0	$-\sqrt{2}/2$	$\sqrt{2}/2$	0
$\|1,0\rangle$	$\dfrac{ac(c-a)}{ad-bc}$	$\dfrac{ac(d-b)}{ad-bc}$	$\dfrac{ac(d-b)}{ad-bc}$	$\dfrac{ad^2-b^2c}{ad-bc}$
$\|1,1\rangle$	0	$-\sqrt{2}/2$	$\sqrt{2}/2$	0

It is easy to verify that L is unitary by Lemma 1 and not hard to show that $L(|\psi,0\rangle)=|\psi,\psi\rangle$ and $L(|\varphi,0\rangle)=|\varphi,\varphi\rangle$.

III. LEMMA 2

Assume that a linear operator L can copy two different states $|\psi\rangle$ and $|\varphi\rangle$. If $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states, then $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal.

Proof: Since $\|\alpha\|=1$, from Eq. (6) we obtain that $P=\|ad-bc\|^2$, and since $\|\beta\|=1$, from Eq. (7) we get that $Q=\|ad-bc\|^2$. Thus $P-Q=0$. Using Eqs. (10) and (11), equation $P-Q=0$ is reduced into the following one:

$$2+2bda^2+2bdc^2-2a^2-2c^2+2ac^3+2a^3c-2ac-2bd=2(a^2+c^2-1)(ac+bd-1)=0.$$

There are two cases. *Case 1*: $a^2+c^2=1$ and *case 2*: $ac+bd=1$. We shall show that in case 1 $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal and case 2 does not occur.

Case 1 in which $a^2+c^2=1$: By simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)] and d^2 by

$(1-c^2)$ [see Eq. (2)], it is reduced that $(ac)^2-(bd)^2=(ac)^2-(1-a^2)(1-c^2)=-1+c^2+a^2=0$. Hence $(ac)^2-(bd)^2=(ac-bd)(ac+bd)=0$. There are two subcases.

1.1 *Subcase 1.1*: $ac+bd=0$, that is, $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal.
1.2 *Subcase 1.2*: $ac-bd=0$, that is,

$$ac=bd. \tag{12}$$

We shall show that in subcase 1.2 $|\psi\rangle$ and $|\varphi\rangle$ are also orthogonal. Let us first compute the determinant of the coefficient matrix (5). Simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)], d^2 by $(1-c^2)$ [see Eq. (2)] and bd by ac [see Eq. (12)], we derive that $(ad-bc)^2=a^2d^2-2acbd+b^2c^2=a^2(1-c^2)-2ac(ac)+(1-a^2)c^2=a^2-4a^2c^2+c^2$. Using $a^2+c^2=1$, it follows that $(ad-bc)^2=1-4a^2c^2=(1-2ac)(1+2ac)$. By requirement for the determinant of the coefficient matrix in Eq. (5), $(ad-bc)^2=(1-2ac)(1+2ac)\neq 0$.

Next let us compute P in Eq. (10) and Q in Eq. (11) by replacing bd by ac [see Eq. (12)] and using $a^2+c^2=1$. We get that $P=1-8a^3c^3=(1-2ac)(4a^2c^2+2ac+1)$ and $\|\alpha\|^2=(4a^2c^2+2ac+1)/(1+2ac)$; $Q=1-8a^3c^3=(1-2ac)(4a^2c^2+2ac+1)$ and $\|\beta\|^2=(4a^2c^2+2ac+1)/(1+2ac)$. Let $\|\alpha\|^2=\|\beta\|^2=1$. Then $ac=0$. From $ac=bd$, we obtain $ac+bd=0$. In other words, $|\psi\rangle$ and $|\varphi\rangle$ are also orthogonal for subcase 1.2.

Consequently when $a^2+c^2=1$, we derive that $ac+bd=0$, namely, $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal.

Case 2 in which $ac+bd=1$: We shall show that case 2 does not occur. If $ac+bd=1$, then $(ac+bd)^2-1=a^2c^2+2acbd+b^2d^2-1=0$. Simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)], d^2 by $(1-c^2)$ [see Eq. (2)] and bd by $(1-ac)$, we infer that $a^2c^2+2ac(1-ac)+(1-a^2)(1-c^2)-1=-(a-c)^2=0$. It follows that $a=c$.

Next let us compute the determinant of the coefficient matrix (5) in the case $ac+bd=1$. Simultaneously replacing b^2 by $(1-a^2)$ [see Eq. (1)], d^2 by $(1-c^2)$ [see Eq. (2)], and bd by $(1-ac)$, we derive that $(ad-bc)^2=a^2d^2-2adbc+b^2c^2=a^2(1-c^2)-2ac(1-ac)+(1-a^2)c^2=(a-c)^2$. By the requirement for the determinant of the coefficient matrix in Eq. (5) $ad-bc\neq 0$, it follows that $a\neq c$.

Therefore this case contradicts our hypothesis for the determinant of the coefficient matrix $ad-bc\neq 0$ in Eq. (5). In other words, case 2 does not happen.

IV. THE NO-CLONING OF NONORTHOGONAL STATES DOES NOT REQUIRE INNER PRODUCT PRESERVING

The authors always used inner product preserving to prove the no-cloning of nonorthogonal states.[6–8] From Lemma 2, it is easy to see that we only need linearity and that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states to prove the no-cloning of nonorthogonal states. It shows that inner product preserving is not necessary for the no-cloning of nonorthogonal states.

The following examples show when $|\psi\rangle$ and $|\varphi\rangle$ are not orthogonal, $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are not unit length states. When $a=3/5$, $b=4/5$, $c=3/5$. and $d=-4/5$, $\|\alpha\|^2=18/25$ and $\|\beta\|^2=337/225$; when $a=\sqrt{3}/2$, $b=1/2$, $c=\sqrt{3}/2$, and $d=-1/2$, $\|\alpha\|^2=5/6$, $\|\beta\|^2=3/2$.

V. CLONING LEADS TO INFINITY OF PROBABILITY AMPLITUDE

Let $|\gamma\rangle=c|0\rangle+d|1\rangle$, where $\|c\|^2+\|d\|^2=1$ and $c\neq 0$. Assume that a linear operator L can copy states $|1\rangle$ and $|\gamma\rangle$, that is, $L(|1,0\rangle)=|1,1\rangle$ and $L(|\gamma,0\rangle)=|\gamma,\gamma\rangle$. By the linearity of L and tensor product, it is easy to derive that $L(|0,0\rangle)=c|0,0\rangle+d|0,1\rangle+d|1,0\rangle+|((d^2-d)/c)|1,1\rangle$. Let $d<0$. Then d tends to -1 as c approaches 0 since $\|c\|^2+\|d\|^2=1$. Therefore the norm of probability amplitude $((d^2-d)/c)$ of state $|1,1\rangle$ tends to plus infinity as c approaches 0. For example, when $c=3/5$ and $d=-4/5$, $\|(d^2-d)/c\|=12/5$. It contradicts that the norm of probability amplitude should be 1 or less than 1.

Let $|\phi\rangle=L(|0,0\rangle)$. Then the norm of $|\phi\rangle$ is $\|\phi\|^2=\|c\|^2+\|d\|^2+\|d\|^2+\|(d^2-d)/c\|^2$ and clearly $\|\phi\|>1$. Notice that the norm of $|0,0\rangle$ is 1. It says again that cloning contradicts the norm preserving. For example, when $c=3/5$ and $d=-4/5$, $\|\phi\|=\sqrt{77/45}>1$.

VI. CONCLUSION

As is well known, the no-cloning theorem has far-reaching consequences for quantum information and quantum computing. Nielsen thought "what if we allow cloning devices that are not unitary?" is a good question which has been the subject of much investigation. See page 532 in Ref. 10.

In this paper we demonstrate that it only needs linearity and that $L(|0,0\rangle)$ and $L(|1,0\rangle)$ are unit length states to prove the no-cloning of nonorthogonal states. Clearly we do not require norm preservation for any state. It means that we do not make any use of unitarity. In theory, it is possible to derive a deeper result than the no-cloning principle by using the unitarity. Intuitively it seems that it is easier to implement the operator required in this paper than a unitary operator.

ACKNOWLEDGMENTS

The paper was supported by NSFC (Grant No. 60433050), the Basic Research Fund of Tsinghua University No. JC2003043 and partially by the State Key Laboratory. of Intelligence Technology and System. Professor Zhenghan Wang, Department of Mathematics, Indiana University, is acknowledged for his helpful comments on this paper.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[3] H. Barnum *et al.*, Phys. Rev. Lett. **76**, 2818 (1996).
[4] V. Buzek *et al.*, Phys. Rev. A **56**, 3446 (1997).
[5] C. H. Bennett, G. Brassard, and N. D. Mermin. Phys. Rev. Lett. **68**, 557 (1992).
[6] P. H. Yuen. Phys. Lett. A **113**, 405 (1986).
[7] G. M. D'Ariano and H. P. Yuen, Phys. Rev. Lett. **76**, 2832 (1996).
[8] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[9] T. Mor. Phys. Rev. Lett. **80**, 3137 (1998).
[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).