Probabilistic cloning and deleting of quantum states

Yuan Feng, Shengyu Zhang, and Mingsheng Ying*
State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084
(Received 17 August 2001; published 10 April 2002)

We construct a probabilistic cloning and deleting machine which, taking several copies of an input quantum state, can output a linear superposition of multiple cloning and deleting states. Since the machine can perform cloning and deleting in a single unitary evolution, the probabilistic cloning and other cloning machines proposed in the previous literature can be thought of as special cases of our machine. A sufficient and necessary condition for successful cloning and deleting is presented, and it requires that the copies of an arbitrarily presumed number of the input states are linearly independent. This simply generalizes some results for cloning. We also derive an upper bound for the success probability of the cloning and deleting machine.

DOI: 10.1103/PhysRevA.65.042324 PACS number(s): 03.67.−a, 03.65.Ta

In quantum mechanics, one well-known fact is the no-cloning theorem [1,2], which asserts that, unlike in classical world, an arbitrary unknown quantum state cannot be cloned perfectly because of the linearity of quantum operations. However, inaccurate copying is possible [3]. On the other hand, states chosen from a linearly independent set can be probabilistically cloned by a unitary-reduction process [4,5]. This is an impressive result, and, more interestingly, using the cloning machine introduced in [6], nonorthogonal states from a linearly independent set can evolve into a linear superposition of multiple cloning states.

Recently, deleting unknown quantum states was also found to be impossible, where ''deleting'' means ''uncopying,'' that is, deleting one or more copies of the input state by a linear trace preserving operation [7]. At first glance it seems that copying and deleting should be treated separately since, as pointed out in Ref. [7], the deleting process is independent of cloning. In general, deleting is not the inverse of copying; only if copying and deleting are performed by unitary operation is it so. By a careful analysis, however, it may be seen that the mechanisms of copying and deleting are quite similar. This suggests that we look for a unified way of dealing with copying and deleting of quantum states.

In this short note, we construct a quantum machine which, taking several copies of an input quantum state, can output a linear superposition of multiple cloning states and multiple deleting states. The probabilistic cloning machine of Duan and Guo [4,5] and the cloning machine of Pati [6] can both be thought of as special cases of our cloning and deleting machine. What we would like to emphasize is that in our construction both the copying and deleting procedures occur in a single machine. We show that if $|\psi_i\rangle$ is chosen from $S=\{|\psi_i\rangle: i=1,2,\ldots,m\}$, then $|\psi_i\rangle^{\otimes k}$ can be probabilistically cloned and deleted if and only $|\psi_1\rangle^{\otimes k}, |\psi_2\rangle^{\otimes k}, \ldots, |\psi_m\rangle^{\otimes k}$ are linearly independent. We also give an upper bound for the success probability of the quantum machine.

Consider a quantum state set $S=\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_m\rangle\}$ whose elements belong to an N_A-dimensional Hilbert space with $N_A \geqslant m$ (the subscript A is used to indicate that this is the original system). A quantum cloning process [4,5] is defined by an evolution as

$$|\psi_i\rangle|\Sigma\rangle|P_0\rangle \rightarrow |\psi_i\rangle|\psi_i\rangle|P_i\rangle,$$

where $|\Sigma\rangle$ is the input state of an ancillary system, and P_0 and P_i are the initial state and the final state after cloning $|\psi_i\rangle$ of the cloning apparatus, respectively. Considering the ability of multiple cloning, the cloning process of [6] is given by

$$|\psi_i\rangle|\Sigma\rangle|P_0\rangle \rightarrow \sum_{n=1}^{M} \sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes(n+1)}|0\rangle^{\otimes(M-n)}|P_n\rangle,$$

where M is the total number of states of the ancilla whose initial state is denoted by $|\Sigma\rangle$ and $p_n^{(i)}$ is the success probability of producing n exact copies of $|\psi_i\rangle$. Obviously, this cloning machine is a generalization of that considered in [4,5], and the major distinction between them is that in the former cloning procedures of different copies are embedded in a single machine.

On the other hand, a quantum deleting machine [7] which can delete one of two copies and replace it with some standard state $|0\rangle$ is defined as

$$|\psi_i\rangle|\psi_i\rangle|P_0\rangle \rightarrow |\psi_i\rangle|0\rangle|P_i\rangle.$$

In general, deleting cannot be seen as the inverse process of copying and they are independent of each other; but if they are performed by unitary operation then deleting is the inverse of copying. By combining ideas from [4,5,7], furthermore, the quantum deleting machine depicted above may easily be extended to a probabilistic multiple deleting process, which can be expressed by the following transformation:

$$|\psi_i\rangle^{\otimes k}|P_0\rangle \rightarrow \sum_{n=1}^{k-1} \sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes n}|0\rangle^{\otimes(k-n)}|P_n\rangle.$$

The purpose of this short note is to extend all the concepts mentioned above in a unified way to answer the following question: if we have several identical copies of $|\psi_i\rangle$, is it possible to have a quantum superposition of the multiple cloning and deleting states described as follows:

*Corresponding author. Email address: yingmsh@tsinghua.edu.cn

$$|\psi_i\rangle^{\otimes k}|\Sigma\rangle|P_0\rangle \rightarrow \sum_{n=1}^{M+k} \sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes n}|0\rangle^{\otimes(M+k-n)}|P_n\rangle,$$

where $p_n^{(i)}$ is the success probability of producing $n-k$ exact copies or deleting $k-n$ copies of $|\psi_i\rangle$ depending upon whether $k<n\leqslant M$ or $1\leqslant n<k$?

This cloning and deleting machine deserves a brief explanation. Initially, the number of existing copies of $|\psi_i\rangle$ is k, and in the right-hand side of the above formula the index n in the summation ranges from 1 to $M+k$. For the case of $1\leqslant n<k$, the number of copies of $|\psi_i\rangle$ in the corresponding summand is smaller than k and some copies of $|\psi_i\rangle$ are deleted; for the case of $k<n\leqslant M+k$, the number of copies of $|\psi_i\rangle$ in the summand is greater than k, and some copies of $|\psi_i\rangle$ are added; and finally for the case of $n=k$, the number of copies is not changed. It is clear that the cloning machine of Pati [6] is a special case of this machine when $k=1$ and, on the other hand, if $p_n^{(i)}=0$ for all $n\geqslant k$, our machine is in fact a probabilistically deleting process that deletes one or more of several copies of the input state. An extreme case is that when $p_k^{(i)}=1$ and $p_n^{(i)}=0$ for all $n\neq k$ the machine is simply an identical evolution. So without loss of generality we assume $p_k^{(i)}<1$.

As pointed out in [4–7], both ideal cloning machines and deleting ones do not exist due to the linearity of quantum operations. This naturally implies the nonexistence of the ideal cloning and deleting machine stated above. But the following theorem indicates that a multiple cloning and deleting machine is possible if a nonzero failure probability is allowed.

Theorem. Let the states $|\psi_i\rangle$ be secretly chosen from a set $S=\{|\psi_i\rangle, i=1,2,\ldots,m\}$; then $|\psi_i\rangle^{\otimes k}$ can be probabilistically cloned or deleted by a unitary process U such that

$$U(|\psi_i\rangle^{\otimes k}|\Sigma\rangle|P_0\rangle)=\sum_{n=1}^{M+k}\sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes n}|0\rangle^{\otimes(M+k-n)}|P_n\rangle + \sum_{l=M+k+1}^{N}\sqrt{f_l^{(i)}}|\Phi_l\rangle_{AB}|P_l\rangle \qquad (1)$$

for all $1\leqslant i\leqslant m$ if and only if $|\psi_1\rangle^{\otimes k},|\psi_2\rangle^{\otimes k},\ldots,|\psi_m\rangle^{\otimes k}$ are linearly independent.

In the above equation, $p_n^{(i)}$ is the success probability of producing $n-k$ exact copies or deleting $k-n$ copies of $|\psi_i\rangle$ depending upon whether $k<n\leqslant M$ or $1\leqslant n<k$, $p_k^{(i)}<1$, and $f_l^{(i)}$ is the failure probability of remaining in the lth failure component. $|P_1\rangle,|P_2\rangle,\ldots,|P_N\rangle$ are N orthonormal basis states of some probing device P which belongs to an N-dimensional Hilbert space, and $|\Phi_l\rangle_{AB}$ are normalized but not necessarily orthogonal states of the composite system AB (A and B are the initial and the ancillary system, respectively).

Before proving the theorem, let us see an example first. Let $S=\{|0\rangle,|1\rangle,(1/\sqrt{2})(|0\rangle+|1\rangle)\}$. Since S is not linearly independent, states secretly chosen from S cannot be cloned in the sense of the cloning proposed in [6]. However, if we have two copies of the chosen state, they can be probabilistically cloned and deleted with our machine for $k=2$ because $|00\rangle,|11\rangle$ and $(1/\sqrt{2})(|0\rangle+|1\rangle)(1/\sqrt{2})(|0\rangle+|1\rangle)$ are linearly independent. This shows in an alternative way that our machine is more general than Duan and Guo's and Pati's cloning machines. On the other hand, when $k=1$, the sufficient and necessary condition reduces to that of Duan and Guo's cloning or Pati's cloning. This example suggests that we consider the relevancy of resources to probabilistic cloning. Since "$|\psi_1\rangle^{\otimes k_1},|\psi_2\rangle^{\otimes k_1},\ldots,|\psi_m\rangle^{\otimes k_1}$ are linearly independent" is a looser condition than "$|\psi_1\rangle^{\otimes k_2},|\psi_2\rangle^{\otimes k_2},\ldots,|\psi_m\rangle^{\otimes k_2}$ are linearly independent" when $k_1>k_2$, there are more states that can be cloned and deleted when k increases. For example, for an arbitrary presumed positive integer m, let $S=\{(|0\rangle+(m+2)|1\rangle)^{\otimes m},(2|0\rangle+(m+1)|1\rangle)^{\otimes m},\ldots,((m+2)|0\rangle+|1\rangle)^{\otimes m}\}$, we can easily check that elements in S are linearly dependent; thus they cannot be exactly copied by a probabilistic cloning machine of type $k=m$. But if more resources are prepared, e.g., we have $m+1$ copies of each state, then we can do this with a machine of type $k=m+1$ since $(|0\rangle+(m+2)|1\rangle)^{\otimes(m+1)},(2|0\rangle+(m+1)|1\rangle)^{\otimes(m+1)},\ldots,((m+2)|0\rangle+|1\rangle)^{\otimes(m+1)}$ are linearly independent. This indicates that resources are essential for probabilistic cloning. It is worth noting that resources are irrelevant to Wootters and Zurek's exact cloning since identical or orthogonal states are required.

The proof of the theorem consists of two parts. First, we prove that if the unitary operator U satisfying Eq. (1) exists, then $|\psi_1\rangle^{\otimes k},|\psi_2\rangle^{\otimes k},\ldots,|\psi_m\rangle^{\otimes k}$ are linearly independent. For an arbitrary $|\psi_j\rangle\in S$, if there exist real numbers $c_1^{(j)},c_2^{(j)},\ldots,c_m^{(j)}$ such that $|\psi_j\rangle^{\otimes k}=\Sigma_{i=1}^m c_i^{(j)}|\psi_i\rangle^{\otimes k}$, then from Eq. (1) we have

$$U(|\psi_j\rangle^{\otimes k}|\Sigma\rangle|P_0\rangle)=\sum_{n=1}^{M+k}\sqrt{p_n^{(j)}}|\psi_j\rangle^{\otimes n}|0\rangle^{\otimes(M+k-n)}|P_n\rangle + \sum_{l=M+k+1}^{N}\sqrt{f_l^{(j)}}|\Phi_l\rangle_{AB}|P_l\rangle. \qquad (2)$$

But on the other hand the linearity of quantum operations yields

$$U\left(\sum_i c_i^{(j)}|\psi_i\rangle^{\otimes k}|\Sigma\rangle|P_0\rangle\right)=\sum_i c_i^{(j)}\sum_n \sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes n}|0\rangle^{\otimes(M+k-n)}|P_n\rangle+\sum_i c_i^{(j)}\sum_l \sqrt{f_l^{(i)}}|\Phi_l\rangle_{AB}|P_l\rangle$$
$$=\sum_n\left(\sum_i c_i^{(j)}\sqrt{p_n^{(i)}}|\psi_i\rangle^{\otimes n}\right)|0\rangle^{\otimes(M+k-n)}|P_n\rangle+\sum_l\left(\sum_i c_i^{(j)}\sqrt{f_l^{(i)}}\right)|\Phi_l\rangle_{AB}|P_l\rangle. \qquad (3)$$

Since the right-hand sides of Eqs. (2) and (3) must be equal, we derive $\Sigma_i c_i^{(j)} \sqrt{p_n^{(i)}} |\psi_i\rangle^{\otimes n} = \sqrt{p_n^{(j)}} |\psi_j\rangle^{\otimes n}$ for any $n \leq M+k$. This implies $c_j^{(j)}=1$ and $c_i^{(j)}=0$ for $i \neq j$ because $p_k^{(i)}<1$. So any state chosen from $S^{\otimes k} = \{|\psi_1\rangle^{\otimes k}, |\psi_2\rangle^{\otimes k}, \ldots, |\psi_m\rangle^{\otimes k}\}$ cannot be expressed as a linear composition of other states in $S^{\otimes k}$; this proves that $|\psi_1\rangle^{\otimes k}, |\psi_2\rangle^{\otimes k}, \ldots, |\psi_m\rangle^{\otimes k}$ are linearly independent.

Now we need only show that the linear independence of $S^{\otimes k}$ implies the existence of the unitary operator satisfying Eq. (1). Taking the overlaps of distinct input states $|\psi_i\rangle^{\otimes k}$ and $|\psi_j\rangle^{\otimes k}$, from Eq. (1) we have

$$\langle \psi_i|\psi_j\rangle^k = \sum_{n=1}^{M+k} \sqrt{p_n^{(i)}} \langle \psi_i|\psi_j\rangle^n \sqrt{p_n^{(j)}} + \sum_{l=M+k+1}^{N} \sqrt{f_l^{(i)} f_l^{(j)}} \tag{4}$$

or, more briefly, a matrix equation as follows:

$$G^{(k)} = \sum_{n=1}^{M+k} A_n G^{(n)} A_n^\dagger + \sum_{l=M+k+1}^{N} F_l, \tag{5}$$

where $G^{(k)} = [\langle \psi_i|\psi_j\rangle^k]_{m\times m}$, $A_n = A_n^\dagger = \mathrm{diag}(\sqrt{p_n^{(1)}}, \sqrt{p_n^{(2)}}, \ldots, \sqrt{p_n^{(m)}})$ and $F_l = [\sqrt{f_l^{(i)} f_l^{(j)}}]_{m\times m}$.

From Lemma 1 in [5], we know that it suffices to find A_n's and F_l's satisfying Eq. (5) in order to get a unitary operator U in Eq. (1). Since $|\psi_1\rangle^{\otimes k}, |\psi_2\rangle^{\otimes k}, \ldots, |\psi_m\rangle^{\otimes k}$ are linearly independent, $G^{(k)}$ is positive definite. So $G^{(k)} - \Sigma_n A_n G^{(n)} A_n^\dagger$ is also positive definite for small enough but positive $p_n^{(1)}, p_n^{(2)}, \ldots, p_n^{(m)}$. This provides us with the required A_n's. Furthermore, the Hermitian matrix $G^{(k)} - \Sigma_n A_n G^{(n)} A_n^\dagger$ can be diagonalized by a unitary matrix V as follows:

$$V^\dagger \left(G^{(k)} - \sum_{n=1}^{M+k} A_n G^{(n)} A_n^\dagger \right) V = \mathrm{diag}(a_1, a_2, \ldots, a_m), \tag{6}$$

where all the $\{a_i\}$ are positive real numbers. We now need only choose $F_l = V\, \mathrm{diag}(g_{(l)1}, g_{(l)2}, \ldots, g_{(l)m}) V^\dagger$ such that $\Sigma_l g_{(l)i} = a_i$. This completes the proof of the theorem.

In the above theorem, the failure component is separated as the tensor of a state of the composite system AB and a state of the probe P. More generally, we may consider the case where the failure component cannot be separated in such a way and it is indeed an entangled state in ABP. This leads us to extend the cloning and deleting machine to a more general one given by

$$U|\psi_i\rangle^{\otimes k}|\Sigma\rangle|P_0\rangle = \sum_{n=1}^{M+k} \sqrt{p_n^{(i)}} |\psi_i\rangle^{\otimes n} |0\rangle^{\otimes (M+k-n)} |P_n\rangle + \sum_{l=M+k+1}^{N} \sqrt{c_{il}} |\Psi_l\rangle_{ABP}, \tag{7}$$

where c_{il} denotes the failure probability of remaining in the lth failure component, $|\Psi_l\rangle_{ABP}$ are orthonormal states of the composite system ABP, and the first term has the usual meaning. The condition

$$|P_n\rangle\langle P_n||\Psi_l\rangle_{ABP} = 0 \quad \text{for any } n \text{ and } l$$

must be satisfied in order to derive perfect copies of the input states by a measurement onto the probe basis $\{P_n\}$. There are no difficulties in generalizing the above theorem to the extended machine.

We now turn to deriving an upper bound for the success probability of multiple cloning and deleting. From Eq. (7) we have

$$|\langle \psi_i|\psi_j\rangle|^k \leq \sum_{n=1}^{M+k} \sqrt{p_n^{(i)} p_n^{(j)}} |\langle \psi_i|\psi_j\rangle|^n + \sum_{l=M+k+1}^{N} \sqrt{c_{il} c_{jl}}. \tag{8}$$

Using the arithmetic-geometric average inequality $\sqrt{ab} \leq \frac{1}{2}(a+b)$ when $a \geq 0$ and $b \geq 0$, we obtain

$$\begin{aligned} |\langle \psi_i|\psi_j\rangle|^k &\leq \sum_n \frac{1}{2}(p_n^{(i)} + p_n^{(j)}) |\langle \psi_i|\psi_j\rangle|^n + \sum_l \frac{1}{2}(c_{il} + c_{jl}) \\ &= \sum_n \frac{1}{2}(p_n^{(i)} + p_n^{(j)}) |\langle \psi_i|\psi_j\rangle|^n + 1 \\ &\quad - \sum_n \frac{1}{2}(p_n^{(i)} + p_n^{(j)}). \end{aligned}$$

The last equality is derived from $\Sigma_n p_n^{(i)} + \Sigma_l c_{il} = 1$. So

$$\frac{1}{2} \sum_{n=1}^{M+k} (p_n^{(i)} + p_n^{(j)})(1 - |\langle \psi_i|\psi_j\rangle|^n) \leq 1 - |\langle \psi_i|\psi_j\rangle|^k. \tag{9}$$

If we adopt the notation of minimum-normed distance [8], the bound can be expressed as

$$\sum_{n=1}^{M+k} p_n D^2(|\psi_i\rangle^{\otimes n}, |\psi_j\rangle^{\otimes n}) \leq D^2(|\psi_i\rangle^{\otimes k}, |\psi_j\rangle^{\otimes k}), \tag{10}$$

where $p_n = \frac{1}{2}(p_n^{(i)} + p_n^{(j)})$ and $D^2(|\psi_i\rangle^{\otimes n}, |\psi_j\rangle^{\otimes n}) = 2(1 - |\langle \psi_i|\psi_j\rangle|^n)$ is the minimum-normed distance between n copies. That is, the sum of the weighted distance between n copies of two distinct states is always bounded by the minimum-normed distance between the original states. This result also coincides with the probabilistic cloning in [4,5] and the cloning in [6].

In summary, we have presented a unified way of dealing with copying and deleting of quantum states by constructing a probabilistic cloning and deleting machine that can perform multiple cloning and deleting in a single operation. We give a sufficient and necessary condition for our machine to successfully clone and delete. An upper bound for the success probability is also derived. We still do not know whether this upper bound is optimal and, on the other hand, what we should point out is that the upper bound above will become worthless when considering only the case of deleting. For

example, if for any $ip_n^{(i)}$ is zero except when $n=N$ where $N>k$, then $\frac{1}{2}(p_N^{(i)}+p_N^{(j)}) \leqslant (1-|\langle\psi_i|\psi_j\rangle|^k)/(1-|\langle\psi_i|\psi_j\rangle|^N)$. Since $N<k$, the right-hand side is greater than 1. So an interesting open problem for further study would be to improve the upper bound or even to find the optimal one.

This work was supported by the National Foundation for Distinguished Young Scholars (Grant No. 69725004), the National Key Project for Basic Research (Grant No. 1998030509), and the National Foundation of Natural Sciences (Grant No. 69823001).

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[3] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] L. M. Duan and G. C. Guo, Phys. Lett. A **243**, 261 (1998).
[5] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[6] A. K. Pati, Phys. Rev. Lett. **83**, 2849 (1999).
[7] A. F. Pati and S. L. Braunstein, Nature (London) **404**, 164 (2000).
[8] A. K. Pati, Phys. Lett. A **159**, 105 (1991).