Quantum Superposition of Multiple Clones and the Novel Cloning Machine

Arun Kumar Pati

Quantum OPHCS and Information Group, SEECs, University of Wales, Dean Street, Bangor LL 57 1UT, United Kingdom

(Received 10 March 1999)

We envisage a novel quantum cloning machine, which takes an input state and produces an output state whose success branch can exist in a linear superposition of multiple copies of the input state and the failure branch can exist in a superposition of composite states independent of the input state. We prove that unknown nonorthogonal states chosen from a set \( S \) can evolve into a linear superposition of multiple clones and failure branches by a unitary process if and only if the states are linearly independent. We derive a bound on the success probability of the novel cloning machine. We argue that the deterministic and probabilistic clonings are special cases of our novel cloning machine.

In recent years the quantum mechanical principles such as linearity, unitarity, and inseparability have been utilized to realize quantum computers [1], quantum teleportation [2], quantum cryptography [3], and so on. On one hand, these principles enhance the possibility of information processing, but, on the other, they put on some limitations. That an unknown quantum state cannot be perfectly copied is a consequence of linearity of quantum theory [4,5]. Similarly, the unitarity of the quantum theory does not allow one to clone two nonorthogonal states [6,7]. This has been generalized to mixed states [8]. Though perfect copies cannot be produced, there are important results on the possibility of producing approximate copies of an unknown quantum state [9–13]. If one allows unitary and measurement processes, then a set of linearly independent nonorthogonal states can be cloned perfectly with a nonzero probability [14,15]. We [16] have proposed a protocol for producing exact copies and complement copies of an unknown qubit using minimal communication from a state preparer. As some applications of the "no-cloning" theorem one finds the possibility of decompressing quantum entanglement [17] and explaining the information loss inside a black hole [18].

In the past various authors have asked the following question: If we have an unknown state \( \ket{\psi} \), is there a device which will produce \( \ket{\psi} \rightarrow \ket{\psi}^{\otimes 2}, \ket{\psi} \rightarrow \ket{\psi}^{\otimes 3}, \ket{\psi} \rightarrow \ket{\psi}^{\otimes M} \), or, in general, \( \ket{\psi}^{\otimes N} \rightarrow \ket{\psi}^{\otimes M} \) copies of an unknown state in a deterministic or probabilistic fashion? This is a "classicalized" way of thinking about a quantum cloning machine. If we pause for a second, and think of the working style of a classical Xerox machine, then we know that it does exactly the same thing. When we feed a paper with some amount of information into a Xerox machine containing \( M \) blank papers, we can get either \( 1 \rightarrow 2 \), or \( 1 \rightarrow 3 \), \ldots \( 1 \rightarrow M \) copies by just pressing the number of copies we want. However, the quantum world is different where one can have linear superposition of all possibilities with appropriate probabilities. If a real quantum cloning machine existed it would exploit this basic feature of the quantum world and produce simultaneously \( \ket{\psi} \rightarrow \ket{\psi}^{\otimes 2}, \ket{\psi} \rightarrow \ket{\psi}^{\otimes 3}, \) and \( \ket{\psi} \rightarrow \ket{\psi}^{\otimes M} \) copies. We ask if it is possible by some physical process to produce an output state of an unknown quantum state which will be in a linear superposition of all possible multiple copies each in the same original state. A device that can perform this task we call the "novel quantum cloning machine."

In this Letter we show that the nonorthogonal states secretly chosen from a set \( S = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle\} \) can evolve into a linear superposition of multiple copy states together with a failure term described by a composite state (independent of the input state) by a unitary process if and only if the states are linearly independent. We prove a bound on the success probability of the novel cloning machine for nonorthogonal states. We point out that the recently proposed probabilistic cloning machine of Duan and Guo [15] can be thought of as a special case of a more general "novel cloning machine." We hope that the existence of such a machine would greatly facilitate the quantum information processing in a quantum computer.

Consider an unknown input state \( |\psi_i\rangle \) from a set \( S \) which belongs to a Hilbert space \( H_A = \mathcal{C}^{N_A} \). Let \( \Sigma_B \) be the state of the ancillary system \( B \) (analogous to a bunch of blank papers) which belongs to a Hilbert space \( H_B \) of dimension \( N_B = N_A^M \), where \( M \) is the total number of blank states each having dimension \( N_A \). In fact, we can take \( |\Sigma_B\rangle = |0\rangle^\otimes M \). Let there be a probe state of the cloning device which can measure the number of copies that have been produced and \( |P\rangle \) be the initial state of the probing device. Let \( \{ |P\rangle \} (n = 1, 2, \ldots, N_C) \in H_C = \mathcal{C}^{N_C} \) be orthonormal basis states of the probing device with \( N_C > M \). If a novel cloning machine exists, then it should be represented by a linear, unitary operator that acts on the combined states of the composite system. The question is as follows: Is it possible to have a quantum superposition of the multiple clones of the input state given by
where $p_n^{(i)} (n = 1, 2, \ldots, M)$ is the probability with which $n$ copies of the original input quantum state can be produced. However, we [19] have recently shown that such an ideal novel cloning machine based on unitarity of quantum theory cannot exist. Nevertheless, a novel cloning machine which can create linear superposition of multycopies with nonunit total success probability does exist. The existence of such a machine is proved by the following theorem.

**Theorem.**—There exists a unitary operator $U$ such that for any unknown state chosen from a set $S = \{|\psi_i\rangle\} (i = 1, 2, \ldots, k)$ the machine can create a linear superposition of multiple clones together with failure probabilities given by

$$
U(|\psi_i\rangle |S\rangle |P\rangle) = \sum_{n=1}^{M} \sqrt{p_n^{(i)}} |\psi_i\rangle^\otimes(n+1)|0\rangle^\otimes(M-n)|P_n\rangle 
+ \sum_{l=M+1}^{N_c} \sqrt{f_l^{(i)}} |\Psi_l\rangle_{AB}|P_l\rangle ,
$$

(2)

if and only if the states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle$ are linearly independent. In the above equation $p_n^{(i)}$ and $f_l^{(i)}$ are success and failure probabilities for the $i$th input state to produce $n$ exact copies and to remain in the $l$th failure component, respectively. The states $|\Psi_l\rangle_{AB}$’s are normalized states of the composite system $AB$, and they are not necessarily orthogonal.

We prove the existence of such a unitary operator in two stages. First, we prove that if an unknown quantum state chosen from a set $S$ exists in a linear superposition of multiple copy states, then the set $S$ is linearly independent. Consider an arbitrary state $|\psi\rangle = \sum_i c_i|\psi_i\rangle$. If we feed this state, then the unitary evolution yields

$$
U(|\psi\rangle |S\rangle |P\rangle) = \sum_{n=1}^{M} \sqrt{p_n} |\psi\rangle^\otimes(n+1)|0\rangle^\otimes(M-n)|P_n\rangle 
+ \sum_{l=M+1}^{N_c} \sqrt{f_l} |\Psi_l\rangle_{AB}|P_l\rangle .
$$

(3)

However, by linearity of quantum theory each of $|\psi_i\rangle$ would undergo transformation under (2) and we have

$$
U(\sum_i c_i|\psi_i\rangle |S\rangle |P\rangle) = \sum_i c_i \sum_{n=1}^{M} \sqrt{p_n^{(i)}} |\psi_i\rangle^\otimes(n+1)|0\rangle^\otimes(M-n)|P_n\rangle + \sum_i c_i \sum_{l=M+1}^{N_c} \sqrt{f_l^{(i)}} |\Psi_l\rangle_{AB}|P_l\rangle .
$$

(4)

Since the final states in (3) and (4) are different, a quantum state represented by $|\psi\rangle$ cannot exist in a linear superposition of all possible copy states. We know that if a set contains distinct vectors $\{|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle\}$ such that $|\psi\rangle$ is a linear combination of other $|\psi_i\rangle$’s, then the set is linearly dependent. Thus linearity prohibits us from creating linear superposition of multiple copy states chosen from a linearly dependent set. Therefore, Eq. (2) exists for any state secretly chosen from $S$ only if its elements are linearly independent. This proves the first part of the theorem.

Now we prove the converse of the statement; i.e., we show that if the set $S$ is linearly independent then there exists a unitary evolution, which can create linear superposition of multiple copy states with some success and failure. If the unitary evolution (2) holds, then the overlap of two distinct output states $|\psi_i\rangle$ and $|\psi_j\rangle$ secretly chosen from $S$ after they have passed through the device would be given by

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

(5)

Conversely, if (5) holds, there exists a unitary operator to satisfy (2). In the sequel we will prove that if the set $S$ is linearly independent then (5) holds. The above equation can be generically expressed as a $k \times k$ matrix equation,

$$
G^{(1)} = \sum_{n=1}^{M} A_n G_n^{(n+1)} A_n^\dagger + \sum_l F_l,
$$

(6)

where the matrices $G^{(1)} = \{|\psi_1\rangle |\psi_2\rangle |\cdots |\psi_k\rangle\}$ is the Gram matrix, $G^{(n+1)} = \{|\psi_1\rangle |\psi_2\rangle |\cdots |\psi_k\rangle\}$, $A_n = A_n^\dagger = \text{diag}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k})$, and $F_l = \sqrt{f_l} f_l^{(i)}$. Now proving the existence of a unitary evolution given in (2) is equivalent to showing that (6) holds for a positive definite matrix $A_n$. It can be shown that if the states $\{|\psi_i\rangle\}$ are linearly independent, then the Gram matrix $G^{(1)}$ is a positive definite and its rank is equal to the dimension of the space spanned by the vectors $|\psi_i\rangle$. Similarly, we can show that the matrix $G^{(n+1)}$ is also positive definite. Because for an arbitrary column vector $\alpha = \text{col}(c_1, c_2, \ldots, c_k)$, we can write $\alpha^\dagger G^{(n+1)} \alpha = \sum_{i,j=1}^{k} c_i^* c_j G_{ij}^{(n+1)} = |\beta|^2$, where $|\beta|^2 = \sum_i c_i^* |\psi_i\rangle^\otimes(n+1)$. Since the square of the length of a vector is positive and cannot go to zero (if the set is linearly independent), this shows that $G^{(n+1)}$ is a positive definite matrix. Also, the matrix $A_n$ is positive definite which suggests $A_n G_n^{(n+1)} A_n^\dagger$ is also a positive definite matrix. Further, we know that the sum of two
positive definite matrices is also a positive definite one. From the continuity argument for a small enough $A_n$ the matrix $G^{(i)} = \sum_{n=1}^{M} A_n G^{(n+1)} A_n^\dagger$ is also a positive definite matrix. Therefore, we can diagonalize the Hermitian matrix by a suitable unitary operator $V$. Thus we have $V^\dagger (G^{(i)} - \sum_{n} A_n G^{(n+1)} A_n^\dagger) V = \text{diag}(a_1, a_2, \ldots, a_k)$, where the eigenvalues $\{a_i\}$ are positive real numbers. Now we can choose the matrix $F_1$ to be $F_i = V \text{diag}(g_{(i)1}, g_{(i)2}, \ldots, g_{(i)k}) V^\dagger$ such that $\sum_{j} g_{(i)j} = a_i$ ($i = 1, 2, \ldots, k$). Thus the matrix equation (6) is satisfied with a positive definite matrix $A_n$ if the states are linearly independent. Once (2) holds, we see that the success and failure probabilities are summed to unity, i.e., $\sum_{n} p_n^{(i)} + \sum_{j} f_j^{(i)} = 1$ as expected. This completes the proof of our main result.

Here we discuss the generality of our novel cloning machine. For example, if $|0\rangle$ and $|1\rangle$ are the computational basis, then a qubit secretly chosen from a set $\{0\}, \alpha|0\rangle + \beta|1\rangle$ or from a set $\{1\}, \alpha|0\rangle + \beta|1\rangle$ can exist in a linear superposition of multiple clones. But a state chosen from a set $\{0\}, |1\rangle, \alpha|0\rangle + \beta|1\rangle$ cannot exist in such a superposition of multiple clones as the set is not linearly independent. It may be noted that the “no-cloning” theorem is a special case of our result because the linear superposition of multiple clones fails if the machine does not fail with some probability. When all the failure probabilities are zero, we have a “no-supersposition of multiple clone” theorem [19]. Then if we take one of the success probabilities as one, we get the Wooters-Zurek-Diek’s no-cloning theorem [4,5].

Our result is consistent with the known results on cloning. In the unitary evolution if one of the positive numbers in the success branch is one (i.e., $p_n^{(i)} = 1$ for some $n$ and all $i$) and all others (including failure branches) are zero, then we have $U(|\psi_i\rangle |\Sigma\rangle |P\rangle) = |\psi_i\rangle^{(n+1)} |0\rangle^{(M-n)} |P_n\rangle$. This tells us that the matrix equation would be $G^{(i)} = G^{(n+1)}$ since $A_n = I$. This will be possible only when the states chosen from a set are orthogonal to each other. Thus a single quanta in an orthogonal state can be perfectly cloned [6]. Here we discuss the condition under which all $f^{(i)}$’s are zero. The orthogonality relation $|\psi_i\rangle |\psi_j\rangle = \delta_{ij}$ is a necessary and sufficient condition on the set $S$ for all $f^{(i)}$’s to be zero. The converse can also be proved. When all $f^{(i)}$’s are zero, from (5) we can obtain $|\langle \psi_i | \psi_j \rangle| \leq \frac{1}{2} \sqrt{\sum p_n^{(i)} p_n^{(j)}} |\langle \psi_i | \psi_j \rangle|^n + 1$. Using two inequalities $p_n^{(i)} p_n^{(j)} \leq \frac{1}{2} (p_n^{(i)} + p_n^{(j)})$ and $|\langle \psi_i | \psi_j \rangle|^n \leq |\langle \psi_i | \psi_j \rangle|^n$ we find $|\langle \psi_i | \psi_j \rangle|^n (1 - |\langle \psi_i | \psi_j \rangle|^n) \leq 0$. Since the quantity inside the bracket is positive and $|\langle \psi_i | \psi_j \rangle|$ cannot be negative, it must be zero. Therefore, the states have to be orthogonal when all $f^{(i)}$’s are zero. Note that another interesting result follows from our proposed cloning machine. If the states are orthogonal and all $p_n^{(i)}$’s are nonzero, then unitarity allows us to have a linear superposition of multiple copies of orthogonal states as the matrix equation is always satisfied. We mention that it would be interesting to investigate the extension of $U$ beyond the elements of $S$ in the future.

After the input state chosen from the set $S$ undergoes unitary evolution in order to know how many copies are produced by the novel cloning machine, one needs to do a von Neumann measurement onto the probe basis. This can be thought of as a measurement of a Hermitian operator. We introduce such an operator, which is called the “Xerox number” operator $N_X$, defined as

$$N_X = \sum_{n=1}^{M} n |P_n\rangle \langle P_n|,$$ (7)

The probe states $|P_n\rangle$ are eigenstates of the Xerox number operator with eigenvalue $n$ where $n$ is the number of clones produced with a probability distribution $pn$. The measurement of the Xerox number operator will give us information about how many copies have been produced by the cloning machine. For example, the novel cloning machine would produce 1 $\rightarrow$ 2 copies with probability $p_1$, 1 $\rightarrow$ 3 copies with probability $p_2$, ..., and 1 $\rightarrow$ $M + 1$ copies with probability $p_M$ in accordance with the usual rules of quantum mechanics.

Here, we derive a bound on the success probability of producing multiple clones through a unitary machine (2). Taking the overlap of two distinct states we find

$$|\langle \psi_i | \psi_j \rangle| \leq \sum_{n=1}^{M} \sqrt{p_n^{(i)} p_n^{(j)}} |\langle \psi_i | \psi_j \rangle|^n + 1 + \sum_{i=M+1}^{N} \sqrt{f_{i}^{(i)} f_{i}^{(j)}}.$$ (8)

On simplifying (8) we get the tight bound on the individual success probability for cloning of two distinct nonorthogonal states as

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

The above bound is related to the distinguishable metric of the quantum state space. Since the “minimum-normed distance” [20] between two nonorthogonal states $|\psi_i\rangle$ and $|\psi_j\rangle$ is $D^2(|\psi_i\rangle, |\psi_j\rangle) = 2(1 - |\langle \psi_i | \psi_j \rangle|)$ and the minimum-normed distance between $n + 1$ clones is $D^2(|\psi_i\rangle^{\otimes n+1}, |\psi_j\rangle^{\otimes n+1}) = 2(1 - |\langle \psi_i | \psi_j \rangle|^{n+1})$, the tight bound can be expressed as

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

where we have defined total success probability $p_n$ for $n$th clones as $p_n = \frac{1}{2} (p_n^{(i)} + p_n^{(j)})$. The minimum-normed-distance function is a measure of distinguishability of two nonorthogonal quantum states. Therefore, the above bound can be interpreted physically as the sum of the
weighted distance between two distinct states of \( n + 1 \) clones always bounded by the original distance between two nonorthogonal states. Also, our bound is consistent with the known results on cloning. For example, if we have \( 1 \rightarrow 2 \) cloning, then in the evolution we have \( p_1^{(i)} \) and \( p_1^{(j)} \) as nonzero and all others as zero. In this case our bound reduces to \( 1/2 \{ p_1^{(i)} + p_1^{(j)} \} \leq \frac{1}{1+|\langle \phi_i | \phi_j \rangle|^2} \), which is nothing but the Duan and Guo bound [15] for producing two clones in a probabilistic fashion. Similarly, if we have \( 1 \rightarrow M \) cloning, then in the evolution we have \( p_n^{(i)} \) and \( p_M^{(j)} \) as nonzero and all others as zero. In this case our bound reduces to \( 1/2 \{ p_n^{(i)} + p_M^{(j)} \} \leq \frac{1-|\langle \phi_i | \phi_j \rangle|^2}{1-|\langle \phi_i | \phi_j \rangle|^2} \), which is nothing but the Chefles-Barnett [13] bound, obtained using the quantum state separation method.

We can imagine a more general novel cloning machine and then show that the probabilistic cloning machine discussed by Duan and Guo [15] can be considered as a special case of the general novel cloning machine. Instead of the unitary evolution (2) one could describe a general unitary evolution of the composite system \( ABC \) as

\[
U(\psi) = \sum_{m=1}^{M} \sqrt{p_m^{(i)}} |\psi_i\rangle^{(n-1)} |\psi_j\rangle^{(M-n)} |P_n\rangle + \sum_{l} c_{i,l} |\Psi_l\rangle_{ABC}.
\]

(11)

Here, the first term has the usual meaning and the second term represents the failure term. The states \( |\Psi_l\rangle_{ABC} \) are normalized states of the composite system. For simplicity we assume that they are orthonormal. Further, since the measurement of the Xerox number operator should yield perfect copies (say, \( n \)) of the input state with probability \( p_n^{(i)} \), this entails that \( |P_n\rangle \langle P_n| \Psi_l\rangle_{ABC} = 0 \) for any and \( l \).

Imposing this physical condition, we find from (11) that the inner product of two distinct states gives \( \langle \phi_i | \phi_j \rangle = \sum_{n=1}^{M} \sqrt{p_n^{(i)}} |\psi_i\rangle^{(n-1)} p_n^{(j)} + \sum_{l} c_{i,l} c_{j,l} \). This can be expressed as a matrix equation \( G^{(i)} = \sum_{n=1}^{M} A_n G^{(n+1)} A_n^\dagger + C^\dagger C \), where \( C = [c_{i,j}] \). From our earlier theorem we can now prove that with a positive definite matrix \( A_n \) we can diagonalize \( G^{(i)} - \sum_{n=1}^{M} A_n G^{(n+1)} A_n^\dagger \) and with a particular choice of the matrix \( C \) the unitary evolution exists.

If we take one of the \( p_n^{(i)} \) as nonzero and all others as zero in (11) we get the Duan-Guo machine. This is given by

\[
U(\psi) = \sqrt{p_n^{(i)}} |\psi_i\rangle^{(n-1)} |P_n\rangle + \sum_{l} c_{i,l} |\Psi_l\rangle_{ABC},
\]

(12)

where we have assumed that there are \( n \) blank states. If one does a measurement of the probe with a postselection of the measurement results, then this will yield \( n (n = 1, 2, \ldots, M) \) exact copies of the unknown quantum states.

Since other deterministic cloning machines are special cases of the Duan-Guo machine, we can say, in fact, that the deterministic and probabilistic cloning machines are special cases of our novel cloning machines.

To conclude, we discovered yet another surprising feature of cloning transformation, which says that the unitarity allows linear superposition of multiple clones of nonorthogonal states along with a failure term if and only if the states are linearly independent. We derived a tight bound on the success probability of passing two nonorthogonal states through a novel cloning machine. We hope that the existence of linear superposition of multiple clones will be very useful in quantum state engineering, easy preservation of important quantum information, quantum error correction, and parallel storage of information in a quantum computer.

I thank S. L. Braunstein for discussions and L. M. Duan for discussions and suggestions. I gratefully acknowledge financial support by EPSRC.

*Electronic address: akpati@sees.bangor.ac.uk