We discuss the usefulness of quantum cloning and present examples of quantum computation tasks for which cloning offers an advantage which cannot be matched by any approach that does not resort to it. In these quantum computations, we need to distribute quantum information contained in states about which we have some partial information. To perform quantum computations, we use state-dependent probabilistic quantum cloning procedure to distribute quantum information in the middle of a quantum computation.

PACS: 03.67.Lx, 42.50.Dv

Cloning is very useful in classical computing and easy to accomplish with classical information. However, quantum cloning turns out not to be possible in general in quantum mechanics. This no-cloning theorem, independently discovered by Wootters and Zurek and Dieks in the early 1980s, is one of the most fundamental differences between classical and quantum information theories. It tells us that an unknown quantum state can not be copied exactly. Since determinately perfect copying is impossible, much effort has been put into developing optimal cloning processes.

The universal quantum cloning machines were first invented by Bužek and Hillery and developed by other authors. The other kind of cloning procedure first designed by Duan and Guo is nondeterministic, consisting in adding an ancilla, performing unitary operations and measurements, with a postselection of the measurement results. The resulting clones are perfect, but the procedure only succeeds with a certain probability $p < 1$. The imperfect nature of quantum cloning procedure results in lower chances of getting the correct computational results. The resulting clones are perfect, but the procedure only succeeds with a certain probability $p < 1$. The imperfect nature of quantum cloning procedure results in lower chances of getting the correct computational results. The resulting clones are perfect, but the procedure only succeeds with a certain probability $p < 1$.

Let us consider the scenario. There are two different quantum computations with first computational step $U_0$ in common. We need to find a scheme that obtains the two computation results with as large a probability as possible, using $U_0$ only once (this may happen if $U_0$ is a complex, lengthy computation). Possible schemes may or may not resort to cloning to distribute quantum information; the quantum computational tasks below show that performance is enhanced if we distribute quantum information using quantum cloning.

Suppose that there are three quantum black-boxes. What each black-box does is to accept one 2-level quantum system as an input and apply a unitary operator to it, producing the evolved state as an output. The black-boxes consist of arbitrary quantum circuits that query a given function only once. The query of function $f_i$ is the unitary such that $|x,y\rangle \rightarrow |x,y \oplus f_i(x)\rangle$, where the symbol $\oplus$ denotes the bitwise XOR operation. Our task will involve determining two functionals, one depending only on $f_0$ and $f_1$, and the other on $f_0$ and $f_2$.

Consider all functions $h_i$ which take $n$ bits to one bit and write $h_{a_0a_1 \cdots a_{n-1}}$ to stand for the function $h$ such that $h(k) = a_k$, $k = 0, 1, \cdots, 2^n - 1$ (e.g. $h_{a_0a_1a_2a_3}$ denotes $h(000) = a_0$, $h(001) = a_1$, $h(010) = a_2$, $h(011) = a_3$, $h(100) = a_4$, $h(101) = a_5$, $h(110) = a_6$, $h(111) = a_7$). We define some sets of functions that will be useful in stating our task:

$$S^3_{f_0} = \{h_{01000000}, h_{01010101}, h_{11000011}\}.$$
\[ S^3_1 = \{ h_{01000000}, h_{10110000}, h_{10001100}, h_{00100101}, h_{00001011}, h_{10010010}, h_{00011010} \}, \]
\[ S^3_2 = \{ h_{00000000}, h_{00001111}, h_{01010101}, h_{00101111}, h_{10010101}, h_{10100101}, h_{10100101} \}, \]
\[ S^3_{f_{12}} = S^3_1 \cup S^3_2, \]
\[ H^3_{00000000} = \{ h_{00000000}, h_{11111111} \}, H^3_{00001111} = \{ h_{00001111}, h_{11110000} \}, H^3_{01010101} = \{ h_{01010101}, h_{10101010} \}, H^3_{00110011} = \{ h_{00110011}, h_{10100110} \}, H^3_{00110100} = \{ h_{00110100}, h_{10101001} \}, H^3_{01001100} = \{ h_{01001100}, h_{10110001} \}, H^3_{01010010} = \{ h_{01010010}, h_{10101101} \}, H^3_{01011000} = \{ h_{01011000}, h_{10111000} \}, H^3_{01011100} = \{ h_{01011100}, h_{10111100} \}, \]
\[ S^3_f = H^3_{00000000} \cup H^3_{00001111} \cup H^3_{01010101} \cup H^3_{00110011} \cup H^3_{00110100} \cup H^3_{01001100} \cup H^3_{01010010} \cup H^3_{01011000} \cup H^3_{01011100} \cup H^3_{01011100}. \]
\[ S^3_{f_0} = \{ h_{a_0a_1a_2\cdots a_{n-1}} | h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_0 \}, \]
\[ S^3_{x_1} = \{ h_{a_0a_1a_2\cdots a_{n-1}a_0a_1a_2\cdots a_{n-1}} | h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_1 \}, \]
\[ S^3_{x_2} = \{ h_{a_0a_1a_2\cdots a_{n-1}a_0a_1a_2\cdots a_{n-1}} | h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_2 \}, \]
\[ S^3_{f_1} = S^3_{x_1} \cup S^3_{x_2}, \]
\[ H^3_{x_1} = \{ h_{a_0a_1a_2\cdots a_{n-1}a_0a_1a_2\cdots a_{n-1}} | h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_1 \}, \]
\[ H^3_{x_2} = \{ h_{a_0a_1a_2\cdots a_{n-1}a_0a_1a_2\cdots a_{n-1}} | h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_2 \}, \]
\[ S^3_f = \bigcup_{h_{a_0a_1a_2\cdots a_{n-1}} \in S^3_2} (H^3_{x_1} \cup H^3_{x_2}). \]

Here \( n = 3, 4, \cdots \) and \( \pi_k = \begin{cases} 0, & \text{if } a_k = 1 \\ 1, & \text{if } a_k = 0 \end{cases} \) for \( k = 0, 1, 2, \cdots, 2^n - 1 \).

Now we randomly choose a function \( f_0 \in S^3_f \) and then pick two other functions \( f_1 \) and \( f_2 \) from the set \( S^3_{f_{12}} \), also at random but satisfying:
\[
f_0 \oplus f_1 \oplus f_2 \in S^3_f. \tag{1}\]

Here the symbol \( \oplus \) is addition modulo 2. The task will be to find in which of the \( 2^n \) sets \( H^n \)'s lie each of the functions \( f_0 \oplus f_1 \) and \( f_0 \oplus f_2 \), applying quantum circuits that query \( f_0 \), \( f_1 \), and \( f_2 \) at most once each. Our score will be given by the average probability of successfully guessing both correctly.

Just as [15] the best no-cloning strategy is as follows. First, from Eq. (1) we know that both \( f_1 \) and \( f_2 \) must be in \( S^3_f \) if \( f_0 = h_{10100000} \), and \( f_1 \) and \( f_2 \) must belong to \( S^3_f \) if \( f_0 \) is either \( h_{01010101} \) or \( h_{11000011} \), where \( \{ a_0a_1 \cdots a_7 \}_{2^n-3} \) means \( 2^n-3 \) copies of \( a_0a_1 \cdots a_7 \). It implies that the probability of both \( f_1 \) and \( f_2 \) in \( S^3_f \) is \( 2/3 \). Assume that it is the case, then we can discriminate between the two possibilities for \( f_0 \) with a single, classical function call. Furthermore, by using the quantum circuit in Fig.1 twice (once each with \( f_1 \) and \( f_2 \)) we can distinguish the \( 2^n \) possibilities for functions \( f_1 \) and \( f_2 \), because this quantum circuit results in one of the \( 2^n \) orthogonal states
\[
|\varphi_i \rangle = 2^{-\frac{n}{2}} \sum_{x=0}^{2^n-1} (-1)^{f_i(x)} |x\rangle. \tag{2}\]

Thus we can determine functions \( f_0, f_1, \) and \( f_2 \) correctly with probability \( p = 2/3 \) and accomplish our task. Even in the case where the initial assumption about \( f_0 \) was wrong, the chances of guessing right are \( 1/2^{2n} \). Therefore, the best no-cloning average score is
\[
p_1 = \frac{2}{3} + \frac{1}{3} \times \frac{1}{2^{2n}} < 0.7. \tag{3}\]
Next we will see that the task which can be much better performed if we use probabilistic quantum cloning. The quantum circuit that we use to solve this problem is depicted in Fig. 2.

Immediately after querying function $f_0$, we obtain one of three possible linearly independent states (each corresponding to one of the possible $f_0$’s):

\[
|h_{(01000000)^{2n-3}}\rangle = 2^{-\frac{n}{2}} \sum_{j=0}^{2^{n-3}-1} (-1)^{j} |2^{3}j\rangle,
\]

\[
|h_{(11000011)^{2n-3}}\rangle = 2^{-\frac{n}{2}} \sum_{j=0}^{2^{n-3}-1} (|2^{3}j\rangle + |2^{3}j + 2\rangle).
\]

By Theorem 2 in [13] and the method in [16] we derive the following exact achievable cloning efficiencies (defined as the probability of cloning successfully) for each of states (4)–(6):

\[
\gamma_1 \equiv \gamma(|h_{(01000000)^{2n-3}}\rangle) = \frac{7}{127},
\]

\[
\gamma_2 \equiv \gamma(|h_{(01010101)^{2n-3}}\rangle) = \gamma_3 \equiv \gamma(|h_{(11000011)^{2n-3}}\rangle) = \frac{112}{127}.
\]

After the cloning process the measurement outcome on a “flag” subsystem will tell us whether the cloning was successful or not. For this particular cloning process, the probability of success is, on average, $P_{\text{success}} = (\gamma_1 + \gamma_2 + \gamma_3)/3 = \frac{77}{127}$. If it was successful, then each of the cloning branches goes through the second part of the circuit in Fig.2, to yield one of the $2^n$ orthogonal states:

\[
|h_{a_0a_1a_2\ldots a_{2n-1}}\rangle = 2^{-\frac{n}{2}} \sum_{x=0}^{2^n-1} (-1)^{a_x} |x\rangle,
\]

which can be discriminated unambiguously. Here $h_{a_0a_1a_2\ldots a_{2n-1}} \in S^n_2$. Therefore, if the cloning process is successful, we manage to accomplish our task.

However, the cloning process may fail with probability $(1 - P_{\text{success}})$. If this occurs, it is much more likely to be $h_{(01000000)^{2n-3}}$ than the other two, because of the relatively low cloning efficiency for the state in Eq. (4), in relation to the states in Eqs. (5) and (6) [see Eqs. (7) and (8)]. Guessing that $f_0 = h_{(01000000)^{2n-3}}$, we are right with probability

\[
P_{(01000000)^{2n-3}} = \frac{(1 - \gamma_1)}{(1 - \gamma_1) + (1 - \gamma_2) + (1 - \gamma_3)} = \frac{4}{5}.
\]

Note that only the $2^n$ functions in $S^n_2$ can be candidates for $f_1$ and $f_2$ on condition that $f_0 = h_{(01000000)^{2n-3}}$. These $2^n$ possibilities can be discriminated unambiguously by running a circuit like that of Fig.1 twice, once with $f_1$ and once with $f_2$, since the circuits produce one of $2^n$ orthogonal states, each corresponding to one of the $2^n$ possibilities for $f_i$. Therefore if our guess that $f_0 = h_{(01000000)^{2n-3}}$ was correct, we are able to find the correct $f_1$ and $f_2$ and therefore accomplish our task. In the case that $f_0 \neq h_{(01000000)^{2n-3}}$ after all, we may still have guessed the right sets with probability $1/2^{2n}$.

The above considerations lead to an overall probability of success given by

\[
P_2 = p_{\text{success}} + (1 - p_{\text{success}})[P_{(01000000)^{2n-3}} + (1 - p_{(01000000)^{2n-3}}) \frac{1}{2^{2n}}]
\]

\[
= \frac{117}{127} + \frac{5}{127 \times 2^{2n-1}}
\]

\[
> \frac{117}{127} > \frac{417}{512}.
\]

It shows that this cloning approach is more efficient than the previous one, which does not use cloning.

If we take

\[
S^2_{f_0} = \{h_{0100}, h_{0011}, h_{1001}\},
\]

\[
S^2_1 = \{h_{0001}, h_{0010}, h_{0100}, h_{1000}\}, S^2_2 = \{h_{0000}, h_{0011}, h_{0101}, h_{1001}\},
\]
that the best no-cloning average score is still

\[ S_{f_{12}}^2 = S_1^2 \cup S_2^2, \]

\[ H^2_{0000} = \{ h_{0000}, h_{1111} \}, H^2_{0101} = \{ h_{0101}, h_{1001} \}, H^2_{0011} = \{ h_{0011}, h_{1100} \}, H^2_{1001} = \{ h_{1001}, h_{1010} \}. \]

\[ S_f^2 = H^2_{0000} \cup H^2_{0101} \cup H^2_{0011} \cup H^2_{1001}; \]

\[ S_{n+1}^{f_0} = \{ h_{a_0a_1a_2\cdots a_{2^n-1}a_0a_1a_2\cdots a_{2^n-1}} \mid h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n \}, \]

\[ S_{n+1}^1 = \{ h_{a_0a_1a_2\cdots a_{2^n-1}a_0a_1a_2\cdots a_{2^n-1}} \mid h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n \}, \]

\[ S_{n+1}^2 = \{ h_{a_0a_1a_2\cdots a_{2^n-1}a_0a_1a_2\cdots a_{2^n-1}} \mid h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n \}, \]

\[ S_{n+1} = S_{n+1}^1 \cup S_{n+1}^2, \]

\[ H_{0011}^{n+1} = \{ h_{a_0a_1a_2\cdots a_{2^n-1}a_0a_1a_2\cdots a_{2^n-1}} \mid h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n \}, \]

\[ H_{0101}^{n+1} = \{ h_{a_0a_1a_2\cdots a_{2^n-1}a_0a_1a_2\cdots a_{2^n-1}} \mid h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n \}, \]

\[ S_f^{n+1} = \bigcup_{h_{a_0a_1a_2\cdots a_{2^n-1}} \in S_f^n} (H_{0011}^{n+1} \cup H_{0101}^{n+1}). \]

Here \( n = 2, 3, 4, \cdots, a_k = \begin{cases} 0, & \text{if } a_k = 1 \\ 1, & \text{if } a_k = 0 \end{cases} \)

\[ k = 0, 1, 2, \cdots, 2^n - 1. \]

Following the same procedure as before, we derive that the best no-cloning average score is still

\[ p_1 = \frac{2}{3} + \frac{1}{3} \times \frac{1}{2^{2n}} < 0.7, \quad (12) \]

but the analytic achievable cloning efficiencies are

\[ \gamma_1 \equiv \gamma(\langle h_{(0100)}^{2^{n-2}} \rangle) = \frac{1}{7}, \quad (13) \]

\[ \gamma_2 \equiv \gamma(\langle h_{(0011)}^{2^{n-2}} \rangle) = \gamma_3 \equiv \gamma(\langle h_{(1001)}^{2^{n-2}} \rangle) = \frac{4}{7}, \quad (14) \]

and the overall probability of success with cloning is

\[ p_2 = \frac{5}{7} + \frac{2}{7 \times 2^{2n-1}} > \frac{7}{7} \]

\[ > p_1. \quad (15) \]

Besides the larger probability of obtaining the correct result, the quantum cloning offers another advantage: the measurement of the 'flag' state makes us to be confident about having the correct result in a larger fraction of our attempts. For the above second probabilistic cloning machine described by \( \gamma_1 = \frac{1}{7}, \gamma_2 = \frac{4}{7} \) this fraction was \( \frac{5}{7} \), but this can be improved by choosing different cloning machine, e.g. the first one above characterized by \( \gamma_1 = \frac{7}{127} \), \( \gamma_2 = \gamma_3 = \frac{112}{127} \), the fraction of which is \( \frac{77}{127} \).

In summary, we study the possible use of quantum cloning machine and give examples of quantum computation tasks which attain optimal performance by using an intermediate quantum cloning step. We show that preserving and distributing quantum information through a cloning process offers advantages over extracting classical information mid-way in the quantum computation.
References

[1] Wootters W K and Zurek W H 1982 Nature (London) 299 802
[2] Dieks D 1982 Phys. Lett. A 92 271
[3] Bužek V and Hillery M 1996 Phys. Rev. A 54 1844
[4] Gisin N and Massar S 1997 Phys. Rev. Lett. 79 2153
[5] Gisin N 1998 Phys. Lett. A 242 1
[6] Werner R F 1998 Phys. Rev. A 58 1827
[7] Keyl M and Werner R F 1999 J. Math. Phys. 40 3283
[8] Bruß D and Macchiavello C 1999 Phys. Lett. A 253 249
[9] Bruß D, Ekert A and Macchiavello C 1998 Phys. Rev. Lett. 81 2598
[10] Bužek V, Hillery M and Bednik R 1998 Acta Phys. Slov. 48 177
[11] Nicolas J. Cerf 2000 J. Mod. Opt. 47 187
[12] Bužek V, Braunstein S, Hillery M and Bruß D 1997 Phys. Rev. A 56 3446
[13] Duan L M and Guo G C 1998 Phys. Rev. Lett. 80 4999
[14] Duan L M and Guo G C 1999 Commun. Theor. Phys. 31 223
[15] Galvão E F and Hardy L 2000 Phys. Rev. A 62 022301
[16] Gao T, Yan F L, and Wang Z X 2004 J. Phys. A: Math. Gen. 37 3211
[17] Gao T, Yan F and Wang Z, e-print archive quant-ph/0308036
[18] Bechmann-Pasquinucci H and Gisin N 1999 Phys. Rev. A 59 4238
FIG. 1: If function $f_i$ is guaranteed to be either in set $S^n_1$ or in $S^n_2$, then this quantum circuit can be used to distinguish between the $2^n$ possibilities in each set. We can determine $f_i$ by measuring the final state $|\varphi_i\rangle = 2^{-\frac{n}{2}} \sum_{x=0}^{2^n-1} (-1)^{f_i(x)} |x\rangle$ in one of two orthogonal bases, depending on which set contains $f_i$. Here $H$ operations are Hadamard gates.

FIG. 2: The cloning procedure in this circuit is probabilistic. After the cloning process we can measure a "flag" subsystem and know whether the cloning was successful or not. If the cloning is successful, we let the clones go through the rest of the circuit, yielding output states $|\varphi_i\rangle = 2^{-\frac{n}{2}} \sum_{x=0}^{2^n-1} (-1)^{f_0(x) \oplus f_i(x)} |x\rangle$ ($i = 1, 2$). These states can be measured in the basis defined by Eqs.(9) to unambiguously decide which of the $2^n$ sets $H^n$’s contains $f_0 \oplus f_i$. 

\[
\begin{align*}
|0\rangle & \quad \text{H} \\
|0\rangle & \quad \text{H} \\
|0\rangle & \quad \text{H} \\
\vdots & \quad \vdots \\
|0\rangle & \quad \text{H} \\
|1\rangle & \quad \text{H} \quad \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
\end{align*}
\]