General impossible operations in quantum information

Arun K. Pati*

Institute of Physics, Sainik School Post, Bhubaneswar 751005, Orissa, India

(Received 10 April 2002; published 30 December 2002)

We prove a general limitation in quantum information that unifies the impossibility principles such as no-cloning and no-anticloning. Further, we show that for an unknown qubit one cannot design a universal Hadamard gate for creating equal superposition of the original and its complement state. Surprisingly, we find that Hadamard transformations exist for an unknown qubit chosen either from the polar or equatorial great circles. Also, we show that for an unknown qubit one cannot design a universal unitary gate for creating unequal superpositions of the original and its complement state. We discuss why it is impossible to design a controlled-NOT gate for two unknown qubits and discuss the implications of these limitations.

DOI: 10.1103/PhysRevA.66.062319 PACS number(s): 03.67.Hk, 03.65.Ta

I. INTRODUCTION

In the microscopic world a qubit carries quantum as well as classical information. To specify the quantum information content of an unknown qubit we need doubly infinite bits [1] of information, whereas to extract classical information we need to do a measurement and that yields only a single bit of information. This makes a qubit so distinct from a classical bit. Unlike classical information there are several limitations on the basic operations that one can perform on quantum information. Using linearity of quantum evolution it can be shown that one cannot copy an unknown state perfectly [2,3]. Further, using unitarity alone it can be shown that nonorthogonal states cannot be copied exactly [4]. Similarly, it was shown that there is no linear, trace preserving operation that takes two copies of an unknown state and delete a copy by acting jointly on both the copies [5,6]. In addition, it was found that one cannot complement an arbitrary qubit, where complementing means flipping a qubit on Bloch sphere [7,8]. It was also shown that one cannot design a machine that will take an unknown qubit and a blank state, and produce the original along with a flipped state [9]. Recently, a stronger no-cloning theorem has been proved which says that the supplementary information needed to make a copy must be as large as possible [10]. At the heart of these fundamental limitations there lies the unknowability of a single quantum state.

On the other hand there are certain types of physical operations that one can perform, in principle, on quantum information. For example, as we all know, one can swap an unknown state with a known or an unknown state perfectly. One can teleport an unknown state with the help of dual classical and quantum channel [11]. One can create universal entangled states of an unknown qubit with two types of reference states [12] using shared entanglement and classical communication. One can also erase [13,14] the content information of an unknown state by swapping it with a standard state and then performing an irreversible operation [5]. Therefore, it is of utmost importance to know what are the impossible and possible operations on quantum information that are allowed by laws of quantum physics. Because these would give rise to serious implications for quantum computing and information processing devices in the future.

The purpose of this paper is multifold. First, we show that there is no allowed transformation that will take an unknown and a blank state at the input port and produce the original along with a function of the original state at the output port. This limitation generalizes and unifies the no-cloning and no-anticloning principle for arbitrary qubits. Second, we show that one cannot design a Hadamard gate that will create a linear superposition of an unknown state along with its complement state with equal amplitudes. Surprisingly, we show that there exist two distinct Hadamard transformations for unknown qubits chosen from the polar and equatorial great circles. We also show that it is not possible to design a unitary transformations that will create an unequal superposition of the original qubit with its complement. Third, we show that one cannot design a controlled-NOT (c-NOT) gate for two unknown qubits and discuss implications of these limitations. Moreover, unlike the qubits in preferred computational basis states, if the qubits are in some arbitrary states then the quantum computational logic gates cannot be designed perfectly.

The organization of our paper is as follows. In Sec. II, we present our generalized limitation. In Sec. III, we discuss nonexistence of universal Hadamard gate and unitary gates. In Sec. IV, we discuss why it is impossible to design a c-NOT gate for two unknown qubits. In Sec. V, we briefly discuss the implications of these limitations for future quantum mechanical computers and the conclusions follows.

II. GENERAL LIMITATION ON QUANTUM INFORMATION

In the sequel we prove a general impossibility theorem for quantum information. Suppose we are given a qubit in an unknown state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}^2$, with α, β being *unknown* complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. This state is isomorphic to any two-state system parametrized by two real parameters as $|\Psi(\theta,\phi)\rangle = \cos\theta/2|0\rangle + \sin\theta/2 e^{i\phi}|1\rangle$ with $0 \leqslant \theta \leqslant \pi$ and $0 \leqslant \phi \leqslant 2\pi$.

Theorem I. Given an arbitrary state $|\Psi\rangle \in \mathcal{H}^2$ of an un-

*Also at School of Informatics, University of Wales, Bangor LL 57 1UT, United Kingdom. Email address: akpati@iopb.res.in known qubit and a blank state $|\Sigma\rangle \in \mathcal{H}^2$, there does not exist a isometric map $\mathcal{M}: \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2 \rightarrow \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2$ that will transform

$$|\Psi\rangle \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow |\Psi\rangle \otimes |\mathcal{F}(\Psi)\rangle \otimes |Q_\Psi\rangle, \tag{1}$$

where $|Q$ and $|Q_\Psi\rangle$ are the initial and final states of the ancilla (it could be the corresponding states of the proposed machine itself). Here $|\mathcal{F}(\Psi)\rangle$ is the function of the original, namely, a state that is a function of α, β or their complex conjugates. It may be related to the original state either by a unitary or antiunitary transformation, i.e., $|\mathcal{F}(\Psi)\rangle = K|\Psi\rangle$, where K can be a unitary operator U or antiunitary operator A. More generally, $|\mathcal{F}(\Psi)\rangle$ may be related to $|\Psi\rangle$ by a sum of unitary and antiunitary operators, i.e., $|\mathcal{F}(\Psi)\rangle = (\sqrt{\lambda}U + \sqrt{(1-\lambda)}A|\Psi$, with $0 \leqslant \lambda \leqslant 1$ and λ is real. Here only those unitaries and antiunitaries may be considered that gives isometric (only norm preserving) transformations in $\mathcal{H}^2$. *Proof*. Since a qubit in the canonical orthogonal states carry classical information and can be measured without any disturbance it can be manipulated at will. Let there be a machine that transforms a qubit in the orthogonal states $|0\rangle \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow |0\rangle \otimes |\mathcal{F}(0)\rangle \otimes |Q_0\rangle$ and $|1\rangle \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow |1\rangle \otimes |\mathcal{F}(1)\rangle \otimes |Q_1\rangle$. First, we consider the case when K is either unitary or antiunitary. If we send an unknown qubit through this machine, then by linearity we have

$$\begin{aligned}|\Psi\rangle \otimes |\Sigma\rangle \otimes |Q\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow \alpha|0\rangle \otimes |\mathcal{F}(0)\rangle \\ \otimes |Q_0\rangle + \beta|1\rangle \otimes |\mathcal{F}(1)\rangle \otimes |Q_1\rangle,\end{aligned} \tag{2}$$

and by antilinearity of map we have

$$\begin{aligned}|\Psi\rangle \otimes |\Sigma\rangle \otimes |Q\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow \alpha^*|0\rangle \\ \otimes |\mathcal{F}(0)\rangle \otimes |Q_0\rangle + \beta^*|1\rangle \otimes |\mathcal{F}(1)\rangle \otimes |Q_1\rangle.\end{aligned} \tag{3}$$

Note the complex conjugation on α and β due to the antilinear nature of the map. Ideally, we should have obtained in the output port a state of the type

$$\begin{aligned}|\Psi\rangle \otimes |\mathcal{F}(\Psi)\rangle \otimes |Q_\Psi\rangle = [\alpha^2|0\rangle \otimes |\mathcal{F}(0)\rangle + \beta^2|1\rangle \otimes |\mathcal{F}(1)\rangle \\ + \alpha\beta(|0\rangle \otimes |\mathcal{F}(1)\rangle + |1\rangle \otimes |\mathcal{F}(0)\rangle)] \\ \otimes |Q_\Psi\rangle\end{aligned} \tag{4}$$

when K is a unitary operator or a state of the type

$$\begin{aligned}|\Psi\rangle \otimes |\mathcal{F}(\Psi)\rangle \otimes |Q_\Psi\rangle = [|\alpha|^2|0\rangle \otimes |\mathcal{F}(0)\rangle + |\beta|^2|1\rangle \otimes |\mathcal{F}(1)\rangle \\ + \alpha\beta^*|0\rangle \otimes |\mathcal{F}(1)\rangle + \alpha^*\beta|1\rangle \\ \otimes |\mathcal{F}(0)\rangle] \otimes |Q_\Psi\rangle\end{aligned} \tag{5}$$

when K is an antiunitary operator. Since the states in Eqs. (2) and (4) and in Eqs. (3) and (5) can never be equal for arbitrary values of α and β, there is no allowed machine to satisfy Eq. (1).

Next we consider the case when $|\mathcal{F}(\Psi)\rangle$ is related to $|\Psi\rangle$ by a sum of unitary and antiunitary operators. In actuality, when we send an unknown and blank states through a machine we will have an output state given by

$$\begin{aligned}|\Psi\rangle \otimes |\Sigma\rangle \otimes |Q\rangle \rightarrow \sqrt{\lambda}\alpha|0\rangle \otimes U|0\rangle \otimes |Q_0\rangle + \sqrt{(1-\lambda)}\alpha^*|0\rangle \\ \otimes A|0\rangle \otimes |Q_0\rangle + \sqrt{\lambda}\beta|1\rangle \otimes U|1\rangle \otimes |Q_1\rangle \\ + \sqrt{(1-\lambda)}\beta^*|1\rangle \otimes A|1\rangle \otimes |Q_1\rangle.\end{aligned} \tag{6}$$

However, ideally we should have obtained an output state given by

$$\begin{aligned}|\Psi\rangle \otimes |\mathcal{F}(\Psi)\rangle \otimes |Q_\Psi\rangle = [\sqrt{\lambda}\alpha^2|0\rangle \otimes U|0\rangle + \sqrt{(1-\lambda)}|\alpha|^2|0\rangle \\ \otimes A|0\rangle + \sqrt{\lambda}\beta^2|1\rangle \otimes U|1\rangle \\ + \sqrt{(1-\lambda)}|\beta|^2|1\rangle \otimes A|1\rangle \\ + \sqrt{\lambda}\alpha\beta|0\rangle \otimes U|1\rangle \\ + \sqrt{(1-\lambda)}\alpha\beta^*|0\rangle \otimes A|1\rangle \\ + \sqrt{\lambda}\alpha\beta|1\rangle \otimes U|0\rangle \\ + \sqrt{(1-\lambda)}\alpha^*\beta|1\rangle \otimes A|0\rangle] \otimes |Q_\Psi\rangle.\end{aligned} \tag{7}$$

Since Eqs. (6) and (7) can never be the same for arbitrary values of α and β, we conclude that the generalized machine does not exist for an unknown qubit. Hence the proof.

The nonexistence of a machine defined in Eq. (1) is a class of general form of limitations that one can impose on quantum information. Some known impossible machines can be thought of as special cases of the above impossible machine. For example, if $|\mathcal{F}(\Psi)\rangle = |\Psi\rangle$, then it is the no-cloning principle, as the unitary operator $K = I$, with I being the identity operation. If $|\mathcal{F}(\Psi)\rangle = |\Psi^*\rangle = \alpha^*|0\rangle + \beta^*|1\rangle = \mathcal{C}|\Psi\rangle$, with $\mathcal{C}$ being conjugation operation, then this limitation suggests that starting with an unknown qubit it is impossible to produce the original and a conjugate qubit. Here, K will be the conjugating operation which is an antiunitary operator. If $|\mathcal{F}(\Psi)\rangle = |\Psi\rangle$, where $|\Psi\rangle = \alpha^*|1\rangle - \beta^*|0\rangle$ then K is flipping operation and is conjugating up to a unitary operator. In this case our limitation becomes impossible of producing a complement copy along with the original starting from a single copy. This can be regarded as a new limitation on quantum information. Note that it is not the same as the no-complementing principle which states that the operation $|\Psi\rangle \rightarrow |\Psi\rangle$ is an impossible operation [7,8]. In the present case, it aims to preserve the original and produce a complement copy and that is an impossible one. Since any antiunitary transformation is conjugating times unitary transformation, one can relate the complement and conjugate states for a qubit as $|\Psi\rangle = (-i\sigma_y)\mathcal{C}|\Psi\rangle$. Thus, we are able to find different limitations as well as unify three principles under a general impossible machine.

When K is a sum of unitary and antiunitary transformation then we have a different type of impossible machine and it becomes very interesting indeed. For example, if $U = I$ and A is complementing operation, then the transformation (1) will suggest

$$|\Psi\rangle\otimes|\Sigma\rangle\otimes|Q\rangle\to[\sqrt{\lambda}|\Psi\rangle\otimes|\Psi\rangle + \sqrt{(1-\lambda)}|\Psi\rangle\otimes|\overline{\Psi}\rangle]\otimes|Q_{\Psi}\rangle, \quad (8)$$

which can be called an impossible "*cloning-cum-complementing*" quantum machine. Because when $\lambda=1$ it will be purely a quantum cloning and when $\lambda=0$ it will be purely quantum complementing machine. For any intermediate value of λ the machine will be a hybrid one. Since we cannot have an exact hybrid machine, it would be very interesting to see how the optimal values of the fidelity for such an approximate machine behave as a function of the known parameter λ. Here fidelity may be defined in the usual sense as the overlap of the ideal output with the actual output state (in general a mixed state) ρ_{actual}, i.e., $F=\langle\mathcal{F}(\Psi)|\rho_{\text{actual}}|\mathcal{F}(\Psi)\rangle$. However, our purpose is not to study approximate machines, but to *discover* physical operations that cannot be done exactly. We can suggest that if in the future one discovers some other limitations, then those may be encompassed by our principle. One may notice that the quantum copy-deleting machine proposed in Ref. [5] does not belong to the above class of machines because the deletion operation maps $|\Psi\rangle\otimes|\Psi\rangle\otimes|Q\rangle\to|\Psi\rangle\otimes|\Sigma\rangle\otimes|Q_{\Psi}\rangle$.

III. NONEXISTENCE OF UNIVERSAL HADAMARD AND UNITARY GATES

In this section we discuss two other limitations that do not belong to the above class. We prove that it is impossible to design some important one-qubit gates for a qubit in some unknown state. First, we show why it is impossible to have a Hadamard gate in a universal way. Second, we show that one cannot design a unitary gate that will create unequal superposition of unknown state with its complement.

It is beyond doubt that in quantum computation and information theory two ubiquitous gates are Hadamard and CNOT. These gates are very useful in various quantum algorithms (like Deutsch-Jozsa, Shor, and Grover, etc.) and information processing protocols [15]. We will prove that one *cannot design these useful logic gates for arbitrary, unknown qubits*. We know that if we are given a qubit in either the $|0\rangle$ or $|1\rangle$ state, then the Hadamard transformation (one-qubit gate) rotates a qubit in the state $|0\rangle\to(1/\sqrt{2})(|0\rangle+|1\rangle)$ and $|1\rangle\to(1/\sqrt{2})(|0\rangle-|1\rangle)$, i.e., it creates superposition of the original and its complement state with equal amplitudes. The question is, if we are given an unknown qubit pointed in some arbitrary direction **n** in a state $|\Psi\rangle$ or in the direction $-$**n** in a state $|\overline{\Psi}\rangle$, can we design a logic gate that will transform these inputs as follows:

$$|\Psi\rangle\to\frac{1}{\sqrt{2}}(|\Psi\rangle+|\overline{\Psi}\rangle)$$

$$|\overline{\Psi}\rangle\to\frac{1}{\sqrt{2}}(|\Psi\rangle-|\overline{\Psi}\rangle), \quad (9)$$

where one can imagine that one half of the Bloch sphere has been chosen to play the role of $|\Psi\rangle$ and the other half to play the role of $|\overline{\Psi}\rangle$. Alternately, a naturally universal way of defining a Hadamard gate would be

$$|\Psi\rangle\to\frac{1}{\sqrt{2}}(|\Psi\rangle+i|\overline{\Psi}\rangle)$$

$$|\overline{\Psi}\rangle\to\frac{1}{\sqrt{2}}(i|\Psi\rangle+|\overline{\Psi}\rangle). \quad (10)$$

The later definition has an advantage that the transformation is invariant if we interchange $|\Psi\rangle$ and $|\overline{\Psi}\rangle$. But as we will see subsequently, both the definitions have their own advantages when applied to special classes of unknown qubits.

Theorem II. There is no Hadamard gate defined by Eqs. (9) or (10) for an unknown qubit that will create an equal superposition of the original state $|\Psi\rangle$ and its complement state $|\overline{\Psi}\rangle$.

We can prove this using either the linearity of quantum evolution or the unitarity. The proof below is based on the unitarity.

Proof. Suppose that there exists a universal Hadamard gate for all possible inputs chosen from Bloch sphere. If it is so, then for any two distinct qubits $\{|\Psi_1\rangle,|\Psi_2\rangle\}$ and their complement states $\{|\overline{\Psi}_1\rangle,|\overline{\Psi}_2\rangle\}$, by Eq. (9) we must have

$$|\Psi_1\rangle\to\frac{1}{\sqrt{2}}(|\Psi_1\rangle+|\overline{\Psi}_1\rangle)$$

$$|\overline{\Psi}_1\rangle\to\frac{1}{\sqrt{2}}(|\Psi_1\rangle-|\overline{\Psi}_1\rangle). \quad (11)$$

And similarly, we must have

$$|\Psi_2\rangle\to\frac{1}{\sqrt{2}}(|\Psi_2\rangle+|\overline{\Psi}_2\rangle)$$

$$|\overline{\Psi}_2\rangle\to\frac{1}{\sqrt{2}}(|\Psi_2\rangle-|\overline{\Psi}_2\rangle). \quad (12)$$

Now taking the inner product, we have

$$\langle\Psi_1|\Psi_2\rangle\to\frac{1}{2}(\langle\Psi_1|\Psi_2\rangle+\langle\Psi_1|\overline{\Psi}_2\rangle+\langle\overline{\Psi}_1|\Psi_2\rangle+\langle\overline{\Psi}_1|\overline{\Psi}_2\rangle)$$

$$\langle\overline{\Psi}_1|\overline{\Psi}_2\rangle\to\frac{1}{2}(\langle\Psi_1|\Psi_2\rangle-\langle\Psi_1|\overline{\Psi}_2\rangle-\langle\overline{\Psi}_1|\Psi_2\rangle+\langle\overline{\Psi}_1|\overline{\Psi}_2\rangle). \quad (13)$$

Similarly, if we consider the Hadamard transformation defined by Eq. (10) then for two arbitrary qubits we have the inner product condition

$$\langle\Psi_1|\Psi_2\rangle\to\frac{1}{2}(\langle\Psi_1|\Psi_2\rangle+i\langle\Psi_1|\bar{\Psi}_2\rangle-i\langle\bar{\Psi}_1|\Psi_2\rangle$$
$$+\langle\bar{\Psi}_1|\bar{\Psi}_2\rangle)$$
$$\langle\bar{\Psi}_1|\bar{\Psi}_2\rangle\to\frac{1}{2}(\langle\Psi_1|\Psi_2\rangle-i\langle\Psi_1|\bar{\Psi}_2\rangle+i\langle\bar{\Psi}_1|\Psi_2\rangle$$
$$+\langle\bar{\Psi}_1|\bar{\Psi}_2\rangle). \qquad (14)$$

Taking $|\Psi_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$ and $|\bar{\Psi}_i\rangle=\alpha_i^*|1\rangle-\beta_i^*|0\rangle$ with $i=1,2,$ we can check that for two arbitrary qubits $\langle\Psi_i|\bar{\Psi}_j\rangle=-\langle\bar{\Psi}_i|\Psi_j\rangle^*$ and $\langle\Psi_i|\Psi_j\rangle=\langle\bar{\Psi}_i|\bar{\Psi}_j\rangle^*$ is always satisfied. With these conditions, it is clear that the inner product is not preserved. Hence a universal Hadamard gate defined by Eqs. (9) or (10) cannot exist for arbitrary qubits. In quantum interferometric language *one cannot design a 50/50 beam splitter for an unknown photon* that creates a equal superposition of photon polarization with its orthogonal counterpart. This is a very important limitation as it suggests that linearity does not allow us to linearly superpose an unknown state with its complement.

One may wonder is there any special class of qubits for which a universal Hadamard gate exists? It may be remarked that even though it is not possible to flip an arbitrary qubit, a qubit chosen from equatorial or polar great circle on a Bloch sphere can be flipped exactly [16]. This is also the largest set of states on a Bloch sphere that can be complemented perfectly [17]. Surprisingly, and somewhat curiously, here we will show that if we restrict our qubits from polar great circle then there *exists* Hadamard transformation (9) for *unknown* values of θ, but not for qubits from equatorial great circle. If we restrict our qubits from equatorial great circle then there *exists* Hadamard transformation (10) for *unknown* ϕ, but not for qubits from polar great circle.

With the computational basis of a qubit, if $|0\rangle$ represents a point on the north pole and $|1\rangle$ represents a point on the south pole $|1\rangle$, then the union of the sets $\mathcal{S}_P^+ U\mathcal{S}_P^-$ represents polar great circle, where $\mathcal{S}_P^+:=\{|\Psi(\theta)\rangle||\Psi(\theta)\rangle=\cos\theta/2|0\rangle+\sin\theta/2|1\rangle, 0\le\theta\le\pi\}$ and $\mathcal{S}_P^-:=\{|\bar{\Psi}(\theta)\rangle||\bar{\Psi}(\theta)\rangle=\cos\theta/2|1\rangle-\sin\theta 2|0\rangle, 0\le\theta\le\pi\}$. Similarly, the union of the sets $\mathcal{S}_E^+ U\mathcal{S}_E^-$ represents equatorial great circle, where $\mathcal{S}_E^+:=\{|\Psi(\phi)\rangle||\Psi(\phi)\rangle=1/\sqrt{2}(|0\rangle+e^{i\phi}|1\rangle), 0\le\phi\le 2\pi\}$ and $\mathcal{S}_E^-:=\{|\Psi(\phi)\rangle||\Psi(\phi)\rangle=1/\sqrt{2}(|1\rangle-e^{-i\phi}|0\rangle), 0\le\phi\le 2\pi\}$. These classes of qubits belong to one-dimensional subspace of S^2 and play a very special role because they are those which can also be remotely prepared using one unit of quantum entanglement and one bit of classical communication [16]. This gives a hint that, maybe for these classes of qubits, one can design Hadamard gates.

First, consider the Hadamard transformation defined in Eq. (9). The reason why a Hadamard gate (9) exists for the polar great circle is that it preserves the inner product condition (13). One can check that for this set if we denote $|\Psi_1\rangle=|\Psi(\theta_1)\rangle$ and $|\Psi_2\rangle=|\Psi(\theta_2)\rangle$ and so on, then one has

$$\langle\Psi(\theta_1)|\bar{\Psi}(\theta_2)\rangle=-\langle\bar{\Psi}(\theta_1)|\Psi(\theta_2)\rangle,$$

$$\langle\Psi(\theta_1)|\Psi(\theta_2)\rangle=\langle\bar{\Psi}(\theta_1)|\bar{\Psi}(\theta_2)\rangle, \qquad (15)$$

for arbitrary nonzero values of θ. This crucial condition ensures that the unitarity (13) is *not violated* for polar qubits. However, if we take qubits from equatorial great circle, then any qubit and its complement can be written as $|\Psi(\phi)\rangle=H(\cos\phi/2|0\rangle-i\sin\phi/2|1\rangle)$ and $|\bar{\Psi}(\phi)\rangle=H(i\sin\phi/2|0\rangle-\cos\phi/2|1\rangle)$ up to an overall phase, where H is the ordinary Hadamard gate. One can check that the following conditions hold for equatorial qubits:

$$\langle\Psi(\phi_1)|\bar{\Psi}(\phi_2)\rangle=\langle\bar{\Psi}(\phi_1)|\Psi(\phi_2)\rangle,$$
$$\langle\Psi(\phi_1)|\Psi(\phi_2)\rangle=\langle\bar{\Psi}(\phi_1)|\bar{\Psi}(\phi_2)\rangle. \qquad (16)$$

With this condition the inner product condition (13) is not preserved and hence there cannot be a Hadamard gate (9) for equatorial great circles.

Second, consider the Hadamard transformation defined by Eq. (10). One can check that if we choose qubits from polar great circle then using conditions (15), the unitarity condition (14) *is violated*. But for qubits chosen from equatorial great circle, using condition (16), unitarity requirement (14) is satisfied. Hence one can design a Hadamard gate defined by Eq. (10) for equatorial qubits but not for polar qubits. So what we have found is that for an arbitrary qubit the Hadamard transformations defined by Eqs. (9) or (10) do not exist. But for a polar qubit the correct Hadamard transform is Eq. (9) and for an equatorial qubit the correct Hadamard transform is Eq. (10).

Below we illustrate how definition (9) is at work for polar qubits. First, notice that we would like to have a unitary transformation that will satisfy Eq. (9). If we send an unknown ''real'' qubit through the ordinary Hadamard gate, we will have

$$|\Psi(\theta)\rangle\to\frac{1}{\sqrt{2}}\left[\left(\cos\frac{\theta}{2}+\sin\frac{\theta}{2}\right)|0\rangle+\left(\cos\frac{\theta}{2}-\sin\frac{\theta}{2}\right)|1\rangle\right]$$
$$|\bar{\Psi}(\theta)\rangle\to\frac{1}{\sqrt{2}}\left[\left(\cos\frac{\theta}{2}-\sin\frac{\theta}{2}\right)|0\rangle-\left(\cos\frac{\theta}{2}+\sin\frac{\theta}{2}\right)|1\rangle\right]. \qquad (17)$$

Ideally, we should have obtained

$$|\Psi(\theta)\rangle\to\frac{1}{\sqrt{2}}\left[\left(\cos\frac{\theta}{2}-\sin\frac{\theta}{2}\right)|0\rangle+\left(\cos\frac{\theta}{2}+\sin\frac{\theta}{2}\right)|1\rangle\right]$$
$$|\bar{\Psi}(\theta)\rangle\to\frac{1}{\sqrt{2}}\left[\left(\cos\frac{\theta}{2}+\sin\frac{\theta}{2}\right)|0\rangle+\left(\sin\frac{\theta}{2}-\cos\frac{\theta}{2}\right)|1\rangle\right]. \qquad (18)$$

The actual and the ideal states are different. Hence the ordinary Hadamard gate cannot be used to create Eq. (18). But the desired unitary transformation is not difficult to find and is given by the original Hadamard matrix times the Pauli spin matrix σ_x, i.e., the Hadamard transformation for polar qubits is given by $H_P=\sigma_x H=1/\sqrt{2}\left(\begin{smallmatrix}1 & -1\\ 1 & 1\end{smallmatrix}\right)$. This will create an equal superposition of any arbitrary real qubit and its complement, i.e., the action of H_P on $|\Psi(\theta)\rangle$ will give $1/\sqrt{2}(|\Psi(\theta)\rangle+|\overline{\Psi}(\theta)\rangle)$ and on $|\overline{\Psi}(\theta)\rangle$ will give $1/\sqrt{2}\,(|\Psi(\theta)\rangle-|\overline{\Psi}(\theta)\rangle)$, up to an overall minus sign in the later case.

Similarly, one can find a unitary Hadamard gate for an equatorial qubit that satisfies Eq. (10). If we send $|\Psi(\phi)\rangle=H(\cos\phi/2|0\rangle-i\sin\phi/2|1\rangle)$ through Eq. (10) we have

$$|\Psi(\phi)\rangle\rightarrow\frac{1}{2}[(1+i)e^{i\phi/2}|0\rangle+(1-i)e^{-i\phi/2}|1\rangle] \quad (19)$$

and if we send $|\overline{\Psi}(\phi)\rangle=H(i\sin\phi/2|0\rangle-\cos\phi/2|1\rangle)$ through Eq. (10) we have

$$|\overline{\Psi}(\phi)\rangle\rightarrow\frac{1}{2}[(1+i)e^{i\phi/2}|0\rangle-(1-i)e^{-i\phi/2}|1\rangle]. \quad (20)$$

The desired Hadamard gate that will do the above job is given by $H_E=1/\sqrt{2}\left(\begin{smallmatrix}1+i & 0\\ 0 & 1-i\end{smallmatrix}\right)$. This will create an equal superposition of any arbitrary equatorial qubit and its complement, i.e., the action of H_E on $|\Psi(\phi)\rangle$ will give $1/\sqrt{2}(|\Psi(\phi)\rangle+i|\overline{\Psi}(\phi)\rangle)$ and on $|\overline{\Psi}(\phi)\rangle$ will give $1/\sqrt{2}(i|\Psi(\phi)\rangle+|\overline{\Psi}(\phi)\rangle)$.

One can also ask if it is possible to create unequal superposition of an unknown qubit with its complement state? If such a device exist then we would have

$$|\Psi\rangle\rightarrow a|\Psi\rangle+b|\overline{\Psi}\rangle)$$

$$|\overline{\Psi}\rangle\rightarrow b^*|\Psi\rangle-a^*|\overline{\Psi}\rangle), \quad (21)$$

where a,b are *known* complex numbers and $|a|^2+|b|^2=1$. Using unitarity one can show that the above gate cannot exists. However, if a qubit is chosen from the polar circle on the Bloch sphere and if a,b are real, then it is possible to create unequal superposition of a state with its complement. We know that if a qubit is in $|0\rangle$ or $|1\rangle$ then one creates $|0\rangle\rightarrow a|0\rangle+b|1\rangle$ and $|1\rangle\rightarrow b|0\rangle-a|1\rangle$ by applying a known unitary transformation $U=\left(\begin{smallmatrix}a & b\\ b & -a\end{smallmatrix}\right)$. One can check that if we apply $U_G=\left(\begin{smallmatrix}b & -b\\ a & a\end{smallmatrix}\right)$ to $|\Psi(\theta)\rangle$, it will give $a|\Psi(\theta)\rangle+b|\overline{\Psi}(\theta)\rangle$ and to $|\overline{\Psi}(\theta)\rangle$ will give $b|\Psi(\theta)\rangle-a|\overline{\Psi}(\theta)\rangle$ up to an over all minus sign in the latter case. The amplitudes a,b in unequal superposition have to be real, otherwise the gate will not be "universal" for real qubits. That is, when applied to two distinct arbitrary qubits, it will not preserve the inner product. To see this, let $\{|\Psi(\theta_1)\rangle,|\Psi(\theta_2)\rangle\}$ be two nonorthogonal states and $\{|\overline{\Psi}(\theta_1)\rangle,|\overline{\Psi}(\theta_2)\rangle\}$ be their complement states. If the gate has to be universal, it should work for all inputs. Suppose a,b are complex, then $|\Psi_1(\theta)\rangle\rightarrow a|\Psi_1(\theta)\rangle+b|\overline{\Psi}_1(\theta)\rangle)$ and $|\Psi_2(\theta)\rangle\rightarrow a|\Psi_2(\theta)\rangle+b|\Psi_2(\theta)\rangle)$. Taking the inner product, we have

$$\langle\Psi_1(\theta)|\Psi_2(\theta)\rangle\rightarrow\langle\Psi_1(\theta)|\Psi_2(\theta)\rangle+(a^*b-ab^*)$$
$$\times\langle\Psi_1(\theta)|\overline{\Psi}_2(\theta)\rangle, \quad (22)$$

where we have used the condition (15). Similarly, by taking the inner product of $\langle\overline{\Psi}_1(\theta)|\overline{\Psi}_2(\theta)\rangle$ we can check that it will not preserve the inner product unless a,b are real. This shows that for unequal superpositions of polar qubit with its complement state to hold the amplitudes in the superposition should be real. In an analogous manner one can find transformations for equatorial qubits also.

Thus, single-qubit gates such as Hadamard and unitary gates cannot be designed in a universal manner. The surprising thing is that linearity does not allow linear superposition of an unknown qubit with its complement!

IV. NONEXISTENCE OF c-NOT GATE FOR UNKNOWN QUBITS

Next, we briefly come to another important gate, namely, the c-NOT gate which is one of the gates needed for universal quantum computation. In this section we discuss why it is impossible to design a c-NOT gate for two qubits that have been prepared in some unknown state. This is a two-qubit gate and takes $|0\rangle|0\rangle\rightarrow|0\rangle|0\rangle, |0\rangle|1\rangle\rightarrow|0\rangle|1\rangle, |1\rangle|0\rangle\rightarrow|1\rangle|1\rangle$ and $|1\rangle|1\rangle\rightarrow|1\rangle|0\rangle$. It flips the second bit if and only if the first qubit is in the state $|1\rangle$, otherwise it does nothing.

One can ask: Does there exist a c-NOT gate for arbitrary two-qubits that will take

$$|\Psi\rangle|\Psi\rangle\rightarrow|\Psi\rangle|\Psi\rangle, \quad |\Psi\rangle|\overline{\Psi}\rangle\rightarrow|\Psi\rangle|\overline{\Psi}\rangle,$$

$$|\overline{\Psi}\rangle|\Psi\rangle\rightarrow|\overline{\Psi}\rangle|\overline{\Psi}\rangle, \quad |\overline{\Psi}\rangle|\overline{\Psi}\rangle\rightarrow|\overline{\Psi}\rangle|\Psi\rangle. \quad (23)$$

Again using linearity it can be easily shown that this gate does not exists. Physically, this impossibility can be traced to the fact that CNOT gate measures the first qubit and flips the second one iff the first qubit is in the state $|\overline{\Psi}\rangle$. As we know, measuring an unknown qubit without disturbing it, is impossible [18]. Hence one cannot design an universal CNOT gate for all qubits. Alternately, the c-NOT operator for two qubits in orthogonal states is given by

$$U_{CNOT}^{(0,1)}=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes\sigma_x \quad (24)$$

cannot be used for arbitrary qubits. Because the desired c-NOT operator for two unknown qubits would be given by

$$U_{CNOT}^{\Psi,\overline{\Psi}}=|\Psi\rangle\langle\Psi|\otimes I+|\overline{\Psi}\rangle\langle\overline{\Psi}|\otimes\sigma_x(\alpha,\beta), \quad (25)$$

where $\sigma_x(\alpha,\beta)=(|\Psi\rangle\langle\overline{\Psi}|+|\overline{\Psi}\rangle\langle\Psi|)$ and this cannot be designed without prior knowledge of the amplitudes. (In fact, the other two Pauli matrices in unknown basis such as $\sigma_y(\alpha,\beta)=-i(|\Psi\rangle\langle\overline{\Psi}|-|\overline{\Psi}\rangle\langle\Psi|), \sigma_z(\alpha,\beta)=(|\Psi\rangle\langle\Psi|-|\overline{\Psi}\rangle\langle\overline{\Psi}|)$ are also impossible to measure.) Thus unknowability of a single quantum rules out the existence of c-NOT gate. Similarly, one can also rule out double-c-NOT and multiple-c-NOT gates for unknown qubits.

V. CONCLUSIONS

Before concluding we briefly mention the implications of the well-known limitations, and those discovered in this paper, on the future design of quantum computers.

We suggest that the general limitations, impossibility of designing Hadamard gate, unitary logic gate, and c-NOT gate for arbitrary qubits can have some serious implications. In a classical computer physical laws do not impose any limitations to performing various logical operations such as NOT, AND, XOR, FANOUT (cloning), and FAN-IN (deleting). Moreover, arbitrary classical operations can be generated through one bit gate such as a NOT and a two-bit gate such as an XOR. In quantum world, information is stored in superposed states and that makes it completely different from classical information. For example, perfect cloning and deleting are not allowed operations in a quantum computer. Nevertheless, it is well known that one-bit and two-bit unitary gates are universal for quantum computation. However, the limitations on the one-bit and two-bit gates suggest that perhaps we need to revise our understanding about universality of quantum computation. In the light of the present work it may be said that even though one-qubit gate (an example being a Hadamard) and two-qubit gate such as a CNOT are universal with respect to designing arbitrary unitary operators, they themselves are not universal with respect to states. In a classical computer these gates are universal with respect to operations as well as physical states on which information is stored. But in a quantum computer it is not so. In the future one would like to investigate further the implications of these fundamental limitations in quantum information.

In conclusion, we have argued that the impossibility of producing a copy and a complement copy are special cases of the general limitation. We proved that *universal* Hadamard and unitary logic operations cannot be performed exactly on arbitrary unknown qubits for creating equal and unequal superpositions. The linear superposition, which is at the heart of quantum mechanics, that itself cannot be created for a single quantum in an unknown basis. However, if a qubit is chosen from polar or equatorial great circle on a Bloch sphere then one can design these logic operations by suitably defining the transformations. We also discussed why we cannot design a c-NOT gate for unknown qubits. Future avenues of exploration lie in designing universal, approximate and optimal general transformations, Hadamard and c-NOT gates for arbitrary qubits in the spirit of universal estimation [19], cloning [20–22], and universal manipulation of qubits [8,23,24]. Also one can try to realize these impossible operations in a probabilistic but exact manner analogous to the probabilistic cloning [25], novel cloning [26], and probabilistic deleting operations [27–29]. In addition, one may try to extend these limitations and possible operations for higher-dimensional and continuous variable quantum systems.

ACKNOWLEDGMENTS

I wish to thank S. Bose, S. L. Braunstein, N. Gisin, and various others for very useful discussions on these ideas at several stages in the last two years. Nevertheless, I am responsible if there are any unavoidable errors in the presentation of these ideas.

[1] R. Jozsa, *Geometric Issues in Foundations of Science*, edited by S. Huggett (Oxford University Press, Oxford, 1997).

[2] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982).

[3] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[4] H.P. Yuen, Phys. Lett. A **113**, 405 (1986).

[5] A.K. Pati and S.L. Braunstein, Nature (London) **404**, 164 (2000).

[6] W.H. Zurek, Nature (London) **404**, 40 (2000).

[7] A. K. Pati, (unpublished).

[8] V. Buzek, M. Hillery, and R.F. Werner, Phys. Rev. A **60**, R2626 (1999).

[9] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).

[10] R. Jozsa, LANL Report, e-print quant-ph/0204153.

[11] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).

[12] A.K. Pati, Pramana, J. Phys. **59**, 217 (2002).

[13] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).

[14] C.H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[16] A.K. Pati, Phys. Rev. A **63**, 014302 (2001).

[17] S. Ghosh, A. Roy, and U. Sen, Phys. Rev. A **63**, 014301 (2001).

[18] C.A. Fuchs, LANL Report, e-print quant-ph/9611006.

[19] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[20] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[21] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[22] R.F. Werner, Phys. Rev. A **58**, 1827 (1998).

[23] L. Hardy and D.D. Song, Phys. Rev. A **63**, 032301 (2001).

[24] L. Hardy and D.D. Song, Phys. Rev. A **63**, 032304 (2001).

[25] L.M. Duan and G.C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).

[26] A.K. Pati, Phys. Rev. Lett. **83**, 2849 (1999).

[27] Y. Feng, S. Zhang, and M. Yim, Phys. Rev. A **65**, 042324 (2002).

[28] D. Qiu, Phys. Rev. A **65**, 052303 (2002).

[29] J. Feng, Y.F. Gao, J.S. Wang, and M.S. Zhan, Phys. Rev. A **65**, 052311 (2002).