On the non-existence of a universal Hadamard gate

Preeti Parashar

Physics and Applied Mathematics Unit

Indian Statistical Institute

203 B T Road, Kolkata 700 108

Email: parashar@isical.ac.in

Abstract

We establish the non-existence of a universal Hadamard gate for arbitrary unknown qubits, by considering two different principles; namely, no-superluminal signalling and non-increase of entanglement under LOCC. It is also shown that these principles are not violated if and only if the qubit states are of the special form obtained in our recent work

The Hadamard gate is a one qubit unitary operator which has played a very crucial role in the developement of quantum algorithms [1, 2, 3]. It rotates the computational basis (CB) states $|0\rangle$ and $|1\rangle$ by creating an equal superposition of the amplitudes, and the new states so obtained are orthogonal to each other. Can this action of the Hadamard gate be generalized to any arbitrary unknown qubit state? It was proved in [4] using unitarity of the evolution, that there does not exist a Hadamard gate for a completely arbitrary qubit state. In other words, the Hadamard gate is not universal. Then the natural question to ask is: What is the most general class of states for which it is possible to design this gate in a universal manner? We endeavored to address this aspect in our recent investigation [5] where a special ensemble of qubits was obtained. The Hadamard gate holds for each and every state belonging to this ensemble.

The restrictions imposed by the structure of quantum mechanics has led to several other *impossible* operations in quantum information theory; for example, the famous no-cloning theorem [6] and the no-deleting principle [7]. There have also been attempts to derive them by applying some other fundamental principles of nature, like no-faster-than-light communication between spatially separated parties [8, 9, 10, 11] and preservation of entanglement for closed systems under local operations [12]. Another important no-go theorem is the non-existence of a universal flipping operator (NOT gate) [13] which would take an arbitrary qubit state to its orthogonal complement. An alternative proof of this was

recently given in [14] from the constraint of no-signalling and also from the consideration that the amount of entanglement shared between two spatialy separated parties cannot be increased by local operations and classical communication (LOCC). These pursuits serve as the chief motivation to undertake the present investigation.

The purpose of this communication is two-fold. Firstly, we prove the non-existence of a universal Hadamard gate by imposing (separately) the two fundamental physical principles mentioned above; namely, (i) the no-superluminal signalling condition of special relativity, and (ii) non-increase of entanglement under LOCC. Secondly, we show that as a consequence of non-violation of these two laws, the qubit states *must* be of a particular type. This gives the largest set of states for which the Hadamard gate is valid, and matches exactly with the result derived in [5] from an altogether different consideration.

Let us take the CB states $|0\rangle$, $|1\rangle$ and a third state $|\psi\rangle$ which is an arbitrary linear superposition of these two. Thus, $|\psi\rangle = a|0\rangle + b|1\rangle$, where a and b are *non-zero* complex numbers satisfying the normalization condition $a^*a + b^*b = 1$. We define the action of the unitary Hadamard operator H on these states as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad H|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\overline{\psi}\rangle), \tag{1}$$

where $|\overline{\psi}\rangle = b^*|0\rangle - a^*|1\rangle$ is the orthogonal complement of $|\psi\rangle$. The Hadamard gate is explicitly represented by the matrix $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. The transformation of $|\overline{\psi}\rangle$ can be easily deduced from that of $|\psi\rangle$ in (1) and reads as $H|\overline{\psi}\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle - |\overline{\psi}\rangle)$.

No-superluminal signalling: First we shall show that the Hadamard operation defined in (1) implies signalling. For this purpose let us consider that Alice and Bob share the entangled state

$$\phi_{AB} = \frac{1}{2}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|\psi\rangle_B + |2\rangle_A|1\rangle_B + |3\rangle_A|\overline{\psi}\rangle_B\right), \tag{2}$$

where Alice's particle is four-dimensional and Bob's is two-dimensional.

The density matrix of the combined system is $\rho_{AB} = |\phi_{AB}\rangle\langle\phi_{AB}|$. Alice's reduced density matrix can be obtained by tracing out Bob's part. So

$$\begin{aligned} \rho_A = tr_B(\rho_{AB}) \quad = \quad & \frac{1}{4}[|0\rangle\langle0| + a|1\rangle\langle0| + b^*|3\rangle\langle0| + a^*|0\rangle\langle1| + |1\rangle\langle1| + b^*|2\rangle\langle1| \\ + \quad & b|1\rangle\langle2| + |2\rangle\langle2| - a^*|3\rangle\langle2| + b|0\rangle\langle3| - a|2\rangle\langle3| + |3\rangle\langle3|]. \end{aligned} \tag{3}$$

Now Bob applies Hadamard transformation on his qubit in Eq(2) but does not communicate anything to Alice. The shared state thus changes to

$$\begin{aligned} (I \otimes H)\phi_{AB} = \phi'_{AB} = \frac{1}{2\sqrt{2}} \quad [\quad & |0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|\psi\rangle + |1\rangle|\overline{\psi}\rangle \\ + \quad & |2\rangle|0\rangle - |2\rangle|1\rangle + |3\rangle|\psi\rangle - |3\rangle|\overline{\psi}\rangle]. \end{aligned} \tag{4}$$

After this operation, Alice's new reduced density matrix becomes

$$
\begin{aligned}
\rho'_A = tr_B(\rho'_{AB}) \;=\; & \frac{1}{8}[2(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|) \\
& + \; (a + b^* + b - a^*)|1\rangle\langle 0| + (a - b^* + b + a^*)|3\rangle\langle 0| \\
& + \; (a^* + b^* + b - a)|0\rangle\langle 1| + (a^* - b^* + b + a)|2\rangle\langle 1| \\
& + \; (a + b^* - b + a^*)|1\rangle\langle 2| + (a - b^* - b - a^*)|3\rangle\langle 2| \\
& + \; (a + b^* - b + a^*)|0\rangle\langle 3| + (a^* - b^* - b - a)|2\rangle\langle 3|].
\end{aligned}
\tag{5}
$$

Comparing the coefficients of each term in (3) and (5), it is clear that $\rho'_A \neq \rho_A$ for arbitrary choices of the parameters a and b. So, in principle, Alice can distinguish between ρ_A and ρ'_A, although Bob has not informed her anything about his operation. This implies that superluminal communication has taken place with the help of quantum non-local resourse (entanglement). But special theory of relativity forbids faster-than-light communication. Hence, we conclude that Hadamard gate does not exist for an arbitrary qubit as it leads to signalling.

If however the no-signalling constraint is imposed, then ρ_A and ρ'_A should be equal because the action of H is a trace preserving local operation performed only at Bob's side. Since a and b are complex, we can write $a = \alpha_a + i\beta_a$, $b = \alpha_b + i\beta_b$, where $\alpha_a, \alpha_b, \beta_a$ and β_b are all real. So $\rho'_A = \rho_A$ implies $a + b^* + b - a^* = 2a$, which gives, $\alpha_b = \alpha_a$. Further, $a - b^* + b + a^* = 2b^*$ yields $2\alpha_a = 2\alpha_b - 4i\beta_b$, i.e., $\beta_b = 0$, implying that b is purely real. Letting $\alpha_a = \alpha$, $\beta_a = \beta$, we find that the qubit state assumes the form

$$
|\psi\rangle = (\alpha + i\beta)|0\rangle + \alpha|1\rangle,
\tag{6}
$$

with the normalization condition $2\alpha^2 + \beta^2 = 1$. This peculiar form has one complex and one pure real amplitude (in CB); the two real parts being equal. Interestingly, this is exactly the same ensemble that was obtained in [5]. It is in fact the largest set of qubit states (along with $|0\rangle$) for which the Hadamard gate can be designed universally. On the other hand, $|\overline{\psi}\rangle = \alpha|0\rangle - (\alpha - i\beta)|1\rangle$ (along with $|1\rangle$) is the set of orthogonal complements. These two sets formed nice trajectories when represented on the bloch sphere.

Non-increase of entanglement under LOCC: Next, we show the non-validity of the Hadamard transformation (1) for a general qubit, by considering the fact that local operations and classical communication cannot increase the entanglement content of a quantum system. Unfortunately, the resource state shared earlier, cannot be used in this case. There is no change in entanglement before and after the Hadamard operation since the eigenvalues of ρ_A and ρ'_A are equal. Therefore, let us consider a different shared state which is of the form [14]

$$
|\Phi\rangle_{AB} = \frac{1}{1 + b^* b}[|0\rangle_A \frac{|0\rangle_{B1}|1\rangle_{B2} - |1\rangle_{B1}|0\rangle_{B2}}{\sqrt{2}} + |1\rangle_A \frac{|0\rangle_{B1}|\psi\rangle_{B2} - |\psi\rangle_{B1}|0\rangle_{B2}}{\sqrt{2}}],
\tag{7}
$$

where the first qubit is with Alice while the other two are with Bob. This state is a product

state in the A:B cut since it can be written as

$$|\Phi\rangle_{AB} = \frac{1}{1+b^*b}[\{|0\rangle_A + b|1\rangle_A\} \otimes \{\frac{|0\rangle_{B1}|1\rangle_{B2} - |1\rangle_{B1}|0\rangle_{B2}}{\sqrt{2}}\}].\tag{8}$$

Following the earlier protocol, we find Alice's reduced density operator

$$\rho_A = \frac{1}{1+b^*b}[|0\rangle\langle0| + b^*|0\rangle\langle1| + b|1\rangle\langle0| + b^*b|1\rangle\langle1|].\tag{9}$$

The eigenvalues of this matrix are 0 and 1. Obviously, the amount of entanglement given by the van Neumann entropy is zero. Now Bob applies the trace preserving Hadamard transformation defined in (1) on the last particle ($B2$) in Eq(7), which results in the state

$$\begin{aligned}|\Phi'\rangle_{AB} = \frac{1}{2\sqrt{N}} \quad [\quad &|000\rangle - |001\rangle - |010\rangle + |011\rangle \\ + \quad &|10\psi\rangle + |10\overline{\psi}\rangle - |1\psi0\rangle - |1\psi1\rangle],\end{aligned}\tag{10}$$

where $N = 2 + \frac{1}{4}((a - a^*)^2 - (a + a^*)(b + b^*))$. Since a and b are arbitrary, so in general, the above state is entangled in the A:B cut. This implies that entanglement has been created by local operation. However, we know that entanglement cannot be increased by local operations even if classical communication is allowed. Therefore, we conclude that Hadamard transformation of an arbitrary, unknown qubit is an invalid operation.

Our next task is to derive the conditions under which the entanglement in the state would remain the same (zero in this case) before and after the application of the Hadamard gate. For this purpose we have to compare the eigenvalues of the respective density matrices on Alice's side. So after Bob's operation

$$\begin{aligned}\rho'_A = \frac{1}{4N}[\quad &4 \quad |0\rangle\langle0| + (a + a^* + b + b^*)|0\rangle\langle1| + (a + a^* + b + b^*)|1\rangle\langle0| \\ + \quad &(4 + (a - a^*)^2 - (a + a^*)(b + b^*))|1\rangle\langle1|].\end{aligned}\tag{11}$$

It is, however, more convenient to express a and b in terms of real and imaginary components as follows:

$$\rho'_A = \frac{1}{N}[|0\rangle\langle0| + \frac{\alpha_a + \alpha_b}{2}|0\rangle\langle1| + \frac{\alpha_a + \alpha_b}{2}|1\rangle\langle0| + (\alpha_a^2 + \alpha_b^2 + \beta_b^2 - \alpha_a\alpha_b)|1\rangle\langle1|],\tag{12}$$

where $N = 1 + \alpha_a^2 + \alpha_b^2 + \beta_b^2 - \alpha_a\alpha_b$. The eigenvalue equation of the above matrix gives two roots:

$$\lambda_\pm = \frac{1}{2} \pm \frac{\sqrt{(N - 2)^2 + (\alpha_a + \alpha_b)^2}}{2N}\tag{13}$$

In order to maintain the same amount of entanglement in the system, we equate these two roots of ρ'_A to the eigenvalues of ρ_A. This yields the constraint:

$$\beta_b^2 = -\frac{3}{4}(\alpha_a - \alpha_b)^2.\tag{14}$$

4

But since α_a and α_b are both real, so the squared term on r.h.s. will always be positive. This implies that β_b is imaginary. However, we know that β_b is also real. Therefore, the only possible solution is that $\beta_b = 0$. Substituting this back in (14) yields $\alpha_a = \alpha_b$. We have thus, rederived the restrictions $\alpha_a = \alpha_b$ and $\beta_b = 0$ from the principle of non-increase of entanglement under LOCC.

In conclusion, we have shown, by considering two different physical principles, that the Hadamard transformation for completely arbitrary unknown qubits is an invalid operation. The Hadamard gate exists if and only if the state belongs to the special ensemble (6). Interestingly, quantum mechanics and no-signalling condition gives exactly the same set of states for a valid Hadamard operation. This bears similarity with optimal fidelity of a qubit [13, 8], the value of which turns out to be exactly the same by these two different considerations. Since the Hadamard gate, just like the NOT gate, is allowed for a certain class of states on the bloch sphere, it imposes a weaker constraint on the quantum system than the no-cloning and no-deleting operations.

It is a pleasure to thank G. Kar for useful discussions.

References

[1] D. Deutsch, *Proc. Royal Society of London A* **425**, 73, (1989).

[2] D. Deutsch and R. Jozsa, *Proc. Royal Society of London A* **439**, 553, (1992).

[3] P.W. Shor, *Proc. 35th Annual Symp. on Found. of Comp. Sc., IEEE Press, Los Alamitos, CA* (1994).

[4] A.K. Pati, *Phys. Rev. A* **66**, 062319, (2002).

[5] A. Maitra and P. Parashar, to appear in *IJQI* (2006), arXiv:quant-ph/0505068.

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

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

[8] N. Gisin, *Phys. Lett. A* **242**, 1 (1998).

[9] L. Hardy and D.D. Song, *Phys. Lett. A* **259**, 331 (1999).

[10] A.K. Pati, *Phys. Lett. A* **270**, 103 (2000).

[11] A.K. Pati and S. Braunstein, *Phys. Lett. A* **315**, 208 (2003).

[12] M. Horodecki, R. Horodecki, A. Sen(De)and U. Sen, quant-ph/0306044.

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

[14] I. Chattopadhyay, S.K. Choudhary, G. Kar, S. Kunkri and D. Sarkar, *Phys. Lett. A* **351**, 384 (2006).