Role of entanglement in quantum computation

Arun K. Pati[1] *AND Samuel L. Braunstein*[1,2]

Abstract | Quantum computers are believed to surpass their classical counterparts in speed-up and efficiency. However, the origin of this speed-up in quantum algorithms is not yet fully understood. There are indications that entanglement plays an important role in quantum computation. Quantum algorithms that do not involve entanglement appear to require an exponential amount of resources and may be efficiently simulated on a classical computer. Here we discuss the role of entanglement in quantum computation. As an illustration, we consider Grover's algorithm and how entanglement arises in this case. We will show that even though entanglement is present throughout the computation, the change of entanglement per iteration is exponentially small for large databases.

1. Introduction

In recent years considerable effort has gone into the realization of practical quantum computers, though they are still far from reality. Nevertheless, our understanding about quantum information has undergone a revolutionary change within the last two decades. In quantum computation and quantum information theory we aim to exploit the principles of quantum mechanics for information processing. The simplest quantum computation paradigm involves initial preparation of logical states followed by the application of a sequence of unitary evolution operators (prescribed by a particular quantum mechanical algorithm) and finally 'reading out' the desired answer. This may be called prepare-compute-measure paradigm of quantum computing. In this context an important question has been whether linear superposition alone is sufficient to yield a speed-up, relative to conventional computation, or whether quantum entanglement suffices. Though the existing quantum algorithms such as Deutsch-Jozsa [1], Grover [2] and Shor [3] require quantum entanglement it is not clear whether, in general, entanglement is the key for quantum speed-up. In particular, various quantum algorithms have been already implemented using NMR setups [4–6]. In that context there has been a debate in the NMR implementation of quantum algorithms as to what provides the power to quantum computers if there is no entanglement generated during computation [7].

The study of quantum entanglement has become a major area of research due to its potential applications for quantum information processing. Quantum entanglement was first recognized by Schrödinger. Einstein used this notion to argue that quantum theory apparently allows 'spooky-actions' at a distance [8] — a situation with which he was very unhappy. However, the spooky-action provided by quantum mechanics cannot be used for faster than light communication and so is not as disturbing as Einstein thought. On the contrary, supplemented by classical communication, quantum entanglement can become a resource for very useful and exotic information processing tasks, such as: dense coding [9], quantum teleportation

[1]*Institute of Physics, Bhubaneswar-751005, Orissa, India*
[2]*Computer Science, University of York, York YO10 5DD, UK*
akpati@iopb.res.in

[10], remote state preparation [11], quantum cryptography [12], etc.

In addition, quantum entanglement may play an important role in quantum algorithms [13] by giving extra power to quantum computers [14]. This leads one to ask whether entanglement is at the heart of quantum computation? There are indications that the answer may be affirmative. Algorithms that do not involve entanglement can be efficiently simulated on a classical computer. For example, the Deutsch-Jozsa algorithm for the single qubit or two qubit case does not involve entanglement [15]. However, for three or more qubits it does [16]. Grover's algorithm for the two qubit case does not require entanglement. However, for more than two qubits both the pure state and pseudo-pure state implementations involve entanglement [17]. Similarly, Shor's algorithm also requires entanglement. Indeed, it has been argued that since Shor's algorithm is exponentially faster than any classical counterpart that it must make use of entanglement [18]. For any quantum algorithm operating on pure states one can prove that the presence of multipartite entanglement, with a number of parties that increases unboundedly with input size, is necessary if a quantum algorithm is to offer an exponential speed-up over classical computation [19]; this occurrence of increasing multipartite entanglement has been explicitly confirmed in Shor's algorithm [19].

In this article, we throw some light on the role of entanglement in quantum computation and consider the implications for the source of the extra power for quantum computation. The article is organized as follows. In section II, we briefly discuss the notion of inherent parallelism in quantum computers and how to understand quantum computing algorithms geometrically. In section III, we discuss the geometry of Grover's algorithm and show how to obtain $\sqrt{N}$ improvement using the idea of the Fubini-Study metric. In section IV, we illustrate the role of entanglement in Grover's algorithm implemented on n-qubit pure states. We will show that even though entanglement is present throughout the computation, the change of entanglement per iteration is exponentially small for large databases. In section V, we discuss several claims that quantum computing is possible without entanglement. However, such schemes are not efficient requiring a heavy price in resources. Towards the end we briefly discuss the role of entanglement in the pseudo-pure state implementations of Grover's algorithm and find that not only is entanglement necessary to achieve a speed-up in quantum searching, but it must be present throughout the computation [17].

2. Quantum parallelism and the geometry of quantum computation

Within the simple paradigm of prepare-compute-measure, a quantum computer consists of n qubits which are initially all in state $|0\rangle$. Thus, the initial n-qubit register is a product state. One then applies Hadamard (H) gates to all qubits to prepare an equal superpositions (which remains a product state)

$$|\Psi_0\rangle = H^{\otimes n}|00\ldots00\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle. \qquad (1)$$

To envision the parallelism in quantum computation, consider a function evaluation process. Let a function $f:\{0,1\}^n \to \{0,1\}$ map an n-bit string to a single bit. In quantum computing, we represent reversible operations as unitary transformations U with $U^\dagger U = UU^\dagger = 1$. If a unitary transformation (the oracle) U_f does function evaluation on one particular n-bit string via the map $|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$, then a single application of U_f on the equal superposition will yield

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle \to \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle. \qquad (2)$$

This happens because of the linearity of quantum theory. Thus, one can compute the function for all possible n-bit strings with a single application of U_f. This is the inherent parallelism offered by the quantum world which is not possible in the classical world (we do not consider classical wave phenomena). Here, note that even in this simple function evaluation, if we look at the state of individual qubits we will typically find that some of them will be in a mixed state. This implies that the state obtained after applying U_f is an entangled state (though it may not be a genuinely n-qubit entangled state). For example, if $n=2$, one has $\frac{1}{2}\sum_{x=0}^{3}|x\rangle|0\rangle \to \frac{1}{2}(|00\rangle|f(00)\rangle + |01\rangle|f(01)\rangle + |10\rangle|f(10)\rangle + |11\rangle|f(11)\rangle)$. Now, if (say) $|f(00)\rangle = |0\rangle, |f(01)\rangle = |1\rangle, |f(10)\rangle = |0\rangle$, and $|f(11)\rangle = |1\rangle$, then the final state is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This shows that the state of the first qubit is pure (not entangled with other two) but the second and third qubits are in a maximally entangled state.

In general, a quantum computation may involve the application of a sequence of unitary operators. Now, at any stage of the computation (say the kth step) we may write the n-qubit state generically as

$$|\Psi_k\rangle = U_k U_{k-1}\cdots U_1|\Psi_i\rangle = \sum_{x=0}^{2^n-1}\alpha_x(k)|x\rangle \qquad (3)$$

with initial state $|\Psi_i\rangle = |\Psi_0\rangle$ as given in (1) and $\alpha_x(k) = \langle x|U_k U_{k-1} \cdots U_1|\Psi_0\rangle$. If these unitary operators are entangling then they will typically generate an entangled state during the quantum computation.

Here, we develop some geometric ideas for understanding quantum algorithms. Consider a quantum computer consisting of n-qubits. Let $\{|\Psi\rangle\}$ be a set of vectors in $\mathcal{H}^{\otimes n}$. The set of rays of $\mathcal{H}^{\otimes n}$ is called the projective Hilbert space $\mathcal{P}(\mathcal{H}^{\otimes n})$. The Hilbert space of n-qubits is isomorphic to $\mathbb{C}^N$, with $N = 2^n$. The projective Hilbert space is $\mathcal{P} = \mathbb{C}^N - \{0\}/U(1)$ which is a complex manifold of dimension $N-1$. This can also be considered as a real manifold of dimension $2(N-1)$. Any quantum state (product or entangled) of a quantum computer at a given instant of time can be represented as a point within $\mathcal{P}$. The evolution of the quantum computer state can be represented by a *curve* $\Gamma : t \to |\Psi(t)\rangle$ in $\mathcal{H}$ whose projection $\Pi(\Gamma) = \hat{\Gamma}$ lies in $\mathcal{P}$. Here, smooth mappings $\Gamma : [0, t] \to \mathcal{L}$ of an interval into a differentiable manifold are called smooth curves in the manifold [20,21]. Any computation starts with an initial state and reaches a final state via a sequence of unitary operators. Therefore, quantum computation can be viewed geometrically as a sequence of curves in the projective Hilbert space of an n-qubit system. Geometrically any quantum computation is such a path and the efficiency of an algorithm will depend on how well we can optimize the path.

The projective Hilbert space of a quantum computer has a natural metric called the Fubini-Study metric which can be defined from the inner product structure of the underlying Hilbert space [22]. This metric defines the distance between any two states of a quantum computer. To solve a problem on a quantum computer, we need to know the number of steps that is involved in reaching the desired state (the final state). Using the notion of distance we can define the number of steps for any problem that can be tackled on a quantum computer. If $|\Psi_i\rangle = |\Psi_0\rangle$ is the initial state and $|\Psi_f\rangle$ is the final state then the total distance between them is given by [20–22]

$$D(|\Psi_i\rangle, |\Psi_f\rangle) = 2\sqrt{1 - |\langle\Psi_i|\Psi_f\rangle|^2}. \qquad (4)$$

If one application of U takes the initial state to $|\Psi_U\rangle$, then it has moved a distance

$$D(|\Psi_i\rangle, |\Psi_U\rangle) = 2\sqrt{1 - |\langle\Psi_i|\Psi_U\rangle|^2}. \qquad (5)$$

Now, we shall suppose that the distance moved in each step of computation is equal — as one might expect in optimal geodesic motion. This allows us to define the number of steps N_S to complete the computation as

$$N_S = \frac{D(|\Psi_i\rangle, |\Psi_f\rangle)}{D(|\Psi_i\rangle, |\Psi_U\rangle)}. \qquad (6)$$

The success of an algorithm depends on how to minimize the number of steps. As it is clear from (6) that $D(|\Psi_i\rangle, |\Psi_f\rangle)$ is fixed for a given problem, to minimize N_S, one has to maximize $D(|\Psi_i\rangle, |\Psi_U\rangle)$. If the system moves along geodesic paths (shortest paths) in the projective Hilbert space then $D(|\Psi_i\rangle, |\Psi_U\rangle)$ can be maximized and it can reach the desired state fastest. An important question is whether the presence of entanglement helps the quantum computer to move along geodesics. The answer to this question is difficult in general, but it could be the case that in some cases entanglement does help. How much entanglement should be present in an n-qubit state so as to move along a geodesic is also not known. These are some of the questions that we hope to answer in the future.

In the next section we will show that in the case of Grover's algorithm the states indeed evolve along geodesics and the number of steps calculated using the above formula is $O(\sqrt{N})$. This was first observed soon after the discovery of Grover's algorithm by one of the authors [23] and it was one of the first geometric ideas in the context of quantum algorithms.

3. Geometry of Grover's algorithm

In this section we illustrate the main geometric idea with one example and that is quantum searching. This search algorithm was discovered by Grover. The role of entanglement in the Grover algorithm was first pointed out in [17]. The original version of Grover's algorithm on multiple qubits in a pure state necessarily involves quantum entanglement, even though the initial and ideal target states are product states. Within pseudo-pure state implementations, by counting each active 'molecule' as contributing to the computational resources, it has been shown in a non-asymptotic analysis that not only is entanglement necessary to achieve a speed-up in quantum searching, but it must be present throughout the computation [17].

In quantum searching, we are given an unknown binary function $f(x)$, which returns 1 for a unique 'target' value $x = y$ and 0 otherwise, where $x = 0, 1, 2, \ldots, N-1$, with $N = 2^n$. Our goal is to find y such that $f(y) = 1$. In Grover's algorithm, the N inputs are mapped onto the states of n quantum bits (qubits) such as spin-$\frac{1}{2}$ particles. The quantum problem thus becomes one of maximizing the

overlap between the state of these n qubits and target state $|y\rangle$. This is equivalent to maximizing the probability of obtaining the desired state upon measurement.

The initial state of the quantum computer is taken to be an equal superposition of all possible bit strings

$$|\Psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{7}$$

The Grover operator is defined as $G = -I_0 H^{\otimes n} I_y H^{\otimes n}$ and is used repeatedly in the algorithm, where $I_0 = \mathbb{I} - 2|\Psi_0\rangle\langle\Psi_0|$, $I_y = \mathbb{I} - 2|y\rangle\langle y|$, with $|y\rangle$ the target (ideally the final) state and H the Hadamard transformation.

The Grover algorithm basically involves the application of a sequence of Grover operators, finally reaching the target state in the appropriate number of steps. The Grover operator corresponds to a small rotation in the two-dimensional subspace spanned by the initial and the target states. Each such rotation requires a *single* evaluation of f. Thus, after k iterations of the Grover operator the combined n-qubit state (7) evolves to

$$|\Psi_k\rangle = \frac{\cos\theta_k}{\sqrt{N-1}} \sum_{x\neq y} |x\rangle + \sin\theta_k |y\rangle, \tag{8}$$

where $\theta_k = (2k+1)\theta_0$ and θ_0 satisfies $\sin\theta_0 = 1/\sqrt{N}$. The search is complete when we reach the target state and that happens for $\theta_k \simeq \pi/2$ which takes $O(\sqrt{N})$ iterations of the Grover operator. Hence we need $O(\sqrt{N})$ evaluations of the function f.

This result can also be understood geometrically in the manner described in the previous section. Note that the total distance the quantum state needs to travel in order to reach the target state in $\mathcal{P}$ is $D(|\Psi_i\rangle, |\Psi_f\rangle) = D(|\Psi_0\rangle, |y\rangle) = \cos\theta_0$. In one application of the Grover operator, the state travels a distance given by $D(|\Psi_i\rangle, |\Psi_U\rangle) = D(|\Psi_0\rangle, |\Psi_1\rangle) = \sin 2\theta_0$. Here, one can check that the state indeed passes along a geodesic during the iteration. We know that if a quantum state evolves along a geodesic, the it satisfies the parallel transport condition. The parallel transport condition in this case will read as

$$\left\langle \Psi_k \middle| \frac{d\Psi_k}{dk} \right\rangle = 0. \tag{9}$$

From (8) it can be seen that $|\Psi_k\rangle$ actually satisfies this condition. Therefore, the number of steps one needs to find the target state is given by

$$N_S = \frac{D(|\Psi_0\rangle, |y\rangle)}{D(|\Psi_0\rangle, |\Psi_1\rangle)} = \frac{\sqrt{N}}{2} = O(\sqrt{N}). \tag{10}$$

If the distance is instead measured via the Hilbert-space angle then the exact number of steps required is obtained. This shows how the geometry of the n-qubit state space and the notion of the Fubini-Study distance help us in understanding the number of steps required to find a target state in Grover's algorithm.

4. Entanglement in Grover's algorithm

In this section we discuss the role of entanglement in Grover's algorithm. We will show that although the initial and target states are product states the intermediate states through which quantum computer evolves are actually entangled. However, we cannot quantify how much entanglement there is in these intermediate states as we do not have a proper measure of multipartite entanglement for n-qubit states. What we do is consider the full system as being bipartite, with one subsystem consisting of a single qubit and the second subsystem the remaining qubits. Then one can use the Schmidt decomposition theorem for bipartite systems. Suppose we are given a bipartite state $|\Psi\rangle \in \mathcal{H}^N \otimes t\mathcal{H}^M$ with

$$|\Psi\rangle = \sum_{ij=1}^{NM} C_{ij} |a_i\rangle \otimes |b_j\rangle, \tag{11}$$

where $\{|a_i\rangle\}(i = 1, 2, \ldots, N)$ and $\{|b_j\rangle\}(j = 1, 2, \ldots, M)$ are the orthonormal basis in their respective Hilbert spaces. The Schmidt decomposition theorem tells us that we can always write $|\Psi\rangle$ as

$$|\Psi\rangle = \sum_{\mu=1}^{\min(N,M)} \sqrt{\lambda_\mu} |\psi_\mu\rangle \otimes |\Phi_\mu\rangle, \tag{12}$$

where λ_μ's are called as the Schmidt coefficients with $\sum_\mu \lambda_\mu = 1$, and $|\psi_\mu\rangle, |\Phi_\mu\rangle$, are the Schmidt basis. Now, the bipartite entanglement is a property which is invariant under $U \otimes V$ and the Schmidt coefficients are actually invariant under such local unitary transformations. The entropy of entanglement is a very good measure of bipartite entanglement which is defined as the von Neumann entropy of any one of the reduced density matrix [24]. The reduced density matrices are given by the partial traces, i.e.,

$$\rho_1 = \mathrm{tr}_2\,(|\Psi\rangle\langle\Psi|) \quad \text{and} \quad \rho_2 = \mathrm{tr}_1\,(|\Psi\rangle\langle\Psi|) \tag{13}$$

Therefore, the entanglement content of $|\Psi\rangle$ is given by

$$\begin{aligned} E(\Psi) &= -\mathrm{tr}\,[\rho_1 \log \rho_1] = -\mathrm{tr}\,[\rho_2 \log \rho_2] \\ &= -\sum_\mu \lambda_\mu \log \lambda_\mu. \end{aligned} \tag{14}$$

The value of entanglement is zero for product states and $\log N$ (if $N < M$) for maximally entangled states.

Thus, using the Schmidt decomposition theorem, we can decompose the *full* state of n-qubits at step k of the Grover algorithm as

$$|\Psi_k\rangle = \sqrt{\lambda_1(k)}|\psi_1\rangle|\Phi_1\rangle - \sqrt{\lambda_2(k)}|\psi_2\rangle|\Phi_2\rangle, \tag{15}$$

where $\{|\psi_1\rangle, |\psi_2\rangle\}$ describes an orthonormal basis for the ℓth qubit and $\{|\Phi_1\rangle, |\Phi_2\rangle\}$ is a pair of Hilbert space vectors for the remaining $(n-1)$ qubits. Here, $\lambda_1(k)$, $\lambda_2(k)$ are the Schmidt coefficients of the state vector at kth iteration.

This allows us to quantify the bipartite entanglement. To find the Schmidt coefficients we calculate the reduced density matrix of any single qubit. The reduced density matrix of the ℓth qubit (say) is

$$\begin{aligned}\rho_\ell(k) &= \mathrm{tr}_{1,2,..,\ell-1,\ell+1,..n}\,(|\Psi_k\rangle\langle\Psi_k|) \\ &= a_k^2 H|0\rangle\langle 0|H + b_k^2|j_\ell\rangle\langle j_\ell| + \frac{a_k b_k}{\sqrt{N}} \\ &\quad \times (2|j_\ell\rangle\langle j_\ell| + |\tilde{j}_\ell\rangle\langle j_\ell| + |j_\ell\rangle\langle\tilde{j}_\ell|), \end{aligned} \tag{16}$$

where $a_k = \sqrt{N/(N-1)}\cos\theta_k$, $b_k = \sin\theta_k - \cos\theta_k/\sqrt{N-1}$ and the single bit $\tilde{j}_\ell = 1 - j_\ell$, $(j_\ell = 0, 1)$. Without loss of generality we take $j_\ell = 1$ and the density matrix $\rho_\ell(k)$ can be expressed in standard form as

$$\rho_\ell(k) = \frac{1}{2}[\mathbb{1} + \vec{s}(k)\cdot\vec{\sigma}] = [1 - s(k)]\frac{\mathbb{I}}{2} + s(k)P, \tag{17}$$

where $\vec{s}(k) \equiv \mathrm{tr}\,[\rho_\ell(k)\vec{\sigma}]$, $\vec{s}(k)\cdot\vec{s}(k) = s(k)^2 \le 1$ and P is a pure state projector. The components of the Bloch vector $\vec{s}(k)$ after k iterations are given by

$$\begin{aligned} s_x(k) &= \frac{N-2}{N-1}\cos^2\theta_k + \frac{1}{\sqrt{N-1}}\sin 2\theta_k \\ s_y(k) &= 0 \\ s_z(k) &= \frac{1}{N-1}\cos^2\theta_k - \sin^2\theta_k. \end{aligned} \tag{18}$$

The eigenvalues of the above density matrix gives us the Schmidt coefficients as

$$\begin{aligned}\lambda_1(k) &= \frac{1}{2}[1 + \sqrt{1 - 4A(k)}] \text{ and } \lambda_2(k) \\ &= \frac{1}{2}[1 - \sqrt{1 - 4A(k)}], \end{aligned} \tag{19}$$

where $A(k) = \frac{N(N-2)}{2(N-1)^2}\sin^2(2k\theta_0)\cos^2\theta_k$.

The bipartite entanglement in the pure state may then be characterized by calculating the von Neumann entropy of this reduced state. The entropy of entanglement with respect to this bipartite partition is given by

$$\begin{aligned} E(\Psi_k) &= -\mathrm{tr}\,[\rho_\ell(k)\log\rho_\ell(k)] \\ &= -\frac{1}{2}(1 + s(k))\log\frac{1}{2}(1 + s(k)) \\ &\quad -\frac{1}{2}(1 - s(k))\log\frac{1}{2}(1 - s(k)), \end{aligned} \tag{20}$$

where $s(k) = \sqrt{1 - 4A(k)}$. This entanglement is independent of the choice of the remaining qubit ℓ, and therefore, holds for any of the qubits against an $(n-1)$-qubit partitioning.

This result shows that the reduced density matrix of any single qubit does not correspond to a maximally entangled state of n qubits, as the von Neumann entropy is not unity. Since the reduced state of Eq. (16) is not pure the full state must be entangled. To see how impure the state in Eq. (16) is one may calculate the linear entropy $L(\rho)$ of it which is given by

$$\begin{aligned} L[\rho_\ell(k)] &= 1 - \mathrm{tr}\,[\rho_\ell(k)^2] = \frac{1 - s(k)^2}{2} \\ &= 2\lambda_1(k)\lambda_2(k). \end{aligned} \tag{21}$$

If the linear entropy is zero the state is pure and as it approaches $\frac{1}{2}$ the state approaches a completely random mixture. In the quantum search algorithm the parameter $s(k)$ can never be zero because that would mean that both $\cos\theta_k$ and $\sin\theta_k$ were simultaneously zero, which cannot be satisfied. So although the reduced density matrix of the qubit may lie close to a completely mixed state it can never become one identically.

We now ask how close this reduced state is to a maximally entangled qubit (using say the Hilbert-Schmidt norm criterion). We therefore calculate the Hilbert-Schimdt norm of the difference of a completely mixed state from the reduced state. This Hilbert-Schmidt distance for the kth iteration during quantum search algorithm is given by

$$\begin{aligned} d(k)^2 &= \left\| \frac{\mathbb{I}}{2} - \rho_\ell(k) \right\|_{HS}^2 = \mathrm{tr}\left[\frac{\mathbb{I}}{2} - \rho_\ell(k)\right]^2 \\ &= \frac{1}{2} - L[\rho_\ell(k)] = \frac{s(k)^2}{2}. \end{aligned} \tag{22}$$

The distance $d(k)$ provides an idea of how the reduced state of an individual qubit behaves during the kth iteration. It shows that the reduced density matrix of the qubit differs from a completely random mixture by $O(s(k))$. From Eq. (18) and (22) we see that for $\theta_0 = \sin^{-1}(1/\sqrt{N})$ and

for $\theta_k = \pi/2$ the reduced density matrix of any remaining qubit is pure, implying that the whole state must have been non-entangled. Thus, we see that although the initial and target states are separable, the intermediate states through which the system evolves are always entangled.

We know that entanglement is present throughout the computation. Now we can discuss how entanglement changes with each Grover iteration. There are several measures of entanglement for bipartite partitioning. All of them are functions of the Schmidt coefficients. One can define the average bipartite entanglement as

$$Q(\Psi_k) = 2 - \frac{2}{n}\sum_j \mathrm{tr}[\rho_j(k)^2]. \quad (23)$$

Since all reduced states are identical the average bipartite entanglement reduces simply to $Q(\psi_k) = 2L[\rho_\ell(k)]$. Therefore, we have

$$Q(\Psi_k) = \frac{2N(N-2)}{(N-1)^2}\sin^2(2k\theta_0)\cos^2\theta_k. \quad (24)$$

One can also use the concurrence [25,26] of the global pure state with respect to any bipartite partitioning, it is given by

$$\begin{aligned} C(\Psi_k) &= \sqrt{2(1-\mathrm{tr}(\rho(k)^2)} \\ &= \frac{\sqrt{2N(N-2)}}{N-1}\sin(2k\theta_0)\cos\theta_k. \end{aligned} \quad (25)$$

This result describes the concurrence as a function of the kth iteration step during Grover's algorithm. Thus, if we want to know how concurrence changes with each iteration we should consider the derivative $dC(\Psi_k)/dk$, which is given by

$$\begin{aligned} \frac{dC(\Psi_k)}{dk} &= \frac{\sqrt{2N(N-2)}}{N-1} \\ &\quad \times 2\theta_0\cos[(4k+1)\theta_0]. \end{aligned} \quad (26)$$

For search of a large database ($N >> 1$), we will have

$$\left|\frac{dC(\Psi_k)}{dk}\right| \leq 2\sqrt{2}\,\theta_0. \quad (27)$$

Thus, we find that for a large database the change of (bipartite) concurrence per iteration is bounded by $2\sqrt{2}/\sqrt{N}$, i.e., $|dC/dk| \leq 2\sqrt{2}/2^{n/2}$, as $N = 2^n$. This means that the entanglement consumed per iteration is exponentially small. So even though entanglement is necessary and sufficient for speed-up its consumption is minimal. This may be one reason why in quantum search we do not find an exponential speed-up (but instead only a quadratic speed-up) relative to classical algorithms. In a recent paper, it has been shown that for Grover's algorithm the change of probability of finding the target state per iteration is related to the concurrence [27]; one can also argue for a quadratic speed-up from this entanglement consideration.

5. Quantum computing without entanglement

In the literature, one can find papers claiming that one can do quantum computing just with linear superposition and one does not need entanglement. For example, in Ref. [28] one can see that it is possible to do quantum searching without entanglement. However, one has to pay a price to implement Grover's algorithm without entanglement. It has been observed that quantum computers that can do searching without entanglement are not universal quantum computers and they generally require exponentially greater resources. Similarly, in Ref. [29] it has been suggested that one can obtain some advantage in the Deutsch-Jozsa algorithm and in Simon's algorithm even without entanglement. For example, in the Deutsch-Jozsa algorithm if one artificially runs the protocol a single time (i.e., restricting oneself to a single oracle call) then the information gain is positive even in the absence of entanglement, whereas classically this gain is precisely zero. However, one may argue that this is simply not what running the Deutsch-Jozsa algorithm actually is about. It may be mentioned that this kind of performance or improvement does not fit within the accepted paradigm of running an algorithm. One may also note that towards the end of Ref. [29] the authors do say that there is no real contradiction between their result and the necessity of requiring entanglement for quantum computing.

One may wonder if entanglement is also necessary in mixed state computation. This has been answered for quantum searching with pseudo-pure states [17]. These states naturally arise in liquid-state NMR machines where one faces the difficulty of accessing a pure state because the system is in thermal equilibrium at room temperature. Instead, one implements Grover's algorithm on a near random ensemble of molecular spins in a liquid, with a small preference for the spins to point along an external magnetic field; the size of this preference is quantified by the purity parameter ϵ [typically $O(10^{-5})$]. For a sufficiently low spin polarization (corresponding to a sufficiently low purity parameter), the system can be well-approximated by a pseudo-pure state representation described by

$$\rho = \frac{1-\epsilon}{N}\mathbb{I}_N + \epsilon|\Psi\rangle\langle\Psi|, \quad (28)$$

where $\mathbb{I}_N$ is the identity matrix of dimension N. If we consider quantum searching on pseudo-pure quantum states, then after k iterations of the Grover search operator, one obtains the state

$$\rho \rightarrow \rho_k = G^k \rho\, G^{\dagger k} = \frac{1-\epsilon}{N}\mathbb{I}_N + \epsilon |\Psi_k\rangle\langle\Psi_k|, \tag{29}$$

where $|\Psi_k\rangle$ is given by Eq. (8). The boundary between separability and entanglement for such states had been obtained in Ref. [17]. If the pseudo-pure state is separable, then we must have

$$\epsilon \leq \epsilon_k \equiv \frac{1}{1+N\sqrt{\lambda_1(k)\lambda_2(k)}} = \frac{1}{1+2^{n-1}C(\Psi_k)}. \tag{30}$$

The density matrix at the kth step of the search could be entangled whenever $\epsilon > \epsilon_k$. This bound quantifies the separability region of pseudo-pure states for each iteration k during Grover's algorithm. Interestingly, the boundary also depends on the concurrence at the kth step. Thus, one can tell at each stage of computation whether the state is definitely separable for a given value of purity parameter. One can show for such pseudo-pure state quantum computing of Grover's algorithm, that entanglement is necessary and sufficient for obtaining a speed-up.

6. Conclusion

Quantum computing exploits two basic features of the quantum world, namely, linear superposition and quantum entanglement. However, in recent years there have been debates as to whether quantum entanglement is necessary for quantum computing. In the usual paradigm of quantum computing (prepare-compute-measure), we find that entanglement appears to be necessary for quantum computation. In particular, it has been shown that for the pure state implementation of Grover's algorithm, one needs entanglement. We find that for large database the entanglement change per iteration is exponentially small in the number of qubits. One may be tempted to say that because of such a tiny consumption of entanglement that the speed-up in Grover's algorithm is not exponential rather only quadratic improvement. Of course, it remains an open question as to how much entanglement is required to give an exponential speed-up over any classical computation. Recently, it has been claimed that highly entangled states are not universal for quantum computation [30]. Entanglement should be consumed in the right amounts in a quantum computation. However, what is the right choice for consuming entanglement in order to enhance quantum computing power, only the future will tell.

Received 18 March 2009.

References

1. D. Deutsch and R. Jozsa, Proc. R. Soc. London **439**, 553 (1992).
2. L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
3. P. W. Shor, Symposium on Fundamentals of Computer Science (FOCS) 56 (1994).
4. N. Gershenfeld and I.L. Chuang, Science **275**, 350 (1997).
5. E. Knill, I.L. Chuang and R. Laflamme, Phys. Rev. A. **57**, 3348 (1998).
6. T. S. Mahesh *et al*, Current Science, **85**, 932 (2003).
7. S. L. Braunstein, et al., Phys. Rev. Lett. **83**, 1054 (1999).
8. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
9. C. H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
10. C. H. Bennett, et al., Phys. Rev. Lett. **70**, 1895 (1993); S. L. Braunstein et al., Phys. Rev. A **64**, 022321 (2001): P. van Loock and S. L. Braunstein, Phys. Rev. A **61**, 010302 (2000).
11. A. K. Pati, Phys. Rev. A **63**, 014320 (2001).
12. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
13. R. Jozsa, *Geometric Issues in the Foundations of Science*, Eds. S. Huggett et al., (Oxford University Press, Oxford, 1997).
14. R. Fitzgerlad, Phys. Today, **53**(1), 20 (2000).
15. D. Collins, K. W. Kim and W. C. Holton, Phys. Rev. A **58**, R1633 (1998).
16. Arvind, Pramana J. of Phys. **56**, 357 (2001).
17. S. L. Braunstein and A. K. Pati, Quantum Information and Computation, **2**(2), 399 (2002).
18. N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).
19. R. Jozsa and N. Linden, Proc. R. Soc. Lond. A **459**, 2011 (2003).
20. A. K. Pati, Phys. Lett. A **159**, 105 (1991).
21. A. K. Pati, Phys. Rev. A **52**, 2576 (1995).
22. J. Anandan and Y. Aharanov, Phys. Rev. Lett. **65**, 1679 (1990).
23. A. K. Pati, Quant-Ph/9807067, (1998).
24. S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
25. W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
26. P. Rungta, et al., Phys. Rev. A **64**, 042315 (2001).
27. P. Rungta, arXiv:0707.1410 (2007).
28. S. Lloyd, Phys. Rev. A **61**, 010301 (2000).
29. E. Biham, et al., Theoretical Computer Science, **320**, 15 (2004).
30. D. Gross, S. Flammia, J. Eisert, arXiv:0810.4331 (2008).

Arun K. Pati has been a theoretical physicist in the Theoretical Physics Division, BARC, Mumbai, India since 1989, and is currently a visiting scientist at the Institute of Physics, Bhubaneswar, India. His research area is mostly quantum information and quantum computation, the theory of geometric phases and its applications, and the foundations of quantum mechanics. He is also interested in the quantum mechanics of bio-systems. He has published over 60 papers on these topics and has edited two books: one in quantum information theory and other in quantum aspects of life. Pati is the recipient of the India Physics Association Award for Young Physicist of the Year (2000) and the Indian Physical Society Award for Young Scientists (1996). His research has been featured in news items in Nature, Science and many national and international newspapers.

Samuel L. Braunstein is Professor of Quantum Computation at the University of York since his joining it in 2003. He has been a recipient of the prestigious Royal Society-Wolfson Research Merit Award and was awarded the honorary title of 2001 Lord Kelvin Lecturer. He is a Fellow of the Institute of Physics and the Optical Society of America. Before joining the University of York, he held a prestigious German Humboldt Fellowship (spent at the University of Ulm). He is editor of three books "Quantum Computing," "Scalable Quantum Computing" and "Quantum Information with Continuous Variables" and serves on the editorial board of the journal Fortschritte der Physik. He initiated and is a Founding Managing Editor of Quantum Information and Computation – the first journal dedicated specifically to this field. Professor Braunstein's most cited work on quantum teleportation was among those chosen as the 'top ten [scientific] breakthroughs' of 1998 by the journal Science.