Quantum Distributed Computing Applied to Grover's Search Algorithm

Debabrata Goswami(✉)

Indian Institute of Technology Kanpur, Kanpur 208016, India
dgoswami@iitk.ac.in

Abstract. Grover's Algorithm finds a unique element in an unsorted stock of N-elements in $\sqrt{N}$ queries through quantum search. A single-query solution can also be designed, but with an overhead of $N \log_2 N$ steps to prepare and post process the query, which is worse than the classical $N/2$ queries. We show here that by distributing the computing load on a set of quantum computers, we achieve better information theoretic bounds and relaxed space scaling. Howsoever small one quantum computing node is, by virtue of networking and sharing of data, we can virtually work with a sufficiently large qubit space.

Keywords: Distributed quantum computing · Grover's quantum search · Optical networking

1 Introduction

Today's digital computer is the cumulation of technological advancements that began with the mechanical clockwork ideas of Charles Babbage in the nineteenth century. However, it is surprising that logically, the high speed modern day computer is not fundamentally different from its gigantic 30 ton ancestors, the first of which were built in 1941 by the German engineer Konrad Zuse. Although computers nowadays have become more compact and considerably faster in their performance, their primary execution methodology has remained the same, which is to derive a computationally useful result via the manipulation and interpretation of encoded bits. The underlying mathematical principles are indistinguishable from those outlined in the visionary Church-Turing hypothesis, proposed in the year 1936, much ahead of the birth of the first computer. Bits, the fundamental units of information, are the smallest working units of a digital computer and are classically represented as either 0 or 1 in a digital computer. Classical bits are recognized by alluding to arbitrary thresholds of high (1) or low (0), and so each classical bit is physically realized through a macroscopic physical system, such as the magnetization of a hard disk or the charge on a capacitor. Information is thus realized as series of such bits, and these bits are manipulated via Boolean logic gates arranged in succession to produce an end result [1].

The idea of quantum mechanical computational devices started in the late 1970s when scientists, while trying to determine the fundamental limits of computation, realized that if technology continued to adhere to the Moore's Law,

C.S. Calude et al. (Eds.): Gruska Festschrift, LNCS 8808, pp. 192–199, 2014.
DOI: 10.1007/978-3-319-13350-8_14

the proposal of continuous diminishment in the circuits' sizes on silicon chips would eventually reach a point, where individual elements would not be larger than a few atoms. At such sizes, the physical laws governing the behavior and properties of such miniaturized circuits would inherently be not classical but quantum mechanical in nature. Consequently, the question of whether a fundamentally new kind of computer could be devised based on the principles of quantum physics surfaced.

Feynman was the first to make efforts to answer this question by producing an abstract model in the year 1982, which showed the process of computation using quantum systems [2]. He also explained the capacity of this machine to efficiently act as a simulator for quantum physics. In other words, a physicist can effectively carry out experiments related to quantum physics inside a quantum mechanical computer. Later, in 1985, Deutsch reaffirmed Feynman's assertion, showing that any physical process could, in principle, be modeled perfectly by a quantum computer, which eventually could result in the creation of a general purpose quantum computer [3]. The search for important applications for such a general purpose quantum computing machine began with this theoretical work of Deutsch.

An important breakthrough came in 1994, when Shor [4] devised a method for using quantum computers to crack factorization, an age-old problem in Number Theory. In this paper, Shor proposed the use of a group of mathematical operations, organized and designed specifically for a quantum computer, to factorize huge numbers extremely rapidly compared to conventional computers. With this, quantum computing went from being a mere scientific curiosity to a world-wide research interest.

A quantum computer exerts control over qubits by executing a series of quantum gates, each a unitary transformation acting on qubits. These quantum gates, when performed in succession, initially result into a complicated unitary transformation of a set of qubits at some point. The measurements of the qubits constitute the final computational result. However, on observation, qubits (similar to their classical counterpart, bits) show that they are of discrete nature and are individually represented by two states. Such inherent similarities in the calculation process of classical and quantum computers suggest that theoretically, a classical computer should be able to simulate a quantum computer. Thus, a classical computer should theoretically be able to do everything that a quantum computer does, naturally raising questions pertaining to the need for a quantum computer. Such questions were refuted by the fact that, though a classical computer is theoretically able to simulate a quantum computer, it is highly inept, and is practically incapable of performing most tasks that a quantum computer can perform at ease. John S. Bell, for the first time, explained that correlations among quantum bits differ qualitatively from the correlations among classical bits [5], making the simulation of a quantum computer on a classical one, a computationally hard problem that is practically irrelevant.

In fact, the amount of data processing required for a classical computer to simulate even a hundred qubit quantum computer is prohibitive. A classical

computer trying to simulate a quantum computer would have to work with exponentially large matrices to perform calculations for each individual state, which is also represented as a matrix; thus requiring an exponentially longer time compared to the time taken by even a primitive quantum computer with only a hundred qubits that exist in a Hilbert space of $\sim 10^{30}$ dimensions. Thus, a system with only 100 qubits is impossible to simulate classically in any comprehensible time frame as it represents a quantum superposition of as many as 2^{100} states. Each of these states is classically equivalent to a single list of one hundred 1's and 0's. Any quantum operation on that system—a particular pulse of radio waves, for instance, whose action might be to execute a quantum gate operation on the 50^{th} and 51^{st} qubits—would simultaneously operate on all the 2^{100} states. Hence in a single step, in one tick of the computer's clock, a quantum operation, unlike the serial computers, computes not just on one machine state, but on 2^{100} machine states at a given time. Eventually, however, the system would collapse to a single quantum state corresponding to a single answer, a single list of one hundred 1's and 0's, dictated by the fundamental measurement axiom of quantum mechanics [6]. This is an amazing observation as it showcases the inherent disparity between quantum and classical computers in computational matters as; what is achieved via the quantum parallelism of superposition by a primitive quantum computer of 100 qubits would require a classical super computer perform the operation simultaneously on $\sim 10^{30}$ distinct processors; a practically impossible feat.

With the clever usage of the properties of superposition, interference, entanglement, non-clonability and non-determinism, exhibited by all quantum systems, a new form of "quantum parallelism" seems to be achievable, wherein an exponential number of computational paths can be explored simultaneously as opposed to sequentially in a single device. The challenge remains in framing computational questions in a way so that the most useful and probabilistic answer is extracted. With the help of right algorithm, it is possible to use this parallelism to solve certain problems in a fraction of the total time taken by a classical computer. Such algorithms are notoriously difficult to formulate, and till date, the most significant examples are Shor's algorithm [4] and Grover's algorithm [7]. Shor's algorithm allows for the extremely quick factorization of large numbers, in polynomial time [4] as compared to exponential time required by classical computers, which in principle, means that in solving some problems, only quantum computers not conventional digital computers, can provide viable solutions.

The other epochal quantum algorithm is the search algorithm [7,8,10], since most of the computable problems in quantum computing can be transformed into the problem of finding the correct answer amongst all the probable possibilities. Taking advantage of the quantum parallelism, Grover's algorithm searches an unsorted database of N entries in $\sqrt{N}$ attempts, while a conventional computer would take an average of $N/2$ attempts. The discovery of the quantum error correction is as significant as the algorithms taking advantage of the quantum parallelism. In fact, the prospects for quantum computing technology would

have remained bleak but for the quantum error correction development. Another important aspect lies in the scaling issues related to quantum computing, which questions the limitations of the current technologies in quantum computing and hence derives continuous efforts towards newer, more reliable approaches. Even conforming to the current practical situation of restricting ourselves to the use of a small interacting molecular system, where only a small number of qubits are available for computation; we show that it is possible to achieve higher computational power provided that the computer systems, each consisting of only a few atoms or molecules acting as compute nodes are networked. Here we shall specifically explore the aspects of quantum distributed computing in light of the possible implementations of Grover's Algorithm.

2 Problem Statement

Grover's search algorithm shows that a quantum mechanical system needs at least $O(\sqrt{N})$ steps in order to identify a unique candidate satisfying a condition out of an unsorted dataset of N candidates [7,8]. This quadratic improvement is less optimal than the possible exponential improvement through quantum computing [6,9] as is seen, for example, in Shore's factorization algorithm [4], but is highly significant as the search problem is a universal necessity in quantum computing. Grover's subsequent work [10] concludes that one can overcome $O(\sqrt{N})$ bottleneck by making more elaborate queries, however, these increase the overhead in preparing and post-processing queries by $O(N \log_2 N)$ steps resulting in a decreased efficiency compared to classical situations.

In this paper, we present a distributed quantum computing approach wherein we propose to solve the classical search problem by performing the computation on all the nodes in the network, thereby providing a better lower bound on the resource usage of Grover's Algorithm. We show that though we are still restricted by the quadratic bound at best, we get more relaxed resource usage. This study is motivated primarily by the fact that at present, achieving a large qubit space is difficult, which is one of the basic bottlenecks for the effective implementation success of many of the proposed algorithms. Given that decoherence [11] is a major concern in quantum computing, the success of quantum teleportation [12] could be utilized as an effective approach towards scaling quantum computing power by establishing a network of smaller qubit space quantum computers and distributing the computing load. The required coherent transfer of information in the network could also benefit from recent developments in coherent optical networking schemes [13]. This network of quantum computers would virtually produce the required qubit space for the effective implementation of various algorithms [14]. Another advantage of such networking lies in the high security offered by quantum information processing [15].

3 Theoretical Model

Let us first outline the search problem and pose it mathematically to suit our quantum distribution needs. Given a database of N elements $(X_1X_2X_3...X_n)$

with exactly one element satisfying a condition (say the required element is X_k). Now there exists a function which knows that the element required is X_k but it functions like a black box answering queries only as high/low. More explicitly if asked whether X_i satisfies the condition it sets output signal high only if $X_i = X_k$ otherwise low. We will refer to such as element satisfying this condition as the qualified element. The problem is to get the high signal in the minimum number of queries. Classically, the optimal way is to ask questions that eliminate half the elements under consideration with each question resulting in approximately $\log_2 N$ queries to reach the answer [7,8].

In Grover's single query approach [10], he considered a quantum system composed of multiple subsystems where each subsystem has an N dimensional state and each basis state of a subsystem corresponds to an element in the database. An appropriate single quantum query, pertaining to information regarding all N elements, resulted in the probability of the state corresponding to the qualified element(s) of each subsystem being amplified by a small amount. This small difference in amplitudes was estimated by making a measurement to determine that the element of the database in each subsystem corresponds to the element indicated by the most subsystems is the qualified element, provided the number of subsystems was sufficiently large. The sole purpose was to amplify the probability of qualified element by performing unitary operations on the subsystems.

Let us now discuss our design of distributed quantum computing wherein we consider a network of quantum computers which can communicate through quantum teleportation. The individual computing nodes in the network function like subsystems as described in Grover's approach earlier. Let us amplify the probability of qualified element by sequence of unitary operations. We move ahead by first applying selective inversion and then performing inversion about selection operation.

Let us define the black box which answers the query as high/low (0/1) is a function $f(z)$ such that $f(z) = 1$ for qualified element, *i.e.*, X_k, otherwise $f(z) = 0$ for all X_i, where $i \neq k$. The work of Boyer *et. al.* [16] shows that there exists a quantum circuit such that state $|x, b\rangle$ can be converted to $|x, f(x) \oplus b\rangle$, and if bit 'b' is placed in superposition of $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, we keep intact the amplitudes of all elements but the qualified element. The amplitude of qualified element gets inverted. Next we apply inversion about average operator to amplify the probability of the qualified item. The inversion about average operation is by definition the unitary operation $D : D_{ij} = \frac{2}{N}$ if $i \neq j$; $D_{ii} = -1 + \frac{2}{N}$; where D can be shown to be physically implemented as a product of three local unitary matrices [8]. Assume that D is applied to a superposition with each element of the superposition having amplitude equal to $\frac{1}{\sqrt{N}}$, excepting one. Then, the single component that is different has an amplitude of -$\frac{1}{\sqrt{N}}$. After the unitary operation, the one that had the negative amplitude now becomes positive and its magnitude increases to approximately $\frac{3}{\sqrt{N}}$; while the rest stay unchanged. This would boost up the amplitude of the qualified element in each subsystem and we have sufficiently large number of identical subsystems (say total η such subsystems) to observe for which element the probability is higher. Each subsystem

has N dimensional state space and each of N basis states actually corresponds to an element in the database. Consider each subsystem to have equal amplitude in all N states. Thus the state vector for the system (which is a tensor product of these η identical subsystems) would be $(|S_1S_1S_1...S_1\rangle + |S_2S_2S_2...S_2\rangle + ...N^\eta$ such terms) if $S_1, S_2, ...S_N$ denote N states.

Let us now query the database: whether the number of subsystems in the state corresponding to the marked item is odd or even. If it is odd, the phase is left untouched otherwise it is inverted. This is selective inversion as discussed earlier. If S_k is the state which stands for the qualified element, we can write the state vector as $(|S_1\rangle + |S_2\rangle + ... + (-|S_k\rangle) + ... + |S_N\rangle)^\eta$. We then perform the inversion about average operation independently on each of subsystems to boost the amplitude of the qualified element. As we discussed before, inversion about average operation allows us to amplify the probability of the state in negative phase by a factor of 3 in the positive direction. Mathematically, therefore, we can represent the vector state as $(|S_1\rangle + |S_2\rangle + ... + (3|S_k\rangle) + ... + |S_N\rangle)^\eta$. We cycle these steps for n times.

4 Results and Discussions

We will now try different values of n to see when it reaches an optimum.

For a generalized case: After n such cycles, the state vector can be written as $(|S_1\rangle + |S_2\rangle + ... + ((2n+1)|S_k\rangle) + ... + |S_N\rangle)^\eta$. The probability of obtaining the basis state corresponding to the qualified element in each of the η subsystems is approximately $\frac{(2n+1)^2}{N}$ and the probability of obtaining a different basis state is approximately $\frac{1}{N}$. Thus, it follows by the law of large numbers [17] that out of η subsystems, $\frac{(2n+1)^2\eta}{N} \pm O(\frac{\sqrt{\eta}}{N})$ lie in state S_k. Assuming n to be large enough the equation is simplified to $\frac{4n^2\eta}{N} \pm O(\frac{\sqrt{\eta}}{N})$ and if we let $\eta = KN$, then the equation can be rewritten as $4n^2K \pm O(\sqrt{K})$. We can test the extreme values of 'n' for which the system will give an optimum value and hence provide both the upper and lower bounds.

For small size case, such as $n = \sqrt{\log_2 N}$: The state vector can be written as $(|S_1\rangle + |S_2\rangle + ... + (2\sqrt{\log_2 N} + 1)|S_k\rangle + ... + |S_N\rangle)^\eta$. The probability of obtaining the basis state corresponding to the marked state in each of the η subsystems is approximately $\frac{4\log_2 N}{N}$ and the probability of obtaining a different basis state is approximately $\frac{1}{N}$. Again it follows by the law of large numbers [17] that out of η subsystems, $4K\log_2 N \pm O(\sqrt{K})$ lie in state S_k, where $K = \frac{\eta}{N}$. In fact, it follows by the central limit theorem [18] that the probability of a particular variable deviating by more than $\pm\gamma\sqrt{K}$ from its expected value is less than $\exp[-O(\gamma^2)]$. Thus, if η is of the order of N then the equation becomes $4\log_2 N \pm O(1)$, which means that the overall effectiveness of the algorithm in this case has no improvement over the classical case.

It is important to note here that the value of n has to be less than $\frac{\sqrt{N}}{2}$ or else it will become a certain condition, with the probability reaching 1, thus all of the subsystems will be in the qualified state. Let us test this other limit now.

Testing the upper limit for $n = \frac{\sqrt{N}}{2}$: The state vector can be written as $(|S_1\rangle + |S_2\rangle + ... + (\sqrt{N}+1)|S_k\rangle + ... + |S_N\rangle)^{\eta}$. The probability of obtaining the basis state corresponding to the qualified state in each of the η subsystems is approximately 1 and the probability of obtaining a different basis state is approximately $\frac{1}{N}$. By the law of large numbers [17], therefore, it follows that out of η subsystems, $\eta \pm O(\frac{\sqrt{\eta}}{N})$ lie in state S_k. Typically, $\eta \ll N$, so the uncertainty due to $O(\frac{\sqrt{\eta}}{N})$ can be neglected. There will be post processing steps of the order $O(\sqrt{\eta})$. Thus, the overall effectiveness of the algorithm increases to $O(\sqrt{N})$, since $\eta \ll N$.

We have, therefore, managed to show that the distributed quantum computing approach essentially preserves the benefits of Grover?s search algorithm for big data problems while for small problems the situation converges to the limit of the classical case. Since the scaling issue is prevalent for large computing sizes, distributing the computing load over smaller quantum nodes is an important feasibility criterion related to the scaling issues in quantum computing.

5 Conclusions

We distributed the computational load of Grover's search algorithm over a quantum network, which is facilitated through ideal teleportation communications. Grover's single-query method carries a lot of overhead pertaining to the preparation and post-processing of the query $[O(N \log_2 N)$ steps]. Hence, we relax the single-query constraint in order to achieve more optimal performance, which is significantly better than classical methodology $[O(\log_2 N)]$. Essentially this extension of Grover's approach, being assisted by quantum-networking ideas is crucial for scaling the problem. We have managed to show that if we replicate Grover's algorithmic approach of amplifying the probability of the eligible candidate in database 'n' times, we are bound by $O(\sqrt{N})$ for a much improved upper limit of n $(n = \frac{\sqrt{N}}{2})$ though the lower bound is an unchanged classical case of $O(N)$ for small n. However, since we would only be distributing the computing load for a large enough data-size, the advantages are evident. Furthermore, our approach addresses and substantially dilutes the practical concern regarding the limited qubit space associated with one quantum computer. Hence it should be seen as a promising computing framework. These results also provide substantial encouragement and impetus for scaling quantum computation by coupling quantum teleportation of multiple small quantum computer nodes.

Acknowledgments. Funds for this research were available from the ISRO STC Funding and Ministry of Human Resource Development (Govt. of India). DG thanks the efforts put in by Devesh Tewari during his BTP project. DG is grateful to S. Goswami and R. Goswami for help with manuscript language editing. DG is highly indebted to the constant support and encouragement from Prof. Gruska for pursing research and teaching in quantum information processing.

References

1. Gruska, J.: Foundations of Computing, ITCP Computer Science Series: (International Thomson Computer Press), 716 pages (1997)
2. Feynman, R.P.: Int. J. Theor. Physics **21**, 467 (1982)
3. Deutsch, D.: Proc. Roy. Soc. London **97**, 400 (1985)
4. Shor, P.W.: Proceedings of the Symposium on the Foundations of Computer Science: Los Alamos, California, pp. 124–134. IEEE Computer Society Press, New York (1994)
5. Bell, J.S.: The Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press (1987)
6. Nielsen, M.A., Chuang, I.L.: Quantum Computing and Quantum Information. Cambridge University Press, Cambridge (2000)
7. Grover, L.K.: Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing: Philadelphia, Pennsylvania, pp. 212–218. ACM Press, New York (1996)
8. Grover, L.K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack. Phys. Rev. Letters, 325–328 (1997)
9. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.: SIAM J. Computing, 1510–1524 (1997)
10. Grover, L.K.: Quantum Computers Can Search Arbitrarily Large Databases by a Single Query. Phys. Rev. Letters, 4709 (1997)
11. Goswami, D.: Laser Phase Modulation Approaches towards Ensemble Quantum Computing. Phys. Rev. Letters, 177901 (2002)
12. Gottesman, D., Chuang, I.L.: Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature, 390–393 (1999)
13. Sinha, M., Goswami, D.: System and method for improved coherent pulsed communication system having spectrally shaped pulses. US Patent (2004) US2004/0208613 A1 (October 21, 2004)
14. Schuch, N., Siewert, J.: Programmable Networks for Quantum Algorithms. Phys. Rev. Letters, 027902 (2003)
15. Miranowicz, A., Tamaki, K.: An Introduction to Quantum Teleportation. Math. Sciences, 28–34 (2002)
16. Boyer, M., Brassard, G., Hyer, P., Tapp, A.: Proceedings of 4th Workshop on Physics and Computation, Boston, MA, pp. 36–43 (1996)
17. Feller, W.: An Introduction to Probability Theory and Its Applications, vols. I and II. John Wiley, New York (1971),
18. Knuth, D.E.: Fundamentals of Algorithms: The Art of Computer Programming. Addison-Wesley, Reading(1973)