Quantum Physics Letters
An International Journal

http://dx.doi.org/10.18576/qpl/060203

A Simple Quantum Algorithm for Exponentially Fast Target Searching in the Unstructured Database

Dhananjay P. Mehendale[*]

Department of Physics, Savitribai Phule University of Pune, Pune, India-411007.

Received: 12 Apr. 2017, Revised: 2 Jun. 2017, Accepted: 16 Jun. 2017
Published online: 1 Aug. 2017

Abstract: We present an exponentially fast simple quantum algorithm for searching the unknown target in the unstructured database. This algorithm provides an eloquent example that clearly demonstrates the enormous advantage of quantum parallalism. The main idea behind achieving exponential speedup for this new quantum algorithm over Grover's quantum algorithm is actually very simple. The idea consists of simultaneously employing $(n/2)$ oracles or black-box functions instead of utilizing only one oracle or black-box function as is done by Grover's quantum algorithm for searching the target in the unordered data set of size $N = 2^n$. We show that we can attain the (explicitly unknown) target in the unstructured database of size $N = 2^n$ by giving in parallel only one call, simultaneously and independently, to appropriately defined $(n/2)$ oracles or black-box functions to be implemented using a quantum computer. The essential idea is to decompose the operation to be done on entire quantum system into $(n/2)$ operations to be carried out in parallel, simultaneously and separately, on individual components of the system and thus to achieve enormous speedup in obtaining the desired target from the unstructured data set of size $N = 2^n$ which is indeed amazing.

Keywords: Unstructured database search, Quantum parallelism, Multiple number of Oracles

1 Introduction

We present an exponentially fast quantum method to be worked on a quantum computer for solving unstructured search problems. We make use of following definition about the action of the *product* operator.

Let A and B be the *operators* from vector spaces V and W respectively into a vector space U, say. Then the action of the *product operator* $A \otimes B$ on *product space* $V \otimes W$ is defined by

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle.$$

where $|v\rangle \varepsilon V$ and $|w\rangle \varepsilon W$.

To generalize, let $A_i, i = 1, 2, \cdots, n$ be the *operators* from vector spaces $V_i, i = 1, 2, \cdots, n$ respectively into vector space U, say. Then the action of the *product operator* $A_1 \otimes A_2 \otimes \cdots \otimes A_n$ on the *product space* $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ is defined by

$$(\prod_{i=1}^{\otimes n} A_i)(\prod_{i=1}^{\otimes n} |v_i\rangle) = (\prod_{i=1}^{\otimes n} A_i|v_i\rangle)$$

where $|v_i\rangle \varepsilon V_i$ for all $i = 1, 2, \cdots, n$.

This definition which appears very natural is at the heart of our algorithm. This important definition allows us to decompose an operation on an entire quantum system into operations on individual components which not only makes the construction of our quantum algorithm much simpler but also causes the exponential rise in its speed.

The problem of searching in an unstructured database can be described through following simple example. Suppose we are given an address book of N names, and we wish to find and contact one individual in the book. Classically, the obvious algorithm to employ is to search from the beginning of the book to the end. We will need to browse through at least $(N/2)$ entries to have 50 percent chance of finding the one we want. In other words, the algorithm takes $O(N)$ operations. One knows that on a quantum computer one can do better by making use of Grover's quantum algorithm [2] which searches an N-object unsorted database for the desired object in $O(\sqrt{N})$ operations, offering a quadratic speedup over its classical counterpart. We propose a new quantum algorithm in this paper which searches an N-object unsorted database for the desired object (target) in just *one operation* and thus offers an exponential speedup

[*] Corresponding author e-mail: dhananjay.p.mehendale@gmail.com

over its classical and quantum (Grover's quantum algorithm) counterparts. Thus, the algorithm proposed in this paper performs search over an unordered data set of size $N = 2^n$ items to find the unique element that satisfies some condition in a single computational step for which the well known classical algorithm requires $O(N)$ steps and Grover's quantum algorithm requires $O(\sqrt{N})$ steps.

2 The Unstructured Search Problem and the Oracle or Black-box function

Consider unordered data set containing $N = 2^n$ items and suppose these items are labelled by indices, x, in the range $0 \leq x \leq N-1$, and that the index of the sought after target is $x = t$. In the classical unstructured search problem we are given a bag of indices, x, and we have to repeatedly dip into this bag, pluck out an index, and ask the so called oracle whether or not this is the target index t. If it is, we stop. If not, we put the index back in the bag (replacement step) and repeat the process. Let us express this classical procedure in quantum mechanical language: a quantum analog of the bag of indices is equally weighted superposition of computational basis states, $|x\rangle$, i.e. $\frac{1}{\sqrt{N}}\sum_{x=1}^{N}|x\rangle$ and a quantum analog of plucking out an index, at random, is reading this superposition state in the index basis which will give us a particular index state, $|x\rangle$ say, and then we will input this $|x\rangle$ to the so called oracle to find out whether or not $|x\rangle = |t\rangle$. Note that since $N = 2^n$ we can express every state in the index basis i.e. $|x\rangle$, using $n = \log_2 N$ qubits and the above mentioned equally weighted superposition state can be easily prepared by applying a separate 1-qubit Hadamard gate H on each of n qubits prepared initially in the state $|0\rangle$, thus $H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=1}^{N}|x\rangle$. When we read this equally weighted superposition we will get a single index nondeterministically, mimicking the classical generate and test procedure which will attain the target in $O(N)$ steps. As stated above, Grover's quantum algorithm [2] has better performence and it attains the target in $O(\sqrt{N})$ steps. Thus, Grover's quantum algorithm achieves *quadratic speedup* over the classical algorithm. C. Zalka [3] has shown that Grover's quantum algorithm is *optimal*. What does this mean? It means that any other quantum algorithm for performing unstructured quantum search *must call the oracle at least as many times as is done by Grover's algorithm*. Can *something else* be done to improve the speed of searching the target in the unstructured database? How about calling a number of oracles simultaneously? We show that fortunately this simple trick of *simultaneously calling sufficiently many oracles* works excellently.

An oracle is basically a black-box function, denoted as $f_t(x)$, where x is any general element in the domain (index set) and t is the target element to be searched in the domain, and when $f_t(x)$ is presented with an index x it can pronounce on whether or not it is the index of the target. Specifically, $f_t(x)$ is defined thus: $f_t(x) = 1$ if $x = t$ and $f_t(x) = 0$ otherwise. A quantum oracle is a quantum black-box function, meaning it can observe and modify the system without collapsing it to a classical state, that will recognize if the system is in correct state. If the system is indeed in the correct state then the operator representing the oracle in effect will rotate the phase of this (correct) state by π radians, and otherwise this quantum oracle will do nothing, effectively *marking* the correct state for further modification by subsequent operations. We note that such a phase shift leaves the probability of the system being in correct state the same.

The quantum algorithm that we propose here defines and makes use of $(n/2)$ oracles or black-box functions, and we present to them indices, x, from index set $\{0,1,2,3\}$ and out of these indices from index set some one predefined index, T_i, will be the target element. Thus, we define $(n/2)$ oracles or black-box functions, $f_{T_1}, f_{T_2}, \cdots, f_{T_{(n/2)}}$ like the one that is defined and used in Grover's quantum algorithm such that $f_{T_i}(x) = 1$ if $x = T_i$ and $f_{T_i}(x) = 0$ otherwise, where $i = 1,2,\cdots,(n/2)$. As was done in Grover's quantum algorithm [2] we use these oracles to create *phase inversion operators*, O_i, $i = 1,2,\cdots,(n/2)$, whose actions on the correct states will cause the phase inversion of those correct states. To create these phase inversion operators, O_i, $i = 1,2,\cdots,(n/2)$, we introduce in all $(n/2)$ ancillae qubits, one for each phase inversion operator, and create in all $(n/2)$ 3− qubit unitary transformations

$$\omega_{f_{T_i}} : \omega_{f_{T_i}}|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_{T_i}(x)\rangle,$$

for some duely defined $(n/2)$ target states $|T_i\rangle$, $i = 1,2,\cdots,(n/2)$, where $|x\rangle \; \varepsilon \; \{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, and we take

$$|y\rangle = H|1\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle].$$

We can now easily check that

$$\omega_{f_{T_i}}|x\rangle|y\rangle = (-1)^{f_{T_i}(x)}|x\rangle|y\rangle$$

when the ancilla qubit $|y\rangle$ is as given above. Thus all the ancilla qubits remain unaffected and we can ignore them all in our calculations and simply create the operators $O_i, i = 1,2,\ldots(n/2)$, acting on elements, $|x\rangle$, where $|x\rangle \; \varepsilon \; \{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, and their action can be depicted as

$$O_i|x\rangle = (-1)^{f_{T_i(x)}}|x\rangle = (I - 2|T_i\rangle\langle T_i|)|x\rangle$$

where I represents *identity operator* and these operators perform the same action as that of these oracles or black-box functions, namely, $O_i(|x\rangle) = -|x\rangle$ if $|x\rangle = |T_i\rangle$ and $O_i(|x\rangle) = |x\rangle$ otherwise, where $|x\rangle \; \varepsilon \; \{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$.

With these preliminaries we now proceed to discuss our exponentially fast quantum algorithm to pick out the desired item from an unordered data set containing $N = 2^n$ items.

3 Algorithm

We begin our algorithm by simultaneously giving call to $(n/2)$ oracles that will modify the system depending on whether or not it is in the correct configaration that we are searching for.

We now proceed with the steps of the algorithm:

(i)Let $D=\{0,1,2,\cdots,N-1\}$ be the given unordered data set containing $N=2^n$ items labeled by numbers $0,1,2,\cdots,N-1$ and let item labeled by label t be our target item which we want to find out from the set. We associate quantum states, which are computational basis states, with these items. Thus we represent item labeled by number 0 by computational basis state $|00\cdots0\rangle$, the item labeled by number 1 by computational basis state $|00\cdots1\rangle$, $\cdots$, the item labeled by number $(N-1)$ by computational basis state $|11\cdots1\rangle$. Clearly, all these computational basis states associated with items have length equal to n.

(ii)We prepare a quantum state, $|\psi\rangle$, which is equally weighted superposition of all computational basis states associated with the items as mentioned above. This equally weighted superposition state represents the unstructured set of items. Thus:

$$|\psi\rangle=\frac{1}{\sqrt{N}}\sum_{i_1,i_2,\ldots i_n}|i_1i_2\ldots i_n\rangle,$$

where each of $i_1,i_2\ldots,i_n$ takes values in $\{0,1\}$. This superposition state represents a quantum register of n qubits where n is the number of qubits that are necessary to represent the entire search space of size $N=2^n$. Thus, the quantum state $|\psi\rangle$ representing quantum bag containing N items out of which any computational basis state will result as an outcome of measurement (i.e. all computational basis states are equally probable as an outcome of measurement), therefore, this state $|\psi\rangle$ correctly represents the unordered set of items.

Now, let us emphasize a very simple but important fact useful for our algorithm. This fact is that the above quantum state $|\psi\rangle$ can be obtained as follows:

$$|\psi\rangle=H^{\otimes n}|0\rangle^{\otimes n}=\prod^{\otimes n}(\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]).$$

Thus, $|\psi\rangle$ is a *Completely Separable* state having n single qubit identical factors, each equal to $|\phi\rangle=\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]$. Once we understand the completely separable nature of the quantum state $|\psi\rangle$ representing the unordered set of items it follows that we can infact give any suitable form to this state, since *tensor product is associative*. For example, we can express $|\psi\rangle$ as

$$|\psi\rangle=(\prod^{\otimes r_1}|\phi\rangle)\otimes(\prod^{\otimes r_2}|\phi\rangle)\otimes\cdots\otimes(\prod^{\otimes r_k}|\phi\rangle)$$

where $r_1,r_2,\cdots,r_k$ are some positive integers such that $r_1+r_2+\cdots+r_k=n$. We call such representation in terms of suitable factors the *tensor product representation* for the quantum state $|\psi\rangle$ representing quantum bag of data.

(iii)We choose the following simple tensor product representation for the quantum state $|\psi\rangle$ representing the unordered data set of items in which we choose $r_1=r_2=\cdots=r_k=2$, and we assume without any loss of generality that n is an even number. Therefore, we have

$$|\psi\rangle=(\prod^{\otimes(n/2)}|\Theta\rangle)$$

where $|\Theta\rangle=\frac{1}{2}[|00\rangle+|01\rangle+|10\rangle+|11\rangle]$.

(iv)Let the target state be $|t\rangle=|t_1t_2\cdots t_n\rangle=|t_1t_2\rangle|t_3t_4\rangle\cdots|t_{n-1}t_n\rangle$. We put $|T_k\rangle=|t_{2k-1}t_{2k}\rangle$. Thus, we can denote target state by $|t\rangle=|T_1T_2\cdots T_{(n/2)}\rangle=|T_1\rangle|T_2\rangle\cdots|T_{(n/2)}\rangle$.

We define $(n/2)$ unitary quantum operators, $O_i=I-2|T_i\rangle\langle T_i|$ and as discussed above they do the job of the oracles and the action of the oracles can be depicted simply in terms of the action of these operators, O_i, operating on the 2-qubit elements, $|x\rangle$, where $|x\rangle\ \varepsilon\ \{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, such that $O_i(|x\rangle)=(-1)^{f_{T_i}(x)}|x\rangle=(I-2|T_i\rangle\langle T_i|)|x\rangle$. Note that

$$O_i|x\rangle=(I-2|T_i\rangle\langle T_i|)|x\rangle=-|x\rangle$$

if $x=T_i$ and

$$O|x\rangle=(I-2|T_i\rangle\langle T_i|)|x\rangle=|x\rangle$$

if $x\neq T_i$.

(v)Our next step is to create $(n/2)$ identical operators W, the so called *Diffusion Transforms*, all equal to $[2|\Theta\rangle\langle\Theta|-I]$. Then we prepare the product operator, $P=(\prod^{\otimes(n/2)}(WO_i))$ and operate this product operator on $|\psi\rangle=(\prod^{\otimes(n/2)}|\Theta\rangle)$. We carry out this final operation in parallel. This action will lead us to the desired target state in a single step. Thus,

$$\begin{aligned}P|\psi\rangle&=(\prod_{i=1}^{\otimes(n/2)}(WO_i))(\prod^{\otimes(n/2)}|\Theta\rangle)\\&=(\prod_{i=1}^{\otimes(n/2)}(WO_i|\Theta\rangle))\\&=(\prod_{i=1}^{\otimes(n/2)}(|T_i\rangle))=|t\rangle.\end{aligned}$$

The desired target state is thus obtained in this single operation.

4 A Remark

Speeding up solutions of NP-complete problems For solving Hamiltonian cycle (HC) problem ([1], page 264), best classical algorithm requires $O(p(n)2^{n[log(n)]})$

operations, Grover's quantum algorithm requires $O(p(n)2^{n[log(n)]/2})$ operations, while our quantum algorithm will require only $O(p(n))$ operations where $p(n)$ is the polynomial factor. The dominant effect in determining the resources required is the exponent in $2^{n[log(n)]}$ or $2^{n[log(n)]/2}$.

5 An example

Suppose we are given an unordered database in terms of $2^{10} = 1024$ labeled items kept inside a bag and items are labeled by numbers $0, 1, 2, \cdots 1023$. Our aim is to pick out item labeled by number 727. We solve quantum version of this problem using our new quantum algorithm.

(1)We prepare quantum bag in terms of quantum state

$$|\psi\rangle = \frac{1}{\sqrt{2^{10}}} \sum_{i_1, i_2, \dots, i_{10}} |i_1 i_2 \dots i_{10}\rangle,$$

where each of $i_1, i_2 \dots, i_{10}$ takes values in $\{0, 1\}$.

(2)The target item is labeled by number $(727)_{10} = (1011010111)_2$.

(3)The target state is $|t\rangle = |1011010111\rangle = |10\rangle|11\rangle|01\rangle|01\rangle|11\rangle$.

(4)We construct the operators, $O_i, i = 1, 2, \cdots, 5$ representing $(n/2) = 5$ oracles, namely, $O_1 = I - 2|10\rangle\langle 10|$, $O_2 = I - 2|11\rangle\langle 11|$, $O_3 = I - 2|01\rangle\langle 01|$, $O_4 = I - 2|01\rangle\langle 01|$, $O_5 = I - 2|11\rangle\langle 11|$, and take five identical diffusion transforms $W = [2|\Theta\rangle\langle\Theta| - I]$, where $|\Theta\rangle = \frac{1}{2}[|00\rangle + |01\rangle + |10\rangle + |11\rangle]$.

(5)We create the product operator, $P = (\prod_{i=1}^{\otimes(5)} (WO_i))$ and operate this product operator on $|\psi\rangle = (\prod^{\otimes(5)} |\Theta\rangle)$. This gives rise to state

$$(\prod_{i=1}^{\otimes(5)} (WO_i|\Theta\rangle)) = |10\rangle \otimes |11\rangle \otimes |01\rangle \otimes |01\rangle \otimes |11\rangle = |t\rangle,$$

the desired target state.

Note that best classical algorithm in the worst case will require 1024 iterations, Grover's quantum algorithm [2] will require 32 iterations, while our new quantum algorithm requires just *one* iteration.

Acknowledgement

I thank Dr. M. R. Modak, S. P. College, Pune-411030, India, for carefully reading the mannuscript and making useful comments and suggestions.

References

[1] Nielsen A and Chuang I *Quantum Computation and Quantum Information*(Cambridge : Cambridge university Press) (2000)

[2] Grover L.K. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing,ACM Press, New York, pp 212-219, (1996).

[3] C. Zalka, Phys. Rev. A. Volume 60, Issue 4, pp 2746-2751, (1999).

Dhananjay P. Mehendale, served as associate professor in S. P. College, affiliated to Savitribai Phule University of Pune, Pune, India-411007. The subjects of his interest and study are Physics, Mathematics, and Engineering and students of science and engineering have successfully completed their project work under his supervision. He taught various courses in Physics, Electronic Science, and Computer Science departments, and has done research in various areas of these subjects. He worked on various science and engineering projects and one of his projects won award in the national science projects competition organized by Department of Science and Technology. His research interest at present is topics in Quantum Computation and Quantum Information.