Overview of the quantum search algorithm

K. Huggins[1]
[1] *Department of Physics, Texas A&M University, College Station TX 77840*

(Dated: April 20, 2010)

The quantum search algorithm, first posed by Grover in 1997 is investigated along with the basic science behind the development of the algorithm's properties. An investigation of the speed of the algorithm versus the classical approach highlights the benefits of a quantum approach to the search of an unsorted database. A detailed look at why the algorithm works as well as implementation is investigated.

PACS numbers: unknown.

I. INTRODUCTION

An unsorted database containing N records has only one object which satisfies a particular property. A classical approach would clearly require O(N) queries before the correct object is found. Under a quantum mechanical approach, first crafted by Grover[1], we are able to find the object in just O($\sqrt{N}$) steps. This is due in part because a quantum mechanical system can perform several operations simultaneously.

The inherent effects generated under a quantum system can generate increases in efficiency of algorithms typically deemed out of reach by modern computers. The genesis of quantum computing formed under the guidance of Benioff and Deutsch[2-4] through the early 80's and 90's. The framework delineated that quantum machines could be faster than their classical analogue. Shor[5] illustrated how a quantum algorithm could factor a prime in time $O(logN)$, a vast improvement and unambiguous evidence of the power of quantum mechanics. Then Grover in 1997 formulated an algorithm which could locate an object in $O(\sqrt{N})$ steps.

Given a superposition of $N = 2^n$ states of quantum bits, the bits are considered "entangled" and any operation on the superposition of states can impact the individual states in one step. However, further research has shown that entanglement may not be exclusively necessary[6]. The first section of this paper covers Grover's algorithm and works out some examples. The next section details the proofs behind the various operations, confirming it as a truly quantum mechanical speedup. The last section will examine applications of the algorithm in physical systems.

II. GROVER'S ALGORITHM

A succinct explanation of Grover's algorithm is in order. We let a system have $N = 2^n$ states which are labeled $a_1, a_2, a_3, ...a_N$. These 2^n states are represented as n bit strings. Let there be a state w that satisfies $f(w) = 1$ and all other $f(a) = 0$. The goal is to identify the state w.

A. Algorithm

(i) Initialize the system to a distribution of equal probability amplitude: $|s\rangle = \frac{1}{\sqrt{N}} \sum_N |a\rangle$.
(ii) Repeat the following unitary operations $O(\sqrt{N})$ times:
(a) Apply the operator $U_f = (-1)^{f(a)}|a\rangle$.
(b) Apply the operator $U_s = 2|s\rangle\langle s| - 1$
(iii) Sample the resulting state. In case there is a unique state w such that $f(w) = 1$, the final state is w with a probability of at least $\frac{1}{2}$.

B. Example

In order to clearly outline how this series of operations will yield us the correct state, we run through an example of $N = 4$ states. Preparing the state $|s\rangle$ such that it each state in the superposition is of equal amplitude

$$|s\rangle = \frac{1}{2}\sum_{a=1}^{4} |a\rangle$$

This could be a string of binary bits, a series of 0s or 1s or both. To implement such an algorithm, we must use the operator U_f to "flip" a bit whose state $|w\rangle$ we are trying to find.

$$U_f|s\rangle = \frac{1}{2}(|\alpha\rangle - |w\rangle$$

where $|\alpha\rangle = \sum_{a\neq w}^{4} |a\rangle$. Our target state's sign is flipped by this operation. This will shift the phase of a bit in the state w yet preserve the amplitude of all the states. We then want to use the U_s to single out the $|w\rangle$ state. Applying U_s yields

$$U_sU_f|s\rangle = |s\rangle\langle s|[\alpha - |w\rangle] - \frac{1}{2}[\alpha - |w\rangle]$$

$$= \frac{2}{4}|s\rangle - \frac{1}{2}[\alpha - |w\rangle]$$

$$= |w\rangle$$

After one application, the probability of our target state being found is 1. We realize that for a 2^2 bit system we can find the desired state exactly with only one application of our algorithm.

C. Example 2

One might suppose that the previous example led to a particularly elegant result; however, the result is unique to the 4 state system. We shall work out an example for $N = 2^4$ states to illustrate more generally the behavior of the algorithm. Again, we set up the problem to find the state w by applying U_sU_f to $|s\rangle$:

$$U_sU_f = [2|s\rangle\langle s| - 1]\frac{1}{4}[|\alpha\rangle - |w\rangle]$$

$$= \frac{14}{8}|s\rangle - \frac{1}{4}[|\alpha\rangle - |w\rangle]$$

$$= \frac{1}{16}[3|\alpha\rangle + 11|w\rangle]$$

where we have again set the sum of every state excluding $|w\rangle$ to $|\alpha\rangle$. After one application, the probability of our target state being found is .47. So we apply it again.

$$[2|s\rangle\langle s| - 1]\frac{1}{16}[3|\alpha\rangle - 11|w\rangle]$$

$$\frac{17}{64}[|\alpha\rangle + |w\rangle] - \frac{4}{64}[3|\alpha\rangle - 11|w\rangle]$$

$$\frac{1}{64}[5|\alpha\rangle + 61|w\rangle]$$

A second application results in the probability of $|w\rangle$ increasing to .9. Since we're doing so great, let's apply it again

$$[2|s\rangle\langle s| - 1]\frac{1}{64}[5|\alpha\rangle - 61|w\rangle]$$

$$\frac{7}{256}[|\alpha\rangle + |w\rangle] - \frac{4}{256}[5|\alpha\rangle - 61|w\rangle]$$

$$\frac{1}{256}[-13|\alpha\rangle + 251|w\rangle]$$

After 3 applications, a measurement of $|s\rangle$ will obtain the desired state with a probability of .96. However, we do not necessarily get better probability with further applications of U_sU_f

$$(U_sU_f)^4|s\rangle = 2|s\rangle\langle s| - 1]\frac{1}{256}[-13|\alpha\rangle - 251|w\rangle]$$

$$= -\frac{223}{1024}[|\alpha\rangle + |w\rangle] - \frac{4}{1024}[-13|\alpha\rangle - 251|w\rangle]$$

$$= \frac{1}{1024}[-171|\alpha\rangle + 781|w\rangle]$$

Here we see that the probability of $|w\rangle$ has decreased to .58. So arbitrarily applying the operator more and more does not yield results approaching unity. In fact, we shall illustrate within this paper that the probability of obtaining the desired state will oscillate between high and low probability.

III. PROOFS

What is this U_s operator? Grover terms it the diffusion transform which is defined as such: $D_{ij} = \frac{2}{N}$ if $i \neq j$ & $D_{ii} = -1 + \frac{2}{N}$. We can write this matrix in operator form by noting that $\langle s|s\rangle = \frac{1}{N}$, so $2\langle s|s\rangle = \frac{2}{N}$. And -1 along the diagonal is just the unitary matrix, yielding $D = 2|s\rangle\langle s| - 1 = U_s$. However, the matrix we defined is not a local transition matrix since we are transitioning from each state to all N states. But we can implement D as a product of three unitary transformations. Consider a system with 2^n possible states. If the initial configuration was the configuration with all n bits in the first state, the configuration will have an identical amplitude of $2^{-\frac{n}{2}}$ in each of the 2^n states. Thus we create a distribution with all the same amplitude. But if the starting case is described by an n bit binary string with some 0s and 1s, the result of performing the transformation M on each bit will be a superposition of states described by all possible n bit binary string with amplitude of each state having an amplitude of $2^{-\frac{n}{2}}$ and either $+$ or $-$ sign. In order to determine the sign, we note that the transition matrix M for a single bit system

$$M = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

changes the phase of the configuration when a bit that was previously a 1 remains a 1 after the transformation is performed. So if x is the $n-$bit binary string describing the starting state and if y is the $n-$bit string describing the final state, then the sign of the amplitude of y is determined by the parity of the bitwise dot product of x and y; $(-1)^{x\cdot y}$. This is commonly referred to as the Fourier transformation. Using this transformation F, along with a rotational transform R, we can say $D = FRF$.

Theorem 1 - The operator U_s is unitary.

For an operator to be unitary, it multiplied by its adjoint should equal unity. Thus $U_s^*U_s = 1$. Using the form of U_s listed above, its adjoint is clearly just U_s. Then,

$$(2|s\rangle\langle s| - 1)(2|s\rangle\langle s| - 1)$$

$$4|s\rangle\langle s| - 2|s\rangle\langle s| - 2|s\rangle\langle s| + 1 = 1$$

Theorem 2 - The time required to find the state is $\frac{\pi\sqrt{N}}{4}$ for N states.

Where does O($\sqrt{N}$) growth rate come from? Farhi and Gutnamn[7] elegantly lay out a proof for the dependence. One can derive the growth rate by taking a function f(a) with a=1,...,N such that f(w)=1 and f(a)=0 for a≠w. We must locate w using Grover's algorithm. Take a vector space that has an orthonormal basis $|a\rangle$. A quantum computer could implement the unitary transformations $U_f = 1 - 2|w\rangle\langle w|$ and $U_s = 2|s\rangle\langle s| - 1$ as outlined above. Now we can also have the vector of states

$$|s\rangle = \frac{1}{N^{\frac{1}{2}}} \sum_a |a\rangle$$

The Grover Algorithm will let $U_s U_f$ act k times on the vector $|s\rangle$. Investigating what happens after apply the operators, we consider the two-dimensional subspace spanned by $|s\rangle$ and $|w\rangle$. We let

$$|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{a \neq w} |a\rangle$$

This implies that $|w\rangle$ and $|r\rangle$ form an orthonormal basis. The $U_s U_f$ operator then takes the form within the $|w\rangle$,$|r\rangle$ basis of

$$U_s U_f = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

with $\cos\theta = 1 - \frac{2}{N}$. This effectively parallels a rotation towards the $|w\rangle$ state. This is only one iteration, though. For more precision, we should apply this operator k times, which yields

$$(U_s U_f)^k = \begin{bmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{bmatrix}.$$

Given N large then $\theta \propto 2N^{\frac{-1}{2}}$ so each application of $U_s U_f$ is a rotation by an angle $\propto 2N^{-\frac{1}{2}}$. Then, in the $|w\rangle$,$|r\rangle$ basis, the initial state $|s\rangle$ is

$$|s\rangle = \begin{bmatrix} N^{-\frac{1}{2}} \\ (1 - \frac{1}{N})^{\frac{1}{2}} \end{bmatrix}$$

which is close to $|r\rangle$. However, after k steps where $k\theta \approx \frac{\pi}{2}$ the algorithm has rotated the initial state to lie along $|w\rangle$. This takes $k \propto \frac{\pi N^{\frac{1}{2}}}{4}$ steps. But since each step actually requires two evaluations of f, the number of evaluations on f required to find w grows like $N^{\frac{1}{2}}$.

IV. IMPLEMENTATION

The challenge behind implementing this algorithm lies in key elements outlined in [8]. It's noted that in order for a physical system to function, the qbits must interact very weakly with the environment yet strongly with each other. Also, the system must be initialized and read out with high efficiency, *i.e.*, the system must be prepared and measured as quickly as possible to optimize the time it takes from beginning to end. Scaling becomes an issue, as increasing the number of qbits produces more decoherence and can destroy the system.

However, a coherent quantum computer can be produced by using a mixed-state ensemble rather than a pure system of qbits by using quantum spins[9]. Chuang demonstrated in [10] that by using NMR analysis, implementation of Grover's algorithm is possible for $N = 4$ states. Under their experiment, a solution of chloroform molecules are used as the quantum ensemble and the spins of the atoms indicated their 0 or 1 configuration. NMR then allows them to test the spins of the state, whereby a weak measurement yields the value of the system. Under this ensemble, Chuang demonstrated that application of the Grover algorithm is possible.

In [6] it was demonstrated that application of entanglement is not necessary for use of the algorithm. Under their framework, a lattice of atoms are prepared, with each lattice connected to a detector. Each $N-1$ lattice is prepared in the $|s\rangle$ state and one lattice, our target state, is prepared in the $|n\rangle$ state. State $|n\rangle$ can be excited to the $|e\rangle$ state while the rest of $|s\rangle$, due to selection rules, cannot be promoted. An incident laser probe excites $|n\rangle$ to $|e\rangle$ and the detector tied to that lattice registers the decay of that excited state, finding the target state. Under a classical framework, the laser probe excites each lattice in turn, finding the target state in $\frac{N}{2}$ attempts. Using quantum coherence to create a superposition of states by widening the laser probe to encompass the entire array would excite the desired state weakly within a superposition of all the states. Thus, the desired state would be found after $\sqrt(N)$ probes.

V. CONCLUSION

Under a quantum framework, searching a database can take less than the classical limit. Grover's algorithm utilizes the superposition principle inherent in quantum mechanics to allow for the application of one operator on a system of states, rather than applying it to each state individually. This quantum speedup produces the target state in $O(\sqrt(N))$ tries. We outlined that implementation of this system poses challenges, from decoherence in setting up a pure state of trapped ions with large N, to accurately measuring the resultant state in an optimum timeframe. However, implementing this algorithm is within physical means of today's technology, and merits pursuit.

VI. ACKNOWLEDGMENTS

I would like to thank Dr. Zubairy for his support and critique in the writing of this paper.

[1] L. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation* (ACM Press, New York, 1996), pp. 212-219.

[2] P. Benioff, *Journal of Stat. Phys*, 22, pp. 563-591

[3] D. Deutsch, R. Jozsa, *Proc. Math. and Phys. Sci.* (Royal Society), Vol. 439, No. 1907 (Dec. 8, 1992), pp. 553-558.

[4] D. Deutsch, *Proc. Royal Society of London*, Ser. A, 400, pp. 96-117.

[5] P. W. Shor, *Proc. 35th Annual Symposium on Fundamentals of Computer Science*, 1994, pp. 116-123.

[6] M. O. Scully, M. S. Zubairy, Phys. Rev. A, **64**, 022304 (2001).

[7] E. Farhi, S. Gutmann, Phys. Rev. A **57**, 4 (1998).

[8] G. Brassard, I. L. Chuang, S. Lloyd, C. Monroe, in *Proc. Natl. Acad. Sci. USA* (ACM Press, New York 1998), Vol. 95, pp. 11032-11033.

[9] N. Gershenfeld, I. L. Chuang, Science **275**, 350 (1997).

[10] I. L. Chuang, N. Gershenfeld, M. Kubinec, Phys. Rev. Lett. **80**, 15 (1998)