Neural, Parallel, and Scientific Computations 20 (2012) 65-80

ON QUANTUM COMPUTATION OF STATISTICAL MEAN USING GROVER'S ALGORITHM

PIJUSH KUMAR KOLEY[1] AND SRIMANTA PAL[2]

[1]Department of Instrumentation Engineering
Jadavpur University, Salt Lake Campus, Kolkata, India
[2]Electronics and Communication Sciences Unit, Indian Statistical Institute
203 B T Road, Kolkata 700 108, India

ABSTRACT. Grover proposed an algorithm for the quantum computation of statistical mean. This algorithm has a complexity of $O\left(\frac{1}{\nu}\right)$ where ν is the error limit. In this paper we study this algorithm. First we prove the correctness of Grover's philosophy for computation of mean. Also we observe some errors in the mean estimation step. We then propose a modification of this estimation step by introducing a new unitary operator. The correctness of the modified algorithm is proved and numerical examples are included to illustrate Grover's algorithm and the proposed modification. The proposed algorithm uses a much simpler unitary operator than Grover's original algorithm.

AMS (MOS) Subject Classification. 68M15, 94C12

1. **Introduction**

Feynman observed that simulation of a quantum mechanical system on an ordinary computer would entail an exponential slowdown in the efficiency (Feynman, 1982). Feynman (1986) wrote *"But the full description of quantum mechanics for a large system with R particles is given by a function $\psi(x_1, x_2, \ldots, x_R, t)$ which we call the amplitude to find the particles $x_1, x_2, \ldots, x_R$, and therefore, because it has too many variables, it cannot be simulated with a normal computer with a number of elements proportional to R ...."* He suggested that one way to overcome this shortcoming would be to simulate the quantum mechanical system on a computer governed by quantum laws. Quantum computing has now emerged as a synthesis of ideas from fields like computer science and quantum mechanics.

Deutsch (1985) established a solid ground for quantum computation. After this, research on quantum computing remained at a low profile until 1994 when Shor (1994) proposed quantum algorithms for factoring integers and extracting discrete logarithms in polynomial time and in 1996 Grover proposed a quantum search algorithm for data-bases, which is quadratically faster than known classical algorithm.

Received August 9, 2011

Over the last few years there has been a rapid development of methods for processing quantum information (Barenco, et al., 1995; Benioff, 1980; Bernstein & Vazirani, 1993; Berthiaume & Brassad, 1992, 1994; Boyer et al., 1998; Chen & Diao, 2000; Deutsch et al., 1995; Deutsch & Jozra, 1992; Grover 1996; Nielsen and Chuang, 2000; Shor, 1994; Simon 1994).

Grover (2000) proposed a quantum algorithm for computation of statistical mean and studied its performance. Grover designed a transformation due to which the amplitude in a particular state becomes proportional to the mean. So, by repeating this transformation, the probability in the desired state can be increased to a detectable level. Finally, a measurement can be made to determine if the system is indeed in the desired state.

In this paper we first briefly describe Grover's algorithm for statistical mean computation and analyze this algorithm with examples. We demonstrate some flaws in this algorithm. Then we propose a correct quantum algorithm for the same problem using a philosophy analogous to that of Grover (2000).

2. **Basic Ideas of Quantum Operations**

Here we discuss quantum gate arrays or quantum acyclic circuits, which are analogous to acyclic circuits in classical computer science. We also discuss reversible computation. Besides the network model of quantum computer, there are two other types of models such as quantum Turing machine (Bernstein & Vazirani, 1993; Deutsch et al., 1995; Yao 1993) and quantum cellular automata (Feynman 1986; Lloyd 1993, 1994, 1995; Margolus 1986, 1990). Quantum Turing machine and quantum gate arrays can compute some function with a small probability of error in polynomial time (Yao 1993).

Suppose a system has n components and each component has two states. Classically, we can represent the system with n bits, but in quantum mechanics we need 2^n complex numbers for a complete description of the system, that is, the state of the quantum system is a point in a 2^n-dimensional Hilbert space. A quantum state is represented by the *ket* notation (first used by Dirac). The Hilbert space associated with this quantum system is the vector space with these 2^n states as basis vectors. A unit-length vector in this Hilbert space represents a state of the system at any instant of time. In quantum computation the superposition of a state is represented by $\sum_{i=0}^{2^n-1} \alpha_i|\mathbf{x}_i\rangle$, where α_i = amplitude of ith state such that $\sum_i |\alpha_i|^2 = 1$ and $|\mathbf{x}_i\rangle$= a basis vector of the Hilbert space.

Quantum circuits allow only local unitary transforms, i.e., unitary transforms on a fixed number of qubits (Benioff, 1982a, 1982b). Two qubit transforms are more useful than any general unitary transform which takes place on n-qubits, because it is not easy to implement n-qubit transforms, whereas two-qubit transformations can be implemented by relatively simple physical systems. These two-qubit transformations are the heart of a quantum computer. For quantum computation there are two well known quantum gates, NOT and controlled-NOT gates. A NOT gate has a single qubit input and a controlled-NOT gate has two qubits input. The input and output of a NOT gate and a controlled-NOT gate are shown in Table 1 and Table 2 respectively.

Table 1: Input and output relation of a NOT gate

Input qubit	Output qubit
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

Table 2: Input and output relation of a controlled-NOT gate

Input qubit	Output qubit
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

As mentioned earlier quantum circuits allow only local unitary transforms. So to realize these gates we need unitary matrices. It is not difficult to construct the unitary matrices to achieve the desired goals. The rows of such a matrix correspond to input basis vectors and the columns represent output basis vectors. If the ith basis vector, when applied as an input to the gate, produces the jth basis vector as the output, then the (i, j)th entry of the matrix is set to the amplitude of the output vector (in this case the amplitude is 1); otherwise, it is set to 0. Thus the matrix M_{NOT} corresponding to the NOT gate is shown in Table 3.

Table 3: Unitary matrix corresponding to a NOT gate

$$\begin{array}{c|cc} & |0\rangle & |1\rangle \\ \hline |0\rangle & 0 & 1 \\ |1\rangle & 1 & 0 \end{array} \quad M_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Similarly, for a controlled-NOT gate the unitary matrix M_{CNOT} is shown in Table 4.

Table 4: Unitary matrix corresponding to a controlled-NOT gate

$$\begin{array}{c|cccc} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \hline |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & 0 & 1 \\ |11\rangle & 0 & 0 & 1 & 0 \end{array} \quad M_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Here we also use another fundamental gate known as Walsh-Hadamard (W-H) gate. There is no classical gate which is compatible to W-H gate. For Walsh-Hadamard gate the input and output relations are given in equation (2.1):

$$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,\ |1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{2.1}$$

A system consisting of n qubits has $N = 2^n$ basis states. Now application of W-H gate on each qubit of a starting state, a string of n binary digits, produces a superposition of states consisting of all possible n bit strings, where the amplitude of each state is $\pm 2^{-\frac{n}{2}}$ (Grover 2000).

Grover's algorithm also requires selective inversion of the phase of the amplitude of certain states. This is needed for amplitude amplification of certain states and a scheme for phase inversion is described by Grover (2000).

3. Amplification of Amplitude

The quantum algorithm discussed in (Grover 2000) uses Grover's quantum searching algorithm (Grover 1996). All quantum algorithms consist of unitary operations applied in series. Any series of unitary operations is again equivalent to a single unitary operation.

Assume that, each point in a domain $B(x)$ is mapped into a state in which t is the target state. Now our objective is to design a system (i.e., a set of states) such that an initial starting state s (say) is transformed to the target state t after a series of unitary operations. The objective is to get the system into state t. Suppose we start with an initial state s and apply a unitary operation U to s and the system reaches the state t with amplitude U_{ts}. Thus, the probability of getting the state t is $|U_{ts}|^2$. So, it takes $O\left(\frac{1}{|U_{ts}|^2}\right)$ iterations before we get a single success. But using Grover's concept, performing only $O\left(\frac{1}{|U_{ts}|}\right)$ iterations it is possible to get a single success. This results in a great improvement in computation, if $|U_{ts}| \ll 1$. We now discuss such a unitary operator G (Grover 2000).

We use the following notations:

I_x : It is a matrix that inverts the amplitude in a single state $|x\rangle$. All diagonals of I_x, except the (x,x) term, are 1; the (x,x) term is -1. The off-diagonal entries are all zeros. We can express I_x as $I - 2|x\rangle|x\rangle^T$, where I is the identity matrix.

$|x\rangle$: The column vector which has all terms zero, except for the xth term which is unity.

G : A unitary operator and it is composed of four operations, $-I_sU^{-1}I_tU$. This implies that G is equivalent to four operations in the following sequence (1) U, (2) I_t, (3) U^{-1} and (4) $-I_s$. Here U^{-1} is the complex transpose of U.

It is shown in (Grover 2000) that G preserves the two dimensional vector space spanned by two vectors: $|s\rangle$ and $U^{-1}|t\rangle$. Consider a superposition state $\alpha|s\rangle+\beta U^{-1}|t\rangle$ and $G=-I_sU^{-1}I_tU$. Applying G on a superposition state we get (3.1):

$$G(\alpha|s\rangle+\beta U^{-1}|t\rangle)=[(1-4|U_{ts}|^2)\alpha-2U_{ts}^*\beta]|s\rangle+[2U_{ts}\alpha+\beta]U^{-1}|t\rangle. \tag{3.1}$$

From equation (3.1) we can conclude that the operator G transforms any superposition of two vectors $|s\rangle$ and $U^{-1}|t\rangle$ into another superposition of the two vectors and preserves the two dimensional vector space spanned by two vectors $|s\rangle$ and $U^{-1}|t\rangle$. According to Grover (2000), if we start with $|s\rangle$, after ξ iterations of G the result will be the superposition $a_s|s\rangle+a_tU^{-1}|t\rangle$ where $a_s=\cos(2\xi|U_{ts}|)$ and $|a_t|=\sin(2\xi|U_{ts}|)$. So, if we choose $\xi=\frac{\pi}{4|U_{ts}|}$, the superposition collapses to $U^{-1}|t\rangle$. After this, if we apply U on it, it provides $|t\rangle$. Thus, we need only $O\left(\frac{1}{|U_{ts}|}\right)$ iterations of G to reach the target state $|t\rangle$ from the starting state $|s\rangle$ with certainty.

4. Grover's Quantum Mean Computation

Grover describes the philosophy behind his quantum algorithm for mean computation (qmean) (Grover 2000) as:

"... a unitary transformation is designed due to which the amplitude in a particular state comes out to be proportional to the statistic we want to estimate. Then by repeating this transformation in the prescribed manner, the probability in the desired state is increased to a detectable level. Finally a measurement is made to determine if the system is indeed in the desired state. By repeating the entire operation sequence a few times and counting the number of observations, one can estimate the probability of occurrence of the desired state and hence the original statistic."

Suppose we have to find the mean of $\{x_0,x_1,\ldots,x_{N-1}\}$. First we change the given set of values $\{x_0,x_1,\ldots,x_{N-1}\}$ in the range $(-0.5,0.5)$ by a suitable scaling. Let the scaled values be $\{x_{d_0},x_{d_1},\ldots,x_{d_{N-1}}\}$. Assume a specified precision ν for the mean M. Choose a relatively large ν_0 such that $|M|<\nu_0$. The process described in Algorithm A.

Algorithm A: Grover's qmean algorithm

```
while ($\nu_0 > \nu$) do
begin
    (1) Estimate the mean $M_e$ such that $|M_e - M| < \frac{\nu_0}{2}$ using the
        "Estimate Algorithm" (Algorithm B) described next.
    (2) Each element is shifted by the newly estimated mean, i.e.,
        $x_{d_i} \leftarrow x_{d_i} - M_e$.
    (3) [Improve precision] $\nu_0 \leftarrow \frac{\nu_0}{2}$
end
```

The mean is estimated as the sum of the estimated M_e in each iteration Step (1) of the loop.

We now provide a proof of the correctness of this result in the following theorem:

Theorem 1. Suppose M is the true mean of $\{x_{d_0}, x_{d_1}, \ldots, x_{d_{N-1}}\}$ such that $|M| < \nu_0$, where ν_0 is relatively large and M_e is the estimated mean computed by Grovers' algorithm, such that $|M_e - M| < \frac{\nu_0}{2}$. Then Algorithm A computes the true mean of the data points as the sum of the estimated means and it will be within precision of ν, where $\nu \leq \frac{\nu_0}{2^k}$ after k iterations.

Proof. Here, $M = \frac{1}{N}\sum_{i=0}^{N-1} x_{d_i}$. In the first iteration

$$M_e^{(1)} = \frac{1}{N}\sum_{i=0}^{N-1} x_i^{(0)} \pm \frac{\nu_0}{2},\ x_i^{(1)} = x_i^{(0)} - M_e^{(1)},$$

where $x_i^{(0)} = x_{d_i}$. After kth iterations

$$M_e^{(k)} = \frac{1}{N}\sum_{i=0}^{N-1} x_i^{(k-1)} \pm \frac{\nu_0}{2^k}$$

and $x_i^{(k)} = x_i^{(k-1)} - M_e^{(k)}$. Now,

$$x_i^{(k)} = x_i^{(k-1)} - M_e^{(k)} = x_i^{(k-2)} - M_e^{(k-1)} - M_e^{(k)} = \cdots = x_i^{(0)} - \sum_{j=1}^{k} M_e^{(j)}$$

and

$$\begin{aligned} M_e^{(k)} &= \frac{1}{N}\sum_{i=0}^{N-1} x_i^{(k-1)} \pm \frac{\nu_0}{2^k} = \frac{1}{N}\sum_{i=0}^{N-1}\left(x_i^{(0)} - \sum_{j=1}^{k-1} M_e^{(j)}\right) \pm \frac{\nu_0}{2^k} \\ &= \frac{1}{N}\sum_{i=0}^{N-1} x_{d_i} - \sum_{j=1}^{k-1} M_e^{(j)} \pm \frac{\nu_0}{2^k}. \end{aligned}$$

Therefore,

$$M_e^{(k)} + \sum_{j=1}^{k-1} M_e^{(j)} = M \pm \frac{\nu_0}{2^k},$$

i.e., $\sum_{j=1}^{k} M_e^{(j)} = M \pm \nu$. Hence sum of estimated mean obtained in each iteration approaches the actual mean M with iteration k. For describing the 'Estimate Algorithm' (Algorithm B) we need to define a set of operators which we do next. Consider a quantum mechanical system with $(2^{n+1} + 1)$ states, where each state is represented by $(n + 2)$ qubits. Given N, we find the smallest n such that $2^n \geq N$. Assume three kinds of state space, P, H and I. These states are used to compute the mean of N given numbers.

Let $P = \{P_0, P_1, \ldots, P_{N-1}\}$ be a state space, where each state P_i is represented by $(n + 2)$ qubits – the first two qubits are 00 and the next n qubits indicate the P_i state (one can view that the n qubits correspond to the index of x_i) as shown in

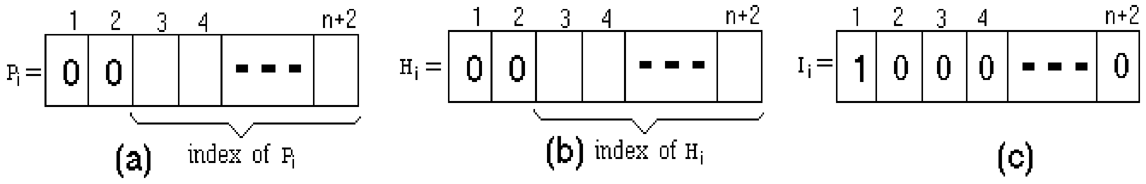

FIGURE 1. (a) State representation of P_i, (b) State representation of H_i, and (c) State representation of I_i for Algorithm B.

Figure 1(a). Similarly, $H = \{H_0, H_1, \ldots, H_{N-1}\}$ be another state space. Each state H_i is represented by $(n+2)$ qubits, where the first two qubits are 01 and the next n qubits indicate the H_i state as shown in Figure 1(b). Also consider another state I in which the first qubit is 1 and the remaining $(n+1)$ qubits are set to zero and the corresponding register is shown in Figure 1(c).

The estimate algorithm requires four unitary operators: L_1, L_2, R_1, and W_1. Grover (2000) suggested to apply the operator $U = L_1 W_1 R_1 W_1 L_2$ on P_0 to find the estimated mean M_e. The definition of four unitary operators L_1, L_2, R_1, and W_1 are as follows:

Operator L_1

The unitary operator L_1 is performed by the following rules.

(a) **If in state P_0:** Goto state I with an amplitude of $\frac{1}{2}$ and remain in state P_0 with an amplitude $\frac{\sqrt{3}}{2}$.

(b) **If in state I:** Goto state P_0 with an amplitude of $\frac{1}{2}$ and remain in state I with an amplitude $-\frac{\sqrt{3}}{2}$.

(c) **If in any other state:** Remains in the same state.

Operator L_2

The following rules define the operator L_2.

(a) **If in state P_0:** Goto state I taking an amplitude of $\frac{1}{\sqrt{2}}$ and remain in the state P_0 with an amplitude $\frac{1}{\sqrt{2}}$.

(b) **If in state I:** Goto state P_0 taking an amplitude of $-\frac{1}{\sqrt{2}}$ and remain in the state I with an amplitude $\frac{1}{\sqrt{2}}$.

(c) **If in any other state:** Remains in the same state.

Operator R_1

The following rules are used for the operator R_1.

(a) **If in state P_β:** Goto state H_β taking an amplitude of $\sqrt{\frac{2}{3} - \frac{4}{3}x_\beta^2}$ and remain in the state P_β with an amplitude of $(\frac{1}{\sqrt{3}} + \frac{2ix_\beta}{\sqrt{3}})$.

(b) **If in state H_β:** Goto state P_β taking an amplitude of $\sqrt{\frac{2}{3} - \frac{4}{3}x_\beta^2}$ and remain in the state H_β with an amplitude of $(-\frac{1}{\sqrt{3}} + \frac{2ix_\beta}{\sqrt{3}})$.

(c) **If in any other state:** Remains in the same state.

Operator W_1

The following rules define the operator W_1.

(a) **If in state P_β:** Perform Walsh-Hadamard transform on P_β state.
(b) **If in any other state:** Remains in the same state.

Grover claimed that application of $U = L_1W_1R_1W_1L_2$ on P_0 will make the amplitude of state P_0 as $\frac{iM}{\sqrt{2}}$. If this claim is true then Algorithm B (the Estimate Algorithm) for estimation of the mean with precision ν_0 will be as follows:

Algorithm B : Estimate Algorithm

(1) Repeat G for $O\left(\frac{1}{\nu_0}\right)$ times on P_0.
(2) Apply U only once on the resultant state.
(3) Measure the amplitude of state P_0 for the estimated mean (with a precision of ν_0).

We shall now show with a numerical example that the application of U on P_0 does not make the amplitude of P_0 as $\frac{iM}{\sqrt{2}}$ as claimed in (Grover 2000).

4.1. **Numerical Example.** Before giving a complete example we first explain how quantum operators act on qubits and what results are produced by such operators. We discuss a useful operator, the Walsh-Hadamard operator, on three qubits input. For simplicity we consider the input $|000\rangle$. Walsh-Hadamard transform can be represented by following matrix:

$$\text{W-H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

We apply W-H transform on $|000\rangle$. The input $|000\rangle$ can be written as $|0\rangle|0\rangle|0\rangle$ or $|0\rangle \otimes |0\rangle \otimes |0\rangle$, where $\otimes$ is the tensor product operator. After applying W-H operator on $|000\rangle$ becomes

$$\left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \bigotimes \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \bigotimes \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right).$$

So we can rewrite as:

$$\begin{aligned} |000\rangle \quad \overset{W-H}{\longrightarrow} & \quad \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \bigotimes \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \bigotimes \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \\ = & \quad \left(\frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}\right) \bigotimes \left(\frac{|00\rangle\ +\ |01\rangle\ +\ |10\rangle\ +\ |11\rangle}{2}\right) \\ = & \quad \frac{|000\rangle\ +|001\rangle\ +|010\rangle\ +|011\rangle\ +|100\rangle\ +|101\rangle\ +|110\rangle\ +|111\rangle}{2^{\frac{3}{2}}} \end{aligned}$$

Suppose $N = 2$ and the two input numbers are x_0 and x_1; $x_0, x_1 \in (-0.5, +0.5)$. We want to estimate the mean of x_0 and x_1. To find the estimated mean M_e, we proceed as follows: Choose $\nu_0 = 0.5$ (in Algorithm A). We shall try to estimate the mean such that $|M_e - M| < \frac{\nu_0}{2}$. Here, $n = 1$ [Since $N = 2^n$]. Now we write P_0 and H_0 corresponding to x_0; P_1 and H_1 corresponding to x_1, and I as described previously.

$$P_0 \equiv |000\rangle \quad H_0 \equiv |010\rangle \quad I \equiv |100\rangle$$

$$P_1 \equiv |001\rangle \quad H_1 \equiv |011\rangle$$

Assume that the starting state is P_0. Now apply the unitary operator $U = L_1W_1R_1W_1L_2$ on P_0. In other words on P_0 we apply the following operators in this sequence L_2, W_1, R_1, W_1 and L_1. After applying each operator the amplitude of the different states are shown in Table 5 to Table 9.

Step 1: We apply L_2 operator on P_0 state. It goes to state I with an amplitude of $\frac{1}{\sqrt{2}}$ and to state P_0 with an amplitude of $\frac{1}{\sqrt{2}}$. This can be written as:

$$|000\rangle \xrightarrow{L_2} \frac{1}{\sqrt{2}}|000\rangle \ + \ \frac{1}{\sqrt{2}}|100\rangle.$$

The amplitudes of different states (P_0 and I) are shown in Table 5.

Table 5: Amplitude of different states after applying operator L_2

State	Amplitude
P_0	$\frac{1}{\sqrt{2}}$
I	$\frac{1}{\sqrt{2}}$

Step 2: Now W_1 operator acts on P_0 state. The operation can be written as:

$$\frac{1}{\sqrt{2}}|000\rangle \quad \xrightarrow{W_1} \quad \frac{1}{\sqrt{2}}\left(\frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{2^{\frac{3}{2}}}\right)$$

$$\equiv \quad \frac{1}{2^2}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right).$$

Amplitudes of different states after applying operator W_1 on the output of Step 1 are shown in Table 6.

Table 6: Amplitudes of different states after applying operator W_1

State	Amplitude
P_0	$\frac{1}{2^2}$
P_1	$\frac{1}{2^2}$
H_0	$\frac{1}{2^2}$
H_1	$\frac{1}{2^2}$
I	$\frac{1}{\sqrt{2}} + \frac{1}{2^2}$

Step 3: We then apply operator R_1. After applying operator R_1 on the output of Step 2 the amplitudes of different states are shown in Table 7.

Table 7: Amplitudes of different states after applying operator R_1

State	Amplitude
P_0	$\frac{1}{2^2}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}\right)$
P_1	$\frac{1}{2^2}\left(\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)$
H_0	$\frac{1}{2^2}\left(\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}-\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}\right)$
H_1	$\frac{1}{2^2}\left(\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}-\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}\right)$
I	$\frac{1}{\sqrt{2}}+\frac{1}{2^2}$

Step 4: The operator W_1 is applied on the output of Step 3. The resulting amplitudes for the states P_0, P_1 and I are shown in Table 8.

Table 8: Amplitudes of different states after applying operator W_1

State	Amplitude
P_0	$\frac{1}{2^3\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}+\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)$
P_1	$\frac{1}{2^3\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}-\frac{1}{\sqrt{3}}-\frac{2ix_1}{\sqrt{3}}-\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)$
I	$\frac{1}{\sqrt{2}}+\frac{1}{2^2}+\frac{1}{2^3\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}+\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)$

Step 5: Applying operator L_1 on the output of Step 6, we get the amplitude of P_0 as shown in Table 9.

Table 9: Amplitude of P_0 state after applying operator L_1

State	Amplitude
P_0	$\frac{\sqrt{3}}{2^4\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}+\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)$ $+\frac{1}{2}\left(\frac{1}{2^3\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}-\frac{1}{\sqrt{3}}-\frac{2ix_1}{\sqrt{3}}-\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)+\frac{1}{\sqrt{2}}+\right.$ $\left.\frac{1}{2^{\frac{3}{2}}\sqrt{2}}+\frac{1}{2^3\sqrt{2}}\left(\frac{1}{\sqrt{3}}+\frac{2ix_0}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_0^2}{3}}+\frac{1}{\sqrt{3}}+\frac{2ix_1}{\sqrt{3}}+\sqrt{\frac{2}{3}-\frac{4x_1^2}{3}}\right)\right)$

Grover claimed that application of U changes the amplitude of P_0 to $\frac{iM}{\sqrt{2}}$, but our example shows that it is not the case even for a very simple example. We now propose a modification of Grover's algorithm to fix this problem. In other words, we propose a new unitary operator that changes the amplitude P_0 to $\frac{iM}{\sqrt{2}}$.

5. Modified Algorithm for Mean Computation

The basic steps of Algorithm A remains unchanged but we propose a new unitary operator which is used by the estimate algorithm (Algorithm B). The required basic unitary operators are described next. Consider a quantum mechanical system with 2^{n+1} states where each state is represented by $(n+1)$ qubits. We are assuming only two kinds of state space, P and H. These states are used to compute the mean of

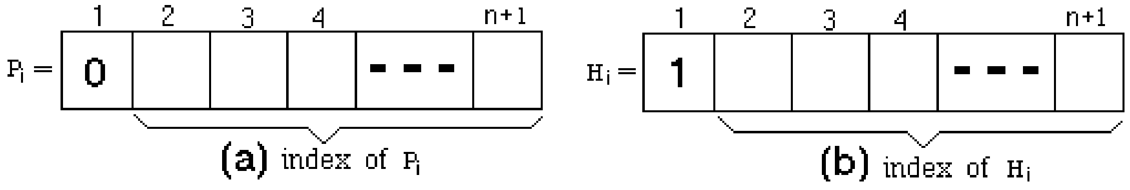

FIGURE 2. (a) Representation of state P_i, and (b) representation of state H_i for algorithm C.

$N = 2^n$ given real values. Let $P = \{P_0, P_1, \ldots, P_{N-1}\}$ be a state space, where each state P_i is represented by $(n+1)$ qubits; the first qubit is 0 and next n qubits indicate the P_i state (one can view that the n qubits correspond to the index of x_i) as shown in Fig. 2(a).

Similarly, $H = \{H_0, H_1, \ldots, H_{N-1}\}$ be another state space, where each state H_i is represented by $(n+1)$ qubits; the first qubit is 1 and next n qubits indicate the index of H_i as shown in Fig. 2(b).

To estimate the mean M_e, the 5-step unitary operator $U = L_1W_1R_1W_1L_2$ of Grover's algorithm is replaced by a 3-step unitary operator $U = W_{m1}R_{m1}W_{m1}$, where the unitary operators W_{m1} and R_{m1} are defined as follows:

Operator R_{m1}

(a) **If in state P_β:** Goto the state H_β with an amplitude of $i\sqrt{\frac{1}{2} - \frac{1}{2}x_\beta^2}$ and remain in the state P_β with an amplitude of $\left(\frac{1}{\sqrt{2}} + \frac{ix_\beta}{\sqrt{2}}\right)$.

(b) **If in state H_β:** Goto the state P_β with an amplitude of $-i\sqrt{\frac{1}{2} - \frac{1}{2}x_\beta^2}$ and, remain in the state H_β with an amplitude of $\left(-\frac{1}{\sqrt{2}} + \frac{ix_\beta}{\sqrt{2}}\right)$.

Operator W_{m1}

Perform Walsh-Hadamard transformation on the state under consideration.

Next, we demonstrate the correctness of our operator.

5.1. Numerical Example.

Consider the same data points x_0 and x_1 as in the previous example in Section 4.1. We assume the same value for ν. The states are represented as follows:

$$P_0 \equiv |00\rangle, \quad H_0 \equiv |10\rangle, \quad P_1 \equiv |01\rangle, \quad H_1 \equiv |11\rangle.$$

Note that, here we do not use any I state. Now apply $U = W_1R_1W_1$ on P_0 state. The amplitude of different states after applying different operators are shown in Table 10–Table 12. The computational steps involved are shown below:

$$(5.1)\ |00\rangle \xrightarrow{W_{m1}} \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

$$\begin{aligned}
&\xrightarrow{R_{m1}} \frac{1}{2}\left(\frac{1}{\sqrt{2}}+\frac{ix_0}{\sqrt{2}}-i\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}\right)|00\rangle+\frac{1}{2}\left(\frac{1}{\sqrt{2}}+\frac{ix_1}{\sqrt{2}}-i\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}\right)|01\rangle+\\
&\qquad \frac{1}{2}\left(i\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}-\frac{1}{\sqrt{2}}+\frac{ix_0}{\sqrt{2}}\right)|10\rangle+\frac{1}{2}\left(i\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}-\frac{1}{\sqrt{2}}+\frac{ix_1}{\sqrt{2}}\right)|11\rangle\\
&\xrightarrow{W_{m1}} \frac{1}{2}\left(\frac{i(x_0\ +\ x_1)}{\sqrt{2}}\right)|00\rangle\ +\ \frac{1}{2}\left(\frac{ix_0}{\sqrt{2}}-\frac{ix_1}{\sqrt{2}}\right)|01\rangle\ +\\
&\qquad \frac{1}{2}\left(\frac{2}{\sqrt{2}}-i\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}-i\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}\right)|10\rangle\\
&\qquad +\frac{i}{2}\left(\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}-\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}\right)|11\rangle
\end{aligned}$$

Step 1: Apply operator W_{m1} on P_0 as shown in (5.1). The amplitudes of different states after application of W_{m1} are given in Table 10.

Table 10: Amplitudes of different states after applying operator W_{m1}

State	Amplitude
P_0	$\frac{1}{2}$
H_0	$\frac{1}{2}$
P_1	$\frac{1}{2}$
H_1	$\frac{1}{2}$

Step 2: Apply operator R_{m1} on the output of Step 1. The amplitude of different states are shown in Table 11.

Table 11: Amplitudes of different states after applying operator R_1

State	Amplitude
P_0	$\frac{1}{2}\left(\frac{1}{\sqrt{2}}+\frac{ix_0}{\sqrt{2}}-i\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}\right)$
P_1	$\frac{1}{2}\left(\frac{1}{\sqrt{2}}+\frac{ix_1}{\sqrt{2}}-i\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}\right)$
H_0	$\frac{1}{2}\left(i\sqrt{\frac{1}{2}-\frac{x_0^2}{2}}-\frac{1}{\sqrt{2}}+\frac{ix_0}{\sqrt{2}}\right)$
H_1	$\frac{1}{2}\left(i\sqrt{\frac{1}{2}-\frac{x_1^2}{2}}-\frac{1}{\sqrt{2}}+\frac{ix_1}{\sqrt{2}}\right)$

Step 3: Apply operator W_{m1} on the output of Step 2. The amplitude of state P_0 is shown in Table 12. Clearly, this amplitude is $\frac{1}{2^2}\left(\frac{2i(x_0+x_1)}{\sqrt{2}}\right)=\frac{iM}{\sqrt{2}}$, where $M=\frac{x_0+x_1}{2}$. This is exactly, what Grover wanted to achieve (Grover 2000).

Table 12: Amplitudes of different states after applying operator W_1

State	Amplitude
P_0	$\frac{1}{2^2}\left(\frac{2i(x_0+x_1)}{\sqrt{2}}\right)$

So after applying $U\equiv W_{m1}R_{m1}W_{m1}$ the amplitude of the state P_0 becomes $\frac{iM}{\sqrt{2}}$. According to the analysis in Section 3, if we apply $G=-I_{P_0}U^{-1}I_{P_0}U$ on P_0 of $O\left(\frac{1}{\nu_0}\right)$

times, followed by an application of U, then Algorithm B will estimate the mean with a precision ν_0. Consequently, Algorithm A will estimate the mean with the desired precision.

We now provide a proof of the correctness of our proposed modified operators in Theorem 2.

Theorem 2. Let M be the true mean of $\{x_0, x_1, \ldots, x_{N-1}\}$. Then the amplitude of the state P_0 becomes $\frac{iM}{\sqrt{2}}$ after applying the operator $W_{m1}R_{m1}W_{m1}$ on P_0.

Proof. Suppose, $H_k = |1b_1^{(k)}b_2^{(k)}\cdots b_n^{(k)}\rangle$ and $P_k = |0b_1^{(k)}b_2^{(k)}\cdots b_n^{(k)}\rangle$, where $(b_1^{(k)}b_2^{(k)}\cdots b_n^{(k)})_2 = k$, $b_j^{(k)} \in \{0,1\}$, $j = 1,2,\ldots,n$; $k = 0,1,2,\ldots,N-1$ and $N = 2^n$. From the definition of W-H transform we know that application of W-H transform on the state $|b_j^{(k)}\rangle$ changes it to $\frac{|0\rangle+(-1)^{b_j^{(k)}}|1\rangle}{\sqrt{2}}$. Now

$$\begin{aligned}
P_0 &= |0b_1^{(0)}b_2^{(0)}\cdots b_n^{(0)}\rangle \\
&\xrightarrow{W_{m1}} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \bigotimes_{p=1}^{n} \frac{|0\rangle+(-1)^{b_p^{(0)}}|1\rangle}{\sqrt{2}} \\
&= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \bigotimes_{p=1}^{n} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \text{ [Since } b_p^{(0)} = 0 \;\forall\; p = 1,2,\ldots,n] \\
&= \frac{1}{2^{\frac{n+1}{2}}} \left(\sum_{k=0}^{N-1} (P_k + H_k) \right) \\
&\xrightarrow{R_{m1}} \frac{1}{2^{\frac{n+1}{2}}} \left[\sum_{k=0}^{N-1} \left\{ \left(i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) H_k + \left(\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} \right) P_k + \right.\right. \\
&\qquad \left.\left. \left(-i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) P_k + \left(-\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} \right) H_k \right\} \right] \\
&= \frac{1}{2^{\frac{n+1}{2}}} \left[\sum_{k=0}^{N-1} \left\{ \left(\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} - i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) P_k + \right.\right. \\
&\qquad \left.\left. \left(-\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} + i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) H_k \right\} \right] \\
&\xrightarrow{W_{m1}} \frac{1}{2^{\frac{n+1}{2}}} \left[\sum_{k=0}^{N-1} \left\{ \left(\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} - i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \bigotimes_{p=1}^{n} \frac{|0\rangle+(-1)^{b_p^{(k)}}|1\rangle}{\sqrt{2}} \right) + \right.\right. \\
&\qquad \left.\left. \left(-\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} + i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}} \bigotimes_{p=1}^{n} \frac{|0\rangle+(-1)^{b_p^{(k)}}|1\rangle}{\sqrt{2}} \right) \right\} \right] \\
&= \frac{1}{2^{\frac{n+1}{2}}} \left[\sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} - i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) \left\{ \frac{1}{2^{\frac{n+1}{2}}} \sum_{r=0}^{N-1} (-1)^{\sum_{j=1}^{n} b_j^{(r)}} (P_r + H_r) \right\} + \right. \\
&\qquad \left. \left(-\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} + i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) \left\{ \frac{1}{2^{\frac{n+1}{2}}} \sum_{r=0}^{N-1} (-1)^{\sum_{j=1}^{n} b_j^{(r)}} (P_r - H_r) \right\} \right]
\end{aligned}$$

Therefore the amplitude of the P_0 state

$$= \frac{1}{2^{n+1}} \left[\sum_{k=0}^{N-1} \left\{ \left(\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} - i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) + \left(-\frac{1}{\sqrt{2}} + \frac{ix_k}{\sqrt{2}} + i\sqrt{\frac{1}{2}-\frac{x_k^2}{2}} \right) \right\} \right]$$

$$=\frac{1}{2^{n+1}}\sum_{k=0}^{N-1}2\frac{ix_k}{\sqrt{2}}=\frac{1}{\sqrt{2}}i\frac{1}{2^n}\sum_{k=0}^{N-1}x_k=\frac{iM}{\sqrt{2}}.$$

5.2. **Complexity Analysis of the entire Algorithm (Algorithm A and B).** Suppose Algorithm A iterates k times to converge the process. Each time the precision is updated as $\nu_0 \leftarrow \frac{\nu_0}{2}$ where ν_0 is the initial precision. If ν is the final desired precision then $\nu \leq \frac{\nu_0}{2^k}$. Therefore, $k \leq \log_2 \frac{\nu_0}{\nu}$. When $k = 1$, M_e is computed with a precision of ν_0. In this case, the required number of iterations, as explained in Section 3, is $O\left(\frac{1}{\nu_0}\right)$. Similarly, when $k = 2$, the required number of iteration is $O\left(\frac{2}{\nu_0}\right)$ and so on. To achieve the desired precision ν, we perform the whole operations $k = \log_2 \frac{\nu_0}{\nu}$ times. And also we replace ν_0 by $\frac{\nu_0}{2}$ after each iteration. Therefore, the total number of iteration $= \sum_{i=0}^{\log_2 \frac{\nu_0}{\nu}} O\left(\frac{2^i}{\nu_0}\right) = O\left(\sum_{i=0}^{\log_2 \frac{\nu_0}{\nu}} \frac{2^i}{\nu_0}\right) = O\left(\frac{2^{\log_2 \frac{\nu_0}{\nu}+1}-1}{\nu_0}\right) \approx O\left(\frac{1}{\nu_0}\frac{\nu_0}{\nu}\right) = O\left(\frac{1}{\nu}\right)$. So the mean M can be estimated with a precision of ν in $O\left(\frac{1}{\nu}\right)$ operations.

6. Conclusion

We discussed Grover's algorithm for mean computation and demonstrated with an example that this algorithm does not produce the desired result. We then proposed a modified algorithm for mean computation using Grover's basic philosophy (Grover 2000). Our proposed unitary operator is simple, produces correct result and more efficient both in terms of number of operations performed as well as the number of qubits used. We proved the correctness of our algorithm and also illustrated it with a numerical example.

REFERENCES

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurther, Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, 1995.

[2] P. Benioff, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by turing machines. *Journal of Stat. Phys.*, 22:563–591, 1980.

[3] P. Benioff, Quantum mechnical Hamiltonian models of turing machines. *J. Statist. Phys.*, 29:515–546, 1982a.

[4] P. Benioff, Quantum mechnical Hamiltonian models of Turing machines that dissipate no energy. *Phys. Rev. Letter*, 48:1581–1585, 1982b.

[5] E. Bernstein and U. Vazirani, Quantum complexity theory. *Proc. 25th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, pp. 11–20, 1993.

[6] A. Berthiaume and G. Brassad, The quantum challenge to structural complexity theory. *Proc. Seventh Annual Structure in Complexity Theory Conference*, IEEE comp. Scociety Press, Los Alamitos, CA, pp. 132–137, 1992.

[7] A. Berthiaume and G. Brassad, Oracle quantum computing. *J. Mod. Optics*, 41:2521–2535, 1994.

[8] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, Tight bounds on quantum searching. *Fortschritte Der Physik* (in arXiv:quant-ph/9605034), 1998.

[9] G. Chen and Z. Diao, Exponentially fast quantum search algorithm. arXiv:quant-ph/0011109, 2000.

[10] D. Deutsch, Quantum theory, the Church-Turing principle and universal quantum computer. *Proc. Roy. Soc. London Ser. A*, 400:96–117, 1985.

[11] D. Deutsch, A. Barenco and A. Ekert, Universality of quantum computation. *Proc. Roy. Soc. London. Ser. A*, 449:669-677, 1995.

[12] D. Deutsch and R. Jozra, Rapid solution of problems by quantum computation. *Proc. Roy. Soc. London Ser. A*, 439:553–558, 1992.

[13] R. P. Feynman, Simulating physics with computers. *Intl. J. of Theoretical Physics*, 21:467, 1982.

[14] R. P. Feynman, Quantum mechanical computers. *Found. Phys.*, 16:507–531, 1986.

[15] L. K. Grover, A fast quantum mechanical algorithm for database search. *Proceedings 28th Annual Symposium on the Theory of Computing (STOC)*, pp. 212–219, 1996.

[16] L. K. Grover, A framework for fast quantum mechnical algorithms. *Proceedings 32th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 618–626, 2000.

[17] S. Lloyd, A potentially realizable quantum computer. *Science*, 261:1569–1571, 1993.

[18] S. Lloyd, Envisioning a quantum supercomputer. *Science*, 263:695, 1994.

[19] S. Lloyd, Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75:346–349, 1995.

[20] N. Margolus, Quantum computation. *Ann. New York Acad. Sci.*, 480:346-349, 1986.

[21] N. Margolus, Complexity, Entropy and the Physics of Information. *Santa Fe Institute Studies in the Sciences of Complexity*, v. VIII, W. H. Zurek, ed., Addision Wesley, Reading, MA, p. 273, 1990.

[22] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information.* Cambridge University Press, 2000.

[23] P. W. Shor, Algorithm for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Fundamentals of Computer Science (FOCS)*, pp. 124–134, 1994.

[24] D. Simon, On the power of quantum computation. *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 116–123, 1994.

[25] A. Yao, Quantum circuit complexity. *Proc. 36th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 352–361, 1993.