ELEMENTS OF QUANTUM PARALLELISM AND ALGORITHMS

Sudebkumar Prasant Pal
Department of Computer Science and Engineering and
Centre for Theoretical Studies
IIT Kharagpur 721302, India
email: spp@cse.iitkgp.ernet.in

October 19, 2009

1 Probabilistic Deustch's algorithm

Deustch's problem is to decide whether a 1-bit input boolean function $f : \{0,1\} \Rightarrow \{0,1\}$, is *flat* or *uneven*, or in other words, whether $f(0) \oplus f(1)$ is 0 or 1. Note that any classical approach to solving this problem would require evaluating the function f two times. However, using quantum parallelism, only one quantum circuit for realizing a *quantum (unitary)* evalution of f suffices in solving this problem, as follows.

We create a superposition of the two basis states in the first qubit by doing a Hadamard operation[1], on the $|0\rangle$ state to create the $|X+\rangle = |0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ state, and then perform a *controlled-U_f* with this superposition on the $|0\rangle$ state in the second qubit. [2] If $f(0) = f(1)$ then we get,

$$\begin{aligned} & \tfrac{1}{\sqrt{2}}\left(|0, f(0)\rangle + |1, f(1)\rangle\right) \\ = \quad & \tfrac{1}{\sqrt{2}}\left(|0,0\rangle + |1,0\rangle\right) \qquad [f(0) = 0] \\ (= \quad & \tfrac{1}{\sqrt{2}}\left(|0,1\rangle + |1,1\rangle\right) \qquad [f(0) = 1]) \end{aligned}$$

For $f(0) = 0$:

$$\begin{aligned} & \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle \\ = \quad & |0'\rangle \tfrac{(|0'\rangle + |1'\rangle)}{\sqrt{2}} \\ = \quad & \tfrac{|0'0'\rangle}{\sqrt{2}} + \tfrac{|0'1'\rangle}{\sqrt{2}} \end{aligned}$$

Here, $|1'\rangle = |X-\rangle$.

[1] The Hadamard operation is defined as $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

[2] The operation is $U_f(|x, y\rangle) \Rightarrow |x, y \oplus f(x)\rangle$, quite like the $CNOT$ operation $|x, y\rangle \Rightarrow |x, x \oplus y\rangle$.

For $f(0) = 1$:

$$\begin{aligned} & \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|1\rangle \\ = \quad & |0'\rangle \tfrac{(|0'\rangle - |1'\rangle)}{\sqrt{2}} \\ = \quad & \tfrac{|0'0'\rangle}{\sqrt{2}} - \tfrac{|0'1'\rangle}{\sqrt{2}} \end{aligned}$$

In both cases if second qubit measures $|1'\rangle$, then first qubit measures $|0'\rangle$ (see [2]).

On the other hand, if $f(0) \neq f(1)$ then,

For $f(0) = 0$:

$$\begin{aligned} & \tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ = \quad & \tfrac{1}{\sqrt{2}}\left(|0'0'\rangle + |1'1'\rangle\right) \end{aligned}$$

For $f(0) = 1$:

$$\begin{aligned} & \tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\ = \quad & \tfrac{1}{\sqrt{2}}\left(\tfrac{|0'\rangle+|1'\rangle}{\sqrt{2}} \otimes \tfrac{|0'\rangle-|1'\rangle}{\sqrt{2}}\right) + \tfrac{1}{\sqrt{2}}\left(\tfrac{|0'\rangle-|1'\rangle}{\sqrt{2}} \otimes \tfrac{|0'\rangle+|1'\rangle}{\sqrt{2}}\right) \\ = \quad & \tfrac{1}{\sqrt{2}}\left(\tfrac{|0'0'\rangle-|0'1'\rangle+|1'0'\rangle-|1'1'\rangle+|0'0'\rangle-|1'1'\rangle+|0'1'\rangle-|1'0'\rangle}{2}\right) \\ = \quad & \tfrac{1}{\sqrt{2}}\left(|0'0'\rangle - |1'1'\rangle\right) \end{aligned}$$

We summarize our observations and conclude that in either case that measuring state $|1'\rangle$ on the second qubit gives state $|1'\rangle$ on the first qubit too (see [2]).

On the other hand, observe that for the four cases above, the $|0'\rangle$ measured on qubit 2 gives no definite information in the first qubit ! So, we see that this method has 50% success probability since the second qubit can measure one of the two X-basis states $|0'\rangle$ and $|1'\rangle$ with equal probabilities.

2 Deterministic Deustch's algorithm

Now consider the second approach. Instead of $|0\rangle$, we start with a $|1\rangle$ for the second qubit and do a Hadamard on both, the fisrt as well as the second qubit. The rest is explained below (see [1, 2]).

$$\begin{aligned} |0\rangle|1\rangle & \overset{H^{\otimes 2}}{\rightarrow} \frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) \\ & \overset{U_f}{\rightarrow} \frac{1}{2}\left(\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle\right)\left(|0\rangle - |1\rangle\right) \\ = \frac{1}{2}(-1)^{f(0)} & \left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)\left(|0\rangle - |1\rangle\right) \end{aligned}$$

The U_f step can be explained as follows:

$$\frac{1}{2}\left(|0\rangle\left(|0\rangle - |1\rangle\right) + |1\rangle\left(|0\rangle - |1\rangle\right)\right)$$

$$\stackrel{U_f}{\rightarrow} \frac{1}{2}\left(|0\rangle\left(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\right) + |1\rangle\left(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\right)\right)$$

$$= \frac{1}{2}\left[\left((-1)^{f(0)}|0\rangle\left(|0\rangle - |1\rangle\right)\right) + \left((-1)^{f(1)}|1\rangle\left(|0\rangle - |1\rangle\right)\right)\right]$$

$$= \frac{(-1)^{f(0)}}{2}\left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right]\left(|0\rangle - |1\rangle\right)$$

So, with 100% success we get $f(0) \oplus f(1)$, if we do a H on first qubit! This is explained as follows.

Let $R = f(0) \oplus f(1)$. Then, we have the following simplification of the above state.

$$\frac{|0'\rangle+|1'\rangle}{2\sqrt{2}} + (-1)^R \frac{|0'\rangle-|1'\rangle}{2\sqrt{2}}$$

$$= \frac{|0'\rangle}{\sqrt{2}}(1 + (-1)^R) + \frac{|1'\rangle}{\sqrt{2}}(1 - (-1)^R)$$

If $R = 1$, i.e.,$f(0) \neq f(1)$, then the above expression is $|1'\rangle$, measuring $|1\rangle$ in the standard basis after a Hadamard operation. Otherwise $R = 0$, i.e., $f(0) = f(1)$, and the above expression is $|0'\rangle$, measuring $|0\rangle$ in the standard basis after a Hadamard operation.

3 The Bernstein-Vazirani problem

The Bernstein-Vazirani problem, like the previous ones, is another example of a problem of mathematical interest that is solvable efficiently on a quantum computer. The problem is as follows. Let a be an unknown positive integer, $0 \leq a < 2^n$. Let f be the evaluation function for this problem that takes another bit string in the range $0 \leq x < 2^n$ and outputs the modulo 2 sum of the bitwise product of a and x, denoted by $a.x$. What we want to determine here is, the number of invocations of the algorithm for evaluating or deciphering a. Surprisingly we need only one invocation quantum mechanically. Doing classically would have taken n invocations. We show this below. Consider U_f applied to $|x\rangle_n|y\rangle$ flipping y if and only if $f(x) = 1$. So, we have

$$U_f|x\rangle_n \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$= (-1)^{f(x)}|x\rangle_n \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

where we prepared $|y\rangle$ as $HX|0\rangle =$

$$H|1\rangle = \frac{(|0\rangle - |1\rangle}{\sqrt{2}}$$

To recap, we know that

$$H|x\rangle = (|0\rangle + (-1)^x|1\rangle)/\sqrt{2}$$

$$= (\sum_{y=0}^{1}(-1)^{xy}|y\rangle)/\sqrt{2}$$

So, now consider

$$(H^{\otimes n} \otimes 1)U_f(H^{\otimes n} \otimes H)|0\rangle_n|1\rangle$$

$$= \frac{1}{2^{n/2}}(H^{\otimes n} \otimes 1)U_f(\sum_{x=0}^{2^n-1}|x\rangle)\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$= \frac{1}{2^{n/2}}(H^{\otimes n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle)\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

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

Now consider the sum for a y over all x (we are given that $f(x) = a.x$):

$$\sum_{x=0}^{2^n-1}(-1)^{a.x}(-1)^{x.y}$$

$$= \sum_{x=0}^{2^n-1}(-1)^{a_0.x_0}(-1)^{a_1.x_1}(-1)^{a_{n-1}.x_{n-1}}(-1)^{y_0.x_0}(-1)^{y_1.x_1}(-1)^{y_{n-1}.x_{n-1}}$$

$$= \sum_{x=0}^{2^n-1}(-1)^{(a_0+y_0)x_0}\cdots(-1)^{(a_{n-1}+y_{n-1})x_{n-1}}$$

$$= \Pi_{j=1}^{n}\sum_{x_j=0}^{1}(-1)^{(a_j+y_j)x_j}$$

At least one sum in the product vanishes if $a_j \neq y_j$, i.e., the product equals 0, unless $y = a$. So, if we measure the input register finally, we get $|a\rangle$ because all $y \neq a$ will give a zero. That is,

$$H^{\otimes(n+1)}U_f H^{\otimes(n+1)}|0\rangle_n|1\rangle = |a\rangle_n|1\rangle$$

if $f(x) = a.x$.

4 Simon's Problem

In the previous sections we have discussed Deutsch's algorithm and the Deutsch-Jozsa algorithm. They deterministically answer whether (i) a given 1-bit Boolean function is constant or balanced, and (ii) a given n-bit Boolean function is constant or balanced (with a promise restriction on the n input bits), respectively. The promise in the second case is that the input string is either constant or balanced. The computation is possible with a single quantum gate for the given function realized as a control gate for that function. The Bernstein-Vazirani problem seeks a deterministic solution; finding an unknown bit string a by using a single quantum gate for the function realized as a control gate, in contrast to several evaluations in the classical case. In this discussion, we study another problem where we have a probabilistic solution with linear computation time, in contrast to a provably exponential time requirement in the classical case. This problem is due to Daniel Simon and this exposition is based on [2]. The function f is defined as $f : \{0,1\}^n \to \{0,1\}^n$, a two-to-one periodic mapping. The problem deals with computing the period of this function.

That is, for two distinct elements x, y (n-bit integers) from the domain, $f(x) = f(y)$ if and only if $y = x \oplus s$, where (i) $\oplus$ is the bitwise modulo 2 addition, (ii) x, y differ by an integral multiple, and (iii) s, the period, is an n-bit integer. We problem is to determine s, the period, given a quantum circuit, function control gate for f. So, we may find out two integers x and y, from the domain, that give rise to a match in $f(x) = f(y)$, giving period $s = y \oplus x$. Finding a match and thereby the period, requires an exponential number of trials in the classical case. To formulate the above problem in mathematical form we state it as follows.
Input: An integer $m \geq 1$ and a function $f : F_2^n \to R$, where R is finite set.
Promise: Does there exists a nonzero element $s \in F_2^n$ such that for all $x, y \in F_2^n, f(x) = f(y)$ if and only if $x = y \oplus s$.
Output: Element s.

As the domain of the problem is of n bits, there will be a total of $N = 2^n$ elements. Below, we present an argument of the necessity of an exponential number of trials for solving the problem classically. We pick elements at random. The probability that we will fail to find a match after the first trial (or for the second trial) is $\frac{N-2}{N-1}$, as we have $N-1$ remaining elements for selection in next trials and $N-2$ unfavourable. After the second trial we have $N-2$ remaining elements to select from and $N-4$ unfavourable cases for in the third choice. So, the probability of failure after the second trial is $\frac{N-4}{N-2}$. Continuing in this manner, the $(m+1)$st has probability of failure $\frac{N-2m}{N-m}$. So, the failure probability for $(m+1)$ trials is,

$$\frac{N-2}{N-1} \times \frac{N-4}{N-2} \times \ldots \times \frac{N-2m}{N-m} = \frac{1-2/N}{1-1/N} \times \frac{1-4/N}{1-2/N} \times \ldots \times \frac{1-2m/N}{1-m/N}$$

For sufficiently large N and small x we use $1 - x \approx e^{-x}$ and simplify the above as

$$= e^{-2/N} \times e^{-4/N} \times \ldots e^{-2m/N} / e^{-1/N} \times e^{-2/N} \times \ldots e^{-m/N}$$

$$= e^{-(2/N+4/N+\ldots+2m/N)+(1/N+2/N+\ldots+m/N)} = e^{-(1/N+2/N+\ldots+m/N)} = e^{-m(m+1)/2N}$$

This failure probability is can be made sufficiently small if $m(m+1)/2$ comparable to N. In other words, appreciable success probability results if m is be of the order of $\sqrt{N}$. So, we observe that an exponential number of trials are required for expecting the result. If $n = 100$ bits then we need approximately $2^{n/2} = 2^{50} = 10^{15}$ trials to get an appreciable chance for finding s.

Now we will see how we can solve this problem using a quantum algorithm. The procedure is as follows: The initial or input state is

$$|0\rangle_n |0\rangle_n$$

The application of the Hadamard operator on the first $|0\rangle_n$ yields the superposition state

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_n$$

The unitary operator ($U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$) converts the state to

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_n$$

Now, applying $H^{\otimes n}$ on the first n-bit register we obtain,

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{x.y}|y\rangle_n|f(x)\rangle_n$$

We observe the resulting state on both vectors to get $|y, f(x)\rangle$. Now for two distinct x say x, x_1, as per the assumption in the problem definition, $f(x) = f(x_1) \Leftrightarrow x_1 = x \oplus s$ and $s \neq 0_n$. So, for both $x_1 = x \oplus s$ and x, $|y, f(x)\rangle$ and $|y, f(x \oplus s\rangle)$ are identical. So their total amplitude is

$$\frac{1}{2^n}((-1)^{x.y} + (-1)^{(x\oplus s).y})$$

If $y.s = 0$ mod2 then $x.y = (x \oplus s).y$ mod 2. So the total amplitude becomes

$$(-1)^{x.y} * 2 * 2^{-n} = (\frac{1}{2})^{n-1}(-1)^{x.y}$$

Suppose we have run the process repeatedly and obtained $n-1$ such linearly independent vectors $y^1, y^2, ..., y^{n-1}$ such that $y^1.s = 0, y^2.s = 0, y^3.s = 0, \ldots y^{n-1}.s = 0$. Solving this set of $n-1$ equations we determine the non-zero value of s, the required period. Since we have defined f to be a two-to-one mapping, we do not have to check for $f(0)$ or $f(s)$. However, if the definition of f is not restricted in the beginning, then we have to check whether f is one-one ($f(0) \neq f(s)$) or two-to-one ($f(0) = f(s)$). The total computation time is proportional to the number of repetitions and the time required for a single evaluation of f on an n-bit input. Let $t(n)$ be and the time required to execute the quantum circuit once. Let the time required to solve these $n-1$ linearly independent equations be $g(n)$. Then, the total required time is $O(nt(n) + g(n))$.

Now we show that the $n-1$ observed vectors are linearly independent with probability at least $\frac{1}{4}$. Consider $y^1, y^2, \ldots, y^{n-1}$, the $n-1$ vectors measured in as many runs. For any set of $i-1$ vectors there are 2^{i-1} vectors resulting due to linear combination of these vectors. The probability that y^i is one of these (dependent vectors) is

$$\frac{2^{i-1}}{2^{n-1}} = \frac{1}{2^{n-i}}$$

because the total number of vectors satisfying $y.s = 0 mod 2$ is 2^{n-1} (the null space has dimension $n-1$). So, the probability that $y^1, y^2, \cdots, y^{n-2}$ are dependent is at most

$$\sum_{i=2}^{n-2}\frac{1}{2^{n-i}} \leq \frac{1}{2}$$

. So, the probability that the $n-2$ vectors are independent is at least $\frac{1}{2}$. Also, the probability that y^{n-1} is independent of the previous $n-2$ vectors is at least $1-\frac{1}{2^{n-(n-1)}} \geq \frac{1}{2}$. Whence, the result.

5 Quantum Fourier transforms and phase estimation

Consider the transformation of $\sum_{j=0}^{N-1} x_j|j\rangle$ to $\sum_{k=0}^{N-1} y_k|k\rangle$ for N-dimensional vectors, where x_j and y_k are complex numbers, and $N = 2^n$, n is the number of qubits. If

y_1, y_2,..., y_k,...,y_{N-1} form the DFT of x_1, x_2,..., x_j,...,x_{N-1} then this transformation is called the QFT. DFT is defined as follows:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N}$$

Naturally QFT is as follows:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

Note that the inverse of this transformation would get back $|j\rangle$ from $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$. So what goes into the phase of QFT viz., j, comes back by inverse QFT as $|j\rangle$. We see below a more complete construction using inverse QFT for estimating the phase in the eigenvalue of a unitary transformation U with eigenvalue $e^{2\pi i \phi}$ and eigenvector $|u\rangle$. That is,

$$U(|u\rangle) = e^{2\pi i \phi} |u\rangle$$

Here, the phase ϕ need be only a fraction as any integral part turns the phase by four right angles. Let the binary representation of (the fraction) ϕ be $0.\phi_1\phi_2 \ldots \phi_n$. We initially assume that the binary representation of this phase is finite and well within n bits so that n qubits suffice in representing a standard basis vector $|\phi_1\phi_2 \ldots \phi_n\rangle$.

The first step in generating the QFT of the standard basis state $|\phi_1\phi_2 \ldots \phi_n\rangle$ in the $2^n = N$ dimensional Hilbert space is the randomization step on the n qubits, where each of the qubits is initialized to $|0\rangle$. The ist qubit ($1 \leq i \leq n$) then performs a controlled-$U^{2^{i-1}}$ operation on the eigen vector $|u\rangle$. The first such operation is for $i = 1$, accumulating a phase $.\phi_1\phi_2 \ldots \phi_n \times 2^0 = \phi$; the last one for $i = n$, collects phase $.\phi_1\phi_2 \ldots \phi_n \times 2^{n-1} = 0.\phi_n$. The ist qubit gathers phase $.\phi_1\phi_2 \ldots \phi_n \times 2^{i-1} = 0.\phi_i\phi_{i+1} \ldots \phi_n$. These phases lead to the computation of the tensor product of qubit states

$$\frac{1}{2^{\frac{n}{2}}} \Pi_{i=1}^{n} (|0\rangle + e^{2\pi i 0.\phi_i\phi_{i+1} \ldots \phi_n} |1\rangle)$$

This is precisely the QFT of the basis vector $|\phi_1\phi_2 \ldots \phi_n\rangle$! [See Nielsen and Chuang [1]]. So, an inverse QFT would take this state to the basis state $|\phi_1\phi_2 \ldots \phi_n\rangle$. In this manner the n bits of the binary representation of the fractional phase can be determined. All we now need to do is to work out a quantum circuit for QFT followed by its counterpart, the quantum circuit for inverse-QFT. We know that the unitary transformation of QFT has its the conjugate transpose operator as its inverse. So, we can construct the circuit for inverse-QFT. In summary, we have now the mechanism for computing the phase exactly, for the eigenvector of an operator U given its eigenvector u.

There are therefore two steps in the ensuing *order finding* algorithm for the integer multiplication operator (modulo a prime N) (see [1]). First, we determine an eigenvector for the operator, and then we determine the phase of the eigenvalue.

Determining/creating the eigenvector is tricky; so, even if we do not have such an eigenstate, we can use any vector $|\psi\rangle = \sum_u c_u |u\rangle$ for eigenstates $|u\rangle$ of U. Use of such a vector would lower the lower bound on the success probability of estimating the right phase by a factor of $|c_u|^2$. See Exercise 5.8 [Nielsen and Chuang] [1].

To illustrate an example, we consider the unitary operator based on modulo N multiplication with a fixed number $x < N$ as

$$U|y\rangle = |xy(modN)\rangle, y \in \{0,1\}^L, L = \log N$$

[Show that U is unitary.] If r is the order of x i.e, $x^r = 1(modN)$, then there are r eigen vectors $|u_s\rangle$ of U, $0 \leq s \leq r-1$ as follows.

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\Pi isk}{r}} |x^k(modN)\rangle$$

We can see that

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\Pi isk}{r}} |x^{k+1}(modN)\rangle \\ &= e^{\frac{2\Pi is}{r}} |u_s\rangle \end{aligned}$$

This can be seen as (i) taking the eigenvalue exponent out increases the negative exponent in the term k by one unit, thereby matching x^{k+1} in the summation and (ii) rolling cyclically as r is the order of x.

Now it is not hard to show that $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$ (see Exercise 5.13, Nielsen and Chuang [1]). So, even in the absence of an eigenvector, we may proceed creating the state $|1\rangle$, which is easy to create. This will however erode the success probability as mentioned above. Nevertheless, we can proceed with phase estimation, initially assuming we have a sufficient number of qubits to represent the binary form of the fractional phase $\phi = 0.\phi_1\phi_2 \ldots \phi_n$ encoded/interpreted as the standard basis state $|\phi_1\phi_2 \ldots \phi_n\rangle$. When we do not have enough (qu)bits for exactly representing an unknown ϕ, certain errors creep leading to approximations upto a limited number of bits with provably specified (high) probability as shown in the standard literature [1]. Phase estimation has several applications, the most well-known being factoring the product of two large primes as in Peter Shor's seminal paper [3].

6 Order finding and factoring

Phase estimation for the eigenvalue(s) of the unitary operator $U|y\rangle = |xy(modN)\rangle$ yields fractional phase $\frac{s}{r}$, $0 \leq s \leq r$, if there are a sufficient number of qubits to fully encode this fraction in as many binary digits. From the fraction $\frac{s}{r}$ computed correctly to at least $2n+1$ bits, it is possible with finite probability to determine r; this is done using the continued fraction expansion of the fractional estimate of the phase $\frac{s}{r}$ (see Theorem 5.1 in [1]).

Now we detail an alternative scheme and its analysis, yielding the same results for the implementation of Shor's algorithm. The second (controlled) register $|y\rangle$ has $n = \log_2 N$ qubits, where N is the product of two large primes. The first register $|j\rangle$ requires $t = 2n + 1 + \lceil \log_2(2 + \frac{1}{2\epsilon}) \rceil$ qubits; the additional n qubits are required for modular exponentiation (see Box 5.2, [1]). The phase $\frac{s}{r}$ is estimated accurately upto $2n+1$ bits with probability exceeding $\frac{(1-\epsilon)}{r}$. The order of a random $x \leq N$ is $r \leq N(= 2^n)$, i.e., $x^r = 1 \bmod N$. We use the function $f(k) = x^k \bmod N$, $0 \leq k \leq M-1$. Here, $t = \log_2 M$.

The (qu)bit basis vector (integer) k, in the randomized superposition of the first register of $t = \log_2 M$ qubits, does a control operation over the second register of $n = \log_2 N$ qubits.

The first step is the usual randomization step of t Hadamard operations, one on each of the t qubits of the first register. This gives the transition

$$|0\rangle^t|0\rangle^n \Rightarrow \frac{1}{\sqrt{M}}(\sum_{k=0}^{M-1}|k\rangle|0\rangle^n)$$

Using a controlled-U_f we further get

$$\frac{1}{\sqrt{M}}(\sum_{k=0}^{M-1}|k\rangle|x^k mod(N)\rangle^n)$$

which may be written (using periodicity of f) as follows.

$$\frac{1}{\sqrt{M}}\sum_{l=0}^{r-1}(\sum_{q=0}^{s_l}|qr+l\rangle|x^l mod(N)\rangle^n) \tag{1}$$

Here, l stands for each partition of the periodic function, q determines the starting index of each run of r elements, and s_l gives the number of full periods for the periods with offset l. Clearly, for $0 \leq l \leq r-1$, $(M-r) \leq s_l r + l + 1 \leq M$

In an initial and simplified analysis, we first measure the second register, yielding $y = x^l \bmod N$, for some l, and thereby the state

$$\frac{1}{\sqrt{s_l+1}}\sum_{q=0}^{s_l}|qr+l\rangle \tag{2}$$

by ignoring the second register.

Assume for simplicity that $s_l + 1 = \frac{M}{r}$, that is, there is exact matching of full periods for index l. Now perform a QFT on the following state yielding the state

$$\sqrt{\frac{r}{M}}\sum_{q=0}^{s_l}|qr+l\rangle \tag{3}$$

yielding the state

$$\frac{1}{\sqrt{M}}\sum_{c=0}^{M-1}\sqrt{\frac{r}{M}}\sum_{q=0}^{s_l}e^{2\Pi ic(qr+l)/M}|c\rangle \tag{4}$$

Note that the probability amplitude of $|c\rangle$ is non-zero if and only if c is a multiple of $\frac{M}{r}$. Even when non-zero, the problematic item l appears in the complex exponent, making its effect irrelevant to the final probability of the different periodic outputs !

A slightly complicated analysis is required when s_l+1 is not the same as $\frac{M}{r}$. Continuing with the state in Equation 1, we perform a QFT on the first register yielding

$$\frac{1}{\sqrt{M}}\sum_{l=0}^{r-1}\sum_{q=0}^{s_l}\frac{1}{\sqrt{M}}\sum_{p=0}^{M-1}e^{\frac{2\Pi ip(qr+l)}{M}}|p\rangle|x^l mod(N)\rangle^n$$

The summation over $s_l + 1$ values of q determines the probability amplitude for each value of l. The multiplicative term $e^{\frac{2\Pi ipl}{M}}$ is inconsequential inspite of l, as it has unit modulus. So, we need only determine

$$b_{p,l} = \frac{1}{M} \sum_{q=0}^{s_l} e^{\frac{2\Pi iprq}{M}}$$

approximated as

$$\frac{1}{M}(\frac{1 - e^{\frac{2\Pi ipr(s_l+1)}{M}}}{1 - e^{\frac{2\Pi ipr}{M}}})$$

Now it is easy to show that $b_{p,l}b^*_{p,l}$ is

$$\frac{1}{M^2} \frac{sin^2(\frac{\Pi pr(s_l+1)}{M})}{sin^2(\frac{\Pi pr}{M})}$$

The outcome p is measured with this probability for a fixed l. This probability is roughly the same for all l since s_l is nearly $\frac{M}{r}$ for all $0 \leq l \leq r-1$. Therefore, the probability of measuring p is about $r|b_{p,l}|^2$, which can be shown to be at least $\frac{2}{5r}$ for p's such that p differs for an integral multiple of $\frac{M}{r}$ by at most $\frac{1}{2}$. Now these integral multiples can be from 0 through $r-1$, that is, r values, thereby rendering the probability of measuring such a p to be at least $r \times \frac{2}{5r} = 0.40$, which is 40% guaranteed success !

The probability calculation goes as follows. We underestimate the numerator and overestimate the denominator in order to show the 40% lower bound on the probability of getting such outcomes p as

$$|p - \frac{dM}{r}| < \frac{1}{2}$$

where d is an integer. So, the overestimation is done by substituting $\frac{\Pi pr}{M}$ by $\Pi(d+e)$ where e is either positive or negative with $|e| = \frac{r}{2M}$. The denominator $M^2 sin^2(\frac{\Pi pr}{M})$ is therefore

$$M^2 sin^2(\Pi(d+e)) = M^2 sin^2(\Pi e) \leq M^2(\Pi e)^2$$

The numerator $sin^2(\frac{\Pi pr(s_l+1)}{M})$ is underestimated as

$$sin^2(\Pi(s_l+1)(d+e)) = sin^2(\Pi(s_l+1)e) \geq (\Pi(s_l+1)e)^2 g^2(\Pi(s_l+1)e)$$

where $g(x) = \frac{sin(x)}{x}$. But $|g(\Pi(s_l+1)e)| = |g(\frac{\Pi}{2}(1+\epsilon))|$ since $(s_l+1)r$ is nearly M and no lesser, whereas $|e| = \frac{r}{2M}$. The numerator's underestimate is therefore

$$(\Pi(s_l+1)e)^2 g^2(\frac{\Pi}{2}(1+\epsilon))$$

which is nearly

$$= \frac{(\Pi(s_l+1)e)^2}{(\frac{\Pi}{2})^2} = 4(s_l+1)^2 e^2$$

The probability estimate is therefore $\frac{4}{r^2\Pi^2}$, which when multiplied by r gives $\frac{4}{r\Pi^2}$, nearly $\frac{2}{5r}$. Furthermore, d can take r values as already mentioned above, thereby enhancing the probability to at least 0.4 or 40%.

Now we have observation outcome p satisfying

$$|\frac{p}{M} - \frac{d}{r}| < \frac{1}{2M} \leq \frac{1}{2N^2} < \frac{1}{2r^2}$$

This enables computing r from the continued fraction of $\frac{p}{M}$ because p (and therefore this fraction), has been computed correct to at least $2n+1$ binary bits (see [1]).

7 Grover's Search

The problem we consider is to identify for a given function $f(x)$ ($f(x)$ is a function from $\{0,1\}^n$ to $\{0,1\}$), that x ($x \in \{0,1\}^n$) for which $f(x)$ is 1. In the classical sense this problem will take $N = 2^n$ evaluations of the function $f(x)$ in the worst case. There can be one or more values of x for which $f(x)$ is 1. Intuitively, however the problem of finding such a x in case $f(x)$ evaluates to 1 for just one x, is at least as hard as finding a x in the scenario where $f(x)$ evaluates to 1 for more that one values of x.

We'll therefore consider the somewht simpler case of where $f(x)$ is 1 for just one x, and will see that the method we develop can be generalized. This method we consider uses quantum parallelism (and other clever techniques) to achieve quadratic speed up ($\sqrt{N}$) over classical methods. Here it goes:-
We are given the quantum implementation of the function f as below

$$O: \quad |x\rangle_n |y\rangle \mapsto |x\rangle_n |y \bigoplus f(x)\rangle$$

If we prepare $|y\rangle$ as $|x-\rangle$ ($H^{\otimes}|1\rangle$), we can re-write above as

$$O: \quad |x\rangle_n \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mapsto (-1)^{f(x)} |x\rangle_n \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Ignoring the state of the last qubit, the action of O on a general state of quantum register is

$$O: \quad \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \mapsto \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \alpha_x |x\rangle.$$

The quantum register is prepared in the state $|0\rangle^{\otimes n}$, which is then put by applying the Hadamard transform $H^{\otimes n}$, in superposition state

$$|\psi\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_n$$

We now apply the following sequence of operations called *Grover* operator:

$$G = H^{\otimes n} P_0 H^{\otimes n} O$$

Where the conditional phase shift P_0 is given by

$$P_0 |x\rangle \mapsto \begin{cases} |x\rangle & x = 0 \\ -|x\rangle & x > 0, \end{cases}$$

OR

$$P_0 = 2|0\rangle\langle 0| - I$$

One can easily verify that the following holds

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

Now,

$$(2|\psi\rangle\langle\psi| - I)(\sum_x \alpha_x|x\rangle) = 2\sum_x |\psi\rangle\langle\psi|\alpha_x|x\rangle - \sum_x \alpha_x|x\rangle$$

$$= 2\psi \sum_x \alpha_x\langle\psi|x\rangle - \sum_x \alpha_x|x\rangle$$

$$= 2\psi \sum_x \frac{\alpha_x}{\sqrt{N}} - \sum_x \alpha_x|x\rangle$$

$$= 2\sum_x |x\rangle \sum_x \frac{\alpha_x}{\sqrt{N}} - \sum_x \alpha_x|x\rangle$$

$$= \sum_x(-\alpha_x + 2\langle\alpha\rangle)|x\rangle \text{ where } \langle\alpha\rangle \text{ is } \sum_x \frac{\alpha_x}{N}$$

It can be noted from the result of application of $(2|\psi\rangle\langle\psi| - I)$ on an arbitrary quantum state(in standard basis representation) that if we had negative amplitude(s), then they get boosted up (positively) at the cost of the remaining positive ones (remember that the square of probability amplitude is normalized to 1). In other words as much as the positive amplitudes of the arbitrary state before application were above the mean value, they will fall down the mean by the same amount after the application; the negative ones will be boosted over the old mean by the amount they were negative with. Application of O is precisely meant to negate the amplitude of those x for which $f(x)$ evaluates to 1 and therefore the above observation become applicable. Also, it is to be note that multiple application of G will keep on increasing the probability amplitude of those x in the original state $|\psi\rangle$ for which $f(x)$ is 1. After a "sufficient" number of applications of G we can expect to find such an x with high probability, completing our search. What exactly do we mean by this sufficient number of applications is discussed now.

Let $T = \{x\}$ for which $f(x) = 1$, and $S = \{0,1\}^n \setminus T$.

$$|\sigma\rangle = \frac{1}{\sqrt{N-1}} \sum_{x\in S} |x\rangle \quad \text{and} \quad |\tau\rangle = |x\rangle \quad ;$$

Now, any state in the hyperplane (of n-dimentional space) induced by $|\sigma\rangle$ and $|\tau\rangle$ can be written as $a|\sigma\rangle + b|\tau\rangle$ with $|a|^2 + |b|^2 = 1$. We have $O(a|\sigma\rangle + b|\tau\rangle) = a|\sigma\rangle - b|\tau\rangle$, which shows that the action of O on the hyper plane induced by $|\sigma\rangle$ and $|\tau\rangle$ is a reflection about $|\sigma\rangle$. We can write $|\psi\rangle$ as $(\sqrt{\frac{N-1}{N}}|\sigma\rangle + \sqrt{\frac{1}{N}}|\tau\rangle)$. It can therefore easily be shown that the action of $(2|\psi\rangle\langle\psi| - I)$ in the $|\sigma\rangle$ and $|\tau\rangle$ plane is a reflection about $|\psi\rangle$. Since the composition of two reflections is a rotation 1, it follows that one application of G rotates state vectors in the $|\sigma\rangle$, $|\tau\rangle$ plane by θ towards $|\tau\rangle$, where $\frac{\theta}{2}$ is the angle between $|\psi\rangle$ and $|\sigma\rangle$, i.e. $|\psi\rangle = \cos(\frac{\theta}{2})|\sigma\rangle + \sin(\frac{\theta}{2})|\tau\rangle$. Hence, after m iterations we have:

$$G^m|\psi\rangle = cos(\tfrac{2m+1}{2}\theta)|\sigma\rangle + \sin(\tfrac{2m+1}{2}\theta)|\tau\rangle$$

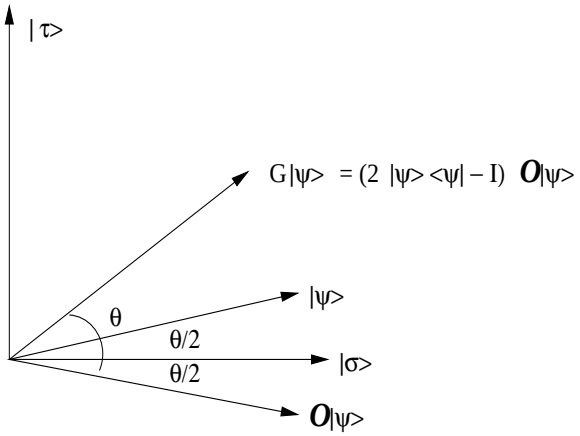

Figure 1: Action of Grover's operation.

It follows that when $\frac{2m+1}{2}\theta \approx \frac{\pi}{2}$, i.e. roughly after $(\frac{\pi}{2\theta} - \frac{1}{2})$ iterations, the state vector is within an angle $\frac{\theta}{2} \leq \frac{\pi}{4}$ of $|\tau\rangle$. Measurement of the state vector now will give a solution with probability at least $\cos^2(\frac{\pi}{4}) = \frac{1}{2}$. Therefore in the light of the following

$$\frac{\theta}{2} \geq \sin(\frac{\theta}{2}) = \sqrt{\frac{1}{N}}$$

we obtain an upper-bound for the number of iterations of G needed to find a solution: $m \leq \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$. The intuition for the general case will be as follows. If $f(x)$ is 1 for more that one values of x, and because θ depends on the angle between $|\psi\rangle$ and $|\sigma\rangle$, θ will be larger than in the case discussed above. In other words the worst case (in terms of the number of iterations req.) will happen if $f(x)$ is 1 for just one value of x and θ will be very small. In the general case the situation can only improve, which is also rational since it is easier to find something with more repetition in a set of fixed size than something which occurs just once.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2002.

[2] J. Gruska, *Quantum Computing*, McGraw-Hill, 1990.

[3] P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring.*, Proc. of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Press, Los Alamitos, CA, 1994.