# Report on Quantum Computing
# Algorithm Analysis and Design Project


Samay Kothari 2019113017
Kunal Jain 2019111037
Naman Ahuja 2019101042


November 2020

# Chapter 1

# Getting Started

## 1.1 Introduction

Quantum mechanics is the branch of physics that governs the world of elementary particles such as protons and electrons, and it is paradoxical, unintuitive, and radically strange.It is impossible to know the whole state of a quantum system because the very act of measuring the state(by which we get to know the state) disturbs the system. Instead of using the wave-particle duality to define the state of elementary particles, it is better to say that they behave in a "quantum mechanical" way.Particles do not have trajectories, but rather take all paths simultaneously (in superposition). And on top of that Richard Feynman infamously said "I think I can safely say that nobody understands quantum mechanics!. Some of the points worth noting about quantum mechanics are:

- The superposition principle explains how a particle can be superimposed between two states at the same time.
- The measurement principle tells us how measuring a particle changes its state, and how much information we can access from a particle.
- The unitary evolution axiom governs how the state of the quantum system evolves in time.

### 1.1.1 Birth of Quantum Mechanics

Until quite recently, the evidence strongly favored wave-like propagation. Diffraction of light, a wave interference phenomenon, was observed in 1655 by Grimaldi. A successful theory of wave-like light propagation, due to Huygens, was developed in 1678. Then, a major breakthrough came from Young's double-slit experiment. Then experiments like the Photoelectric effect and Black body radiations came long which were found inconsistent with the wave's nature of light. These phenomena were then explained by considering light as particles containing discrete packets of energy, called photons.

### 1.1.2 Young's Double Slit Experiment

The interference pattern observed on the screen from the two slits was explained appropriately by the wave's nature of light. Now consider placing a photo detector at the viewing screen, an bring down the intensity to the level that it only records the arrival of a photon occasionally. Initially, we would observe that as we turn down the intensity of the source, the magnitude of each click remains constant, but the time between successive clicks increases. From here, we can infer that light is emitted from the source as discrete particles (photons) — the intensity of light is proportional to the rate at which photons are emitted by the source. And since you turned the intensity of the light source down sufficiently, it only emits a photon once every few seconds. Now when a photon is emitted from a source, a question worth asking is where will the particle be detected on the screen. In other words, we can look at it from a probabilistic sense that what is the probability that the photon is detected on the screen as a function of x which is the distance from the mean position. Now, when only a single slit is opened, we observe that the probabilities are directly in sync with the interference pattern observed from a single slit. Intuitively, one would guess that if both the slits are opened, the probabilities of a photon being detected will directly be the sum of the probabilities observed when one of the two slits are opened separately. But, what we observe is the probabilities observed are again in sync with the interference pattern(intensities) observed when both the slits are open. This is where the particle nature, fails to explain the behaviour of particles . The nature of the contradiction can be seen even more clearly at "dark" points x, where the probability of detection is 0 when both slits are open, even though it is non-zero if either slit is open. This truly defies reason! Particles do not have trajectories, but rather take all paths simultaneously (in superposition). Explanation of this phenomenon: We posit that instead of taking a single path from the source to the screen, it has a probabilistic amplitude A1(y) with which, it goes through slit 1 and A2(y) with which, it travels through the second slit. There is no specific path decided for the photon, but the photons follow a "superposition of both the paths". In essence, the exact path of the photon is unknown.

### 1.1.3 EPR Paradox and Bell's inequality

In 1935, Albert Einstein, Boris Podolsky, and Nathan Rosen developed a thought experiment to demonstrate what they felt was a lack of completeness in quantum mechanics. A principal feature of quantum mechanics is that not all the classical physical quantities can be defined with unlimited precision. They believed that there must exist a different set of observables that give qualitatively different but complete and accurate descriptions of a quantum mechanical system. A perfect analogy for this can be given by defining it by an experiment. Consider the examples of tossing a coin. For all common purposes, we believe that the outcome of a coin toss is completely random-heads and tails with equal probability. Now, one could argue that if one knew all the parameters like position,

momentum, then we could use Newton's law to calculate which side will face up. One more way to say this is that this coin flip amplifies our lack of knowledge about the system which makes the output completely random. Similarly, Einstein believed that the randomness of quantum measurements reflected our lack of knowledge about additional degrees of freedom, or what Einstein called "hidden variables", of the quantum system. He gave this famous statement in regard to this experiment, "God does not play dice" arguing that there was an objective truth that was undiscovered in the field of quantum mechanics that didn't rely on probabilistic measurements.

Bell came up with the following experiment to test the EPR paradox. Let us assume that two particles are produced in the Bell state $|\psi+\rangle$ in a laboratory, and then fly in opposite directions to two distant laboratories. Upon arrival, each of the two qubits is subject to one of two measurements. The decision about which of the two experiments is to be performed at each lab is made randomly at the last moment, so that speed of light considerations rule out information about the choice at one lab being transmitted to the other. The measurements are cleverly chosen to distinguish between the predictions of quantum mechanics and any local hidden variable theory. Concretely, the experiment measures the correlation between the outcomes of the two experiments. The choice of measurements is such that any classical hidden variable theory predicts that the correlation between the two outcomes can be at most 0.75, whereas quantum mechanics predicts that the correlation will be at most $cos^2\pi/80.85$. Thus the experiment allows us to distinguish between the predictions of quantum mechanics and any local hidden variable theory! Therefore this ruled out any theories about a hidden variable and verified the fact that the qubits/electrons are in-fact, in a superposition of states complete information about their orientation can not be known.

# Chapter 2

# Delayed Measurement and Quantum Eraser

## 2.1 Introduction

The double slit experiment led to discussions about the mysterious quantum mechanics and how to encapsulate the wave nature(the interference behaviour) and particle behaviour(no-interference) of the light into a single unified theory. As per the most common double-slit experiment, either the slit from which the photon passes through is not observed and interference is obtained on the screen or we can place detectors for getting the information about the slit from which the particle is passed and there is no interference.

These two experiments are completely different from each other because we can't detect the slit of the photon without destroying the interference pattern. This is an illustration of the complementarity or the uncertainty principle. One of the explanation that can be given is, the observation about the slit causes disturbance to the photon which results to loose the interference pattern.

This led Wheeler to propose "delayed choice" experiment to analyze when exactly the photon "decides" to which behaviour it is going to adopt. The choice of measurement(whether to measure or not) is made at very last moment.

## 2.2 Delayed Choice Experiment

### 2.2.1 The experiment:

Delayed choice experiment was a an extension of double slit experiment and was proposed by **Wheeler**, rather than a fixed screen to detect light, it had a removable screen and behind that was two detectors(pointing precisely at each of the slits) for detecting the the slit from which the photons came through.

The basic essence of this experiment and the others which followed it, was that the choice to detect the slit from which the photon went through can be made at last moment. If the screen in present we can't get knowledge about the slit from which the photon passed but the interference will be observed, and if the screen is removed then only one of the detector clicks giving us the knowledge about the path of the photon.

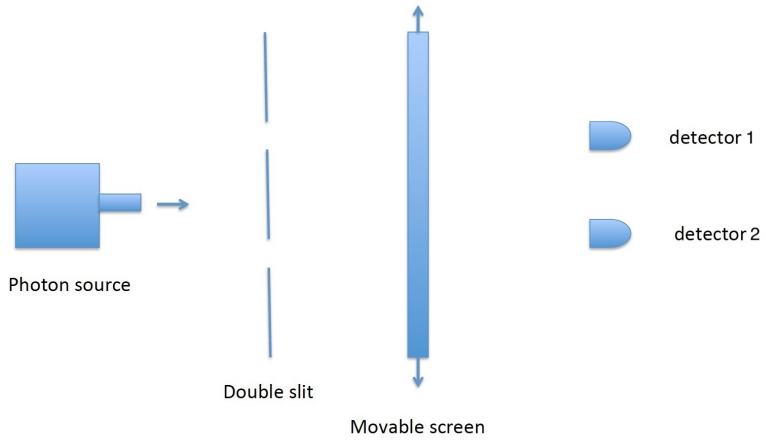



Figure 2.1: Delayed choice double slit experiment

The usual presentation of this behaviour can be given as when the screen is present(interference), each photon decides to travel through both of the slits, but when the screen is removed then the photon decides only one of the slit to pass through. *This is strange.* A possible interpretation can be that the photon is "informed" of the presence of absence of screen. A delayed choice here means we can increase the distance between the slit and the screen and remove or add the screen well after the time the photon passed through the slit. So in simple but absurd words we can say that "*the decision to keep or remove the screen is having an influence on the decision that has been made in past*".

### 2.2.2 Mathematical Interpretation

**When the screen is present**

We can write the wave function of the photon immediately after it crosses the slits as a sum of two spherical waves:

$$\psi(\vec{r}) = \frac{1}{|\vec{r} - \vec{r_1}|} e^{ik|\vec{r}-\vec{r_1}|} + \frac{1}{|\vec{r} - \vec{r_2}|} e^{ik|\vec{r}-\vec{r_2}|} \tag{2.1}$$

Where we have k as the wave number of the photon and $\vec{r_1}$ and $\vec{r_2}$ are the locations of the slits. Also we know the distance between the slits can be approximated to $d \sin\theta$ where d is the distance between the slit and the screen

and $\theta$ is the angle between the point of interference and center of the slits. So we can write:

$$|\vec{r} - \vec{r_1}| - |\vec{r} - \vec{r_1}| \sim d \sin\theta \tag{2.2}$$

Using this in the expression of the wave function:

$$\psi(\vec{r}) \sim \frac{1}{|\vec{r} - \vec{r_1}|} e^{ik|\vec{r}-\vec{r_1}|}(1 + e^{ikd\sin\theta}) \tag{2.3}$$

Using this equation we can say that constructive and destructive interference will occur at the points $kd\sin\theta = 2n\pi$ and $kd\sin\theta = 2(n+1)\pi$ respectively. Thus the light will be showing a wave like behaviour and the screen is behaving as an apparatus that measures continuous position variable.

**When the screen is absent**

Now if we remove the screen and the measure the momentum(detectors measure the momentum of the incoming photons) the incoming photons with a narrow detection range then we can write the wave function as:

$$\psi(\vec{r}) \sim \frac{1}{|\vec{r} - \vec{r_1}|} e^{i\vec{k_1}(\vec{r}-\vec{r_1})} + \frac{1}{|\vec{r} - \vec{r_2}|} e^{i\vec{k_2}(\vec{r}-\vec{r_2})} \tag{2.4}$$

Where $\vec{k_1}$ and $\vec{k_2}$ are wave-vectors of size $k$ in the direction of slit to the point of detection, direction specifically given by $\vec{r_T} - \vec{r_1}$ and $\vec{r_T} - \vec{r_2}$ where $\vec{r_T}$ is the location of the detectors(since we are considering narrow detection range).

Since the detector measures the momentum of the incoming photon we can say that when the detector1($D_1$) clicks, the momentum of photon becomes close to $\vec{k_1}$ and when detector2($D_2$) clicks, the momentum of photon becomes close to $\vec{k_2}$. We can consider this as an apparatus that measures a two valued($D_1$ and $D_2$) momentum observable. So when the wavefunction is measured using this apparatus, it can be written as:

$$\psi(\vec{r}) \sim \frac{1}{|\vec{r} - \vec{r_1}|} e^{i\vec{k_1}(\vec{r}-\vec{r_1})}|D_1 clicks\rangle + \frac{1}{|\vec{r} - \vec{r_2}|} e^{i\vec{k_2}(\vec{r}-\vec{r_1})}|D_2 clicks\rangle \tag{2.5}$$

(Wavefunction not normalised)
Thus we have a superposition of states and the probability of each of the states $D_1$ and $D_2$ click are proportional to $\frac{1}{|\vec{r}-\vec{r_1}|}$ and $\frac{1}{|\vec{r}-\vec{r_2}|}$ respectively, which are equal, so clicking of each detector has a 50 percent probability.

### 2.2.3 Possible Explanation

The mathematical formulation gives us an idea about how the weird behaviour of the delayed measurement can be explained, the argument that the path followed by the photon is dependent on its measurement is false. A better explanation to this will be that the photon has quantum behaviour(as depicted by $\psi(\vec{r})$in

equation 1) from the moment it is generated till point it is measured(by the screen or the detector), that is until a measurement is made on it.

It means that photon as depicted by $\psi(\vec{r})$ follows both the route until it is measured. After the measurement, the quantum state(wave function) collapses to one of the possible eigen-vector of the observable measured(two valued momentum observable in case of the detectors and a continuous position observable in case of screen). This measurement is reflected by the interference pattern on the screen or the clicking of the detector in their respective experiment setup.

Considering all the counter arguments against the claim, "that you can influence the decisions of the past", it now seems useless because the photon followed both the path before it was measured and removing or adding the screen at the very last moment seems of no special interest now.

## 2.3 Delayed Choice Quantum Erasure

These experiments are somewhat a generalisation of the entanglement situation. They show that the loss of interference or information about the slit on one particle is not due to the uncertainty principle, but because of the measurement of the twin(entangled) particle.

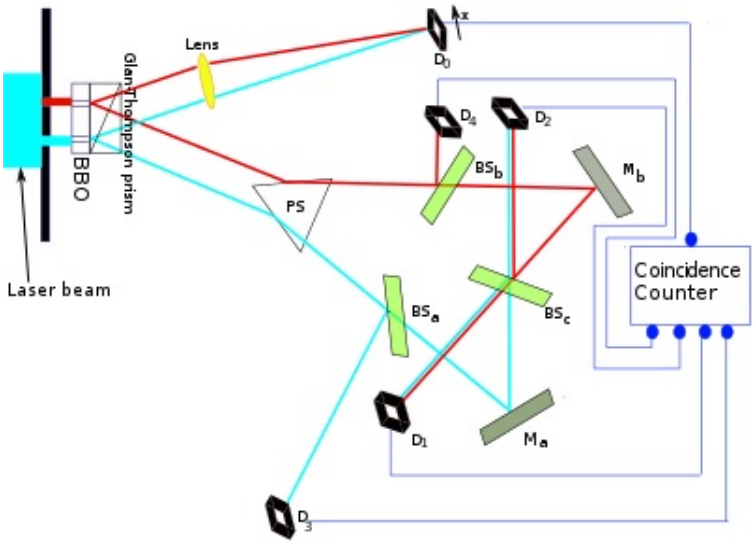



Figure 2.2: Delayed choice quantum eraser

### 2.3.1 Experiment

For this experiment after the point when the photons passes through the slits, they are encountered by BBO crystal, which converts each of the photon into two entangled photons of half energy than the original photon, here $D_0$ is a movable detector that detects the interference pattern for the photons that are travelling upward(called the *signal photons*) and the photons travelling downwards(called the *idler photons*) are received by a prism and a set of beam splitters(BS) and mirrors(M). The idler photons then are detected by the detectors $D_1 - D_4$(depending upon the path the photon chooses). Also the setup is such that path of signal photons from the crystal to the detector is shorter as compared to the path in case of idler photons.

Here we can see that if the detectors $D_3$ or $D_4$ clicks then the photon has travelled through one of the routes, but if the detectors $D_1$ or $D_2$ clicks then we are not sure about the path that the photon has travelled. The beam splitter $BS_c$ is acting as a quantum erasure because if it present it no more possible to know the path of the photon which was detected by $D_1$ and $D_2$ and if it is absent then we can know the path of the photons, if $D_1$ clicks then upper slit and if $D_2$ clicks then the lower slit and the interference pattern is lost.

So we can say that the keeping or removing of the quantum eraser is affecting the measurement of the signal photons, but the measurement of the signal photons is done earlier in time(because of short path). *This is quite strange.* Another argument to this can be that the measurement and the results of the detector 0 can be used to predict the future(whether the quantum eraser is removed in future or not). *Again this is also quite strange.*

### 2.3.2 Discussion

At first glance at the observations of the experiment seems very amusing but they are quite misleading. One important point to notice here is that, it is possible to extract an interference pattern or a discrete pattern only through extraction from all the detections by $D_0$ for corresponding $D_i's$. Blatantly looking for pattern at $D_0$ doesn't gives us anything but a pattern of random points. Mathematically we can say that

$$D_0 = \sum_{i=1}^{4} D_i$$

Meaning that the information(peak and troughs) at $D_0$ is the sum of the information of all sensors, detected using the idler photos.

This has a consequence, that it is impossible to use this device to transmit information from the future to the past because recognizing an interference pattern is possible only when one have the knowledge of which detection of signal

photon by $D_0$ corresponds to which detector $D_i$ of the twin idler photon.

The tempting idea of removing or adding the beam splitter($BS_0$) in far future to produce the interference($BS_0$ present) or to remove the interference($BS_0$ absent) in present, is not working because of the fact that you can't extract the information about the interference patter of discrete pattern just by looking at the screen(detector $D_0$), since the interference pattern related to $D_1$ and $D_2$ have a $\pi$ phase shift, thus they produce exactly the same image as it is produced when there is no interference pattern.

### 2.3.3 Mathematical Interpretation

We can use the fact about the entangled particles that the order of measurement does not affect the conditional probabilities.
We can write the wave function right after the slit but before the crystal as:

$$|I\rangle \rightarrow \frac{1}{\sqrt{2}}[|U\rangle + |L\rangle] \tag{2.6}$$

Where $|U\rangle$ and $|L\rangle$ signifies photons passing through upper slit and lower slit respectively, equation 6 signifies the superposition of the paths. Then the each component are split into entangled pairs, one going upwards and one going downwards.

$$|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}\left[|US\rangle|UI\rangle + |LS\rangle|LI\rangle\right] \tag{2.7}$$

Where S and I indicates the signal and idler photons(for example $|US\rangle$ refers to photon coming from upper slit and going upward towards the screen $D_0$).
Now the idler photons are measured by the set of detectors $D_1 - D_4$, we can mathematically write this as:

$$|]\psi\rangle \rightarrow |US\rangle\left[\frac{1}{2}|4\rangle + \frac{1}{2\sqrt{2}}|1\rangle + \frac{1}{2\sqrt{2}}|2\rangle\right] + |LS\rangle\left[\frac{1}{2}|3\rangle + \frac{1}{2\sqrt{2}}|1\rangle + \frac{1}{2\sqrt{2}}|2\rangle\right] \tag{2.8}$$

This equation is similar to equation of bell's entangled pair(EPR pair), to see it more clearly we can write it as:

$$|]\psi\rangle \rightarrow |U\rangle^S\left[\frac{1}{2}|4\rangle + \frac{1}{2\sqrt{2}}|1\rangle + \frac{1}{2\sqrt{2}}|2\rangle\right]^I + |L\rangle^S\left[\frac{1}{2}|3\rangle + \frac{1}{2\sqrt{2}}|1\rangle + \frac{1}{2\sqrt{2}}|2\rangle\right]^I \tag{2.9}$$

Wave function for an entangled pair can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|+\rangle^A|-\rangle^B - |-\rangle^A|+\rangle^B\right] \tag{2.10}$$

Here S and I stands for two entangled particles A and B, and $|U\rangle$ and $|L\rangle$ stands for the states of particle A $|+\rangle$ and $|-\rangle$, while the second part of both terms stand respectively for states $|-\rangle$ and $|+\rangle$ for particle B. So we can see that equation 9 and 10 are similar and equation 10 represent entangled particles.

Now we know that the correlations between the measurements on the two particles will be independent of the order in which the measurements are done. So we can assume that the measurement of the idler photon is done first. We can rewrite the equation 9 as:

$$|\psi\rangle = \frac{1}{2\sqrt{2}}|1\rangle^I \left[|U\rangle + |L\rangle\right]^S + \frac{1}{2\sqrt{2}}|2\rangle^I \left[|U\rangle + |L\rangle\right]^S + \frac{1}{2}|4\rangle^I |U\rangle^S \qquad (2.11)$$

Now if we look at the wave function written in this form we can see that when the idler photon is detected by $D_1$ or $D_2$ then we will observe an interference pattern for the signal photon and the path of the photon will be unknown and if it is detected by $D_3$ or $D_4$ then we will not have interference pattern for the signal photon but will have deterministic knowledge about the slit from which the photon came through.

- While this mathematical interpretation may seem clear because we reversed the order of measurement arguing the independence of order of measurement on entangled particles, but the very physical meaning of this order independence is quite unclear.
- Another problem is that we are taking for granted the reduction postulate and the collapse of the wave function.

## 2.4 Conclusion

Thus the reasoning of this experiment came to the phenomena of entanglement and how it can happen in time independent manner and what is the physical meaning of collapse of wave function. These are one of the most weird and controversial results of the quantum mechanics.

But thinking from a different view, we can use this experiment to understand how a quantum mechanics system hides information from us, we tried our best to get the path as well the interference pattern for the photon but the quantum mechanical system chose to hide it from us.

This can be pointed out as one of the short comings of quantum information and quantum computation(because if it is possible then you can get exponential increase on already existing quantum computing algorithms which are themselves a big improvement on the classical algorithms), you can be so close to the solution but still be very far, because of the very reason that you can't access the probability distribution of a single particle, because as soon as you measure it, the wave function collapse.

# Chapter 3

# Simon's algorithm

## 3.1 Introduction

Let $N = 2^n$ and the set $\{0, 1, ..N-1\}$ be written as $\{0,1\}^n$ and let $i + j$ be bitwise modulo 2 addition of $i$ and $j$.
For example, $110 + 011$ would result in 101 as $1 + 0 = 1 \mod 2$ for the first bit, $1 + 1 = 0 \mod 2$ for the second bit and $0 + 1 = 1 \mod 2$ for the third bit.

## 3.2 The problem

For a given $N$, let there be a secret function $x = (x_0, x_1, ..., x_{N-1})$ where $x_i = \{0,1\}^n$ with the property that for some unknown $s$, $x_i = x_j$ iff $i = j$ or $i = j + s$.

Our task is to find out $s$ using the function $x$

## 3.3 Classical solutions

One of the most simple and efficient classical algorithms for this is to randomly get $X$ values from the function $x$. Let the set of distinct numbers be $\{a_1, a_2, ..., a_X\}$. The probability that atleast 2 of them yield us the same value can be calculated with the help of the birthday paradox.
The number of pairs in our selected set that could yield us the same value are ${}^TC_2 \sim \frac{X^2}{2}$ and the probability for any given pair to have the same value is $\frac{1}{N-1}$.
Using linearity of expectation, we can expect approximately $\frac{T^2}{2*N}$ pairs to have the same value.
Thus, choosing $T = \sqrt{2^{(n+1)}}$, we can expect about 1 pair to have the same value and thus find the value of $s$.

## 3.4 Quantum solution

Given the exponential complexity for the simon's algorithm using classical computers, using the quantum algorithms we can improve the time complexity to linear time.

1. We use 2n zero qubits $|0^n\rangle|0^n\rangle$ and then apply hadamard transforms to the first n qubits only, which will result in state:
$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|0^n\rangle$$
2. Now this state is passed through the black box, that is given to us and is known to be periodic, this query turns this into:
$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|x_i\rangle$$
3. Now the second n-bit register is measured and the state collapses to one of the given distinct answers that are possible for the function with probability $\frac{1}{\sqrt{2^n}}$, now the state can be written as:
$$\frac{1}{\sqrt{2}}(|i\rangle + |i \bigoplus s\rangle|x_i\rangle)$$
4. Now we will ignore the second n bit register that have the $|x_i\rangle$ state and then apply Hadamard transforms(inverse fourier transform) to the first n qubits. We can write the state further as:
$$\frac{1}{\sqrt{2^{n+1}}} \left( \sum_{j \in \{0,1\}^n} (-1)^{i.j}|j\rangle + \sum_{j \in \{0,1\}^n} (-1)^{(i \bigoplus s).j}|j\rangle \right)$$
5. Now this can be written as(using $(i \bigoplus s).j = (i.j) \bigoplus (s.j)$:
$$\frac{1}{\sqrt{2^{n+1}}} \left( \sum_{j \in \{0,1\}^n} (-1)^{i.j}(1 + (-1)^{(s.j)}|j\rangle) \right)$$
6. Now if we look at the state equation we can see that $|j\rangle$ has non-zero amplitude if and only if $s.j = 0 \mod 2$. Measuring the state gives us a uniformly random element from the set $\{j | s.j = 0 \mod 2\}$. So we will get a linear equation that gives information about s since we already know what j is(result of measurement of after the inverse fourier transform is done).
7. Now we repeat these steps until we get distinct $n-1$ linear equation for s. The solutions to linear equation will give us correct s(can be done in complexity of $\mathcal{O}(n^3)$. You will get $n-1$ linearly independent equations in $4n$ steps of this algorithm with 0.99% probability.

## 3.5 Analysis and comparison

Thus, we see an exponential speed up in this case.
The classical algorithm gives an expected value of $\sqrt{\frac{2^n}{2}}$ required queries to find out the value of $s$ while the quantum algorithm can find $s$ in 4n queries and some polynomial classical computations(for solving the linear equations) with 0.99 probability.
This speeds up our expected query complexity from $\Omega(\sqrt{N})$ to $\mathcal{O}(n)$
The speed up serves a major speed up for Shor's algorithm and is a subset of the Abelian hidden subgroup problem.

# Chapter 4

# Shor's factoring algorithm

## 4.1 Introduction

Given a number $N$, we are trying to find it's prime factors.

## 4.2 Classical solutions

The numbers that are the hardest to factorize have found to been products of 2 large prime numbers. The best classical algorithm published till now is the General Number Field Sieve (GNFS) Algorithm that runs on a $b$ bit number $n$ times in time complexity:

$$exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)\right)$$

which is still exponential.

## 4.3 Importance and RSA encryption

Almost all modern cryptography techniques rely on the assumption that it is very hard to factorize numbers that are the products of 2 large prime numbers, and that this can not be done in better than exponential time with respect to number of digits. Such numbers are called semi-primes.
RSA, named after it's creators Rivest, Shamir and Adleman, is one of the oldest and most widely used algorithm that relies on this assumption. RSA laboratories even released a list of semi-primes in 1991 as part of the RSA Factoring Challenge for people to factories and even rewarded the people who did. The largest semi prime released by them had 2048 digits, the largest that has till now gotten factored has 250.
This goes on to show how integral the lack of a classical fast factorization algorithm for semi-primes is to the world of cryptography.

## 4.4 Period Finding

The cornerstone observation of Shor's algorithm is it's reduction of factoring to period finding. There already exists an efficient algorithm for period finding which uses quantum computing.
Suppose we are trying to factor a number $N$. If $N$ is even or a prime power, we check and solve those using efficient classical algorithms. For the cases when $N$ is odd and not a prime power, we randomly pick a number $x \in \{2, ..., N-1\}$. We can check if $x$ is coprime to $N$ or not using classical algorithms again.
Now, we have $N$, which is odd and not a prime power, and $x$, which is a coprime to $N$. Considering the sequence $x^0 = 1\, mod N, x\, mod N, x^2\, mod N, ...$ in the multiplative group $\mathbb{Z}_{\mathrm{N}}^*$. The sequence cycles itself after some time. Assuming the period to be $r$, we can say that

$$x^r = 1 \mod N$$

$$x^r - 1 = 0 \mod N$$

$$(x^{\frac{r}{2}})^2 - 1^2 = 0 \mod N$$

$$(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = 0 \mod N$$

$$(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = k\mathrm{N} \text{ for some k}$$

Now, we can prove that the probability of $r$ being even and $x^{\frac{r}{2}} + 1$ and $x^{\frac{r}{2}} - 1$ are not multiple of $N$ is $\geq 1/2$.
Hence, when that is the case, we can compute compute $gcd(N, x^{\frac{r}{2}} + 1)$ and $gcd(N, x^{\frac{r}{2}} - 1)$ to get 2 non trivial factors of $N$!

## 4.5 Shor's Algorithm

1. We are given a number B which is an m bit number and is product of two large prime numbers P and Q. Consider $m \simeq 1000$ and P and Q to be $m/2$ bit numbers

2. Then we assume R as non-trivial square root of 1 mod $B$

$$R \neq \pm 1 \mod B$$

$$R^2 - 1 = 0 \mod B$$

$$(R-1)(R+1) = 0 \mod B \;\; also\, B = P * Q$$

3. Since P and Q are prime numbers so we will have $P/(R-1)$ and $Q/(R+1)$

4. So we have that gcd$(R+1, B)$ gives us either P or Q

5. Now we have to find R

6. Let us consider

$$\begin{aligned} Z_B^* &= \{integers A \in Z_B \; with \; \gcd(A,B) = 1\} \\ &= \{integers A \in Z_B \; such \; that \; A^{-1} \mod B \; exists\} \end{aligned}$$

7. Now we pick A randomly between 0 to B-1 and calculate $\gcd(A, B)$, let's take A to be about $m/2$ bit number.

   - If the $\gcd(A, B) = 1$ (which will be the case most of the times) then we can proceed further.
   - If the $\gcd(A, B) \neq 1$, which is very less likely, then there is no need to proceed further, A will be P or Q.

8. Now we can see that

$$\begin{aligned} A &\mod B \\ A^2 &\mod B \\ A^3 &\mod B \\ &\vdots \\ A^L &\mod B = 1 \end{aligned}$$

   Also for each of powers of A, $A^i \mod$ B will be distinct, because if it is not $A^{i-j} \mod B = 1$ for i and j having same value for $A^x \mod B$.

9. Now we can define L as the order of A in $Z_B^*$

   Since we have B as pretty large, then L is also large, so we can't just keep on calculating for powers of A modulo B to find L. This is where we incorporate quantum computing into the picture, before this all of the computations are be done classically.

   We now have a function which is L periodic given by $F_A(X) = A^X \mod B$, the period L of the function is dependent on randomly chosen A.

## 4.6 Analysis and comparison

We can calculate the function F using modular exponentiation, which makes it solvable in "P", the complexity for the same will be $\mathcal{O}(m^3)$, in fact this can be reduced to $\mathcal{O}(m^2)$ time. Now this function can be implemented using $m^3$ classical logic gates.
Thus using $m^3$ quantum gates(quantum circuit $Q_F$) we can implement F in a reversible manner.
Thus we will be having a quantum circuit which implements a periodic function with period L(which is unknown to us).

Even the best of classical algorithms are able to factorize semiprime numbers

in exponential time whereas Shor's algorithm is able to do so in polynomial complexity ($\mathbb{O}(m^3)$ quantum gates and $\mathbb{O}(m^3)$ classical gates).

# Chapter 5

# Grover's Search Algorithm

## 5.1 Introduction

Searching an item in an unsorted table or array of size N costs a classical computer O(N) running time. Grover, in 1995 posited that a quantum computer can perform the same search in $O(\sqrt{N})$.Though this speedup is not as an exponential speedup as seen in prime factoring natural numbers (Shor's Algorithm), Grover's algorithm still has various applications such as speedup algorithms for NP-complete algorithms. In 1994, before Grover's algorithm, it was proved that a quantum computer needs to make atleast $\sqrt{N}$ queries to perform a successful search.

## 5.2 Setup

Let our sorted list contain $N = 2^n$ elements. The length of the list is usually taken to be an exponential power of 2 for easier understanding as we can represent every element in the list by a state given by the superposition of the n qubits we'll be using. We define two function; An Oracle Function and a Diffusor Function that we will be repeatedly using in the algorithm.

### 5.2.1 The Problem

Let us model the problem as follows: Let f:{1,2,3....N} $\rightarrow$ {0,1} be a boolean function where it is given that f(a) = 1 for exactly one a $\epsilon$ {1,.....N}. Obviously, a is the element we are looking for. Therefore, we can model the problem as finding the value of a such that f(a) = 1 .

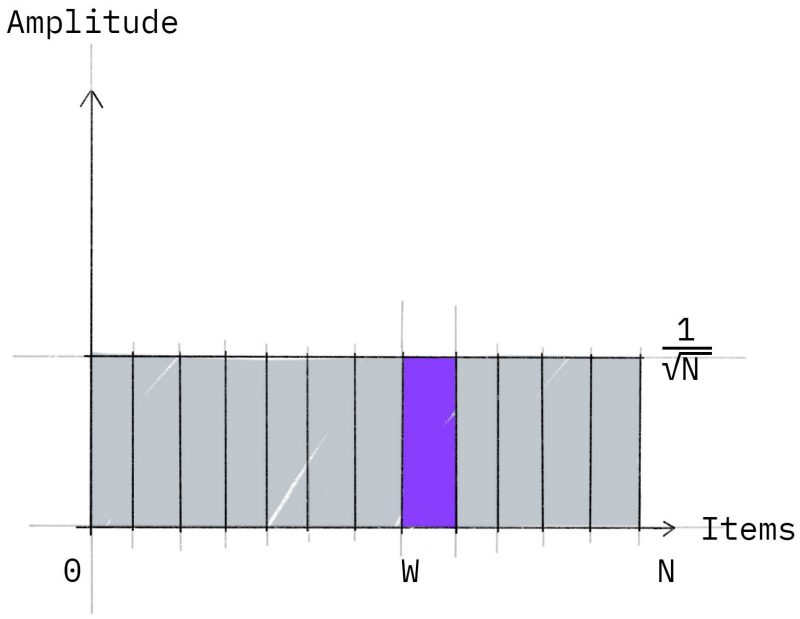
### 5.2.2 Qubits

To start off, we prepare a uniform superposition of n qubits ($N = 2^n$; N is total number of elements.) Let $|\psi_t\rangle$ represent the state of the qubits at any iteration.

This can be easily done by using n hadamard gates $|s\rangle = H^{\otimes n}|0\rangle^n$ . Therefore we get

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

.




### 5.2.3 Oracle Function

We define an oracle function for f:{1,2,.....N} → {0,1} defined as:

$$U_\omega|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

The oracle function will be a diagonal matrix, where the entry corresponding to the marked item will have a negative phase. Therefore our oracle function takes a proposed solution x, and returns f(x) = 0 if $x \neq \omega$ and f(x) = 1 for $x = \omega$ . Note that the oracle function depends on the answer we are searching for and changes accordingly with the answer we are looking for. The oracle can

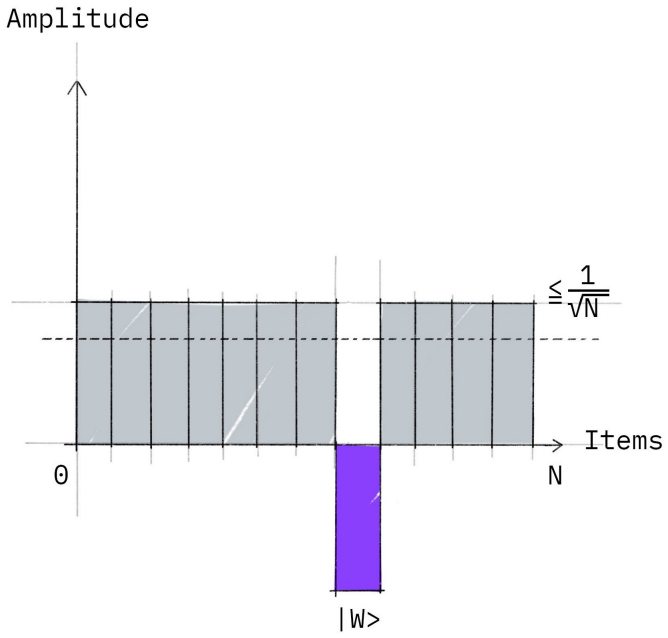
be written as:

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle$$

The oracle matrix will be a diagonal matrix defined as:

$$U_\omega = \begin{bmatrix} (-1)^{f(0)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(1)} & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(2^n)} \end{bmatrix}$$

Let $|a\rangle$ be the answer state.After creating a superposition of the qubits, we now apply the oracle matrix to s. As explained in the setup before, the superposition obtained has the phase of the $|a\rangle$ flipped. We have $|\psi_t\rangle = (U_f)|s\rangle$.




### 5.2.4 Diffusor Function

The Diffusor function, also known as the Grover Operator or the Amplitude Amplification Operator is a linear operator which takes as input n amplitudes and "flips them about their mean". It means taking a reflection of the amplitudes about their mean. For example consider a superposition of 3 qubits with amplitudes :

$$A(|x\rangle) = \begin{cases} \frac{-1}{2\sqrt{2}} & \text{for } x = |011\rangle \\ \frac{1}{2\sqrt{2}} & \text{otherwise} \end{cases}$$

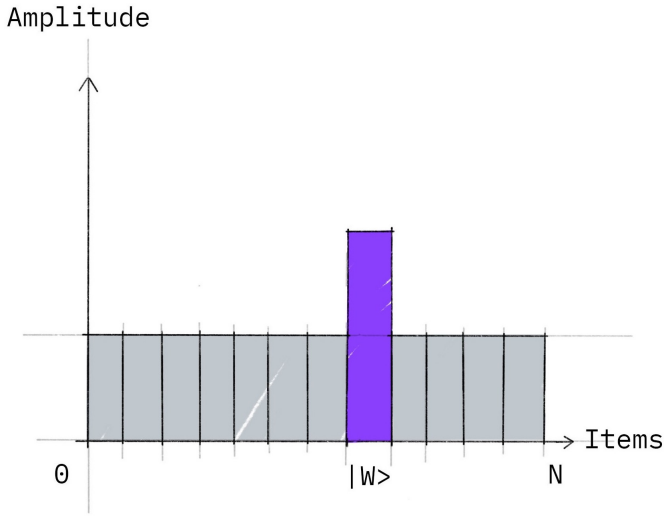
The two figures graphically show the amplitudes distribution before and after applying the Diffusion operator or flipping the amplitudes about its average. Mathematically the operator is defined as $U_s = 2|s\rangle\langle s| - 1$. After applying the Diffusion Operator we get $|\psi_t\rangle = (U_s U_f)|s\rangle$.Now, one iteration of the algorithm is complete.

Now after one iteration(applying oracle and diffusion once) we see that the amplitude of the answer state has increased. Ofcourse, our goal is to increase that amplitude as much as possible, (bring it close to 1) so that when we measure it, the qubit always collapses to the required answer state.

Initially,

$$A_0 = A_1 = ....A_{N-1} = 1/\sqrt{N}$$

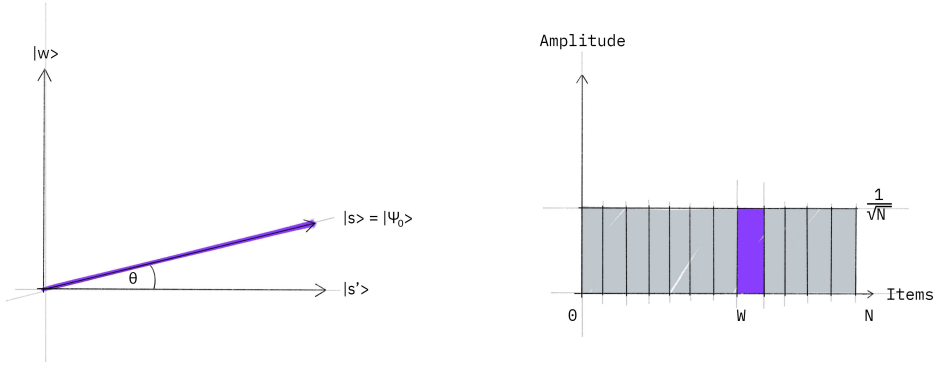
Average of amplitudes after amplitude negation $= (1 - 2/N)1/\sqrt{N}$. After applying the diffusion operator, the ampltiude of the answer state which was $1/\sqrt{N}$ grows approximately by $1/\sqrt{N}$ every iteration. Therefore after t iterations, we get $|\psi_t\rangle = (U_s U_f)^t|s\rangle$ However, since we are dealing with amplitudes and not probabilities, the vector space's dimension enters as a square root. Therefore it is the amplitude, and not just the probability, that is being amplified in this procedure.



## 5.3 Another Approach

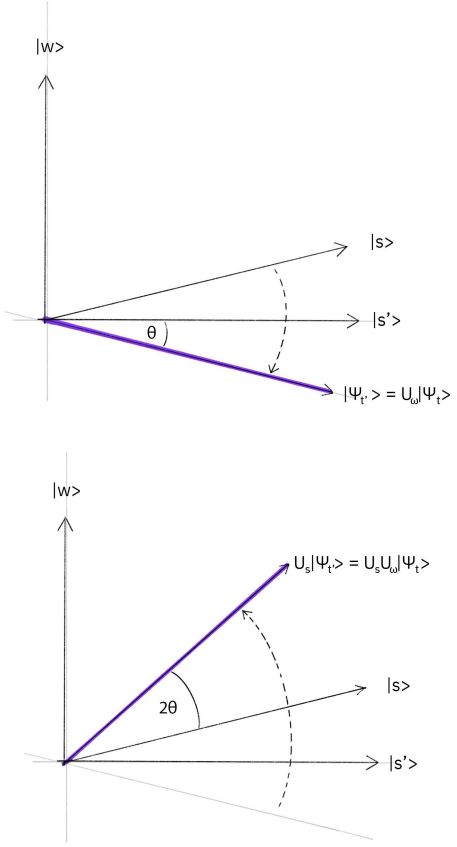
One approach of looking at the Grover's algorithm is to consider N different states and then after every iteration looking at the decrease in the amplitude of the non-answer states and the amplitude of the answer state trying to reach 1 in approximately $\sqrt{N}$ iterations. The second approach stems from this idea that the non-answer states behave almost similarly and the superposition of the non-answer states be treated a single vector. Therefore we consider two states the answer state $|\omega\rangle$ and the superposition $|s\rangle$. These two vectors span a two dimensional- plane in the vector space $C^N$. These two vectors are not linearly independent or perpendicular as the vector $|\omega\rangle$ is a part of the superposition $|s\rangle$ with an amplitude $1/\sqrt{N}$. In the case that there are multiple solutions, M , it can be shown that roughly $\sqrt{N/M} iterations will suffice.$

To resolve this problem, we introduce another vector $|s'\rangle$ which is obtained from removing the vector $|\omega\rangle$ from $|s\rangle$.




Now, the oracle function is supposed to invert the amplitude of the answer state $|\omega\rangle$, geometrically that transforms directly to taking a reflection of the state $|s\rangle$ about the $|s'\rangle$ because this transformation means that the amplitude of $|\omega\rangle$ becomes negative resulting in amplitude negation

The Grover operator ($U_s$) takes the amplitudes and flips them about their mean which is equivalent to taking their reflection from $|s\rangle$ .The net effect of these two reflections, as we will see, is to increase the angle between the state and $|\omega\rangle$ and $|s\rangle$. Repeating this pair of reflections moves the state farther and farther from $|s'\rangle$, and therefore closer and closer to $|\omega\rangle$. Once it is close enough,measuring the state results in outcome a with good probability.




## 5.4 More about the quantum oracle

From our boolean function f:{1,2,3....N} $\rightarrow$ {0,1} we know that we can construct a quantum circuit $U_f$ to carry out this computation. Since we know f can be computed classically in polynomial time, we can also compute it in superposition:

$$\sum_x \alpha_x |x\rangle|0\rangle \rightarrow \sum_x \alpha_x |x\rangle|f(x)\rangle$$

There is also a tricky way to put our result into a form that equally contains all of the information relevant to our problem. We can put the answer register in the superposition $|-\rangle$, so that when we implement f the information is stored in the phase or sign of the result:

$$U_f : \sum_x \alpha_x |x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \mapsto \sum_x \alpha_x \left( \frac{|x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle}{\sqrt{2}} \right)$$

In more detail:

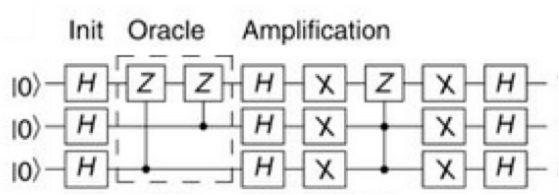
$$= \sum_x \alpha_x |x\rangle \left( \frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right)$$

$$= \sum_x \alpha_x |x\rangle (-1)^{f(x)} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$U_f$ has the property that when x = a, the phase of the state will be multiplied by -1. We will see that this implementation of the circuit is equivalent to a reflection over the vector $|s'\rangle$

## 5.5 Quantum Circuit

We now go through the example of Grover's algorithm for 3 qubits with two marked states —101⟩ and —110⟩ , following the implementation found in Reference [2]. The quantum circuit to solve the problem using a phase oracle is:




## 5.6 Analysis and Comparison

As compared to our normal linear search on a shuffled random list, Grover's search gives us a quadratic speed-up where a classical search takes O(N) times, Grover's search runs in O($\sqrt{N}$) of time. However, this a probabilistic model where in we consciously try to increase the amplitude of the answer state which can be increased to approximately 1 in about $\sqrt{N}$ iterations but there may be a small probability that we may not find the answer in these iterations.

# Chapter 6

# Conclusions

## 6.1 Takeaways

Our major takeaways from studying quantum computing till now have been:

1. One of the most significant advantages that quantum computing provides is that qubits can exist in super positions which helps us to do parallel computations.

2. Qubits can theoretically store infinite amount of information by being in a superposition state, but this information can not be accessed though, because of the anomaly of measurement and collapse of wave function.

3. Quantum computing, by it's nature, works with matrices(since they are vectors in vector space of possible quantum states). This provides us speed ups in performing unitary matrix operations. This is the major mathematical advantage they provide apart from parallel computations.

## 6.2 Future plans

1. Learn about the application of quantum computing in field of medicine and finance.

2. Read research paper about quantum algorithms for machine learning and how it can be used to optimize the existing algorithms.

3. Study about quantum hardware, how our algorithms might be limited by the garbage qubits they might require, how the comparison of complexity actually translate into time (e.g, 100 quantum gates might actually be slower than 10000000 classical gates!) and how quantum gates and qubits can be efficiently incorporated with classical computers.