Recovering Solutions of Grover’s Algorithm with an Imprecise Oracle

James Saslow

***Abstract*—In this research, we obtain solutions to Grover’s algorithm with an imprecise, ’broken’ oracle while still maintaining a quantum advantage. Grover’s Algorithm, a search algorithm that uses quantum superposition to perform a parallelized search in $O(\sqrt{t})$ time, is structured by a two-step process: an Oracle call followed by a Diffusion operation. In contrast to standard Grover’s, where a multi-control Z gate is implemented to return maximum probabilistic gain, we implement a multi-control phase gate $CP(\theta)$ to deviate away from the peak of the probabilistic gain curve. Then, we determine a maximum error bound for ϵ in $\theta = \pi \pm \epsilon$ that still gives probability $> 50\%$ for measuring the marked states as a function of qubit size. It can be shown that the necessary Oracle phase precision scales exponentially with the number of qubits, which sets experimental limitations defined by laser coherence.**

I. Introduction

A. Grover’s Algorithm

We begin by outlining Grover’s algorithm from a gate-based and geometrical perspective. Grover’s algorithm utilizes quantum parallelization to achieve a search in $O(\sqrt{t})$ time, as opposed to classical searches that run in $O(t/2)$ time. Grover’s algorithm is first initialized into an equal superposition state $|s>$. This can be done by applying a Hadamard Transform. Next, we iterate an Oracle and Diffusion operator in succession $t = int(\frac{\pi}{4}\sqrt{2^n})$ number of times. A circuit diagram for this general process is shown below.

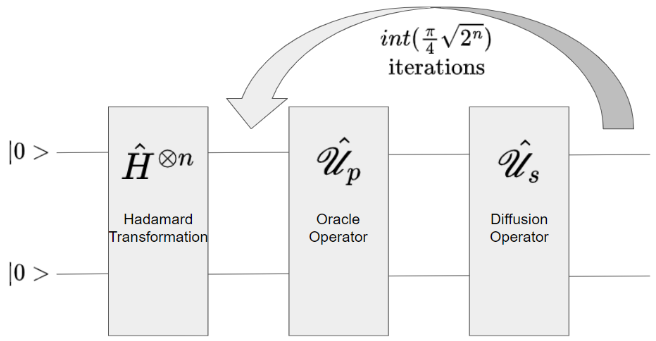

Figure: 1 Quantum Circuit Schematic of Grover’s Algorithm

B. The Oracle Operator

In standard Grover’s, the usual choice of the Oracle $\mathcal{U}_p$ is nothing but a multi-control Z gate. For an n qubit system, that’s a $CCC...(n\ times!)...Z$. We can abbreviate this multi-control Z gate as a C^nZ gate for n qubits. In short, all the oracle does is mark the state of all ones $|11...11>$ with a minus sign (a π phase). This fact is derived upon inspection of the C^nZ gate in matrix form. Take a CZ gate, for instance.

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{1}$$

The CZ gate is exactly equivalent to the identity matrix for every basis state *except* for the $|111...111>$ state, which picks up a minus sign from the element in the bottom right corner.

We define the state of all ones as the *Marked State*. After t Grover iterations, the marked state is amplified in probability, making it likely for the $|111...111>$ bit-string to be retrieved as a result of the quantum search. This probability amplification (or more commonly known as *Amplitude Amplification*) is most effectively achieved because $\theta = \pi$. But what if we have a faulty Oracle due to laser decoherence and can’t guarantee an infinite precision 3.14159265358979323846264... pi-pulse? Then, θ won’t be π exactly but will be bounded with some error given by $\theta = \pi \pm \epsilon$. We can model this using a multi-control phase gate, a natural extension of the multi-control Z gate. So, instead of tacking each marked state with a π phase, the multi-control phase Oracle marks the state of all ones with an $e^{i\theta}$ term. We will use the multi-control phase gate to model an imprecise Oracle.

C. The Diffusion Operator

The Diffusion Operator is similar to the Oracle operator, except the Diffusion Operator is sandwiched in between several single qubit gates as shown below in Figure 2.

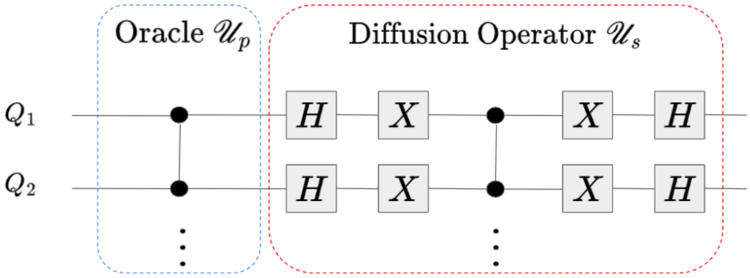

Figure: 2 Gate-based Representation of Oracle and Diffusion Operators.

We could work out the matrix equivalent for the Diffusion Operator, but inspecting it in matrix form won’t give us any obvious intuition for what the Diffusion Operator is actually doing. The best way to interpret the mean point is as a reflection about the *average amplitude* (commonly referred to as the mean point). We compute the mean point by first locating all of our complex amplitudes α_i contained within the wavefunction.

$$|\psi >= \sum_{k=0}^{2^n-1} \alpha_k |k> \tag{2}$$

Then, we do an average over all complex amplitudes to compute the mean point.

$$\bar{\alpha} = \sum_{k=0}^{2^n-1} \alpha_k \tag{3}$$

In summary, the Diffusion operator performs a reflection about the mean point $\bar{\alpha}$ to boost the amplitude of the marked state.

D. Scope of the Imprecise Oracle Problem

In the analytics section, we will show that if the Oracle applies an arbitrary angle θ (the marked state picks up a phase of $e^{i\theta}$)

$$\mathfrak{U}_p : |11...11> \longrightarrow \ e^{i\theta}|11...11> \tag{4}$$

where $\theta = \pi \pm \epsilon$

The diffusion "reflection about the mean point" operation will amplify the error in ϵ, creating a cascading error with each Grover iteration, making it more difficult to extract answers from large qubit sizes reliably.

The primary concerns we will address in this paper are

- Can we recover practical solutions of Grover's algorithm with an imprecise Oracle?
- What is the upper bound on ϵ before we lose the quantum advantage?
- This upper bound is actually the half width half maximum of the probability gain curve given by $\epsilon_{50\%}$. This is where we have a 50% chance of measuring marked or unmarked, thus losing the quantum advantage anywhere below this threshold.
- In an experiment, we strive for $\epsilon < \epsilon_{50\%}$ to maintain the quantum advantage even in the presence of an imprecise oracle.
- Calculate $\epsilon_{50\%}$, $\epsilon_{65\%}$, and $\epsilon_{80\%}$ as a function of qubit size to get a general idea about the spread of our error tolerances.

II. Analytics

A. Geometrical Interpretation

We will show with the geometrical definitions of $\mathfrak{U}_p$ and $\mathfrak{U}_s$ that Grover's is unstable for imprecise oracle calls.

Let's call α_M the complex amplitude of the marked state and α_N as the complex amplitude of one of the marked states. We should note that there is only one α_M and exactly 2^{n-1} α_N's. Let's also define $s \equiv \frac{1}{\sqrt{2^n}}$

Hadamard Transformation

The Hadamard initializes the wave function at an equal superposition state. Thus

$$\alpha_N = s \tag{5}$$

$$\alpha_M = s \tag{6}$$

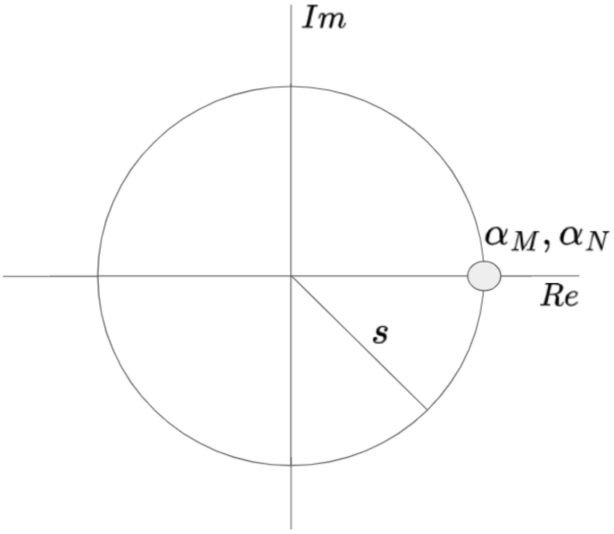

Figure: 3 Geometrical Representation of Hadamard Transformation

Oracle Operation

The Oracle call only tacks a phase to the marked amplitude and leaves the rest of the amplitudes alone

$$\mathfrak{U}_p : \alpha_M \longrightarrow \alpha_M e^{i\theta} = -se^{-i\epsilon} \tag{7}$$

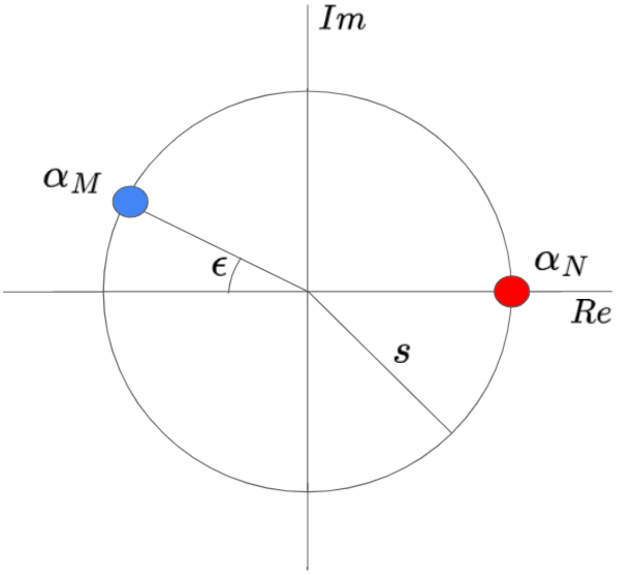

Figure: 4 Geometrical Representation of Oracle Operator

Mean Point

Here, we calculate the mean point $\bar{\alpha}$ by taking an average of all the complex amplitudes in our wave function $|\psi>$

$$\begin{aligned}\bar{\alpha} &= \frac{\alpha_N * \text{\# of non-marked states} + \alpha_M * \text{\# of marked}}{\text{total \# of states}} && (8)\\ &= \frac{\alpha_N * (2^n - 1 + \alpha_M)}{2^n} && (9)\\ &= \alpha_N(1-s^2) + s^2\alpha_M && (10)\\ &= s - s^3(1+e^{-i\epsilon}) && (11)\end{aligned}$$

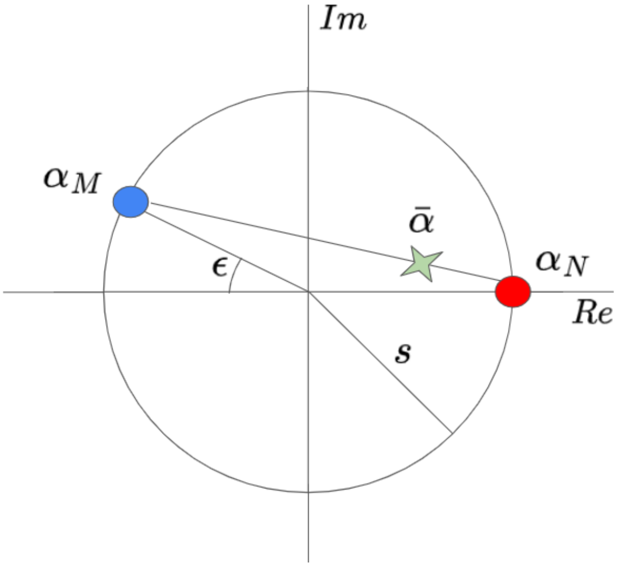

Figure: 5 Geometrical Representation of the Mean Point

Diffusion Operation

Now we enact the Diffusion Operator by doing a reflection of α_M and α_N about the mean point $\bar{\alpha}$ in amplitude space.

In particular, we want to transform α_M and α_N in the following way

$$\alpha_M \longrightarrow 2\bar{\alpha} - \alpha_M \quad (12)$$
$$\alpha_N \longrightarrow 2\bar{\alpha} - \alpha_N \quad (13)$$

We find

$$\alpha_N = s - 2s^3(1+e^{-i\epsilon}) \quad (14)$$
$$\alpha_M = s(2+e^{-i\epsilon}) - 2s^3(1+e^{-i\epsilon}) \quad (15)$$

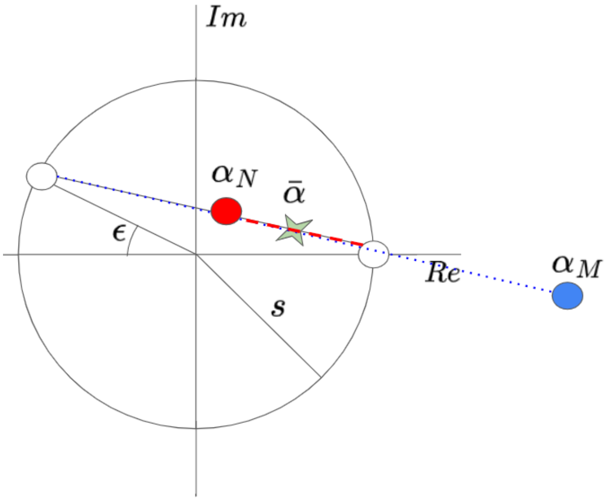

Figure: 6 Geometrical Representation of the Diffusion Operation & reflection about the Mean Point

Now, we can find probabilities of measuring α_M by taking the magnitude squared times the number of marked states. Since there is only one marked state, we multiply by 1.

$$\mathbb{P}(|marked>) = |\alpha_M|^2 \quad (16)$$

This is equivalent to taking the distance from α_M to the origin, squared. We can infer from Figure 6 that α_M has a greater probability of measurement after Diffusion compared to before. This process is known as *Amplitude amplification* since the amplitude of the marked state is being amplified.

We notice that for ϵ closer to 0, the marked state experiences optimal amplitude amplification, and in the limit where $\epsilon = \pi$, the 'marked' state and unmarked states share the same phase and are indistinguishable, which implies no amplitude amplification.

References

[1] [1] D. Koch, L. Wessing, and P. M. Alsing, "Introduction to coding quantum algorithms: A tutorial series using Qiskit," arXiv.org, https://arxiv.org/abs/1903.04359 (accessed Sep. 29, 2023).

[2] [2] H. Y. WONG, Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps. S.l.: SPRINGER INTERNATIONAL PU, 2023.