Adversarial State Initialization in Quantum Search

Alan Bidart
Department of Chemistry
Brown University
Providence, RI 02906
alan_bidart@brown.edu

Abstract

In this study, we frame quantum state initialization as an adversarial problem. We present a novel variant of the renowned Grover’s Algorithm, the single-shot Grover’s Algorithm (ss-GA), inspired by recent work by [9]. ss-GA is characterized by having a single invocation of the quantum search oracle per execution. This algorithm is specifically designed to probe the robustness of quantum search algorithms in the face of adversarial qubit initialization. This work delves into the intricacies of quantum search dynamics, particularly emphasizing the impacts of adversarial actions on the algorithm’s efficiency and reliability. Through comprehensive simulations conducted using IBM’s Qiskit environment, we explore the algorithm’s performance under varied adversarial conditions. Our findings reveal nuanced insights into the behavior of quantum search algorithms, highlighting the delicate interplay between algorithmic structure, oracle dynamics, and adversarial influences. This research not only contributes to the advancement of quantum computing resilience but also establishes an Adversarial Qubit Initialization algorithm which can serve as a framework for future investigations into the robustness of more complex quantum computing paradigms.

1 Introduction

Analogous to how the implementations of the algorithms we use every day can be reduced to gates running on electrical circuits, all quantum algorithms can be reduced to a circuit composed of “quantum wires” carrying qubits and quantum gates. The most popular quantum circuits have one thing in common: they all start from a set of $|0\rangle$ states. In the case of other quantum algorithms that require a specific quantum state as in input, such as the HHL Algorithm or several Quantum Machine Learning algorithms, those quantum states are typically prepared separately, starting from a set of $|0\rangle$ states Duan et al. [2].

The experimental errors in preparing $|0\rangle$ states for circuit initialization are not as impactful on the overall circuit’s probability of success as the experimental errors within the quantum gates in a circuit. Since most circuits have a multitude of quantum gates that run one after the other, any small imperfection on the gates compounds as circuits move forward in time. Thus, experimental errors in state preparation are usually modeled as a fixed constant that affects the circuit’s probability of success (Harper et al. [3]).

Our work aims to connect the Theoretical Computer Science literature on adversarial robustness and the experimental Physics and Chemistry literature on state initialization. By proposing an adversarial interaction around qubit initialization, directly inspired by the literature on noise mitigation, we ask the question of what would happen if errors in state initialization could no longer be approximated by a fixed constant. In this project, we chose to focus on how would the adversarial interaction proposed affect our ability to perform a quantum search, given that quantum search is a key component of Quantum Machine Learning models (Du et al. [1]).
An adversary, characterized by power parameter \( \theta \), would invert the amplitude of a given state marked by the oracle. Grover’s Algorithm, the most ubiquitous quantum search algorithm in quantum computing, consists of the oracle step followed by an amplification step. The oracle step is typically followed by an amplification step. The amplification takes in a superposition of states and amplifies the amplitude of the searched state by putting it \( \pi \) radians out of phase with respect to the other states in the superposition. Note that \( e^{i\pi} = -1 \).

The following are some examples of the action of \( O_{101} \), a 3-qubit oracle with the ability to mark the state \( |101\rangle \) by putting it \( \pi \) radians out of phase with respect to the other states in the superposition. Let \( \psi = e^{i\pi} = -1 \).

\[
O_{101} \left[ \frac{1}{2} (|000\rangle + |100\rangle + |101\rangle + |111\rangle) \right] = \frac{1}{2} (|000\rangle + |100\rangle - |101\rangle + |111\rangle) 
\]

(2)

\[
O_{101} \frac{1}{\sqrt{2}} (|000\rangle + |100\rangle) = \frac{1}{\sqrt{2}} (|000\rangle + |100\rangle) 
\]

(3)

\[
O_{101} |101\rangle = - |101\rangle = |101\rangle 
\]

(4)

The oracle step is typically followed by an amplification step. The amplification takes in a superposition of states and inverts the amplitude of all states about the mean amplitude. Given an equal superposition of \( N \) states, where all states are in-phase with each other, the mean amplitude is equal to \( \frac{1}{\sqrt{N}} \). If only one of these states is out of phase by \( \pi \) radians—meaning that its amplitude is \( -\frac{1}{\sqrt{N}} \) as opposed to \( \frac{1}{\sqrt{N}} \)—the mean amplitude will remain close to \( \frac{1}{\sqrt{N}} \). Thus, one amplification step would invert the amplitude \( -\frac{1}{\sqrt{N}} \) about \( \sim \frac{1}{\sqrt{N}} \), resulting in bringing the state back into phase, with an amplitude of roughly \( \sim \frac{1}{\sqrt{N}} \).

The combination of the oracle and the amplification step is sometimes referred to as the Grover Operator or the Grover Iteration. Repeated applications of the same Grover Operator will continue to put out of phase and then amplify a given state marked by the oracle. Grover’s Algorithm, the most popular quantum algorithm, will succeed with probability \( O(1) \) after \( O(\sqrt{2^n}) \) operations.

\section{Problem Definition}

Let \( Q \) be a quantum circuit comprised of \( n \)-qubits, \( \{|q_i\rangle\} \) for \( 0 \leq i < n \), where all qubits are initialized to the \( |0\rangle \) state and the final step of \( Q \) consists of measuring all qubits in the computational basis. The result of executing \( Q \) once will be a bitstring \( \hat{b} = q_{n-1}q_{n-2}...q_1q_0 \in \{0, 1\}^n \) where \( q_i \) will equal the result of the measurement of \( |q_i\rangle \) in the final step. Let \( S \subseteq \{0, 1\}^n \) be a set of predetermined target bitstrings. Define the success criterion for \( Q \) as the event that, for a given run of \( Q, \hat{b} \in S \). The probability that \( Q \) succeeds—the probability that \( \hat{b} \in S \) for a single execution—is denoted as \( p \).

An adversary, characterized by power parameter \( \theta \in [0, \pi] \), is permitted to interact with the initialization step of \( Q \) by corrupting an \( \varepsilon \)-amount of the \( n \) initial states \( |0\rangle \) states, where \( \varepsilon \ll 1 \). The interaction is defined in Algorithm \[1\].

\begin{algorithm}
\caption{Adversarial Interaction Algorithm}
\end{algorithm}

Let \( \hat{Q} \) be the resulting corrupted circuit, \( \hat{b} \) the result of a given execution of \( \hat{Q} \), and \( \hat{p} \) the probability of success—still defined as the probability that \( \hat{b} \in S \) for a single execution. Lastly, let \( \hat{R}(Q) = \hat{p} / p \) be defined as the robustness of circuit \( Q \) with respect to this adversarial interaction. For two circuits
Algorithm 1: Adversarial Initialization Algorithm on n qubits

Input: Adversarial power $\theta$, corruption amount $\epsilon$, and $n$ qubits initialized to the $|0\rangle$ state

Output: $\epsilon$-corrupted $|0\rangle^\otimes n$ state

Steps:
1. The adversary selects, uniformly at random without replacement, $\epsilon \cdot n$ qubits to corrupt
2. For each selected qubit $|q_i\rangle$, the adversary chooses an angle $\varphi_i$ uniformly at random from the interval $[0, 2\pi)$
3. Each $|q_i\rangle$ is “kicked” out of the initial $|0\rangle$ state, in direction $\varphi_i$, by applying the transformation $|0\rangle \rightarrow \cos(\theta/2)|0\rangle + e^{i\varphi_i}\sin(\theta/2)|1\rangle$. Note that, in the Bloch Sphere representation for $|q_i\rangle$, $\theta$ will correspond to the angle with respect to the $+z$ axis and $\varphi_i$, to the angle with respect to the $+x$ axis.

$Q_0$ and $Q_1$ we will say that $Q_0$ is more robust than $Q_1$ if $R(Q_0) > R(Q_1)$ and equally robust if $R(Q_0) = R(Q_1)$.

In this work, our goal was to set a baseline robustness that we could use to evaluate the robustness of quantum search algorithms against adversarial initialization. Then, we aimed at exploring if different algorithms showcase different levels of robustness. Our final goal was the Adversarial Initialization Algorithm in the context of quantum search and derive empirical insights to better understand the properties of quantum search.

3 Methods and Robustness Analysis

3.1 Baseline: Measurement Circuit

We started by modeling the effect of this adversarial interaction for the case in which $Q_{\text{meas}}$ is composed of only the initialization step and the measurement step. In this scenario, the only element in $S$ is the all-zero bitstring. Additionally, $p = 1$, since we expect all qubits to return 0 as a result when measured in the computational basis. In the case of $\tilde{Q}_{\text{meas}}$, the probability that a given qubit $q_i$ will be corrupted is equal to $\epsilon$. Moreover, the state of a corrupted qubit will be $\cos(\theta/2)|0\rangle + e^{i\varphi_i}\sin(\theta/2)|1\rangle$, which implies that the probability of it returning 0 when measured will equal to $\cos(\theta/2)^2$. Since all the bits in $\tilde{b}$ must equal 0 for $\tilde{Q}_{\text{meas}}$ to succeed, all $\epsilon n$ corrupted qubits must measure to 0. It follows that:

$$\tilde{p} = \cos\left(\frac{\theta}{2}\right)^{2\epsilon n}$$  \hfill (5)

This allows us to express the robustness of $Q_{\text{meas}}$ as a function of $n$, $\epsilon$, and $\theta$:

$$R(Q_{\text{meas}}) = \frac{\tilde{p}}{p} = \cos\left(\frac{\theta}{2}\right)^{2\epsilon n}$$  \hfill (6)

It is a natural choice to move forward using $R(Q_{\text{meas}})$ as a baseline for the robustness of other circuits given its simplicity and the fact that its first and final step match most quantum circuits—including all of those that abide by the definition of $Q$.

3.2 Single-shot Grover’s Algorithm

Inspired by the work of Pokharel and Lidar [9] on the Bernstein-Vazirani quantum algorithm, our empirical study began by proposing a constrained variant of quantum search: the single-shot Grover’s Algorithm (ss-GA). This variant permits only a single invocation of the oracle per execution. While this limitation significantly diminishes the algorithm’s success probability, ss-GA serves as a pivotal model for examining adversarial qubit initialization. ss-GA features a complete cycle of the Grover operator (Steps 3 and 4 combined in Algorithm 2), which is the core component of Grover’s Algorithm. The only distinction between ss-GA and its unconstrained version lies in the number of iterations of the Grover operator. The fact that additional iterations of the Grover operator in the original
Figure 1: Measurement circuit on 4 qubits. Although qubits in a circuit are assumed to start in the $|0\rangle$ unless otherwise noted, we added reset gates to clearly distinguish the initialization and the measurement step.

Figure 2: Success rate on 8 qubits for different $\varepsilon$. The gray lines represent $\cos^{2\varepsilon n}(\theta/2)$ for the $\varepsilon$ values.

algorithm serve to amplify the probabilities of the marked state, as opposed to altering which states are present in the superposition resulting from the first iteration, suggests that insights obtained from the robustness analysis of ss-GA might help understand the robustness of the original algorithm.

As the number of qubits employed in the quantum search algorithms increases, analytical methods may quickly become intractable, rendering empirical approaches more feasible and informative. On this regard, our research employs noiseless simulations run using IBM’s Qiskit environment—a state-of-the-art quantum computing framework. This empirical approach allows us to model how the adversarial interaction impacts ss-GA by collecting data over repeated executions.

Using the language of Section 2, let $Q_{sG}(\psi')$ be a circuit implementation of the ss-GA algorithm on $n$ qubits featuring oracle $O_{\psi'}$, where $\psi' \in \{0, 1\}^{n-1}$. For a given execution, the $n$ measured qubits will translate to bitstring $b \in \{0, 1\}^n$. Since the result of measuring the auxiliary qubit is not relevant to the recovery of $\psi'$, we can assume w.l.o.g. that the first bit in $b$ will correspond to the measurement of the auxiliary qubit. Thus, we define $S = \{0\psi', 1\psi'\}$ and will $p$ will equal the probability that $b \in S$, which equals the probability of retrieving $\psi'$ after measuring only the $n - 1$ non-auxiliary qubits.

To study the robustness of $Q_{sG}, R(Q_{sG})$ empirically, we focused on varying the parameters $n, \varepsilon$ and $\theta$. We adopted a methodical procedure that addresses potential biases and ensures the validity of our results. For each execution of either $Q_{sG}$ or $\tilde{Q}_{sG}$, a new circuit was compiled, with a fresh
**Algorithm 2** Single-shot Grover’s Algorithm on n qubits

**Input:** Black box oracle $O_{\psi'}$, defined in [1] that acts on $n - 1$ qubits. The implementation of $O_{\psi'}$ that we used also requires an additional auxiliary qubit in the $|0\rangle + |1\rangle/\sqrt{2}$ state to perform its operations.

**Output:** $\psi'$ (succeeds with probability $\sim 9/2^{n-1}$)

**Steps:**
1. $|0\rangle |0\rangle \otimes n-1 \quad \triangleright$ Initialization (the first qubit is an auxiliary qubit)
2. $HX |0\rangle H \otimes n-1 |0\rangle \otimes n-1 = |0\rangle - |1\rangle \sqrt{2} \frac{1}{\sqrt{2^n-1}} \psi' 
\quad \triangleright$ Amplification step
3. $O_{\psi'} \left[ |0\rangle - |1\rangle \sqrt{2} \frac{1}{\sqrt{2^n-1}} \psi' \right] = \frac{1}{\sqrt{2^n-1}} \left| \psi' \right\rangle + \sum_{\psi=0}^{2^n-1} \left( 1 - \delta_{\psi,\psi'} \right) \left| \psi \right\rangle 
\quad \triangleright$ Amplification step
4. $\sim \frac{3}{\sqrt{2^n}} |\psi'\rangle + \sim \frac{1}{\sqrt{2^n-1}} \sum_{\psi=0}^{2^n-1} \left( 1 - \delta_{\psi,\psi'} \right) |\psi\rangle$
5. Measure the $n - 1$ non-auxiliary qubits to retrieve $\psi'$ with probability $\sim 9/2^{n-1}$

---

**Figure 3:** Robustness calculations for Single-shot Grover’s Algorithms. The x-marks represent the values for robustness calculated across different values of $\varepsilon$ via 5000 simulations. The dashed line represents the baseline obtained from the measurement circuit.

$|\psi'\rangle$ sampled uniformly at random from $0, 1^{n-1}$. This is important because the performance of $Q_{sG}$ circuits vary greatly as a function of $|\psi'\rangle$. Moreover, we apply the adversarial interaction from scratch in each circuit, rather than implementing it once and reusing the altered state in multiple runs. This approach is adopted to closely mimic real-world scenarios where environmental interactions can occur independently in each execution. The adversarial interaction is modeled using $R_y$ and $R_x$ quantum gates, which represent rotations around the $x$ and $y$ on the Bloch Sphere. Furthermore, for each different studied parametrization of $Q_{sG}$ and $Q_{mG}$, the results reported are averaged over at least 5000 circuits, resulting in a representative sample of search strings and adversarial "kick" phases $\varphi$.

A summary of the key result can be found in Figure 3, which suggests $R(Q_{sG}) > R(Q_{mG})$ and is representative of the results we obtained for smaller and larger values of $n$. In Figure 4, we show $R(Q_{sG})$ for increasing values of $n$ and fixed value $\theta = \pi/2$ and $\varepsilon = 1/\theta$. The empirical results suggest that ss-GA remains more robust than $Q_{mG}$ even as the number of qubits increases. Lastly, visualization of our implementation of $Q_{sG}$ on 4 qubits can be seen in Figure 7.

**3.3 Grover’s Algorithm**

A similar analysis was done for the complete Grover’s Algorithm treating it as circuit implementation $Q_G$ and using analogous definitions and methods to those described in the previous subsection. The results are shown in Figure 5. Surprisingly, the data suggests that $R(Q_G) = R(Q_{mG})$, which is to say that any robustness inherent to $Q_{sG}$ gets phased out via repeated iterations of the Grover Operator.
4 Conclusions and future work

In this work, we framed the experimental challenges of qubit initialization as an adversarial problem. In the definition of our problem, the adversary corrupts our initial state every time we attempt to run a circuit, much like the environment does at the start of any quantum computation. We then defined a way to measure how robust a given quantum algorithm against this adversarial interaction. By studying the measurement circuit, a basic circuit that does not have any quantum gates, we derived a baseline for robustness, and compared to two quantum search algorithms.

Our simulations suggest that, despite the many quantum gates involved in Grover’s search algorithm, the canonical quantum search algorithm is as robust as the measurement circuit. On the other hand, the single-shot Grover’s Algorithm we propose in this paper, inspired by the recent work of Pokharel and Lidar [9] on the Bernstein-Vazirani algorithm, appears to be more robust than the baseline. This is a surprising result since the single-shot Grover’s Algorithm encompasses the first iteration of the Grover Operator in Grover’s algorithm. As a consequence, this suggests that the remaining iterations
Figure 6: Robustness calculations for Grover’s Algorithms with an increasing number of qubits. $\epsilon$ is to $1/n$ for all executions and power $\theta$ is fixed at $\pi/2$. The dashed line represents baseline robustness for these parameters, then from the measurement circuit.

of the Grover Operator must be less robust than the baseline, to counteract the initial increase in robustness. However, since the iterations of the Grover Operator in Grover’s Algorithm on $n$ qubits grow proportional to $\sqrt{2^n}$, we can ask if the robustness of Grover’s Algorithm against this interaction will decrease to below the baseline as $n$ grows much larger than the values we were able to simulate in this work.

Throughout this work, many quantum circuits were studied and simulated in the context of this adversarial interaction. Most studied circuits, including the Bernstein-Vazirani Algorithm and the Quantum Phase Estimation, were shown to be as robust to the adversarial interaction as the measurement circuit. The exceptions were circuits with built-in error correction but no standalone applicability, such as Shor’s 9-qubit-code (not to be confused with Shor’s Algorithm), and circuits for which defining the $S$ was not a straightforward process, such as the circuit for preparing entangled states. This makes the results found in the context of quantum search particularly interesting.

In conclusion, this research opens the door to numerous intriguing avenues for future exploration, particularly relevant to the fields of theoretical computer science and machine learning. The questions raised by our study are not only central to understanding the robustness of quantum algorithms like the HHL algorithm but also pivotal in advancing machine learning techniques that leverage quantum computing. These include investigating the resilience of machine learning algorithms to adversarial quantum interactions and exploring strategies for quantum models to adaptively counteract such adversarial influences. Furthermore, understanding how an adversary might strategically plan interactions to optimally disrupt algorithmic success leads to deeper insights into the security aspects of quantum computing. Another intriguing aspect is the modeling of adversaries with variable power, where the adversary’s interaction is defined within a range, adding a layer of complexity and realism to our understanding of quantum robustness. The answers to these questions hold significant implications for the development of more secure, efficient, and reliable quantum computing methodologies, resonating strongly with the goals of both theoretical computer scientists and machine learning practitioners. This work not only contributes to a deeper understanding of quantum computing dynamics but also lays foundational knowledge crucial for the advancement of these rapidly evolving fields.
Figure 7: Single-shot Grover’s Algorithm on 4 qubits. The different steps of the proposed algorithm are divided by vertical dashed barriers. The circuit starts with an example adversarial initialization, with the adversary corrupting the third qubits, $q_1$, with power $\theta = \pi/2$. The next sections correspond to the steps in Algorithm 2. In this example, the oracle marks the state $|110\rangle$.  

---

8
5 Data and code availability

The code used for all the simulations will be available shortly at https://github.com/abidart/quantum_robustness.

References


A Appendix

This section includes a basic introduction to the topics needed to visualize the problem definition.

A.1 The Qubit

When transitioning from Classical Computation to Quantum Computation, the classical computational unit, the bit, gets replaced by the quantum-bit, or qubit. The key difference between a bit and a qubit $|q\rangle$ is that, at a given point in time, $b$ stores one of either a 0-state or a 1-state, whereas $|q\rangle$ can be thought of as a quantum-mechanical wavefunction that stores one of the infinitely-many complex superpositions of $|0\rangle$ and $|1\rangle$ (the quantum analog of the classical 0 and 1-states). In particular, given $(\alpha, \beta) \in \mathbb{C}^2 \setminus \{(0, 0)\}$:

$$|q\rangle = \alpha |0\rangle + \beta |1\rangle$$

(7)

where $\frac{\alpha^2}{\alpha^2 + \beta^2}$ is the probability that the qubit is found to be in state $|0\rangle$ when measured across the computational basis $\{|0\rangle, |1\rangle\}$. The probability of being found in the state $|1\rangle$ is $\frac{\beta^2}{\alpha^2 + \beta^2}$. 

9
A.2 Normalization and phases

It is common practice to select \( \alpha \) and \( \beta \) such that they satisfy \(|\alpha|^2 + |\beta|^2 = 1\), known as the normalization condition for a wavefunction in quantum mechanics. For any \((\alpha_0, \beta_0) \in \mathbb{C}^2 \setminus \{(0,0)\}\) that does not satisfy the normalization condition, we can construct \(\alpha'_0 = \alpha / \sqrt{|\alpha_0|^2 + |\beta_0|^2}\) and \(\beta'_0 = \beta / \sqrt{|\alpha_0|^2 + |\beta_0|^2}\) such that \((\alpha'_0, \beta'_0) \in \mathbb{C}^2 \setminus \{(0,0)\}\) satisfies \(|\alpha'_0|^2 + |\beta'_0|^2 = 1\). If \(|q_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle\), we say that \(|q'\rangle = \alpha'_0 |0\rangle + \beta'_0 |1\rangle\) is the normalized wavefunction of \(|q\rangle\).

Moreover, given a set of wavefunctions, we say that the wavefunctions are equal up to normalization if their normalized wavefunctions are equal. For example, \(|q_0\rangle = |0\rangle + |1\rangle\), \(|q_1\rangle = 2|0\rangle + 2|1\rangle\) and \(|q_3\rangle = 3|0\rangle + 3|1\rangle\), all equal superpositions of \(|0\rangle\) and \(|1\rangle\), are equal up to normalization since they all normalize to \(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\).

Similarly, it is also common practice to omit factors of the form \(e^{i\varphi}, \varphi \in [0, 2\pi]\) that are acting on the state. Note that factors of this form, called \(\varphi\) phases, all have absolute value one, so they do not interfere with the normalization of a state. When a factor of this form is acts on an entire state, we refer to it as a global phase. Global phases do not manifest observable consequences in the behavior of quantum systems and do not affect the probabilities of measurements outcomes.

We say that two states \(|\psi_0\rangle, |\psi_1\rangle\) are equal up to a global phase if \(e^{i\varphi}|\psi_0\rangle = |\psi_1\rangle\) for some \(\varphi\). Thus, given \(|\psi_0\rangle = \alpha |0\rangle + \beta |1\rangle\), we can always find \(|\psi_1\rangle = \alpha' |0\rangle + \beta' |1\rangle\) where \(\alpha' \in \mathbb{R}\), equal to \(|\psi_0\rangle\) up to a global phase. This is the reason why, for example, \(-|0\rangle\) is thought of as being equal to \(|0\rangle\) (both are 100% likely to be found in the \(|0\rangle\) when measured along the computational basis). Additionally, we say that \(\beta'\) is the phase between the states \(|0\rangle\) and \(|1\rangle\) in \(|\psi_1\rangle\).

A.3 Bloch Sphere

Although we originally started with a definition of the qubit that would require 4 values to parameterize, the real and imaginary parts of \(\alpha\) and \(\beta\), we can use the properties described in the previous section to bring that number down to 2. If \(|\psi\rangle = \alpha |0\rangle + \beta |1\rangle\) is normalized and \(\alpha \in \mathbb{R}\), we can express \(|\psi\rangle\) as \(\cos \left(\frac{\varphi}{2}\right) + e^{i\varphi} \sin \left(\frac{\varphi}{2}\right)\), where \(\varphi\) is the relative phase between the states \(|0\rangle\) and \(|1\rangle\) in the superposition. This is called the Bloch Sphere representation of the qubit. In particular, the vector \((\cos(\varphi) \sin(\theta), \sin(\varphi) \sin(\theta), \cos(\theta))\), called the Bloch vector, allows us to visualize the qubit as a points on a sphere, with the caveat that its north and south pole are perpendicular (see \(\text{Fig. 8}\)). We can also use the Bloch Sphere to visualize transformations (see \(\text{Fig. 9}\)).
Figure 9: Bloch sphere representation of a transformation that rotated a $|0\rangle$ $\frac{\pi}{9}$ radians around the y-axis.