Amplitude Amplification

Proseminar Report

Saurabh Gupta

March 21, 2022

Quantum Information: From Foundations to Algorithms

Contents

1 Introduction

Quantum computing is a field at the junction of theoretical physics and theoretical computer science. Quantum computers containing tens of qubits, the largest being the 127-qubit system by IBM [1], have been demonstrated experimentally. Yet, the field is far from developed and desktop quantum computers remain a distant dream. On the one hand, we need viable realisations of qubits which can be used to build large-scale quantum computers. On the other hand, we also need to develop quantum algorithms which can exploit the quantum advantage such systems offer over classical computers. The biggest leaps in this area came in the 90s, with the development of Shor's algorithm [2] and Grover's algorithm [3].

Grover's algorithm is a quantum algorithm used to solve the unstructured search problem. Consider a Boolean function $f : \{0, 1, ..., N-1\} \to \{0, 1\}$. The goal is to find any $x_0 \in \{0, 1, ..., N-1\}$ such that $f(x_0) = 1$. The most efficient classical algorithm to solve this problem is linear searching, which will find such an x_0 in $\mathcal{O}(N)$ queries to the f. Grover's algorithm on the other hand takes just $\mathcal{O}(\sqrt{N})$ to find an x_0, albeit with an associated error probability [4].

This report discusses the quantum amplitude amplification algorithm [5], which is a generalisation of Grover's quantum search algorithm for unstructured data. Amplitude amplification works using any quantum algorithm $\mathcal{A}$ that uses no measurement, in place of the Walsh-Hadamard operator $H^{\otimes n}$ used in Grover's algorithm. We can thus choose an algorithm which produce a non-uniform superposition biased towards the target object instead of producing a uniform superposition.

The report begins with a description of Grover's search algorithm in section 2. I present an induction based proof of the effect of multiple iterations of the Grover subroutine on the initial state. In section 3, the more general amplitude amplification algorithm is presented and an algebraic proof is given for the effect of multiple iterations of the amplitude amplification subroutine. It is shown that the probability of measuring the target state after j iterations of the algorithm subroutine is $\sin^2[(2j+1)\theta]$, where $\sin^2\theta = a$ is the initial success probability of algorithm $\mathcal{A}$. A query complexity analysis of amplitude amplification is presented in section 4. I discuss the query complexity of the algorithm in two cases – when a is known prior to the experiment and when it is unknown. It is shown that the algorithm takes $\mathcal{O}(\sqrt{N})$ queries to the function f in both cases, demonstrating a clear quantum advantage over classical algorithms.

2 Grover's Quantum Search Algorithm

2.1 Problem statement

Consider a Boolean function $f : \{0,1\}^n \to \{0,1\}$. The goal is to find any "good solution" to the function f, i.e., any $x_i \in \{0,1\}^n$ such that $f(x_i) = 1$.

2.2 Solution setting

Let $\mathcal{H}$ denote the Hilbert space of a 2-dimensional quantum system and let $\{|z\rangle\}_{z\in\{0,1\}}$ be the computational basis of this system. We also assume that we have n copies of this system. We can represent the computational basis of the composite system, $\mathcal{H}^{\otimes n}$ as $\{|x\rangle\}_{x\in\{0,1\}^n}$. We note that the set $\{0,1\}^n$ can be invertibly mapped to the set $\{0,1,..,N-1\}$, where $N = 2^n$, such that binary number $x \in \{0,1\}^n$ is mapped to its decimal equivalent $y \in \{0,1,..,N-1\}$.

The Boolean function f partitions $\mathcal{H}^{\otimes n}$ into two orthogonally complementary subspaces: $\mathcal{H}_{\text{good}}$ is the subspace spanned by the states $\{|x\rangle : f(x) = 1, x \in \{0,1\}^n\}$ and $\mathcal{H}_{\text{bad}}$ is the subspace spanned by the remaining basis kets. It is easy to see that $\mathcal{H}_{\text{good}}$ and $\mathcal{H}_{\text{bad}}$ are orthogonal complements. Any state $|\phi\rangle \in \mathcal{H}$ may be decomposed into its components on $\mathcal{H}_{\text{good}}$ and $\mathcal{H}_{\text{bad}}$ as $|\phi\rangle = |\phi_{\text{good}}\rangle + |\phi_{\text{bad}}\rangle$.

We define quantum phase oracles U_f and $U_{|0\rangle}$ whose action on the basis vectors is given as

$$U_f |x\rangle = \begin{cases} -|x\rangle, & \text{if } f(x) = 1 \\ |x\rangle, & \text{if } f(x) = 0, \end{cases}$$

$$U_{|0\rangle} |x\rangle = \begin{cases} -|x\rangle, & \text{if } x = 0 \\ |x\rangle, & \text{otherwise.} \end{cases}$$

Additional qubits may be required for the internal workings of the phase oracles that we use to solve this problem, for instance to convert the bit oracles $O_{|0\rangle}$ and O_f to phase oracles $U_{|0\rangle}$ and U_f respectively. Throughout this derivation we will assume access to these oracles as black boxes and not concern ourselves with their internal working.

We note that the oracles $U_{|0\rangle}$ and U_f are equivalent to reflection operators which reflect the input state along $|0\rangle$ and along $\mathcal{H}_{\text{good}}$ respectively. They can be represented in functional form as

$$\begin{aligned} U_{|0\rangle} &= \mathbb{1} - 2\,|0\rangle\langle 0| \\ U_f &= \mathbb{1} - 2\sum_{x\in\mathcal{H}_{\text{good}}} |x\rangle\langle x|\,. \end{aligned} \tag{1}$$

2.3 Algorithm outline and proof

We start with the $|0\rangle^{\otimes n}$ state, and apply a Walsh-Hadamard transformation to achieve an equal superposition state

$$|\psi\rangle = H^{\otimes n}\,|0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,. \tag{2}$$

We now define a subroutine known as the *Grover iteration*, which we denote by G. The iteration has the following steps:

1. Apply the oracle U_f
2. Apply the Walsh-Hadamard transformation $H^{\otimes n}$
3. Apply the oracle $-U_{|0\rangle}$
4. Apply the Walsh-Hadamard transformation $H^{\otimes n}$.

The circuit for the above iteration is given in figure 1. The combined effect of steps 2, 3 and 4 is $H^{\otimes n}(2\,|0\rangle\langle 0| - \mathbb{1})H^{\otimes n} = 2\,|\psi\rangle\langle\psi| - \mathbb{1}$. Thus, the combined iteration may be written as $G = (2\,|\psi\rangle\langle\psi| - \mathbb{1})U_f$.

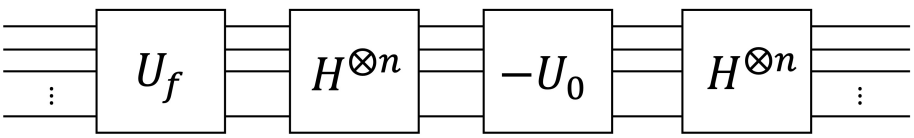

Figure 1: Schematic circuit for the Grover iteration G. The oracles U_f and U_0 may use additional workspace qubits for their internal functioning which are not depicted here. We consider the oracles to be black box operators and assume that we have access to such operators for the system of interest.

Theorem 1 *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function and let $x_i \in \{0,1\}^n$ such that $f(x_i) = 1$ be the good solutions of f. Let there be t good solutions out of $N = 2^n$ possible inputs. The probability of measuring a good solution, i.e, $|x_i\rangle$ such that $f(x_i) = 1$, after j iterations of the Grover iteration G starting from the initial state $|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n}$ is given by $\sin^2[(2j+1)\theta]$, where θ is defined so that $\sin^2\theta = t/N$ and $0 < \theta \leq \pi/2$.*

Proof. We decompose $|\psi\rangle$ its components on $\mathcal{H}_{\text{good}}$ and $\mathcal{H}_{\text{bad}}$,

$$|\psi\rangle = |\psi_{\text{good}}\rangle + |\psi_{\text{bad}}\rangle .$$

We rewrite the above decomposition in terms of normalised components $|\psi_1\rangle = \frac{|\psi_{\text{good}}\rangle}{\sqrt{\langle\psi_{\text{good}}|\psi_{\text{good}}\rangle}}$ and $|\psi_0\rangle = \frac{|\psi_{\text{bad}}\rangle}{\sqrt{\langle\psi_{\text{bad}}|\psi_{\text{bad}}\rangle}}$ as

$$|\psi\rangle = \sin\theta\,|\psi_1\rangle + \cos\theta\,|\psi_0\rangle , \tag{3}$$

and define parameter θ as $\sin^2\theta = a = \langle\psi_{\text{good}}|\psi_{\text{good}}\rangle$, where a is the *success probability* of the algorithm $H^{\otimes n}$. If we have t good solutions to the Boolean function, the success probability $a = t/N$. Applying the Grover iteration G to $|\psi\rangle$ we get

$$\begin{aligned}
G|\psi\rangle &= (2|\psi\rangle\langle\psi| - \mathbb{1})U_f(\sin\theta\,|\psi_1\rangle + \cos\theta\,|\psi_0\rangle) \\
&= (2|\psi\rangle\langle\psi| - \mathbb{1})(-\sin\theta\,|\psi_1\rangle + \cos\theta\,|\psi_0\rangle) \\
&= -2\sin\theta\,\langle\psi|\psi_1\rangle\,|\psi\rangle + 2\cos\theta\,\langle\psi|\psi_0\rangle\,|\psi\rangle + \sin\theta\,|\psi_1\rangle - \cos\theta\,|\psi_0\rangle \\
&= \{\sin\theta(1-2\sin^2\theta) + \cos\theta(2\sin\theta\cos\theta)\}\,|\psi_1\rangle + \{\cos\theta(1-2\sin^2\theta) + \sin\theta(2\sin\theta\cos\theta)\}\,|\psi_0\rangle \\
&= \sin 3\theta\,|\psi_1\rangle + \cos 3\theta\,|\psi_0\rangle .
\end{aligned}$$

Similarly, it can be shown through induction that applying G a total of j times yields the state $G^j|\psi\rangle = \sin[(2j+1)\theta]\,|\psi_1\rangle + \cos[(2j+1)\theta]\,|\psi_0\rangle$. To complete the process, we measure the final state $G^j|\psi\rangle$ in the computational basis, which yields a state in $\mathcal{H}_{\text{good}}$ with probability $\sin^2[(2j+1)\theta]$. We can find the optimal $j \in \mathbb{N}$ to maximise the probability of measuring a state in $\mathcal{H}_{\text{good}}$. A circuit diagram for the algorithm is provided in figure 2.

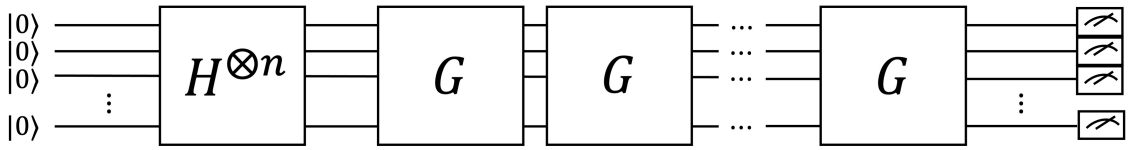

Figure 2: Schematic circuit for Grover's algorithm.

Geometrically, the action of a single Grover iteration can be represented as a reflection along the state $|\psi_{\text{bad}}\rangle$ followed by a reflection along the original state $|\psi\rangle$. The process is depicted in figure 3. As we apply further Grover iterations, the state vector aligns more closely to $|\psi_{\text{good}}\rangle$. Upon applying further iterations, the vector once again begins to move away from $|\psi_{\text{good}}\rangle$ and the success probability upon measurement of the final state decreases.

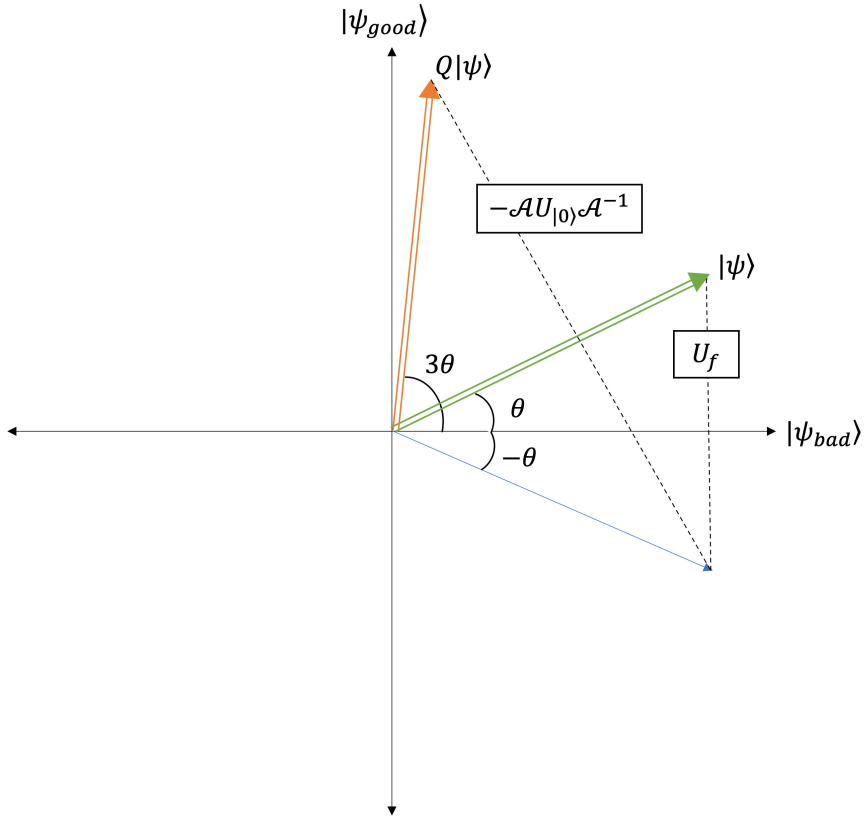

Figure 3: Geometric visualisation of the effect of applying a single iteration of G to $|\psi\rangle$. Here, $\mathcal{A} \equiv H^{\otimes n}$ and $Q \equiv G$. Initially, the angle between $|\psi\rangle$ and $|\psi_{bad}\rangle$ is θ, which changes to $-\theta$ on applying U_f. The angle between $U_f|\psi\rangle$ and $|\psi\rangle$ is 2θ. Upon applying $-H^{\otimes n}U_{|0\rangle}H^{\otimes n}$ to this state, we get the final state $G|\psi\rangle$ which is a reflection about $|\psi\rangle$. Since the angle between $G|\psi\rangle$ and $|\psi\rangle$ is 2θ and the angle between $|\psi\rangle$ and $|\psi_{bad}\rangle$ is θ, the total angle between $G|\psi\rangle$ and $|\psi_{bad}\rangle$ is 3θ.

3 Amplitude Amplification

3.1 Problem statement

Consider a Boolean function $f : \{0, 1, ..., N-1\} \to \{0, 1\}$. The goal is to find any "good solution" to the function f, i.e., any $x \in \{0, 1, ..., N-1\}$ such that $f(x) = 1$.

3.2 Solution setting

Let $\mathcal{H}$ denote the Hilbert space of an n-dimensional quantum system and let $\{|x\rangle\}_{x\in\{0,1,...,N-1\}}$ be the computational basis of this system. The Boolean function f partitions $\mathcal{H}$ into two orthogonally complementary subspaces: $\mathcal{H}_{\text{good}}$ is the subspace spanned by the states $\{|x\rangle : f(x) = 1, x \in \{0, 1, ..., N-1\}$ and $\mathcal{H}_{\text{bad}}$ is the subspace spanned by the remaining computational basis vectors.

We again define quantum phase oracles U_f and $U_{|0\rangle}$ as we did in section 2, whose action on the basis vectors is given as

$$U_f |x\rangle = \begin{cases} -|x\rangle, & \text{if } f(x) = 1 \\ |x\rangle, & \text{if } f(x) = 0, \end{cases}$$

$$U_{|0\rangle} |x\rangle = \begin{cases} -|x\rangle, & \text{if } x = 0 \\ |x\rangle, & \text{otherwise.} \end{cases}$$

We note that the oracles $U_{|0\rangle}$ and U_f are equivalent to reflection operators which reflect the input state along $|0\rangle$ and $\mathcal{H}_{\text{good}}$ respectively. They can be represented in functional form as shown in equation 1

$$U_{|0\rangle} = \mathbb{1} - 2|0\rangle\langle 0|$$
$$U_f = \mathbb{1} - 2\sum_{x\in\mathcal{H}_{\text{good}}} |x\rangle\langle x|.$$

Let $\mathcal{A}$ be any quantum algorithm that acts on $\mathcal{H}$ and uses no measurements. By virtue of being an algorithm, $\mathcal{A}$ is unitary and thus invertible. We start with the $|0\rangle$ state, and apply $\mathcal{A}$ to achieve a state $|\psi\rangle$,

$$|\psi\rangle = \mathcal{A}|0\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle. \tag{4}$$

We now define a subroutine which we denote by Q. The subroutine has the following steps:

1. Apply the oracle U_f
2. Apply the quantum algorithm $\mathcal{A}^{-1}$
3. Apply the oracle $-U_{|0\rangle}$
4. Apply the quantum algorithm $\mathcal{A}$.

The combined effect of steps 2, 3 and 4 is $\mathcal{A}(2\,|0\rangle\,\langle 0| - \mathbb{1})\mathcal{A} = 2\,|\psi\rangle\,\langle\psi| - \mathbb{1}$. Thus, the combined subroutine may be written as $Q = (2\,|\psi\rangle\,\langle\psi| - \mathbb{1})U_f$.

3.3 Algorithm outline and proof

Theorem 2 *Suppose $f : \{0, 1, ..., N-1\} \to \{0, 1\}$ is a Boolean function and let $x_i \in \{0, 1, ..., N-1\}$ such that $f(x_i) = 1$ be the good solutions of f. Let $\mathcal{A}$ be a quantum algorithm that uses no measurements and let a be the initial success probability of $\mathcal{A}$. The probability of measuring a good solution, i.e, $|x_i\rangle$ such that $f(x_i) = 1$, after j iterations of the subroutine Q starting from the initial state $|\psi\rangle = \mathcal{A}\,|0\rangle$ is given by $\sin^2[(2j+1)\theta]$, where θ is defined so that $\sin^2\theta = a$ and $0 < \theta \leq \pi/2$.*

Proof. We now rewrite $|\psi\rangle$ as a superposition of its components in $\mathcal{H}_{\text{good}}$ and $\mathcal{H}_{\text{bad}}$,

$$|\psi\rangle = |\psi_{\text{good}}\rangle + |\psi_{\text{bad}}\rangle$$

and define parameter θ as $\sin^2\theta = a = \langle\psi_{\text{good}}|\psi_{\text{good}}\rangle$, where a is called the *success probability* of the algorithm $\mathcal{A}$. We define $\mathcal{H}_\psi$ as the subspace spanned by $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{bad}}\rangle$. The subspace is 2-dimensional if a is neither 0 nor 1, and 1-dimensional otherwise. We denote by $\mathcal{H}_\psi^\perp$ the orthogonally complementary subspace of $\mathcal{H}_\psi$ in $\mathcal{H}$.

Since $(2\,|\psi\rangle\,\langle\psi| - \mathbb{1})$ acts as the identity operator in $\mathcal{H}_\psi^\perp$, Q can be written as $-U_f$ in $\mathcal{H}_\psi^\perp$. Thus, Q^2 acts as the identity operator in $\mathcal{H}_\psi^\perp$, and so every eigenvector of Q in $\mathcal{H}_\psi^\perp$ has eigenvalue $+1$ or -1. On the other hand, the action of Q on $\mathcal{H}_\psi$ can be given as $(2\,|\psi\rangle\,\langle\psi| - \mathbb{1})(\mathbb{1} - \frac{2}{a}\,|\psi_{\text{good}}\rangle\,\langle\psi_{\text{good}}|)$.

$$\begin{aligned} Q\,|\psi_{\text{good}}\rangle &= (1-2a)\,|\psi_{\text{good}}\rangle - 2a\,|\psi_{\text{bad}}\rangle \\ Q\,|\psi_{\text{bad}}\rangle &= 2(1-a)\,|\psi_{\text{good}}\rangle + (1-2a)\,|\psi_{\text{bad}}\rangle\,, \end{aligned}$$

which shows that the subspace spanned by $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{good}}\rangle$, $\mathcal{H}_\psi$ is stable under the application of subroutine Q.

Since Q is a unitary operator, its eigenvectors form an orthogonal basis. Since $\mathcal{H}_\psi$ is stable under the action of Q and 2-dimensional, the orthogonal basis of $\mathcal{H}_\psi$ consists of two eigenvectors of Q,

$$|\psi_\pm\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{a}}|\psi_{\text{good}}\rangle \pm \frac{\iota}{\sqrt{1-a}}|\psi_{\text{bad}}\rangle\right), \tag{5}$$

provided $0 < a < 1$. The corresponding eigenvalues are $\lambda_\pm = e^{\pm\iota 2\theta}$.

In the eigenvector basis, $|\psi\rangle$ can be decomposed as

$$\mathcal{A}|0\rangle = |\psi\rangle = \frac{-\iota}{\sqrt{2}}\left(e^{\iota\theta}|\psi_+\rangle - e^{-\iota\theta}|\psi_-\rangle\right). \tag{6}$$

After j iterations of the subroutine Q, we arrive at the state

$$\begin{aligned} Q^j|\psi\rangle &= \frac{-\iota}{\sqrt{2}}\left(e^{(2j+1)\iota\theta}|\psi_+\rangle - e^{-(2j+1)\iota\theta}|\psi_-\rangle\right) \\ &= \frac{1}{\sqrt{a}}\sin\left((2j+1)\theta\right)|\psi_{\text{good}}\rangle + \frac{1}{\sqrt{1-a}}\cos\left((2j+1)\theta\right)|\psi_{\text{bad}}\rangle. \end{aligned} \tag{7}$$

It follows that if $0 < a < 1$ and if we compute $Q^j|\psi\rangle$ for some integer $j > 0$, then a final measurement will produce a good state with the probability $\sin^2[(2j+1)\theta]$.

If the initial success probability a is either 0 or 1, then the subspace $\mathcal{H}_\psi$ spanned by $|\psi_{\text{good}}\rangle$ and $|\psi_{\text{bad}}\rangle$ has dimension 1 only, but the conclusion remains the same: If we measure the system after j rounds of amplitude amplification, then the outcome is good with probability $\sin^2[(2j+1)\theta]$.

4 Query Complexity Analysis of Quantum Amplitude Amplification Algorithm

Having laid down the algorithm, we would like to know the query complexity of this algorithm so that it can be compared to classical algorithms which solve the same problem. Query complexity is defined as the number of times the function f has to be queried in the implementation of this algorithm.

We want the value of $\sin^2[(2m+1)\theta]$ to be as close to 1 as possible in order to maximise the probability of collapsing to a good solution upon measuring the final state. There is an

optimal number of iterations m to maximise the success probability of the algorithm. The query complexity of the algorithm critically depends on this number of iterations m.

Unfortunately, our ability to choose m wisely depends on our knowledge of θ, and as a consequence on a. Depending on the amount of prior knowledge we have about a, we can come up with different approaches to maximise the success probability. The two extreme case are when we know the value exactly and when we have no prior knowledge about a.

In the following sections, it is shown that regardless of whether the value of a is known exactly or completely unknown, the quantum amplitude amplification algorithm finds a solution to the problem in the $\mathcal{O}(\frac{1}{\sqrt{a}})$ queries to the function f.

4.1 Query complexity with known a

Solving the equation $\sin^2((2m+1)\theta) = 1$, we have $m = \pi/4\theta - 1/2$. Since the number of iterations has to be an integer, we define $\widetilde{m} = \lfloor \pi/4\theta \rfloor$. We note that $|\widetilde{m} - m| \leq 1/2$ so $\widetilde{m}$ is the closest we can get to m iterations. We also note that $\widetilde{m} \leq \pi/4\theta = \frac{\pi}{4}\sqrt{1/a}$, which means that the search algorithm will terminate in $\mathcal{O}(\sqrt{1/a})$ iterations of the subroutine Q.

It also follows from $|\widetilde{m} - m| \leq 1/2$ that $|(2m+1)\theta - (2\widetilde{m}+1)\theta| \leq \theta$. But $(2\widetilde{m}+1)\theta = \pi/2$ by definition of $\widetilde{m}$. Therefore $|\cos((2m+1)\theta)| \leq |\sin\theta|$. This means that the probability of failure after exactly $\widetilde{m}$ iterations of Q is given by $\cos^2((2m+1)\theta) \leq \sin^2\theta = a$, and hence the probability of success is at least $1 - a$.

If a is very large, then we have a big chance of failure even after optimal number of iterations. In that case, we could simply measure the original state $\psi = \mathcal{A}|0\rangle$ which would collapse to a state in the good subspace with probability a.

Theorem 3 (Quadratic speedup) *Let $\mathcal{A}$ be any quantum algorithm that uses no measurements, and let $f : \{0, 1, ..., N-1\} \to \{0, 1\}$ be any Boolean function. Let a be the initial success probability of algorithm $\mathcal{A}$. Suppose $a > 0$, and set $m = \lfloor \pi/4\theta \rfloor$, where θ is defined so that $\sin^2\theta = a$ and $0 < \theta \leq \pi/2$. Then, if we compute $Q^m\mathcal{A}|0\rangle$ and measure the system, the outcome is good with probability at least $\max(1-a, a)$.*

4.2 Query complexity with unknown a

Lemma 4 *For any real numbers α and β, and any positive integer m,*

$$\sum_{j=0}^{m-1} \cos(\alpha + 2\beta j) = \frac{\sin(m\beta)\cos(\alpha + (m-1)\beta)}{\sin\beta}\,.$$

In particular, when $\alpha = \beta$,

$$\sum_{j=0}^{m-1} \cos((2j+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha}\,.$$

Lemma 5 *Let a be the (unknown) initial success probability of algorithm $\mathcal{A}$ and let θ be such that $\sin^2\theta = a$. Let m be an arbitrary positive integer. Let j be an integer chosen at random according to the uniform distribution between 0 and $m-1$. If we measure the final state after applying j iterations of the subroutine Q starting from the initial state $|\psi\rangle = \mathcal{A}|0\rangle$, the probability of obtaining a solution is exactly*

$$P_m \;=\; \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)}\,.$$

In particular $P_m \geq 1/4$ when $m \geq 1/\sin(2\theta)$.

Proof. The probability of success if we perform j iterations of subroutine Q is $\sin^2((2j+1)\theta)$. It follows that the average success probability when $0 \leq j < m$ is chosen randomly is

$$\begin{aligned} P_m &= \sum_{j=0}^{m-1} \frac{1}{m}\sin^2((2j+1)\theta) \\ &= \frac{1}{2m}\sum_{j=0}^{m-1} 1 - \cos((2j+1)2\theta) \\ &= \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)}\,. \end{aligned}$$

If $m \geq 1/\sin(2\theta)$ then

$$\frac{\sin(4m\theta)}{4m\sin(2\theta)} \leq \frac{1}{4m\sin(2\theta)} \leq \frac{1}{4}\,.$$

The conclusion follows.

We are now ready to describe the algorithm for finding a solution when the initial success probability a is unknown. For simplicity we assume at first that $0 \leq a \leq 3/4$.

1. Initialize $m = 1$ and set $\lambda = 6/5$.
   (Any value of λ strictly between 1 and 4/3 would do.)
2. choose j uniformly at random among the nonnegative integers smaller than m.
3. Apply j iterations of Q starting from initial state $|\psi\rangle = \mathcal{A}\,|0\rangle$.
4. Observe the register: let $|x_i\rangle$ be the outcome.
5. If $f(x_i) = 1$, the problem is solved: *exit*.
6. Otherwise, set m to $\min(\lambda m, \sqrt{N}\,)$ and go back to step 2.

Theorem 6 *This algorithm finds a solution in expected time in* $\mathcal{O}(\sqrt{1/a}\,)$.

Proof. Let θ be the angle so that $\sin^2\theta = a$. Let

$$m_0 = 1/\sin(2\theta) = \frac{1}{2\sqrt{(1-a)a}} < \sqrt{\frac{1}{a}}$$

(recall that we assumed $a \leq 3/4$).

We shall estimate the expected number of times that the subroutine Q is performed: the total time needed is clearly in the order of that number. On the s^{th} time round the main loop, the value of m is λ^{s-1} and the expected number of subroutines Q is less than half that value since j is chosen randomly so that $0 \leq j < m$. We say that the algorithm reaches the *critical stage* if it goes through the main loop more than $\lceil \log_\lambda m_0 \rceil$ times. The value of m will exceed m_0 if and when the algorithm reaches that stage.

The expected total number of subroutines needed to reach the critical stage, if it is reached, is at most

$$\frac{1}{2}\sum_{s=1}^{\lceil \log_\lambda m_0 \rceil} \lambda^{s-1} < \frac{1}{2}\frac{\lambda}{\lambda - 1} m_0 = 3m_0\,.$$

Thus, if the algorithm succeeds before reaching the critical stage, it does so in a time in $\mathcal{O}(m_0)$, which is in $\mathcal{O}(\sqrt{1/a}\,)$ as required.

If the critical stage is reached then every time round the main loop from this point on will succeed with probability at least 1/4 by virtue of Lemma 5 since $m \geq 1/\sin(2\theta)$. It follows

that the expected number of subroutines Q needed to succeed once the critical stage has been reached is upper-bounded by

$$\frac{1}{2}\sum_{u=0}^{\infty}\frac{3^u}{4^{u+1}}\,\lambda^{u+\lceil \log_\lambda m_0\rceil} < \frac{\lambda}{8-6\lambda}m_0 = \frac{3}{2}m_0\,.$$

The total expected number of subroutines, in case the critical stage is reached, is therefore upper-bounded by $\frac{9}{2}m_0$ and thus the total expected time is in $\mathcal{O}(\sqrt{1/a}\,)$ provided $0 \leq a \leq 3/4$. Note that $\frac{9}{2}m_0 \approx \frac{9}{4}\sqrt{1/a}$ when $a \ll 1$, which is less than four times the expected number of iterations that we would have needed had we known the value of a ahead of time. The case $a > 3/4$ can be disposed of in constant expected time by classical sampling.

Theorem 7 (Quadratic speedup without knowing a) *Let $\mathcal{A}$ be any quantum algorithm that uses no measurements, and let $f : \{0,1,...,N-1\} \to \{0,1\}$ be any Boolean function. Let a be the initial success probability of algorithm $\mathcal{A}$ and suppose $a > 0$. Then, there exists an algorithm that finds a good solution using queries to f which are in the $\mathcal{O}(\sqrt{1/a})$.*

5 Conclusion

In this report I presented the quantum amplitude amplification algorithm to solve the unstructured search problem. Given a Boolean function $f : \{0,1,...,N-1\} \to \{0,1\}$, the goal is to find a *good solutions*, i.e, any x_0 such that $f(x_0) = 1$. The following points were presented in this report:

- Amplitude amplification algorithm finds a good solution to the Boolean function with query complexity in $\mathcal{O}(\sqrt{1/a})$, where a is the initial success probability of quantum algorithm $\mathcal{A}$.
- The query complexity remains the same even if the initial success probability a is unknown ahead of time. The algorithm thus achieves a quadratic speedup even in the worst case over the expected complexity of classical algorithms.
- The probability of measuring a good solution after j iterations of the algorithm subroutine Q, starting from the initial state $|\psi\rangle = \mathcal{A}\,|0\rangle$, is given by $\sin^2[(2j+1)\theta]$ where θ is defined so that $\sin^2\theta = a$. We can choose an optimal number of iterations $m \in \mathcal{O}(\sqrt{1/a})$ so that $\sin^2[(2m+1)\theta] \approx 1$.

References

[1] IBM. "IBM Quantum breaks the 100-qubit processor barrier" (2021). URL: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.

[2] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/s0097539795293172. URL: https://doi.org/10.1137%2Fs0097539795293172.

[3] L. K. Grover. *A fast quantum mechanical algorithm for database search*. 1996. DOI: 10.48550/arxiv.quant-ph/9605043. URL: https://arxiv.org/abs/quant-ph/9605043.

[4] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. "Tight Bounds on Quantum Searching". *Fortschritte der Physik* 46.4-5 (1998), pp. 493–505. DOI: 10.1002/(sici)1521-3978(199806)46:4/5⟨493::aid-prop493⟩3.0.co;2-p. URL: https://doi.org/10.1002%2F%28sici%291521-3978%28199806%2946%3A4%2F5%3C493%3A%3Aaid-prop493%3E3.0.co%3B2-p.

[5] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. *Quantum amplitude amplification and estimation*. 2002. DOI: 10.1090/conm/305/05215. URL: https://doi.org/10.1090%2Fconm%2F305%2F05215.