QUANTUM COMPUTATION AND GROVER'S ALGORITHM

AARON KRAHN

Abstract. This paper provides an introduction to quantum computation by developing the qubit, quantum gate, and quantum circuits. Three simple quantum algorithms provide a nice illustration of the fundamentals and help the reader become familiar with standard quantum computational techniques. Finally, we provide a detailed proof of Grover's searching algorithm. Throughout, we attempt to show the advantages of quantum algorithms over their classical counterparts.

Contents

In classical computation, there are a of number problems that cannot be solved with efficient algorithms. For example, the best classical algorithm for factorizing a large integer N increases exponentially with the size of the integer. If we continue to increase the size of the integer, it does not take long before our algorithm takes longer than the age of the universe to complete itself. In the searching problem (locating a target object in an N object database), the best classical algorithm increases directly as the size of the database. Quantum computation is a new computational model that utilizes the principles of quantum physics with a number of applications. Its goal is both to solve problems that cannot be solved classically as well as solve a number of problems *much more* efficiently! In particular, quantum algorithms for both the factorizing problem and the searching problem are more efficient than the best classical alternatives. Our approach will closely follow [1] and [2].

Throughout the rest of the paper, we will adopt Dirac notation to be consistent with that

used in quantum physics. We will denote a vector v in a vector space $\mathcal{V}$ by $|v\rangle$. The inner product of two vectors v and w will be denoted by $\langle v|w\rangle$.[1] We can interpret a linear operator O either as simply acting on a vector v, as $O|v\rangle$ or by acting as $\langle v|O^\dagger$, where $O^\dagger$ is the Hermitian adjoint to O. These conventions are in place to ensure that the inner product of two vectors is defined in the standard way. We will also always assume that any vector spaces are over the complex numbers.

1. Preliminaries

1.1. **The tensor product.**

Definition 1.1: Suppose that $\mathcal{V}$ and $\mathcal{W}$ are vector spaces. Let $\{|a_1\rangle, \ldots, |a_n\rangle\}$ and $\{|b_1\rangle, \ldots, |b_k\rangle\}$ be bases for $\mathcal{V}$ and $\mathcal{W}$ such that for any $|v\rangle$ in $\mathcal{V}$ and $|w\rangle$ in $\mathcal{W}$, we have $|v\rangle = \sum_{i=1}^{n} v_i\,|a_i\rangle$ and $|w\rangle = \sum_{j=1}^{k} w_k\,|b_k\rangle$, where v_i and w_j are sets of scalars from the associated fields. Then we define the *tensor product of* $\mathcal{V}$ *and* $\mathcal{W}$ as a space $\mathcal{U} = \mathcal{V} \otimes \mathcal{W}$ whose basis elements are given by pairs $(|a_i\rangle, |b_j\rangle)$ and are denoted by

$$\{|a_i\rangle \otimes |b_j\rangle \,:\, i = 1, \ldots, n\,;\, j = 1, \ldots, k\}. \tag{1.1.1}$$

Definition 1.2: For two vectors $|v\rangle$ in $\mathcal{V}$ and $|w\rangle$ in $\mathcal{W}$, we define the map $\otimes : (|v\rangle,\, |w\rangle) \mapsto |v\rangle \otimes |w\rangle$ by

$$|v\rangle \otimes |w\rangle = \sum_{i=1}^{n} \sum_{j=1}^{k} (v_i\, w_j)\, |a_i\rangle \otimes |b_j\rangle.$$

We can easily verify a number of properties. For $|u\rangle$, $|v\rangle$ in $\mathcal{V}$ and $|w\rangle$ in $\mathcal{W}$, we have

$$(|u\rangle + |v\rangle) \otimes |w\rangle = |u\rangle \otimes |w\rangle + |v\rangle \otimes |w\rangle. \tag{1.1.2}$$

Similarly, for $|v\rangle$ in $\mathcal{V}$ and $|w_1\rangle, |w_2\rangle$ in $\mathcal{W}$, we have

$$|v\rangle \otimes (|u\rangle + |w\rangle) = |v\rangle \otimes |u\rangle + |v\rangle \otimes |w\rangle. \tag{1.1.3}$$

Definition 1.3: Let A and B be linear transformations (which we will usually call operators) from $\mathcal{V}$ and $\mathcal{W}$, respectively. Then the action of $A \otimes B$ is defined by

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle. \tag{1.1.4}$$

This definition appears very natural, but it is not at first clear why we can define the action of the operator in this way. Is this definition even unique? It turns out that it is, and this observation is at the heart of quantum computation. It allows us to

[1] The convention $\langle v|$ is used to denote the dual-vector and is conjugate linear.

decompose an operation on a entire quantum system into operations on individual components and makes the construction of quantum algorithms much simpler. To prove that this definition is unique, we must first abstract ourselves from our first definition of the tensor product.

Definition 1.4: Suppose that $\mathcal{V}$ and $\mathcal{W}$ are vector spaces. Then the tensor product of $\mathcal{V}$ and $\mathcal{W}$ is a pair $(\mathcal{U}, \otimes)$ where $\mathcal{U} = \mathcal{V} \otimes \mathcal{W}$ is a vector space and $\otimes : \mathcal{V} \times \mathcal{W} \to \mathcal{U}$ is a bilinear map which satisfies the following property:
for any space $\mathcal{F}$ and any bilinear function $F : \mathcal{V} \times \mathcal{W} \to \mathcal{F}$, there is a unique linear function $G : \mathcal{V} \otimes \mathcal{W} \to \mathcal{F}$ such that $F(|v\rangle, |w\rangle) = G(|v\rangle \otimes |w\rangle)$.

Proposition 1.1: Definition 1.1 satisfies Definition 1.4.

Proposition 1.2: Let $A : \mathcal{V} \to \mathcal{V}'$ and $B : \mathcal{W} \to \mathcal{W}'$ be linear operators. Then there is a unique linear operator $A \otimes B : \mathcal{V} \otimes \mathcal{W} \to \mathcal{V}' \otimes \mathcal{W}'$ such that for any $|v\rangle$ in $\mathcal{V}$ and $|w\rangle$ in $\mathcal{W}$, we have $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$

The proofs of these two propositions are given in [1].

1.2. **The basics of quantum computation.**

In classical computation, the notion of a *bit* is highly fundamental. Classically, a bit can be in one of two states— 0 or 1. For example, the two states of a bit may correspond to the position of a switch in a particular circuit (on and off), so the bit has a lot of physical motivation. In quantum computation, however, we generalize and abstract this notion. We allow a 'bit' to be in the states 0 and 1, but also in a superposition of these states, i.e. a linear combination of the states 0 and 1. We call this mathematical object a 'qubit' and define it more carefully:

Definition 1.5: A *qubit* is described up to a phase factor by a unit vector in $\mathbb{C}^2$.

By convention, we will always take the basis of $\mathbb{C}^2$ to be

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.2.1}$$

such that the state of qubit can written in the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. The requirement that $|\alpha|^2 + |\beta|^2 = 1$ (that it is a unit vector) comes from the fact that in quantum mechanics, if we

measure a vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we will obtain the state $|0\rangle$ with probability $|\alpha|^2$ and the state $|1\rangle$ with probability $|\beta|^2$, and these probabilities must sum to one.

Remark: Multiplying $|\psi\rangle$ by a factor $e^{\imath\phi}$ (ϕ real) results in an indistinguishable state, since for any complex number $\alpha, |\alpha\, e^{\imath\phi}|^2 = |\alpha|^2$. This means that we can only define the state of a qubit up to a phase.

We can therefore re-write $|\psi\rangle$, using the the fact that $|\alpha|^2 + |\beta|^2 = 1 \Leftrightarrow \alpha = \cos\frac{\theta}{2}$ and $\beta = e^{\imath\phi}\sin\frac{\theta}{2}$.

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\imath\phi}\sin\frac{\theta}{2}|1\rangle \tag{1.2.2}$$

where θ and ϕ are real numbers and $|0\rangle$ and $|1\rangle$ are the standard basis states. We have written the state of the system in such a way that the numbers θ and ϕ define a point on a three-dimensional unit sphere, which we call the *Bloch Sphere*. This is a useful way of viewing a single qubit because quantum gates and circuits have simple analogs when viewed from the Bloch Sphere representation.

Definition 1.6: Given a qubit in a state described by the Bloch Sphere Representation, we define the unit vector $(\cos\phi\sin\theta, \cos\phi\cos\theta, \sin\theta)$ to be the state's Bloch vector.

Now we can consider a system with multiple qubits. It is defined in the natural way.

Definition 1.7: An *$n-$qubit system* is described by a unit vector in $\overbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{n\ times}$ where each of the factors $\mathbb{C}^2$ corresponds to the space of a single qubit. We denote this space by $\mathbb{C}^{2^{\otimes n}}$ or $\mathcal{B}^{\otimes n}$, where $\mathcal{B}$ is equal to the space $\mathbb{C}^2$ with the $|0\rangle, |1\rangle$ basis.

By definition of the tensor product, the basis states for $\mathcal{B}^{\otimes n}$ are therefore all possible products of the form

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle, \qquad x_j \in \{0,1\} \tag{1.2.3}$$

which, we often write as either $|x_1, x_2, \ldots, x_n\rangle$ or $|x\rangle,\ x \in \{0,1\}^n$. Given these basis states, the state of an arbitrary n-qubit system can be written in the form

$$\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle, \quad where \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1 \tag{1.2.4}$$

Once again, the requirement that the amplitudes squared of all of the basis states sum to one is because the vector is defined as having unit length.

Example 1.1: Consider a 3-qubit system. By definition, the state of the system is a unit vector in $\mathcal{B}^{\otimes 3}$ and can written as

$$|\psi\rangle = \alpha_{000}|000\rangle+\alpha_{001}|001\rangle+\alpha_{010}|010\rangle+\alpha_{100}|100\rangle+\alpha_{011}|011\rangle+\alpha_{101}|101\rangle+\alpha_{110}|110\rangle+\alpha_{111}|111\rangle \tag{1.2.5}$$

Definition 1.8: A *quantum gate* on an n-qubit system is an arbitrary operator U acting on an ordered set $M, |M| \leq n$ of qubits and the identity operator acting on the remaining qubits, and is denoted by $U[M]$.

Proposition 1.3: Only unitary operators are valid quantum gates.

Proof. Let

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle, \quad where \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1 \tag{1.2.6}$$

and let $|\phi\rangle = U|\psi\rangle$. Then

$$\sum_{x\in\{0,1\}^n} \Pr(|\phi\rangle = |x\rangle) = \sum_{x\in\{0,1\}^n} \langle\phi|x\rangle\langle x|\phi\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1. \tag{1.2.7}$$

□

Since unitary operators preserve the inner product, they preserve the length of unit vectors. This is a necessity for any quantum mechanical system since any state vector of a system must have unit length.

In the case that M is just a single arbitrary qubit, the action of $U[M]$ is just the operator U acting on the space of the qubit and the identity operator acting on the remaining qubits.

Example 1.2: Let H be a two-by-two Hadamard matrix, defined by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.2.8}$$

Then

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{1.2.9}$$

Similarly,

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{1.2.10}$$

Thus, H acts on each computational basis state by bringing it to a superposition of both basis states.[2] Likewise, for a two-qubit system, a Hadamard gate applied to each qubit brings any basis state to a superposition of all four basis states.

Definition 1.9: Let U be a set of quantum gates over an n-qubit system. Then a *quantum circuit* over the set U is a sequence $U_1[M_1], U_2[M_2], \ldots, U_m[M_m]$, where every U_i is in U and M_i denotes an ordered set of qubits.

We can draw quantum circuits using quantum circuit diagrams. We let each qubit of the system reside in a row of the diagram and then move left to right acting with quantum gates, which we denote with the operator name. We surround each gate with a box and connect all gates with wires. For a list of the different components of a quantum circuit diagram, consult Nielsen and Chuang.

2. Simple Quantum Algorithms

2.1. **Deutsch's Algorithm.**

Suppose that Alice, living in Albany, and Bob, living in Boise, are playing the following game. Alice picks a number 0 or 1, and tells Bob her choice by sending him a letter with the number enclosed. When Bob receives the letter, he sends a either a 0 or a 1 back to Alice. Then, Alice selects the other number and sends it to Bob, who responds in the same way. Alice's job is to figure out whether Bob's response function is one-one or not by eliciting the smallest number of responses from Bob.

In mathematical terms, this amounts to the following question: Given a function $f : \{0, 1\} \to \{0, 1\}$, is f one-one?

Classically, the solution algorithm is trivial: it always takes two evaluations of the function. We first compute $f(0)$ and then compute $f(1)$. If they yield the same output, then f is one-one. A quantum computer, however, can solve this problem by evaluating f only once.

[2]Equations (1.2.9) and (1.2.10) allow us to write the action of H on a basis state of a single qubit very succinctly. Namely,

$$H|x\rangle = \sum_{z\in\{0,1\}} \frac{(-1)^{xz}}{\sqrt{2}}.$$

This fact is very useful and will be referenced later in quantum algorithms.

Deutsch's Algorithm: Prepare a two-bit quantum system initialized to $|\psi\rangle = |01\rangle$. Then perform the following quantum circuit:

$$H[1], H[2], W[1,2], H[1], \tag{2.1.1}$$

where W is defined by $W|x, y\rangle = |x, y \oplus f(x)\rangle$ and $\oplus$ means addition modulo 2. Finally, we perform a measurement of the first qubit.

Proof. We start by preparing a 2-qubit system in which the first qubit is in the state $|0\rangle$ and the second qubit is in the state $|1\rangle$, that is, $|\psi\rangle = |01\rangle$. We then apply a Hadamard gate to each qubit to give

$$|\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{2.1.2}$$

Then if we apply W to $|\psi\rangle$, we are brought to the state

$$|\psi\rangle = \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & : f(0) = f(1) \\ \\ \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & : f(0) \neq f(1) \end{cases} \tag{2.1.3}$$

Acting with a Hadamard gate on the first qubit then gives

$$|\psi\rangle = \begin{cases} \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & : f(0) = f(1) \\ \\ \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & : f(0) \neq f(1) \end{cases} \tag{2.1.4}$$

If we measure the first qubit of $|\psi\rangle$, we will obtain $|0\rangle$ if f is not one-one and $|1\rangle$ if it is. Since this algorithm solves the problem using only 1 evaluation of f, it is faster than any possible classical algorithm. □

2.2. **The Deutsch-Josza Algorithm.**

The Deutsch algorithm is a very simple example, but it is a useful illustration of the potential of the quantum computer. Now let's make the game harder. Suppose that Alice is given a natural number $N = 2^n$ for some positive n, and Bob is instructed to assign a value 0 or 1 to each positive integer less than or equal to N. Let's also assume that Bob is a nice guy—-he is either going to assign the same value to each

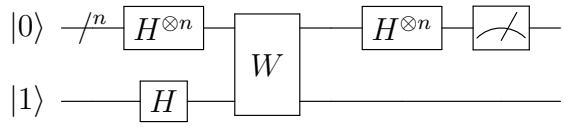
number he is given, or he will assign a 0 to half of the numbers he is given and a 1 to the other half. Alice's job is to figure out which method Bob is using by sending him one number at a time and seeing how he responds. Clearly, in the worst case scenario, Alice would need to send Bob a number $\frac{N}{2}+1$ times to determine his response function.

Mathematically, this is equivalent to the following problem:
Given a function $f:\{0,1\}^n \to \{0,1\}$ that is either balanced or constant, determine using the least number of evaluations of f which one it is.
Since there are 2^n distinct inputs for f, we can associate each n-bit string to a positive integer less than or equal to N.

The Deutsch-Josza Algorithm: Prepare an n+1 qubit system initialized to $|0\rangle^{\otimes n}|1\rangle$. Then perform the following quantum circuit:

$$H[1,2,\ldots,n,n+1], W[1,\ldots,n+1], H[1,\ldots,n].$$

Finally, we perform a measurement of the first n qubits.



Proof.
We start by preparing an $n+1$ qubit system in which the first n qubits are in the state $|0\rangle$ and the last qubit is in the state $|1\rangle$, that is, $|\psi\rangle = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n\,times} \otimes |1\rangle$. We then apply a Hadamard gate to each qubit of $|\psi\rangle$. This action on the first n qubits results in an equal superposition of all the basis states for $\mathcal{B}^{\otimes n}$, and the action on the $(n+1)$th qubit is as usual.

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{2.2.1}$$

Applying W to $|\psi\rangle$ results in

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), \tag{2.2.2}$$

since for any $|x\rangle$, if $f(x) = 0$, then $W|x, y\rangle = |x, y\rangle$ and if $f(x) = 1$, then $W|x, y\rangle = (-1)|x, y\rangle$.

The Hadamard gate is then applied to each of the first n qubits, which gives

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{\sqrt{2^n}} \left[\sum_{k=1}^{n} \frac{(-1)^{x_k\, z_k}|z_k\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{2.2.3}$$

$$= \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{\sqrt{2^n}} \left[\sum_{z\in\{0,1\}^n} \frac{(-1)^{x_1 z_1 \oplus x_2 z_2 \oplus \cdots \oplus x_n z_n}|z\rangle}{\sqrt{2^n}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{2.2.4}$$

$$= \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \left[\frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \tag{2.2.5}$$

where $x \cdot z \equiv x_1 z_1 \oplus x_2 z_2 \oplus \cdots \oplus x_n z_n$.

Now let's consider the probability that the first n qubits of $|\psi\rangle$ are in the state $|0\rangle^{\otimes n}$. As postulated in quantum mechanics, this probability is just the modulus squared of the amplitude of $|0\rangle^{\otimes n}$, which in this case is just

$$\left[\sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n}\right]^2. \tag{2.2.6}$$

If f is constant, then either $f(x) = 0$ for all x or $f(x) = 1$. In either case, the probability of the first n qubits being in the state $|0\rangle^{\otimes n}$ is just 1. This means that the coefficients of the other basis states have to be zero! In other words, if f is constant and we measure the first n qubits, then we will always obtain the state $|0\rangle^{\otimes n}$! On the other hand, if f is balanced, the probability of the first n qubits being in the state $|0\rangle^{\otimes n}$ is 0. □

The Deutsch-Josza algorithm is able to solve the problem with certainty using only one evaluation of the function f, as compared to the classical approach which takes $\frac{N}{2} + 1$ evaluations. This is because the quantum algorithm takes advantage of the superposition of all possible states in order to extract information about f much more quickly than is possible classically.

Yet, despite the seemingly impressive result of this algorithm, there are a few setbacks. First of all, this problem in and of itself is not very useful—it has few known

applications. In addition, if we allow ourselves to use a probabilistic classical computer rather than a deterministic one, the problem becomes almost trivial. Let us turn to a much more important result, the quantum search algorithm.

2.3. **The Quantum Fourier Transform.**

For the last of our basic quantum algorithms, we will discuss the quantum version of the fourier transform and how to implement it with a quantum circuit.

Definition 2.1: The *Quantum Fourier Transform* on an arbitrary orthonormal basis $|1\rangle, |2\rangle, \ldots, |N\rangle$ is a linear operator defined by

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=1}^{N} e^{2\pi \imath jk/N} |k\rangle, \tag{2.3.1}$$

where $|j\rangle$ is a member of the orthonormal basis.

For the rest of this section, we will assume that $N = 2^n$ for some natural number n so that an n-qubit system system with the standard basis states can be expressed as $|1\rangle, |2\rangle, \ldots, |N\rangle$. Then, for $j \in \{1, \ldots, N\}$, we have $|j\rangle = |j_1 j_2 \ldots, j_n\rangle$, with each $j_i \in \mathcal{B}$. More formally, we have

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^n. \tag{2.3.2}$$

Proposition 2.1: The quantum fourier transform (QFT) is unitary.

Proof. We must show that the QFT preserves the inner product. By definition,

$$\langle j|QFT^\dagger QFT|i\rangle = \frac{1}{\sqrt{N}} \frac{1}{\sqrt{N}} \sum_{k=1}^{N} e^{-2\pi \imath jk/N} \sum_{k=1}^{N} e^{2\pi \imath ik/N} \langle k|k\rangle = \frac{1}{N} \sum_{k=1}^{N} e^{2\pi \imath k(i-j)/N}. \tag{2.3.3}$$

This is just a geometric series, whose sum is given by

$$\frac{1 - e^{2\pi \imath (i-j)}}{1 - e^{2\pi \imath (i-j)/N}} = \delta_{ij} \tag{2.3.4}$$

□

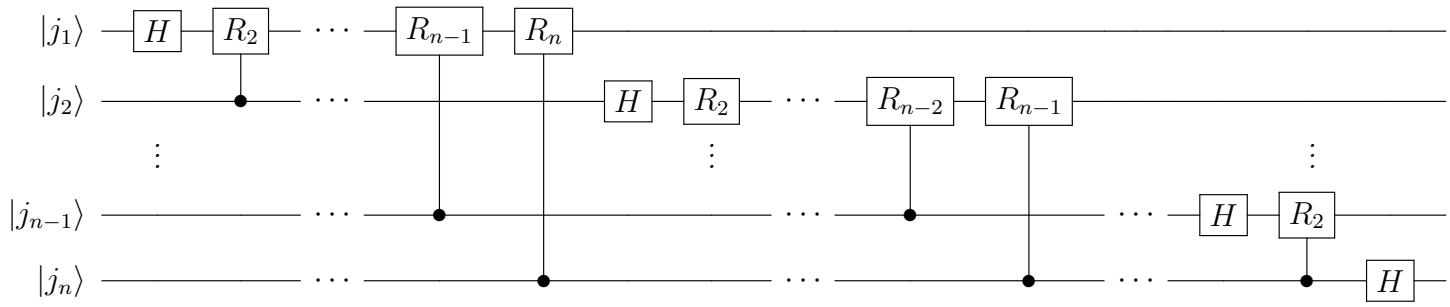
Proposition 2.2 Let $|j\rangle = |j_1, j_2, \ldots, j_n\rangle$ be an arbitrary basis state. Then

$$QFT|j\rangle = \frac{(|0\rangle + e^{2\pi\imath j_n/2}|1\rangle)(|0\rangle + e^{2\pi\imath(j_{n-1}/2+j_n/4)}|1\rangle)\cdots(|0\rangle + e^{2\pi\imath(j_1/2+j_2/4+\cdots+j_n/2^n)}|1\rangle)}{2^{n/2}} \tag{2.3.5}$$

That is, the QFT can be given a product representation.[3]

Proof. Straightforward algebra ([2] has a direct proof). □

Theorem 2.3.1. *The following quantum circuit implements the QFT.*



The gate R_k is defined by

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi\imath/2^k} \end{pmatrix} \tag{2.3.6}$$

By the vertical connecting wires, we mean that we only apply the gate R_k if the connected qubit (with a black dot) is in the state $|1\rangle$. We do not apply R_k if the qubit is in the state $|0\rangle$.

3. Grover's Quantum Search Algorithm

Suppose we are given an address book of N names, and we wish to find and contact one individual in the book. Classically, the obvious algorithm to employ is to search from the beginning of the book to the end. We will have to browse through $N/2$ entries to have a 50% chance of finding the one we want. In other words, the algorithm takes $O(N)$ operations, meaning that the number of steps of the algorithms asymptotically grows as the length of the list. On a quantum computer, we can make our lives much easier by using Grover's Algorithm. Grover's Algorithm searches an

[3]This product representation is often taken to be the definition of the QFT, but we choose to define it with a sum so that it can be compared more easily with its classical analog.

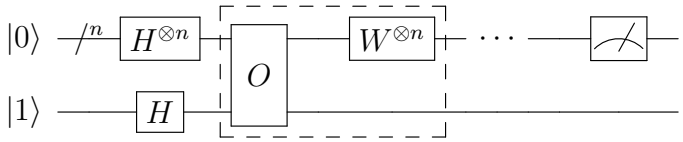
N-object unsorted database for an object in $O(\sqrt{N})$ operations, offering a quadratic speedup from its classical counterpart. We will use the same approach as [2].

Theorem 3.1. *Let N be a large positive integer such that $1, 2, \ldots, N-1, N$ is an N-object unsorted database. Assume that $N = 2^n$ for some natural number n and let y be a positive integer in the database such that there is a function f from the database to the set $\{0,1\}$that satisfies $f(y) = 1$ and $f(x) = 0$ for each $x \neq y$ in the database. Then the following algorithm outputs the target object y with $O(\sqrt{N})$ operations and succeeds with probability $O(1)$.*

Initialize an $n+1$ qubit system to the state $|0\rangle^{\otimes n}|1\rangle$. Define operators O and W by $O|x,z\rangle = |x\rangle|z \oplus f(x)\rangle$ and $W = 2|\psi\rangle\langle\psi| - I$. Then perform the following quantum circuit:

$$H[1,2,\ldots,N,N+1],\overbrace{[O[1,\ldots,N],\, W[1,\ldots,N]}^{R\ times}, \tag{3.0.7}$$

where $R \approx \frac{\pi\sqrt{N}}{4}$. Finally, measure the first n qubits.



where the three dots on the top wire indicate that we iterate the grouped gates R times.

Before we prove this main theorem, we will prove a few other results from which Grover's Algorithm will follow rather directly.

Proposition 3.1: Consider an $n+1$ qubit quantum system intialized to

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

Let $f : \{0,1\}^n \to \{0,1\}$ be a function with the restriction that there is only one x in $\{0,1\}^n$ such that $f(x) = 1$, which we denote by y. Let O be defined as in the statement of the theorem. Then the action of the operator O can be viewed as flipping the amplitude of the basis state $|y\rangle$ and leaving all other states unchanged.

Proof. As in the Deutsch-Josza algorithm, applying O to $|\psi\rangle$ gives

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

We can decompose this sum into two parts in order to simplify it.

$$|\psi\rangle = \sum_{x\neq y} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} + \frac{(-1)^{f(y)}|y\rangle}{\sqrt{2^n}} = \sum_{x\neq y} \frac{|x\rangle}{\sqrt{2^n}} - \frac{|y\rangle}{\sqrt{2^n}}, \tag{3.0.8}$$

since $f(x) = 0$ for $x \neq y$.[4] □

In the statement of the theorem, we assumed that we had an N-object unsorted database with $N = 2^n$ for some n. Since there are 2^n computational basis states for an n-qubit system and 2^n objects in the database, we can associate each object in the database to a basis state of the quantum system. In other words, we associate object 1 of the database with the basis state $|0\ldots0\rangle$, object 2 with the basis state $|0\ldots1\rangle$ and so on and so forth.

This allows us to rewrite an equal superposition of all basis states of an n-qubit system, which we denote by $|\psi\rangle$, in terms of N rather than n:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} = \sum_{x=1}^{N} \frac{|x\rangle}{\sqrt{N}}. \tag{3.0.9}$$

In fact, we can go further, by decomposing the sum into its solution and non-solution components in the following way:

$$|\psi\rangle = \sum_{x\neq y} \frac{|x\rangle}{\sqrt{N}} + \frac{|y\rangle}{\sqrt{N}}. \tag{3.0.10}$$

Definition 3.1: We define the normalized state $|\alpha\rangle$ by

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x\neq y} |x\rangle, \tag{3.0.11}$$

such that Equation (3.0.10) can be rewritten as

$$|\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|y\rangle. \tag{3.0.12}$$

[4]We ignore the $(n+1)$ qubit in the last steps because it is unchanged by the operator O.

Lemma 3.1: Given a quantum system in the state given by Equation (3.0.12), the operator O performs a reflection of the vector $|\psi\rangle$ about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|y\rangle$.

Proof. Let

$$|\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|y\rangle,$$

such that $|\psi\rangle$ is in the space spanned by $|\alpha\rangle$ and $|y\rangle$. Then by Proposition 3.1,

$$O|\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle - \frac{1}{\sqrt{N}}|y\rangle, \tag{3.0.13}$$

since by definition, $|\alpha\rangle$ is the collection of non-solutions. □

Lemma 3.2 Let the state of a quantum system be given by

$$|\phi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle - \frac{1}{\sqrt{N}}|y\rangle.$$

Let $|\psi\rangle$ be as in Lemma 3.1. Then the operator W can be viewed as a reflection of the vector $|\phi\rangle$ about $|\psi\rangle$ in the space spanned by $|\alpha\rangle$ and $|y\rangle$.

Proof. By straightforward computation. □

The two above lemmas shows that the action of O followed by W is a *rotation* in the space spanned by $|\alpha\rangle$ and $|y\rangle$, since the product of these two reflections is a rotation by twice the angle between the initial vectors (simple fact from geometry). Now the methodology of Grover's Algorithm is becoming clear. We construct a vector $|\psi\rangle$ in the span of $|\alpha\rangle$ and $|y\rangle$ and successively rotate it using the operators O and W, moving it closer and closer to our solution vector, $|y\rangle$. We are now ready to prove the main theorem.

Proof. (Theorem 3.1) We start with a quantum system in the $|0\rangle^{\otimes n}|1\rangle$. After applying the Hadamard gate for each qubit, we are brought to a superposition of the computational basis states, as in the Deutsch-Josza algorithm:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{3.0.14}$$

We can now rewrite the first n qubits, as we did in Equation (3.0.10) and then again in Equation (3.0.12), giving

$$|\psi\rangle = \left(\frac{\sqrt{N-1}}{\sqrt{N}}|\alpha\rangle + \frac{1}{\sqrt{N}}|y\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{3.0.15}$$

Now, let us denote the angle between $|\psi\rangle$ and $|\alpha\rangle$ by $\frac{\theta}{2}$. By a property of the inner product, $\cos(\pi - \frac{\theta}{2}) = \langle y|\psi\rangle = \frac{1}{\sqrt{N}}$. In other words, rotating $|\psi\rangle$ by $\arccos(\frac{1}{\sqrt{N}})$ radians brings it to $|y\rangle$. We know by the remark below Lemma 3.2 that O and then W acting on $|\psi\rangle$ rotates it by θ radians. Therefore, we will need to iterate this rotation

$$R = \mathrm{CL}\left(\frac{\arccos\sqrt{1/N}}{\theta}\right)^{5},$$

times in order to rotate $|\psi\rangle$ to within an angle $\theta/2$ of $|y\rangle$.

This is the exact value of R. However, for practical purposes, it is much more useful to have a simpler and more intuitive expression for R. To achieve this, we use the fact that the arccos function is bounded above by π and the fact that since there is only one solution to the search problem, θ is small, so

$$\frac{\theta}{2} \approx \sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}. \tag{3.0.16}$$

This gives that

$$R \leq \frac{\pi\sqrt{N}}{4}, \tag{3.0.17}$$

or in other words, $R = O(\sqrt{N})$. □

Example 3.1: Take $N = 4$. Let f be a function such that $f(3) = 1$ and $f(x) = 0$ for $x = 1, 2, 4$. Choose a two-qubit system, $n = 2$, so that $2^n = N$. Initialize it to $|\psi\rangle = |00\rangle|1\rangle$. Following Theorem 3.1, we apply the Hadamard gate to each qubit, which gives

$$\left(\frac{|00\rangle}{2} + \frac{|01\rangle}{2} + \frac{|10\rangle}{2} + \frac{|11\rangle}{2}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{3.0.18}$$

[5]By CL, we mean the closest integer, rounding down. For example, CL(3.7) = 4.

We now rewrite the state of the system following Equations (3.0.10) and (3.0.12) and ignore the last qubit due to footnote 4 .

$$\left(\frac{|1\rangle}{2}+\frac{|2\rangle}{2}+\frac{|3\rangle}{2}+\frac{|4\rangle}{2}\right)=\frac{\sqrt{3}}{2}|\alpha\rangle+\frac{1}{2}|3\rangle, \tag{3.0.19}$$

where $|\alpha\rangle$ is, by definition, equal to $\frac{1}{\sqrt{3}}|1\rangle+\frac{1}{\sqrt{3}}|2\rangle+\frac{1}{\sqrt{3}}|4\rangle$. Finally, we apply Grover's Iteration $R=1$ time and then measure.

$$O|\psi\rangle=\frac{\sqrt{3}}{2}|\alpha\rangle-\frac{1}{2}|3\rangle. \tag{3.0.20}$$

$$WO|\psi\rangle=|3\rangle. \tag{3.0.21}$$

If we measure the state of the system, we will get $|3\rangle$ with certainty! And, we were able to search for the target object with only application of Grover's Iteration. This is faster than any classical search algorithm!

Acknowledgments: It is my pleasure to thank my mentor, Matthew Wright, for helping me organize and consolidate my original ideas as well as for giving me insight along every step of the editing and writing process. I would also like to thank Peter May for organizing and planning this year's REU program and allowing me to be a part of it.

References

[1] Kitaev, A. Yu., A. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. Providence, RI: American Mathematical Society, 2002. Print.

[2] Nielsen, Michael A., and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge: Cambridge UP, 2000. Print.