Effects of laser focusing in an ion trap quantum computer

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science with Honors in Physics from the College of William and Mary in Virginia,

by

Christopher Mayes

Accepted for ____

(Honors, High Honors or Highest Honors)

Advisor: Dr. Cooke

Dr. Griffioen

Dr. Spitkovsky

Williamsburg, Virginia May 2002

Abstract

This thesis analyzes the constraints that are imposed from laser focusing on the trapped ion implementation of a quantum computer. We give the foundations for quantum computation, the Shor algorithm, and the ion trap. A new model for the fields of a tightly focused laser is developed, as well as approximations for near-focus and far-from-focus regions. These fields are then examined in the context of the ion trap.

Contents

1	Intr	roduction	1			
2	Fundamentals					
	2.1	Classical Binary Fundamentals	3			
	2.2	The 'qubit'	4			
	2.3	Quantum Logic	7			
	2.4	Deutsch's Problem	10			
3	The	The Shor Algorithm				
	3.1	Some Number Theory	13			
	3.2	The Quantum Fourier Transform	15			
	3.3	Algorithm	17			
4	The Ion Trap					
	4.1	Introduction	19			
	4.2	Ion Spacing	20			
	4.3	Ion-Laser Interaction	21			
5	Tightly Focused Electromagnetic Beams 23					
	5.1	Basic Electromagnetism	23			
	5.2	Paraxial Approximation	25			
6	The	e Ring Potential	30			
	6.1	The Radius of the Ring	31			
	6.2	Approximating the Ring Potential	32			
	6.3	Large r	34			
	6.4	Small r	36			
	6.5	Near b	39			

7	' Fields				
	7.1 Application to the Ion Trap	48			
8	Conclusions	51			
\mathbf{A}	Bessel function integrals	52			

1 Introduction

For nearly a century Quantum Mechanics has been used to describe interactions at the atomic level with unprecedented precision. Some consider it to be the best physical theory that we know of. Recently it has been realized that the mechanics that govern quantum mechanical systems can be used to solve fundamentally difficult mathematical problems, such as integer factorization, in few steps relative to classical methods, and excitement in this ability has generated an entirely new field of study.

The development of the field of Quantum Computation began in 1980, when Benioff discovered that the evolution of a quantum mechanical Hamiltonian could be used to realize any Turing machine [1], suggesting that such a process is at least as powerful as this classical computational model [2]. Feynman suggested that a quantum computer could be more powerful than a Turing machine [3], and Deutsch actually proved this in 1985.

Deutsch does this by taking the Church-Turing principle, which can be written as "Every function which would naturally be regarded as computable can be computed by a Turing machine," and incorporating physics in it. His new formulation is called the Strong Version of the Church-Turing principle, which reads "Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means." He then shows that the Turing machine does not satisfy this principle, and that a quantum theory for computation does [4].

A quantum computer essentially takes advantage of quantum mechanical superpositions and interference effects that are a result of the unique way in which probabilities are calculated from a wavefunction. The power of such a computer is demonstrated by a quantum algorithm discovered by Shor in 1994 to factor large integers in exponentially fewer steps than any known classical one [5]. While this is only one of a few useful quantum algorithms that we know of, it is plausible that equally powerful ones exist, which could revolutionize certain aspects of information processing. While the theory supporting a quantum computer has been well developed, the actual building of a physical device is far behind. To give a sense of this, in December 2001 IBM's Almaden Research Center used 10¹⁸ molecules in a nuclear magnetic resonance quantum computing experiment in order to factor the number 15.¹ The difficulty lies in being able to coherently control several quantum mechanical systems over relatively long time scales, which is experimentally difficult due to thermodynamic effects from the environment.

One of the more reasonable approaches to build a quantum computer was proposed by Cirac and Zoller in 1995, and it is their implementation that the majority of this thesis is concerned with [6]. Their proposal uses a chain of ions contained in a linear Paul trap and cooled to their ground state of motion, with lasers target individual ions in order to carry out a computation. The high spatial localization of these ions makes this possible.

In order for this process to work, the laser must be tightly focused and cause a transition in a single ion without affecting the electronic state of neighboring ions. To insure this, the fields that describe the laser must be accurately known up to the dimensions of the trap. However, the typical Gaussian approximation to a laser beam does not provide this knowledge on the edges of the laser beam.

This thesis will develop a method for accurately describing these fields, and will give suggestions on how to target the ions. We will begin by giving an overview of quantum computation and the ion trap.

¹http://www.research.ibm.com/resources/news/20011219_quantum.shtml

2 Fundamentals



2.1 Classical Binary Fundamentals

Figure 1: Some basic binary logic gates. Bits A and B represent the input bits, with C and D being the corresponding output bits. For example, if A = 0 and B = 1, then the output of the AND gate would be C = 0. Notice in the AND and XOR gates that the computation flows one way; the input cannot always be determined from the output.

Before we define the elements of quantum computation, it is useful to recall basics from a more familiar device, the modern digital computer. Terms such as 'bits', 'registers', 'gates', and 'algorithms' will have intuitive quantum analogues.

A bit is a fundamental unit of binary information which can assume one of two discrete values, usually denoted as 0 or 1. In TTL logic, for example, the voltage on a wire between ground and +.8V is considered a 0, whereas a voltage greater than +2.0V is considered a 1. By grouping many bits in an ordered array we create a register. If the register has L bits, it can represent up to 2^{L} different numbers.

A gate takes an input array of bits and produces an output of bits. Some common binary gates are shown in Fig. 1 with truth tables for their inputs and outputs. Notice that we can count the number of different inputs exactly and determine their individual outputs exactly, as shown in the truth tables.

An algorithm is essentially the same as a gate, but usually takes a larger input array to produce an output. Because the digital computer is a deterministic machine, the algorithm's input and output can be written down as a truth table. Combinations of the AND and NOT gates (and, implicitly, the COPY gate) can be put together to realize any such algorithm.

2.2 The 'qubit'

The 'qubit' is the fundamental unit of quantum information. Keeping the classical bit in mind, suppose we choose an orthogonal basis $\{|0\rangle, |1\rangle\}$ and make the following definition:

$$qubit \equiv a|0\rangle + b|1\rangle,\tag{1}$$

in which a and b are complex numbers satisfying the normalization condition $|a|^2 + |b|^2 = 1$. A measurement would yield the state $|0\rangle$ with probability $|a|^2$, or the state $|1\rangle$ with probability $|b|^2$. Thus while the classical bit can only be 0 or 1 at an instant in time, the qubit can be both. If a = 0 or b = 0, the qubit can be represented by a classical bit.²

Keeping with the classical analogy, we can build a register of L qubits by ordering them such that the total state of the register Ψ reads

$$|\Psi\rangle = (a_1|0\rangle_1 + b_1|1\rangle_1) \otimes (a_2|0\rangle_2 + b_2|1\rangle_2) \otimes \ldots \otimes (a_L|0\rangle_1 + b_L|1\rangle_L).$$
(2)

The symbol \otimes stands for 'combined with', and since the qubit states are independent,

²This is ignoring an overall phase, which is not important

this is simply multiplication. Notice that the expansion of Eq. 2 contains states ranging from $|0\rangle_1|0\rangle_2...|0\rangle_L$ to $|1\rangle_1|1\rangle_2...|1\rangle_L$, each of which can be identified with the binary numbers ranging from 0 to $2^L - 1$. For example, if we let x = 5, then $|x\rangle \equiv |5\rangle \equiv |1\rangle_1|0\rangle_2|1\rangle_3 \equiv |101\rangle$. If we denote c_x as the certain combination of the complex numbers a_i and b_i that multiplies state $|x\rangle$, then the total state is equivalent to

$$|\Psi\rangle = \sum_{x=0}^{2^{L}-1} c_{x} |x\rangle.$$
(3)

The measurement of every qubit would necessarily yield only one of the eigenvectors of $|\Psi\rangle$. Since the a_i 's and b_i 's were originally normalized,

$$\sum_{x=0}^{2^{L}-1} |c_x|^2 = 1.$$
(4)

This new basis set $\{|x\rangle\}$ is referred to as the *computational basis*, which will usually only span at most a 2 qubit subspace.

It is useful to use a matrix representation of qubits. A single qubit is then written as

$$a|0\rangle + b|1\rangle \equiv \begin{pmatrix} a \\ b \end{pmatrix}.$$
 (5)

An array of L qubits in the computational basis is written as

$$\sum_{x=0}^{2^{L}-1} c_{x}|x\rangle \equiv \begin{pmatrix} c_{1} \\ c_{2} \\ \vdots \\ c_{2^{L}-1} \end{pmatrix}.$$
 (6)

As an example, suppose we have 2 qubits q_1 and q_2 , independently prepared such that $q_1 = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$ and $q_2 = \sqrt{\frac{1}{6}}|0\rangle + i\sqrt{\frac{5}{6}}|1\rangle$. The total state $|\Psi\rangle$ of this system would be

$$|\Psi\rangle = \left(\sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle\right)\left(\sqrt{\frac{1}{6}}|0\rangle + i\sqrt{\frac{5}{6}}|1\rangle\right) \tag{7}$$

$$= \sqrt{\frac{1}{8}}|0\rangle|0\rangle + i\sqrt{\frac{5}{8}}|0\rangle|1\rangle - \sqrt{\frac{1}{24}}|1\rangle|0\rangle - i\sqrt{\frac{5}{24}}|1\rangle|1\rangle \tag{8}$$

$$= \sqrt{\frac{1}{8}}|00\rangle + i\sqrt{\frac{5}{8}}|01\rangle - \sqrt{\frac{1}{24}}|10\rangle - i\sqrt{\frac{5}{24}}|11\rangle$$
(9)

$$\equiv \begin{pmatrix} \sqrt{\frac{1}{8}} \\ i\sqrt{\frac{5}{8}} \\ -\sqrt{\frac{1}{24}} \\ -i\sqrt{\frac{5}{24}} \end{pmatrix}.$$
(10)

The equality in Eq. 10 is in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

At this point we can see the enormous complexity involved: classically the state of a register of 300 qubits would require $2^{300} - 1 \approx 2 * 10^{90}$ complex numbers to describe completely, since each qubit has 2 complex numbers attributed to it and an overall phase can be factored out. Even if we could store a complex number for every particle in the universe, it would be impossible to classically store this state.

2.3 Quantum Logic

In digital electronics the 'NAND' gate is *called* 'universal', meaning that any digital circuit can be constructed entirely of NAND gates. In view of the Stong Version of the Church-Turing principle, however, true universal gates must be the components needed to build a universal computer, which must be quantum mechanical in nature. To reiterate, a *universal computer* is a single machine that can perform any physically possible computation [7]. Since a Turing machine can perfectly emulate any digital circuit, but does not satify the above principle, then none of the components of the circuit could be universal. A quantum computer, however, is a universal computer.

A quantum computation can be defined as a series of unitary transformations on a quantum mechanical state followed by an experimental measurement. This measurement collapses a subspace of the wavefunction and yields information about the computation. A particularly useful unitary operator is $\mathbf{U} = e^{-i\mathbf{H}t/\hbar}$, found by the formal integration of the Schrödinger equation with a Hamiltonian **H**.

If we adopt the matrix representation for a single qubit, as in Eq. 5, then any unitary transformation³ U(2) on this qubit is called a 1-qubit gate. Any such matrix can be written as a product of four fundamental 1-qubit gates:

$$\mathbf{U}(2) = V_1 V_2 V_3 V_4,\tag{11}$$

where

³A matix **U** is unitary if and only if $\mathbf{U}^* = \mathbf{U}^{-1}$.

$$V_1 = \begin{pmatrix} e^{i\delta} & 0\\ 0 & e^{i\delta} \end{pmatrix}$$
(12)

$$V_2 = \begin{pmatrix} e^{i\alpha/2} & 0\\ 0 & e^{-i\alpha/2} \end{pmatrix}$$
(13)

$$V_3 = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$
(14)

$$V_3 = \begin{pmatrix} e^{i\beta/2} & 0\\ 0 & e^{-i\beta/2} \end{pmatrix}, \tag{15}$$

in which δ , α , θ , and β are real [8]. If we take $\theta = \pi/2$, $\alpha = \pi$, $\beta = 0$, and $\delta = -\pi$, then Eq. 11 is called the Hadamard gate:

$$\mathbf{R} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1\\ 1 & -1 \end{pmatrix}.$$
 (16)

Thus ${\bf R}$ acting on the eigenvectors $\{|0\rangle,|1\rangle\}$ would give

$$\mathbf{R}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{17}$$

$$\mathbf{R}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{18}$$

Now consider L qubits, with **U** being a $2^L - 1$ dimensional unitary matrix. Deutsch has shown that any such transformation can be reduced to a product of unitary matrices, one spanning a 2 qubit subspace, the others being single qubit gates, which are often referred to as rotations. Such 2 qubit gates are *universal gates* [7]. One of the most intuitive universal gates is the 'Controlled-Not' or **CNOT** gate. In the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ it is written as

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$
(19)

or more compactly

$$\mathbf{CNOT} : |C\rangle|T\rangle = |C\rangle|T \oplus C\rangle, \tag{20}$$

in which $C \in \{0,1\}$ is the control, $T \in \{0,1\}$ is the target, and \oplus denotes addition modulo 2. The target's eigenstate is flipped if and only if the control's eigenstate is $|1\rangle$. Notice that this process is reversible; the input can be entirely determined from the output. If both qubits are in a pure eigenstate, then the CNOT gate is simply a classical XOR gate.



Figure 2: $|C\rangle$ represents the Control qubit, $|T\rangle$ represents the target qubit. The wires (horizontal lines) contain the state of each qubit. Notice that the computation may proceed in either direction: this is a reversible gate.

For example, if $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$, then $\mathbf{CNOT}|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Notice

that this operation effectively entangles the two qubits. Originally, Ψ was in a factorable product state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle)$. After the **CNOT** gate is applied, Ψ cannot be factored, thus measurement of one qubit necessarily changes the state of the other qubit. This is what is meant by entanglement. A conceptual diagram is given in Fig. 2.

Thus, in principle, we only need a CNOT gate and the rotation operators to build any multi-qubit quantum gate. If we choose δ , α , θ , and β in (11) to be irrational multiples of π , then we only require 4 1-bit gates, since any rotation can be approximated with arbitrary accuracy by iterating the gate a certain number of times. Thus only 5 gates are needed to perform any computation to any desired accuracy.

Notice the absence of a quantum mechanical COPY gate. It turns out that, in general, a qubit cannot be copied. A simple proof is given by Wooters and Zurek [9].

$|0\rangle$ R R Measure $|1\rangle$ R U_f

2.4 Deutsch's Problem

Figure 3: A quantum circuit that solves Deutsch's problem. The first qubit is initially set to $|0\rangle$, while the second is set to $|1\rangle$.

Deutsch's problem shows how a quantum computation is performed. Suppose we have a black box \mathbf{U}_f that computes the function $f : \{0, 1\} \longrightarrow \{0, 1\}$ through the operation

$$U_f: |a\rangle |b\rangle = |a\rangle |b \oplus f(a)\rangle, \tag{21}$$

in which $a, b \in \{0, 1\}$. The \oplus operation is simply XOR. In words, if f(a) = 0, then $|b\rangle$ is left unchanged. If f(a) = 1, then b is flipped in $|b\rangle$.

The challenge is to determine whether f(0) = f(1) in a single use of the black box, a task that would require 2 accesses to the box classically. The quantum circuit solving this problem in a single access of the box is shown in Fig. 3, which makes use of the Hadamard gate in Eq. 17. The first qubit is initially set to $|0\rangle$, while the second is set to $|1\rangle$. Following the computation from left to right,

$$|0\rangle|1\rangle \longrightarrow (\boldsymbol{R}|0\rangle)(\boldsymbol{R}|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$
(22)

$$\longrightarrow U \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle)$$
(23)

$$= U\frac{1}{2}(|0\rangle|0\rangle + |1\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|1\rangle)$$
(24)

$$= \frac{1}{2} (|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$$
(25)

$$-|0\rangle|\neg f(0)\rangle - |1\rangle|\neg f(1)\rangle$$
(26)

$$= \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle)$$
(27)

$$\rightarrow \frac{1}{2}((-1)^{f(0)}\boldsymbol{R}|0\rangle + (-1)^{f(1)}\boldsymbol{R}|1\rangle)(|0\rangle - |1\rangle$$
(28)

$$= \frac{1}{2} [((-1)^{f(0)} + (-1)^{f(1)})|0\rangle$$
(29)

$$+((-1)^{f(0)} - (-1)^{f(1)})|1\rangle]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
(30)

$$\longrightarrow (measurement) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle). \tag{31}$$

Thus if f(0) = f(1), then a measurement of the first qubit would yield the state $|0\rangle$ with 100% probability. If $f(0) \neq f(1)$, the same measurement would yield the state $|1\rangle$ with 100% probability. A single access of the box has solved the problem exactly.

Now that we understand the elements of a quantum computation, we are prepared to discuss a more complex quantum circuit and algorithm.

3 The Shor Algorithm

Given an integer N, how does one find its prime decomposition? We will define the size of a number as $\lceil \log_2 N \rceil$, the number of bits required to store N.⁴ One approach would be to divide N by the primes 2,3,5,... until a factor is found. While this method will work, it is not practical, for as the size of N becomes larger the number of divisions required grows exponentially.⁵ The following definition is made to clarify the situation:

We say that an algorithm is *efficient* if the number of steps required grows slower than a fixed polynomial of its input size.

Currently no efficient classical algorithm had been discovered to factor large integers. Consequently number factorization is the basis for RSA (Rivest, Shamir, Adleman) encryption, the most popular method for securing communications over the internet [10].

We will need some number theory in order to understand a better way to factor large integers.

3.1 Some Number Theory

Suppose we are given an integer N composed of at least 2 prime factors. Let us assume that N is odd and is not a prime power, since there exist efficient classical algorithms for factoring in those cases. Choose an integer $X \neq 1$ such that gcd(X, N) = 1, where gcd is the greatest common divisor function (Note that Euler's algorithm can compute this function efficiently). Now consider the function

$$g(a) = X^a \mod N. \tag{32}$$

 $^{^4\}lceil x\rceil$ denotes the least integer greater than x.

⁵To make this clear, let the size $S = \log_2 N$. If we multiply the size by a number α , then $\alpha S = \alpha \log_2 N =$

 $log_2 N^{\alpha} \equiv log_2 N'$, thus the new number considered N' is exponentially larger than the previous number N.

Euler's theorem shows that there exists a least power $r \neq 0$ of X such that

$$X^r \equiv 1 \mod N. \tag{33}$$

This r is called the *order* of g, and since integer multiples of r leave Eq. 33 invariant it is also called the *period* of g. In the case that r is even, we may subtract 1 from both sides of Eq. 33 and factor, yielding

$$(X^{r/2} - 1)(X^{r/2} + 1) \equiv 0 \mod N.$$
(34)

This implies that N divides the left hand side of Eq. 34. It is impossible for N to divide $(X^{r/2} - 1)$, since that would imply that the order of g equals $r/2 \neq r$. So, if N does not divide $(X^{r/2} + 1)$, then both of the terms in Eq. 34 must contain all of the factors of N. One then simply computes $gcd(X^{r/2} \pm 1, N)$ to find the factors of N.

Thus in order to insure nontrivial factors of N in this process we must choose an X with even order such that $X^{r/2} \neq 1 \mod N$. Fortunately, the probability P of this happening (which is equivalent to the probability of choosing a 'good' X) is always at least 1/2:

$$P \ge 1 - \frac{1}{2^{k-1}},\tag{35}$$

in which k is the number of unique prime factors of N [11].

Therefore the problem of factorization can be reduced to finding the order of g. No classical algorithm has been discovered to do this efficiently, although no one has proven that such an algorithm does not exist. However, a quantum algorithm does exist to compute r efficiently, which uses the so-called Quantum Fourier Transform.

3.2 The Quantum Fourier Transform

The quantum fourier transform is an essential element in the Shor algorithm. Suppose we have L qubits, on which we want to perform the transform. By writing the total state of these qubits in the computational basis, as in Eq. 3, and setting $q = 2^{L}$, the transform is

$$\mathbf{QFT}_{\mathbf{q}}|x\rangle = \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{2\pi i \frac{xy}{q}} |y\rangle.$$
(36)

To make this clear, suppose we want to perform this transform on 2 qubits, where the total state reads $\Psi = |1\rangle|0\rangle$. This is equivalent to $|2\rangle$ in the computational basis⁶. Therefore

$$\mathbf{QFT}_{4}|10\rangle = \frac{1}{2} \sum_{y=0}^{3} e^{2\pi i \frac{y}{4}} |y\rangle$$
(37)

$$= \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle) \tag{38}$$

$$\equiv \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \tag{39}$$

$$= \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle).$$
 (40)

Completely enumerating the transformations for 2 qubits,

$$\mathbf{QFT_4}|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{41}$$

$$\mathbf{QFT}_{4}|01\rangle = \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$$
(42)

$$\mathbf{QFT}_{4}|10\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$
(43)

$$\mathbf{QFT_4}|11\rangle = \frac{1}{2}(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle). \tag{44}$$

 ${}^{6}\Psi = |x\rangle = |1\rangle|0\rangle \equiv |2\rangle$ since 01 in binary is 2 in base 10.

Now consider the sequence of gates R_2 , $S_{2,1}$, R_1 starting from the right, where R_i is the Hadamard gate in Eq. 17 acting on the i^{th} qubit, and $S_{1,0}|11\rangle \rightarrow i|11\rangle$, leaving the other combinations the same. This sequence acting on the state $|0\rangle_1|1\rangle_2$ is

$$R_1|0\rangle_1|1\rangle_2 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle$$
(45)

$$= \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \tag{46}$$

$$S_{2,1}\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + i|11\rangle)$$

$$(47)$$

$$R_2 \frac{1}{\sqrt{2}} (|01\rangle + i|11\rangle) = \frac{1}{2} (|00\rangle - |01\rangle + i|10\rangle - i|11\rangle).$$
(48)

Eq. 48 looks similar to Eq.42, but they are not quite the same. Notice that by reversing the order of the qubits in Eq. 48, the final state becomes

$$\frac{1}{2}(|00\rangle - |01\rangle + i|10\rangle - i|11\rangle) \longmapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle), \tag{49}$$

which is precisely Eq.42, the quantum fourier transform of $|0\rangle|1\rangle$. Shor proved that this process can be extended to operating on L qubits using the sequence

$$(R_L)(S_{L-1,L}R_{L-1})(S_{L-2,L}S_{L-2,L-1}R_{L-2})\dots(S_{1,L}S_{1,L-1}\dots S_{1,3}S_{1,2}R_1),$$
(50)

operating from right to left, and finally reversing the order of the qubits [5]. The operator $S_{m,n}$ is given by

$$\mathbf{S_{m,n}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{n-m}} \end{pmatrix},$$
(51)

which simply changes the phase of the total state containing $|1\rangle_m |1\rangle_n$. Notice that there are *L* instances of **R**, and L(L-1)/2 instances of **S**, for a total of L(L+1)/2operations. Thus the quantum fourier transform acting on *L* qubits can be reduced to L(L+1)/2 operations, each acting on 1 and 2 qubit subspaces. The following algorithm can be made efficient because of this polynomial scaling in the number of operations as *L* increases.

3.3 Algorithm



Figure 4: A graphical representation of the Shor algorithm. Register Φ_1 is initially set to 0.

The Shor Algorithm requires two registers of qubits: Φ_1 and Φ_2 . The first register Φ_1 has $L = \lceil 2 \log_2 N \rceil$ qubits. As before, we take $q = 2^L$. The second register Φ_2 must have at least $\lceil \log_2 N \rceil$ qubits.

Initially we set $\Phi_1 = |0\rangle |0\rangle \dots |0\rangle_L$. Then we apply the QFT_q gate to this register, which is equivalent to applying the \mathbf{R}_i gate to each qubit. Now the register is in an equal superposition of all the possible binary numbers it can store. The next step is to set $\Phi_2 = X^{\Phi_1} \mod N$, and perform a measurement on this register.

This measurement will always return an eigenstate of the computational basis of Φ_2 , call it C. This number must then be of the form $C = X^l \mod N$, and since $1 \equiv X^{mr} \mod N$ with m being a positive integer less than $M = \lfloor (q-l)/r \rfloor$, it must also be equivalent to

$$C = X^{l+mr} \mod N. \tag{52}$$

Thus Φ_1 must contain numbers of the form l + mr, a smaller subset of its previous contents. Without loss of generality, let us assume that r divides q. Application of the next $\mathbf{QFT}_{\mathbf{q}}$ gate will help us extract r.

$$\mathbf{QFT}_{\mathbf{q}}: |\Phi_1\rangle = \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} e^{2\pi i \frac{lm}{r}} |m\frac{q}{r}\rangle.$$
(53)

Finally we measure $|\Phi_1\rangle$, which will yield an integer multiple of q/r. This multiple has a high probability $(1 - 1/\log_2 r)$ of having no common factors with r. Since we know q and C, r can be determined from a series of irreducible fractions [11]. Referring to Section 3.1 one can then find a nontrivial factor of N.

4 The Ion Trap



Figure 5: The laser targets the ion in the center of the diagram. At the center of the string, a_0 is given by Eq. 56, otherwise it is larger, and must be calculated.

4.1 Introduction

In 1995 Cirac and Zoller proposed a scheme to implement CNOT, QFT, and 1-qubit quantum gates using a string of cold trapped ions [6]. Their idea is to use two energy eigenstates of an ion as a single qubit. The center of mass (COM) mode of the string provides a phonon which serves as a 'bus qubit' to convey an interaction between any two ions. Two types of laser pulses are needed: One changes the internal state of an ion as a single qubit rotation, while the other couples an ion's internal state with a COM phonon. This requires one to be able to individually target an ion with a laser and induce a transition without affecting the internal quantum states of the neighboring ions. The situation is depicted in Fig. 5.

4.2 Ion Spacing

Consider a string of L ions, each of mass m, charge Ze, in a linear Paul trap [12], [13]. They are tightly bound in the x and y directions and weakly bound by a harmonic potential in the z direction with angular frequency ω_z . Thus considering only the harmonic potential and Coulomb interaction, the potential energy of the chain is

$$V = \sum_{m=1}^{L} \frac{1}{2} m \omega_z^2 z_m(t)^2 + \sum_{\substack{n,m=1\\m\neq n}}^{N} \frac{Z^2 e^2}{8\pi\epsilon_0} \frac{1}{|z_n(t) - z_m(t)|}.$$
 (54)

If we assume that $z(t)_m \approx z_m^{(0)} + q(t)$, where $z_m^{(0)}$ is the equilibrium position of the $m^t h$ ion and $q_m(t)$ is a small displacement, then the equilibrium positions can be solved by using

$$\left(\frac{\partial V}{\partial z_m}\right)_{z_m = z_m^{(0)}} = 0.$$
(55)

This will lead to L coupled equations, which can be solved numerically. We define a_0 as the minimum spacing of ions, which occurs at the center of the trap. This spacing has been calculated by James [14], and is approximated by:

$$a_0 = \left(\frac{Z^2 e^2}{4\pi\epsilon_0 m\omega_z^2}\right)^{1/3} \frac{2.018}{L^{0.559}}.$$
(56)

Ion	$\lambda(\mu m)$	$\omega_z/2\pi (kHz)$	a_0 for 10 ions (μm)	a_0 for 100 ions (μm)
Beryllium 9	.313	452	6.9	1.9
Calcium 40	.397	63	88.3	24.3

Table 1: Minumum spacings a_0 are given for select ions in 2 proposed schemes [15].

Some proposed ions with their transition wavelengths and trap frequencies are shown in Table 1. Note that the spacing can be increased by lowering the trap frequency. While this may seem advantageous, the result would be a slower quantum computer.

4.3 Ion-Laser Interaction

Energy Levels in an ion



Figure 6: Energy levels within an ion. Levels $|g\rangle$ and $|e_0\rangle$ will be our $|0\rangle$ and $|1\rangle$ qubit eigenstates, respectively. The third level is used only to change the relative phase of the qubit levels; it is never left populated. The energy levels of the trap, with spacing $\delta = \omega_z$, are superimposed on the diagram.

We envision a 3 level system within each ion, as shown in Fig. 6. The energy levels $|g\rangle$ and $|e_0\rangle$ will represent the qubit eigenstates $|0\rangle$ and $|1\rangle$, respectively. The third level $|e_1\rangle$ is coupled only to the state $|g\rangle$, and will never be left populated. The Hamiltonian for a laser focused on the n^{th} ion and coupling the ground state $|g\rangle$ to $|e_q\rangle$ is

$$\mathbf{H}_{\mathbf{n},\mathbf{q}} = \frac{\eta}{\sqrt{L}} \frac{\Omega}{2} \left(|e_q\rangle_n \langle g|a + |g\rangle_n \langle e_q|a^\dagger \right), \tag{57}$$

in which

$$\eta = \sqrt{\frac{\hbar}{2m\omega_z}} \mathbf{k} \cdot \hat{\mathbf{z}}.$$
(58)

The quantity $\mathbf{k} \cdot \hat{\mathbf{z}}$ is the component of the laser wave vector along the axis of the trap, and Ω is the Rabi frequency. For interactions between the qubit levels the laser is detuned by $\delta = -\omega_z$, which creates or annihilates a COM phonon. For example, if the ion is in the $|e_0\rangle$ state, then a detuned laser pulse would induce stimulated emission and introduce a phonon. The operators a^{\dagger} and a in Eq. 57 are the creation and annihilation operators for this phonon. The time evolution of this Hamiltonian is given by

$$U_{n,q}^{l} = \exp\left(-ikt\frac{\pi}{2}|e_{q}\rangle_{n}\langle g|a+ikt\frac{\pi}{2}|g\rangle_{n}\langle e_{q}|a^{\dagger}\right),\tag{59}$$

in which $t = l\pi/(\Omega\eta\sqrt{L})$ is the time that the laser is on. Notice that a COM phonon is created only in a transition from $|e_0\rangle \rightarrow |g\rangle$, and is annihilated in the reverse transition. If we denote the phonon states as $|0\rangle_{phonon}$ and $|1\rangle_{phonon}$, then the operator in Eq. 59 would cause the following transitions:

$$U_{n,q}^{l}|g\rangle_{n}|0\rangle_{phonon} = |g\rangle_{n}|0\rangle_{phonon}$$

$$\tag{60}$$

$$U_{n,q}^{l}|g\rangle_{n}|1\rangle_{phonon} = \cos(l\pi/2)|g\rangle_{n}|1\rangle_{phonon} - i\sin(l\pi/2)|e_{l}\rangle_{n}|1\rangle_{phonon}$$
(61)

$$U_{n,q}^{l}|e_{q}\rangle_{n}|0\rangle_{phonon} = -i\sin(l\pi/2)|g\rangle_{n}|1\rangle_{phonon} + \cos(l\pi/2)|e_{q}\rangle_{n}|1\rangle_{phonon}.$$
 (62)

Suppose we want to perform a CNOT gate on two ions, with the control qubit being the m^{th} ion and the target qubit being the n^{th} ion. In the computational basis, only one of the eigenstates is altered:

$$U_{m,0}^{1}U_{n,1}^{2}U_{m,0}^{1}|e_{0}\rangle_{m}|e_{0}\rangle_{n} = -|e_{0}\rangle_{m}|e_{0}\rangle_{n}.$$
(63)

To see that this performs a CNOT gate, consider the state $|\pm\rangle = \frac{1}{\sqrt{2}}(|g\rangle \pm |e_0\rangle)$. Then these 3 pulses would leave the state $|g\rangle_m |\pm\rangle_n$ unchanged while transforming the state $|e_0\rangle_m |\pm\rangle_n$ into $|g\rangle_m |\mp\rangle_n$, which is precisely the controlled-not operation.

5 Tightly Focused Electromagnetic Beams

To realize the targeting of an ion, we must be able to describe the fields of a tightly focused laser beam. We begin by reviewing some elementary electromagnetism.

5.1 Basic Electromagnetism

Consider a harmonically varying monochromatic beam propagating in the z direction, focused on the point where z = 0, and assume the absence of source charges. It follows from Maxwell's equations that a vector potential $\mathbf{A}(\mathbf{r}, t)$ and a scalar potential V completely describe the beam. We pick the Lorentz gauge

$$\nabla \cdot \mathbf{A}(\mathbf{r}, t) = -\frac{1}{c} \frac{\partial}{\partial t} V, \tag{64}$$

which implies that the vector potential must satisfy the wave equation

$$\left(\nabla^2 - \frac{1}{c^2} \frac{\partial^2}{\partial t^2}\right) \mathbf{A}(\mathbf{r}, t) = 0.$$
(65)

Call the angular frequency of the beam ω . The wavelength $\lambda = 2\pi c/\omega$ and the wave number $k = \omega/c$, where c is the speed of light in a vacuum. Since we have assumed a harmonically varying beam, we can write $\mathbf{A}(\mathbf{r}, t) = \mathbf{A}(\mathbf{r})e^{-i\omega t}$ in complex notation. Eq. 65 can then be replaced by the time-independent Helmholtz equation

$$\left(\nabla^2 + k^2\right) \mathbf{A}(\mathbf{r}) = 0, \tag{66}$$

which, in cylindrical coordinates (r, θ, z) , is

$$\left(\frac{\partial^2}{\partial r^2} + \frac{1}{r}\frac{\partial}{\partial r} + \frac{1}{r^2}\frac{\partial^2}{\partial \theta^2} + \frac{\partial^2}{\partial z^2} + k^2\right)\mathbf{A}(r,\theta,z) = 0.$$
(67)

The electric and magnetic fields are given by

$$\mathbf{E}(\mathbf{r},t) = -\nabla V - \frac{1}{c} \frac{\partial}{\partial t} \mathbf{A}(\mathbf{r},t)$$
(68)

$$\mathbf{B}(\mathbf{r},t) = \nabla \times \mathbf{A}(\mathbf{r},t). \tag{69}$$

By assuming the same harmonic dependence in V as in **A** and using Eq. 64 we can write the spatial part of the electric field as

$$\mathbf{E}(\mathbf{r}) = \frac{i}{k} \left(\nabla (\nabla \cdot \mathbf{A}(\mathbf{r})) + k^2 \mathbf{A}(\mathbf{r}) \right).$$
(70)

The real time dependent electric and magnetic fields are

$$\mathbf{E}(\mathbf{r},t) = Re\{\mathbf{E}(\mathbf{r})e^{-i\omega t}\}\tag{71}$$

$$\mathbf{B}(\mathbf{r},t) = Re\{\mathbf{B}(\mathbf{r})e^{-i\omega t}\}.$$
(72)

The energy and momentum densities u and \mathbf{p} are

$$u = \frac{\epsilon_0}{2} (\mathbf{E}^2 + c^2 \mathbf{B}^2) \tag{73}$$

$$\mathbf{p} = \epsilon_0 (\mathbf{E} \times \mathbf{B}). \tag{74}$$

By time averaging these quantities over a cycle the densities become

$$\overline{u} = \frac{\epsilon_0}{4} \left(\mathbf{E}(\mathbf{r}) \cdot \mathbf{E}^*(\mathbf{r}) + c^2 \mathbf{B}(\mathbf{r}) \cdot \mathbf{B}^*(\mathbf{r}) \right)$$
(75)

$$\overline{\mathbf{p}} = \frac{\epsilon_0}{2} Re\{ \mathbf{E}(\mathbf{r}) \times \mathbf{B}^*(\mathbf{r}) \}.$$
(76)

The energy flux density is given by the Poynting vector

$$\mathbf{S} = \frac{1}{\mu_0} (\mathbf{E} \times \mathbf{B}) = c^2 \mathbf{p},\tag{77}$$

whose time average is simply

$$\overline{\mathbf{S}} = c^2 \overline{\mathbf{p}}.\tag{78}$$

From now on let us refer only to the time averaged quantities, so we relabel the following: $\overline{u} \to u$, $\overline{\mathbf{p}} \to \mathbf{p}$, $\overline{\mathbf{S}} \to \mathbf{S}$. We will also only be concerned with linearly polarized beams, so in Cartesian coordinates (x, y, z), the spatial part of the vector potential takes the form

$$\mathbf{A}(\mathbf{r}) = A_0(\psi, 0, 0),\tag{79}$$

in which A_0 is a constant and $\psi = \psi(\mathbf{r})$. Also, all references to the Poynting vector and energy and momentum densities will be to the time-averaged forms.

5.2 Paraxial Approximation

The intensity profile of a typical laser beam is approximately Gaussian shaped, so usually a Gaussian shaped vector potential is sought from Eq. 65. The procedure begins by assuming the most rapidly varying z dependence of the vector potential lies in the factor e^{ikz} . If we write a component of the vector potential $\psi = G(r, \theta, z)e^{ikz}$, then Eq. 67 becomes

$$\left(\frac{\partial^2}{\partial r^2} + \frac{1}{r}\frac{\partial}{\partial r} + \frac{1}{r^2}\frac{\partial^2}{\partial \theta^2} + \frac{\partial^2}{\partial z^2} + 2ik\frac{\partial}{\partial z}\right)G(r,\theta,z) = 0.$$
(80)

The paraxial approximation assumes that

$$\left|\frac{\partial^2 G}{\partial z^2}\right| \ll k \left|\frac{\partial G}{\partial z}\right|,\tag{81}$$

so we can neglect the former term. By assuming axial symmetry, the $\frac{\partial^2 G}{\partial \theta^2}$ term is zero. Thus Eq. 80 is reduced to

$$\left(\frac{\partial^2}{\partial r^2} + \frac{1}{r}\frac{\partial}{\partial r} + 2ik\frac{\partial}{\partial z}\right)G(r,\theta,z) = 0,$$
(82)

which admits the solution

$$\psi = \frac{b}{\sqrt{b^2 + z^2}} e^{-\frac{kbr^2}{2(b^2 + z^2)}} e^{i\left(kz - tan^{-1}\left(\frac{z}{b}\right) + \frac{kzr^2}{2(b^2 + z^2)}\right)}.$$
(83)

The parameter b is the diffraction length (also called the Rayleigh length), which is defined to be the distance from the focal point that the area of the beam doubles⁷. The waist, or radius of the beam at the focus, is given by

$$w = \sqrt{\frac{2b}{k}}.$$
(84)

⁷The edge of the beam at a given z coordinate is defined to be the point where ψ drops to 1/e of it's value at the center of the beam



Figure 7: A representation for a beam focused at z = 0. The parameter w is the radius of the beam at the focus, and b is the diffraction length.

These quantities are illustrated in Fig. 7.

Unfortunately the paraxial approximation breaks down when the beam waist is on the order of a wavelength. Furthermore, the Gaussian profile in Eq. 83 leads to fields that do not satisfy Maxwell's equations. This problem was addressed by Lax, Louisell, and McKnight, who developed a consistent method for expanding solutions of Eq. 80 in terms of a small parameter, of which the first satisfies the paraxial approximation [16].

Couture and Belanger later showed that all of these solutions converged to a spherical point source given by

$$\psi = \frac{e^{-ikR_c}}{kR_c},\tag{85}$$

in which $R_c = \sqrt{r^2 + (z - ib)^2}$ [17]. Although this is a solution to the Helmholtz equation, it is not physical, for when z = 0 and r = b, the vector potential will

diverge. Sheppard and Saghafi resolve this problem by considering a superposition of incoming and outgoing spherical point sources [18], which can be written as

$$\psi = \frac{\sin(kR_c)}{kR_c}.$$
(86)

We also know exact solutions to the Helmholtz equation that generalize Eq. 86:

$$\psi_{lm} = j_l(kR)P_{lm}(\cos\theta_c)e^{\pm im\theta}.$$
(87)

The complex polar angle θ_c is defined by $\cos \theta_c = \frac{z-ib}{R}$. With $\mathbf{r_0}$ being the location of the source in the plane perpendicular to the z axis,

$$R = \sqrt{(\mathbf{r} - \mathbf{r_0})^2 + (z - ib)^2}.$$
(88)

The j_l is the l^{th} spherical Bessel function, and P_{lm} is an associated Legendre polynomial [19]. In fact, Eq. 86 is simply $\psi_{00} = j_0(kR)$ when $\mathbf{r_0} = 0$.

Lekner has examined ψ_{00} in detail [19], and has shown that it cannot be physically realizable, because any realistic electromagnetic beam must possess a finite amount of energy in any finite length of the beam:

$$\int_{z_1}^{z_2} dz \int_{-\infty}^{\infty} r dr \int_{-\pi}^{\pi} d\theta \ \overline{u} < \infty.$$
(89)

This requires that each component ψ of the vector potential be normalizable at a given z coordinate:

$$\int_{-\infty}^{\infty} r dr \int_{-\pi}^{\pi} d\theta \ |\psi|^2 < \infty.$$
(90)

The ψ_{00} source does not satisfy this criteria, and therefore cannot be a component in a vector potential that yields physical fields, since the following integral diverges logarithmically:

$$\int_{-\infty}^{\infty} r dr \int_{-\pi}^{\pi} d\theta \ |\psi_{00}|^2 \longrightarrow \infty.$$
(91)

However, this solution should not be abandoned, for it will still yield physical fields.

6 The Ring Potential

We will now construct a solution of the Helmholtz equation that satisfies Maxwell's equations and yields physical fields. This is done by considering a special distribution of ψ_{00} sources (Eq. 86) which is normalizable in the sense of Eq. 90. In cylindrical coordinates (r, θ, z) , a single source ψ_{00} placed at a point $(r_0, \phi_0, -ib)$ would have an R (Eq. 88) of the form

$$R = \sqrt{(r^2 + r_0^2 - 2rr_0\cos(\theta - \phi_0) + (z - ib)^2)}.$$
(92)

Since we require ψ to be cylindrically symmetric, any distribution of ψ_{00} sources must also have that same symmetry. One such distribution is a continuous ring of radius a, which is represented by the following integral:

$$\psi = \int_{-\infty}^{\infty} r_0 dr_0 \int_{-\pi}^{\pi} d\phi_0 \,\,\delta(r_0 - a) \frac{\sin(k\sqrt{(r^2 + r_0^2 - 2rr_0\cos(\theta - \phi_0) + (z - ib)^2})}{k\sqrt{(r^2 + r_0^2 - 2rr_0\cos(\theta - \phi_0) + (z - ib)^2}} = a \int_{-\pi}^{\pi} d\phi_0 \,\frac{\sin(k\sqrt{(r^2 + a^2 - 2ra\cos(\theta - \phi_0) + (z - ib)^2})}{k\sqrt{(r^2 + a^2 - 2ra\cos(\theta - \phi_0) + (z - ib)^2}}$$
(93)

$$= a \int_{-\pi}^{\pi} d\phi \, \frac{\sin(k\sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2)})}{k\sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2)}}.$$
(94)

Eq. 93 is simply the integration over the delta function $\delta(r_0 - a)$, and Eq. 94 relabels ϕ_0 as ϕ and ignores θ due to cylindrical symmetry. We suppress a, since it is simply a multiplicative constant, and obtain the final form for the ring:

$$\psi_{Ring} = \int_{-\pi}^{\pi} d\phi \; \frac{\sin(k\sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2)})}{k\sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2}}.$$
(95)

The vector potential for this ring, in Cartesian coordinates, is therefore

$$\mathbf{A}_{Ring} = A_0(\psi_{Ring}, 0, 0). \tag{96}$$

6.1 The Radius of the Ring

Now we will determine the radius a of the ring such that ψ_{Ring} is normalizable. First, we asymptotically expand $\sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2)}$ about r at infinity:

$$R = \sqrt{(r^2 + a^2 - 2ra\cos(\phi) + (z - ib)^2)}$$
(97)

$$= \frac{1}{r}\sqrt{\left(1 + \frac{a^2}{r^2} - \frac{2a\cos(\phi)}{r} + \frac{(z-ib)^2}{r^2}\right)}$$
(98)

$$\sim r - a\cos(\phi) + \mathcal{O}\left(\frac{1}{r}\right).$$
 (99)

So for large r Eq. 95 asymptotically approaches

$$\psi_{Ring} \sim \int_{-\pi}^{\pi} d\phi \, \frac{\sin(kr - ka\cos(\phi))}{kr - ka\cos(\phi)}$$
(100)

$$\sim \int_{-\pi}^{\pi} d\phi \, \frac{\sin(kr - ka\cos(\phi))}{kr}$$
(101)

$$= 2\pi J_0(ka) \frac{\sin(kr)}{kr}, \qquad (102)$$

in which J_0 is the zeroth order Bessel function of the first kind. We now find that, by setting ak to be the zero of this Bessel function, that the 1/r behavior of ψ_{Ring} vanishes. If a_i is any zero of J_0 , then we choose

$$a = \frac{a_i}{k}.\tag{103}$$



Figure 8: A comparison of ψ_{Ring} 's using different a_i values $(J_0(a_i) = 0)$, showing that the smallest one forms a function most similar to a Gaussian function (Eq. 83) of the same parameters, shown in black. The plots are done with a waist of 2λ at z = 0. Lighter lines represent higher a_i values.

From Fig. 8, we see that the first zero most closely approximates a Gaussian curve of the same parameters; thus we will pick this zero, which to 20 decimal digits is 2.4048255576957727686.

6.2 Approximating the Ring Potential

Unfortunately the angular integral in Eq. 95 has no simple solution. The approximation we will now develop is valid as $r \to \infty$ and near the center of the beam.

We first define q to be the terms in R (Eq. 97) that do not depend on $\cos(\phi)$:

$$q^{2} \equiv r^{2} + a^{2} + (z - ib)^{2}.$$
(104)

Then R becomes

$$R = \sqrt{q^2 - 2ra\cos(\phi)}.$$
(105)

We define Δ to be R minus it's leading order terms in an asymptotic expansion⁸:

$$\Delta \equiv \sqrt{q^2 - 2ra\cos(\phi)} - \left(q - \frac{ra\cos(\phi)}{q}\right). \tag{106}$$

Now Eq. 95, without the integral, can be written in terms of Δ :

$$\frac{\sin(kR)}{kR} = \frac{1}{2ik} \left(\frac{e^{ikR}}{R} - \frac{e^{-ikR}}{R} \right)$$
(107)

$$= \frac{1}{2ik} \left(\frac{e^{ik(\Delta + q - \frac{i\alpha\cos(\varphi)}{q})}}{R} - \frac{e^{-ik(\Delta + q - \frac{i\alpha\cos(\varphi)}{q})}}{R} \right)$$
(108)

$$= \frac{1}{2ik} \left(e^{ikq} e^{-i\frac{kra\cos(\phi)}{q}} \frac{e^{ik\Delta}}{R} - e^{-ikq} e^{i\frac{kra\cos(\phi)}{q}} \frac{e^{-ik\Delta}}{R} \right)$$
(109)

$$= \frac{1}{2ik} \left(e^{ikq} e^{-i\frac{kra\cos(\phi)}{q}} A - e^{-ikq} e^{i\frac{kra\cos(\phi)}{q}} B \right),$$
(110)

where

$$A \equiv \frac{e^{ik\Delta}}{R} \tag{111}$$

$$B \equiv \frac{e^{-ik\Delta}}{R}.$$
(112)

Now we expand A and B asymptotically about q at infinity:

$$A \sim \frac{1}{q} + \frac{ar\cos(\phi)}{q^3} - \frac{ia^2kr^2\cos^2(\phi)}{2q^4} + \mathcal{O}\left(\frac{1}{q^5}\right)$$
(113)
$$\frac{8\sqrt{q^2 - 2ra\cos(\phi)} \sim q - \frac{ra\cos(\phi)}{q} + \mathcal{O}(\frac{1}{q^3})}{q}$$

$$B \sim \frac{1}{q} + \frac{ar\cos(\phi)}{q^3} + \frac{ia^2kr^2\cos^2(\phi)}{2q^4} + \mathcal{O}\left(\frac{1}{q^5}\right).$$
 (114)

Notice that Eqs. 113-114 each contain powers of $\cos(\phi)$. For example, keeping terms to order $1/q^3$ we can now integrate Eq. 110 (see Appendix):

$$\int_{-\pi}^{\pi} d\phi \; \frac{\sin(kR)}{kR} \; = \; \int_{-\pi}^{\pi} d\phi \; \frac{1}{2ik} \left(e^{ikq} e^{-i\frac{kra\cos(\phi)}{q}} A - e^{-ikq} e^{i\frac{kra\cos(\phi)}{q}} B \right) \quad (115)$$

$$\cong \frac{e^{ikq}}{2ik} \int_{-\pi}^{\pi} d\phi \ e^{-i\frac{kra\cos(\phi)}{q}} \left(\frac{1}{q} + \frac{ar\cos(\phi)}{q^3}\right)$$

$$-\frac{e^{-ikq}}{2ik} \int_{-\pi}^{\pi} d\phi \ e^{i\frac{kra\cos(\phi)}{q}} \left(\frac{1}{q} + \frac{ar\cos(\phi)}{q^3}\right)$$

$$(116)$$

$$= \frac{2ik}{2ik} \int_{-\pi} \left(\frac{q}{q^3} \frac{q^3}{q^3} \right)$$

$$= \frac{e^{ikq}}{2ik} \left(\frac{2\pi J_0(kra/q)}{q} - \frac{2\pi iar J_1(kra/q)}{q^3} \right)$$

$$- \frac{e^{-ikq}}{2ik} \left(\frac{2\pi J_0(kra/q)}{q} + \frac{2\pi iar J_1(kra/q)}{q^3} \right)$$

$$= \frac{2\pi J_0(kra/q)}{kq} \sin(kq) - \frac{2\pi ar J_1(kra/q)}{kq^3} \cos(kq). \quad (118)$$

This procedure is easily generalized to obtain any higher order term. Let us label $\psi_{Ring}^{(n)}$ as the approximation to ψ_{Ring} keeping *n* terms in the asymptotic expansion in Eqs. 113-114. With 3 terms the approximation to ψ_{Ring} is

$$\psi_{Ring}^{(3)} = \frac{2\pi J_0\left(\frac{kra}{q}\right)}{kq} \sin(kq) - \frac{2\pi ar J_1\left(\frac{kra}{q}\right)}{kq^3} \cos(kq) + \frac{\pi a^2 r^2 \left(J_2\left(\frac{kra}{q}\right) - J_0\left(\frac{kra}{q}\right)\right)}{2q^4} \cos(kq)$$
(119)

6.3 Large r

Since $q \approx r$ for large values of r, our asymptotic expansion gets better as $r \to \infty$. However, it is important to know how many terms we must keep. Notice that $(kra/q) \to ka$ as $r \to \infty$. Therefore the first term in Eq. 119 goes to zero, since ak was chosen to be precisely a zero of J_0 . Furthermore, all other Bessel functions in the approximation go to a constant, and $\sin(kq), \cos(kq)$ oscillate, so we must look at the r dependence of their coefficients. The second term is shown in Eq. 118, from which we gather that the r dependence goes like $1/r^2$. However, the third term (seen in Eq. 119) also goes as $1/r^2$. It can be shown that the remaining terms drop off as $1/r^n$ where $n \geq 3$, thus we only need to keep three terms for the asymptotic expansion to work as $r \to \infty$.

	ψ_{Ring} evaluated at an arbitrary point r:				
Approximation	$r=10^2\lambda$	$r = 10^3 \lambda$	$r = 10^4 \lambda$	$r = 10^5 \lambda$	
1 Term	0.0860162	-1.26286×10^{-7}	-1.17417×10^{-11}	-1.17329×10^{-15}	
2 Terms	0.0907007	-3.859×10^{-7}	-2.0046×10^{-9}	-1.98716×10^{-11}	
3 Terms	0.089324	-2.5606×10^{-7}	-1.00817×10^{-9}	-9.93639×10^{-12}	
4 Terms	0.0893905	-2.56049×10^{-7}	-1.00817×10^{-9}	-9.93639×10^{-12}	
5 Terms	0.0895554	-2.56025×10^{-7}	-1.00817×10^{-9}	-9.93639×10^{-12}	
Exact	0.0895243	-2.56025×10^{-7}	-1.00816×10^{-9}	-9.93639×10^{-12}	

Table 2: Accuracy of the asymptotic expansion at arbitrary values of r. Approximations are compared to the 'exact' numerical integration of ψ_{Ring} . Other parameters used: $w = 2\lambda$, $z = 10\lambda$. These results show that one must use at least 3 terms to accurately model ψ_{Ring} at large r.

Table 2 gives evidence for this conclusion. The reference 'Exact' solution is a numerical integration of Eq. 95, which begins to fail beyond $r = 10^5 \lambda$. Therefore, for large values of r, we will use Eq. 119 as an accurate representation for ψ_{Ring} .

6.4 Small r

Since we have used an asymptotic expansion, one would expect to have a singularity somewhere. This occurs where q = 0, which is where $(kr)^2 = (kb)^2 - (ka)^2 - (kz)^2 + 2ik^2bz = \frac{1}{4}(kw)^4 - (ka)^2 - (kz)^2 + 2ik^2bz$. Since r is always real, the singularity must be where z = 0 and $(kr)^2 = \frac{1}{4}(kw)^4 - (ka)^2 \approx \frac{1}{4}(kw)^4$, or simply when $r \approx b$. This aspect of the approximation allows it to not only be used as $r \to \infty$, but also near r = 0, so long as the singularity is avoided.

At r = 0, all but the first term in Eq. 119 drop out, for q is most likely non-zero there.⁹ Thus we postulate that $\psi_{Ring}^{(1)}$ will adequately describe ψ_{Ring} near r = 0. This is supported in Figs. 9 -10, which plot the approximations at z = 0 and z = b and their errors, taken to be the difference between the approximation and numerical integration of Eq. 95. Only in the case of tight focusing ($w = 2\lambda$) does the error seem to show up, and even then it is minuscule.

⁹If b = a, however, we could have problems at z = 0. This would only occur in a beam of a waist exactly $\sqrt{a_1/\pi}\lambda \approx 0.87\lambda$, where a_1 is the first zero of J_0 .



Figure 9: Plots of the first approximation $\psi_{Ring}^{(1)}$ at z = 0 and z = b with errors given by the difference between this approximation and the numerical integration of Eq. 95. These plots suggest that only the first term in the approximation in Eq. 119 is needed for the region where r is small.



Figure 10: Similar to Fig. 9, these plots consider a larger waist of 10λ . Notice that the errors are quite small.

6.5 Near b



Figure 11: The behavior of our approximations near the singularity at z = 0, r = b for a beam of waist 2λ , compared to ψ_{Exact} , which is a numerical integration of ψ_{Ring} (Eq. 95). For r < b the $\psi_{Ring}^{(1)}$ solution is used, while $\psi_{Ring}^{(3)}$ is used for r > b. The latter approximation becomes quite good just 2 wavelengths past the singularity.

As outlined above, the approximation fails at z = 0, r = b. Fortunately it fails for only a small region, roughly a couple wavelengths to either side of b. For a beam of waist 2λ this can be seen in Fig. 11. If one needed to know the fields in this region, a simple numerical integration of Eq. 95 would suffice. The parameter b is proportional to the beam waist squared (Eq. 84), so the singularity region moves into obscurity as the waist gets larger.

Now, using $\psi_{Ring}^{(3)}$, we can show that ψ_{Ring} is normalizable. As $r \to \infty$, $q \to r$, and $kra/q \to ka = a_i$. Eq. 119 then goes to a much simpler form:

$$\psi_{Ring}^{(3)} \rightarrow -\frac{2\pi a J_1(ka)}{kr^2} \cos(kr) + \frac{a^2 J_2(ka)}{2r^2} \cos(kr)$$
 (120)

$$= \frac{\frac{1}{2}a_i^2 J_2(a_i) - 2\pi a_i J_1(a_i)}{(kr)^2} \cos(kr)$$
(121)

$$\cong -\frac{5.27534}{(kr)^2}\cos(kr).$$
(122)

Since ψ_{Ring} is finite everywhere, the integral in Eq. 90 converges because $\int r dr 1/r^4 \rightarrow 0$ as $r \rightarrow \infty$.

To summarize, our approximation in Eq. 119 is accurate enough to adequately describe ψ_{Ring} at all points in space other than a small region about r = b, z = 0. For r < b, only the first term in the expansion is needed. From now on these approximations will be used for calculations.

7 Fields



Figure 12: The electric field at z = 0. Notice that the field is highly polarized in the x direction.

We are now prepared to compute the electric and magnetic fields of a beam given by $\mathbf{A}_{\mathbf{Ring}}$ (Eq. 79). We will use a tightly focused beam with a waist of 2λ from now on. Using Eq. 70 and Eq. 69 the Cartesian components of the spatial parts of the fields are

$$E_x = A_0 \frac{i}{k} \left(\cos^2 \theta \frac{\partial^2}{\partial r^2} + \frac{\sin^2 \theta}{r} \frac{\partial}{\partial r} + k^2 \right) \psi_{Ring}$$
(123)

$$E_y = A_0 \frac{i \sin 2\theta}{2k} \left(\frac{\partial^2}{\partial r^2} - \frac{1}{r} \frac{\partial}{\partial r} \right) \psi_{Ring}$$
(124)

$$E_z = A_0 \cos \theta \frac{\partial^2}{\partial r \partial z} \psi_{Ring} \tag{125}$$

$$B_x = 0 \tag{126}$$

$$B_y = A_0 \frac{\partial}{\partial z} \psi_{Ring} \tag{127}$$

$$B_z = -A_0 \sin \theta \frac{\partial}{\partial r} \psi_{Ring} \tag{128}$$

The Cartesian components of the Poynting vector are then

$$S_x = \frac{1}{2\mu_0} Re\{E_y B_z^* - E_z B_y^*\}$$
(129)

$$S_y = -\frac{1}{2\mu_0} Re\{E_x B_z^*\}$$
(130)

$$S_z = \frac{1}{2\mu_0} Re\{E_x B_y^*\}$$
(131)



Figure 13: The z component of the Poynting vector on the plane z = 0. The intensity is highly symmetric.



Figure 14: A cross section of the Poynting vector along the plane $z = 2\lambda$. Notice in the lower left plot that the angular component is very small compared to the radial one; the momentum density is almost entirely cylindrically symmetric. In the lower right plot we see that the momentum density is strongest at $r = 1.05\lambda$, with a value of roughly .7% of that of the z component of the Poynting vector at z = 2.



Figure 15: The beam radius of the Gaussian model (Eq. 83) is compared to that found from the ring model (Eq. 95) for a beam waist $w = 2\lambda$. The blue dots indicate the radius where S_r is the strongest, which correspond to half of the beam radius.

The x and y components at z = 0 of the electric field are shown in Fig. 12. Notice that the field is highly polarized, just as we specified.

The Poynting vector is strongest in the direction of propagation, as expected, and is shown in Fig. 13 The perpendicular components S_x and S_y can easily be transformed into radial and angular components:

$$S_r = S_x \cos\theta + S_y \sin\theta \tag{132}$$

$$S_{\theta} = S_x \sin \theta - S_y \cos \theta \tag{133}$$

As seen in Fig. 14 the radial component is highly symmetric about the z axis. The



Figure 16: A superposition of Fig. 15 on a contour plot of the values of S_r relative to those of S_z at the same z coordinate. White indicates higher intensity, which implies that the beam is diverging. vector field indicates that the beam is diverging, with more of the momentum going in the radial direction.

The radius of the beam at a given z coordinate is defined to be the value of r where S_z drops to $1/e^2$ of its value at r = 0. The Gaussian model (Eq. 83) gives a compact form for the radius:

$$BeamRadius(z) = w\sqrt{1 + (z/b)^2}$$
(134)

This is compared with our model in Figs. 15-16. Also shown is the peak of S_r , which





Figure 17: This contour plot shows the value of S_r relative to the value of S_z at the focus. This value is maximized within a beam waist and within a diffraction length, achieving 1.8% of S_z at the center of the beam.

is located at a point half of the beam radius at a given z.

Fig. 17 shows us that there is a small region where S_r is particularly strong, around z = .74b, $r = .63\lambda$, with a value of 1.8% of that at the center of the beam. Notice that S_r is zero on the focal plane z = 0; all of the momentum is in the z direction.

If we let $\sqrt{r^2 + a^2 + (z - ib)^2} \to r$ in S_r and S_z , it can be shown that the fields drop off as $1/r^6$ and $1/r^5$, respectively, in the region where r > b. This is where the Gaussian model (Eq. 83) clearly fails. However, after normalization one realizes that at r > b the fields have already dropped by e^{-kb} . This can be seen by letting $r \to 0$ and $z \to 0$ in $\psi_{Ring}^{(1)}$:

$$\begin{aligned} |\psi_{Ring}^{(1)}(r=0)| &= |2\pi \frac{\sin(k\sqrt{a^2 - b^2})}{\sqrt{a^2 - b^2}}| \\ &\approx \frac{\pi}{14} e^{kb}. \end{aligned}$$
(135)

$$\frac{\pi}{kb}e^{kb}.$$
(136)



Figure 18: The z component of the Poynting vector on the plane z = 0 beyond $r = b = 12.5\lambda$, compared to S_z at the center of the beam. Even though this field drops off as a polynomial in this region, it is so small compared to the center that its influences can be ignored.

Even in the tightly focused case when $w = 2\lambda$ the fields are negligible, as seen in Fig. 18.



Figure 19: The geometry of a laser with a beam of waist w focused on an ion at an angle γ to to the ion trap.

7.1 Application to the Ion Trap

Now we will relate these developments with the ion trap quantum computer. Notice in Eqs. 57-58 on page 21 that the strength of the interaction between the laser and an ion is proportional to $\mathbf{k} \cdot \hat{\mathbf{z}}$. Physically this is the momentum along the ion trap's axis that is transferred to an ion in order to create or annihilate a phonon, a necessity for any quantum computation to work.

Suppose that a laser is focused on an ion at the origin, and the angle between the trap axis and the beam axis is γ , seen in Fig. 19. The geometry of this configuration tells us that the r and z coordinates associated with another ion of distance a_0 away are

$$r = a_0 \sin \gamma \tag{137}$$

$$z = a_0 \cos \gamma. \tag{138}$$

From Eq. 78, we see that the momentum density is proportional to the Poynting vector. The angular component of the Poynting vector is negligible, so the momentum density in the direction of the trap is

$$p_z = p_0 \left(S_r \sin \gamma + S_z \cos \gamma \right), \tag{139}$$

in which p_0 is a constant.



Figure 20: The minimum acceptable angle that the laser can make with the trap axis in order to keep p_z at the point a_0 under 1% of that at the center of the beam. This is plotted for a tight focus with a waist $w = 2\lambda$. Note that it is impossible to achieve this if $a_0 < 1.56w$

Now we will calculate the minimum acceptable angle γ_{min} that the laser can make with the trap axis. We will define this point by where p_z achieves a value of 1% of that at the targeted ion. Using a tightly focused beam with a waist $w = 2\lambda$, we find that a neighboring ion could be 2.26 beam waists away from the targeted ion, with a minimum angle of 45 degrees, and still stay within this 1% threshold. A continuous set of values is shown in Fig. 20.

Taking the extreme case of Beryllium from Table 1 on page 20, and using Eq. 56, we find that such a trap could support up to 170 ions with a laser at an angle $\gamma = \pi/4$ and a beam waist of 2λ . Thus it would seem that the constraints on the angle are minimal in an ion trap quantum computer.

8 Conclusions

We have shown that, by integrating over a ring, the ψ_{00} point source in Eq. 86 can be made normalizable by picking the radius of the ring to be a_1/k , where a_1 is the first zero of the Bessel function of the first kind. Since the ψ_{00} source is a solution to the Helmholtz equation (Eq. 66) and Maxwell's equations, our construction ψ_{Ring} (Eq. 95) is also a solution. Since the integral in Eq. 95 is intractable, we have developed an approximation method for vector potential near and far from the focal point.

Within several beam waists our approximation is very similar to the Gaussian. We find that beyond the diffraction length b, in the radial direction, that the fields drop off as $1/r^n$, much slower than a Gaussian. However even for tightly focused beams the prefactor e^{-kb} , which normalizes the fields to the center of the beam, effectively eliminates the need to worry about the fields at the edges of the beam (Eq. 136).

In the ion trap quantum computer, it would be possible to focus a laser perpendicular to the ion string slightly off-center in order to get momentum in the direction of the string, as shown in Fig. 17. However, a 2 degree shift in the laser beam would give nearly the same momentum density at that point, thus it is advisable to focus the laser on an angle.

This angle γ , illustrated in Fig. 19, has a limit, because too sharp of an angle would shine unwanted light onto a neighboring ion, potentially causing an undesirable transition. However, we have shown that the constraints on γ are quite minimal, and conclude that tightly focused lasers will impose few limits on future ion trap quantum computers.

A Bessel function integrals

We want to evaluate the integral

$$I = \int_{-\pi}^{\pi} d\phi e^{ix\cos(\phi)} \cos^n(\phi).$$
(140)

We know that

$$\int_{-\pi}^{\pi} d\phi e^{ix\cos(\phi)} = 2\pi J_0(x).$$
(141)

Notice by taking the $n^{th} x$ derivative of both sides that the integral I is solved:

$$\frac{\partial^n}{\partial x^n} \int_{-\pi}^{\pi} d\phi e^{ix\cos(\phi)} = \frac{\partial^n}{\partial x^n} 2\pi J_0(x) \tag{142}$$

$$\int_{-\pi}^{\pi} d\phi \frac{\partial^n}{\partial x^n} e^{ix\cos(\phi)} = \frac{\partial^n}{\partial x^n} 2\pi J_0(x)$$
(143)

$$\int_{-\pi}^{\pi} d\phi e^{ix\cos(\phi)} i^n \cos^n(\phi) = \frac{\partial^n}{\partial x^n} 2\pi J_0(x).$$
(144)

It follows that

$$\int_{-\pi}^{\pi} d\phi e^{\pm ix \cos(\phi)} \cos^n(\phi) = 2\pi (\mp i)^n \frac{\partial^n}{\partial x^n} J_0(x).$$
(145)

The first few derivatives of $J_0(x)$ are

$$\frac{\partial}{\partial x}J_0(x) = -J_1(x) \tag{146}$$

$$\frac{\partial^2}{\partial x^2} J_0(x) = \frac{1}{2} \left(J_2(x) - J_0(x) \right)$$
(147)

$$\frac{\partial^3}{\partial x^3} J_0(x) = \frac{1}{4} \left(3J_0(x) - J_2(x) + J_4(x) \right)$$
(148)

$$\frac{\partial^4}{\partial x^4} J_0(x) = \frac{1}{8} \left(J_2(x) - J_0(x) \right).$$
(149)

References

- A. Turing, On computable numbers, with an application to the Entscheidungsproblem, Proceedings of the London Mathematical Society 42, 230 (1936-7).
- [2] P. Benioff, The computer as a physical system: ..., J. Stat. Phys. 22, 563 (1980).
- [3] R. Feynman, Simulating Physics with computers, Int. J. Theo. Phys. 21, 467 (1982).
- [4] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. R. Soc. Lond. A 400, 97 (1985).
- [5] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logrithms on a Quantum Qomputer, LANL quant-ph archive 9508027(1995).
- [6] J. I. Cirac, P. Zoller, Quantum Computations with Cold Trapped Ions, Phys. Rev. Lett. 74, 4091 (1995).
- [7] D. Deutsch, A. Barenco, and A. Eckert, Universality in Quantum Computation, Proc. Roy. Soc. London Ser. A 449, 669 (1995).
- [8] A. Barenco, R. Cleve, D. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Phys. Rev. A 52, 3457 (1995).
- [9] W. K. Wooters, W. H. Zurek, A single quantum cannot be cloned, Nature 299, 802 (1982).
- [10] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21, 120 (1978).
- [11] A. Eckert, R. Jozsa, Quantum Computation and Shor's factoring algorithm, Rev. Mod. Phys. 68, 733 (1996).

- [12] S. R. Jefferts, C. Monroe, E. W. Bell, and D. J. Wineland, Coaxial-resonatordriven rf (Paul) trap for strong confinement, Phys. Rev. A 51, 3112 (1995).
- [13] M. Raizen, J. Gilligan, J. Bergquist, W. Itano, and D. Wineland, *Ionic crystals in a linear Paul trap*, Phys. Rev. A 45, 6493 (1992).
- [14] D. F. V. James Quantum Dynamics of cold trapped ions with application to quantum computation, Appl. Phys. B 66, 181 (1998).
- [15] A. Steane, C. F. Roos, D. Stevens, A. Mundt, D. Leibfried, F. Schmidt-Kaler, and R. Blatt Speed of ion-trap quantum-information processors, Phys. Rev A 62, 042305 (2000).
- [16] M. Lax, W. Louisell, and W. McKnight, From Maxwell to paraxial wave optics, Phys. Rev. A 11, 1365 (1975).
- [17] M. Couture and P. Belanger, From Gaussian beam to complex-source-point spherical wave, Phys. Rev. A 24, 355 (1981).
- [18] C. Sheppard and S. Saghafi, Beam modes beyond the paraxial approximation: A scalar treatment, Phys. Rev. A 57, 2971 (1998).
- [19] J. Lekner, TM, TE, and 'TEM' beam modes: exact solutions and their problems,J. Opt. A 3, 407 (2001).